**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ**

**(БАНК РОССИИ)**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

**Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации Территориальных учреждений для РАБИС-НП и АРМ АС ЭКР 2.0**

На 317 листах

Москва 2017 г.**Лист изменений**

| **Версия** | **Дата создания версии** | **Причина изменений** | **Описание изменений** |
| --- | --- | --- | --- |
| 1.0 | 19.10.2016 | Исходная версия, разосланная ГУБиЗИ письмо ГУБиЗИ от 17.11.2016 № 23-4-3-5/2848 | Исходная версия |
| 2.0 | 27.03.2017 | Модифицированная версия, автор ЗАО «ЛАНИТ». Доработки по факту выхода новых версий СЗИ. Инкапсулированы результаты проверок ответственных ТУ Банка России | Обновлены версии:   1. системного ПО контроллеров СЗИ от НСД «Аккорд-АМДЗ» 2. СПО «Аккорд-Win32» версии 4.0.9.43 3. или «Аккорд-Win64» версии 5.0.9.43 4. СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 3 (версия 10.2.5.3201) и управляющих компонент СЗ от ВВК до версий Kaspersky Security Center 10 Service Pack 2 (версия 10.3.407) 5. унифицирована версия программного комплекса «Паспорт АРМ УОС» версии 4.15 |
| 2.1 | 21.04.2017 | Внесены требования 410-П в части структуры паролей | Внесены требования 410-П в части структуры паролей, настройки доменной политики при настройке СЗИ от НСД «Аккорд» |
| 3.0 | 20.06.2017 | Модифицированная версия, автор ЗАО «ЛАНИТ». Доработки по факту выхода новых версий СЗИ | Обновлены версии:   1. СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294) и управляющих компонент СЗ от ВВК до версий Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (версия 10.4.343) 2. системы «Контроль-ПУ» на базе программного комплекса (ПК) DeviceLock (версия 8.2.69641) |
| 3.1 | 06.07.2017 | Инкапсулированы результаты проверок ответственных ТУ Банка России | 1. Отражены настройки в части взаимодействия компьютера и терминала сбора данных Datalogic Falcon X3 2. Дополнено описание настроек СЗИ от НСД «Аккорд» |
| 3.2 | 07.08.2017 | Инкапсулированы результаты проверок ответственных ТУ Банка России | 1. Дополнено задание для модели ЗПС СЗИ от НСД SecretNet «Задание ЗПС для ЕСМИБ ТУ – ПО АРМ персонала системы». 2. Устранена дублирующая информация в разделе 2.4. 3. Приняты редакторские предложения и замечания в части описания настроек СЗ от ВВК и ПАК СЗИ от НСД «Аккорд». 4. В пп 3.2.1 и 3.3.1 отражено обязательное условие использования УК СЗИ для РАБИС-НП и АС ЭКР: применение политик и настроек рекомендованных к доменной структуре Active Directory. |
| 3.3 | 24.08.2017 | Инкапсулированы результаты тестирования настроек параметров групповой политики для РАБИС-НП | Внесены требования в части настроек параметров групповой политики «CachedLogonsCount», «AutoAdminLogon», «DisablePwdCaching» |
| 3.4 | 30.08.2017 | Инкапсулированы результаты проверок ответственных ТУ Банка России | 1. В механизм КЦ на аппаратном уровне добавлен файл hashfile.exe. 2. Обновлен перечень файлов ОС, для которых средствами СЗИ от НСД установлен запрет на выполнение. 3. Актуализированы номера приложений, указанных в эксплуатационной документации на СЗИ от НСД Аккорд. |
| 3.5 | 13.09.2017 | Инкапсулированы результаты проверок ответственных ТУ Банка России | 1. Отклонены изменения в версию документа 3.2 п.1. 2. Дополнено задание для модели ЗПС СЗИ от НСД SecretNet «Задание ЗПС для ЕСМИБ ТУ – ЕСМИБ по журналу (группа ресурсов)» |
| 4.0 | 20.09.2017 | Модифицированная версия, автор ЗАО «ЛАНИТ». Доработки по факту выхода новых версий СЗИ | Обновлены версии:   1. Система паспортизации ПК «Паспорт АРМ УОС» версии 5.17.8.4; 2. СПО «Аккорд-Win32» (версия 4.0.9.50); 3. СПО «Аккорд-Win64» (версия 5.0.9.50); 4. СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 4 (версия 10.2.6.3733); 5. СЗ от ВВК Dr.Web Enterprise агенты Agent for Windows (версия 11.0.1.05150) и Agent for Windows supporting Active Directory (версия 11.00.05180), а так же серверная часть комплекса (управляющая компонента) Dr.Web Enterprise Security Suite (версия 10.01.0) |
| 4.1 | 10.10.2017 | Внесены замечания ГУБиЗИ Банка России | Учтены требования Положения Банка России от 25.11.2015 № 506-П в части использования сертифицированных версий СЗИ;  Учтено использование встроенных механизмов защиты ЕСМИБ ТУ в соответствии с типовыми решениями ЕСМИБ ТУ;  Учтено использование входящего в состав СЗИ от НСД Secret Net механизма защиты дисков совместно с аппаратным средством защиты RuToken S. |
| 4.2 | 17.10.2017 | Внесены замечания ГУБиЗИ Банка России | Учтены замечания ГУБиЗИ Банка России в части использования системы «Контроль-ПУ» для стендов тестирования территориальных учреждений Банка России |
| 4.3 | 02.11.2017 | Внесены замечания Отделения – Национального банка по Республике Татарстан Волго-Вятского ГУ Банка России | В настройки механизма КЦ комплекса Аккорд на программном уровне добавлен исполняемый файл hashfile.exe СКАД «Сигнатура» версии 5 (раздел 2.5.6.2). |
| 4.4 | 22.11.2017 | Внесены замечания Отделения – Национального банка по Республике Хакасия Сибирского главного управления Центрального банка Российской Федерации | Учтены замечания в части настроек антивирусных политик СЗ от ВВК антивирус Kaspersky |
| 4.5 | 24.11.2017 | Внесены замечания Отделения по Омской области Сибирского главного управления Центрального банка Российской Федерации | Учтены замечания в части настройки антивирусной политики СЗ от ВВК антивирус Kaspersky Endpoint Security версия 10.2.4.674 |
| 4.6 | 28.11.2017 | Внесены замечания Отделения по Воронежской области Главного управления Центрального банка Российской Федерации по Центральному федеральному округу | Учтены замечания в части конкретизации по настройке системы паспортизации (Паспорт АРМ УОС) версия 5.17.8.4 |
| 4.7 | 30.11.2017 | Внесены замечания Отделения по Омской области Сибирского главного управления Центрального банка Российской Федерации | Добавлены условия использования более ранних версий клиентской части (агента) Dr.Web Agent for Windows СЗ от ВВК, отличных от описанных в данном документе |
| 4.8 | 30.11.2017 | Внесены замечания Отделения по Воронежской области Главного управления Центрального банка Российской Федерации по Центральному федеральному округу и Отделения по Омской области Сибирского главного управления Центрального банка Российской Федерации | Описаны условия опционального использования системы «Контроль-ПУ» на основе программного комплекса DeviceLock на стендах тестирования ТУ |
| 4.9 | 06.12.2017 | Внесены замечания ГУБиЗИ Банка России | Учтены замечания ГУБиЗИ Банка России в части редакторских правок и утверждения ряда замечаний ответственных ТУ Банка России |

**Содержание**

[1. Общие положения 11](#_Toc496019725)

[2. Область применения 12](#_Toc496019726)

[3. Описание плана обновления (актуалиазации) унифицированныХ конфигурациЙ сзи для РАБИС-нп, арм ас экр 2.0 территориальных учреждений банка россии 13](#_Toc496019727)

[3.1 Подготовительные работы 13](#_Toc496019728)

[3.1.1 Проверка технологических карт обновлений версий СЗИ 13](#_Toc496019729)

[3.1.2 Доработка унифицированных конфигураций и технологических карт обновлений версий СЗИ для РАБИС-НП, АРМ АС ЭКР 2.0 13](#_Toc496019730)

[3.1.3 Принятие решения и направление письма о переводе ТУ на унифицированные конфигурации, направление решения в ТУ 13](#_Toc496019731)

[3.2 Установка унифицированных конфигураций на стендах тестирования территориальных учреждений 14](#_Toc496019732)

[3.2.1 Настройка доменной структуры на стенде 14](#_Toc496019733)

[3.2.2 Установка и настройка унифицированных версий СЗ от ВВК на стенде 14](#_Toc496019734)

[3.2.3 Установка и настройка средств защиты информации от несанкционированного доступа на стенде 16](#_Toc496019735)

[3.2.4 Установка и настройка унифицированной версии системы «Контроль-ПУ» 17](#_Toc496019736)

[3.2.5 Установка и настройка унифицированной версии системы паспортизации 18](#_Toc496019737)

[3.3 Установка унифицированных конфигураций в платежном сегменте территориальных учреждений 19](#_Toc496019738)

[3.3.1 Настройка доменной структуры в платёжном сегменте ТУ Банка России 19](#_Toc496019739)

[3.3.2 Установка и настройка СЗ от ВВК в платёжном сегменте ТУ Банка России 20](#_Toc496019740)

[3.3.3 Установка и настройка СЗИ от НСД в платёжном сегменте ТУ Банка России 21](#_Toc496019741)

[3.3.4 Установка и настройка системы паспортизации в платёжном сегменте ТУ Банка России 21](#_Toc496019742)

[3.3.5 Доработка технорабочих проектов на РАБИС-НП и АС ЭКР 2.0 ТУ БР 22](#_Toc496019743)

[ПРИЛОЖЕНИЕ 1 НАСТРОЙКА СЗ ОТ ВВК 23](#_Toc496019744)

[П1.1 Параметры настройки СЗ от ВВК «Kaspersky Security Center 10.3.407» 23](#_Toc496019745)

[П1.2 Параметры настройки задач СЗ от ВВК Kaspersky Security Center 10.3.407 28](#_Toc496019746)

[П1.3 Параметры настройки СЗ от ВВК «Kaspersky Security Center 10.4.343» 31](#_Toc496019747)

[П1.4 Параметры настройки задач СЗ от ВВК Kaspersky Security Center 10.4.343 40](#_Toc496019748)

[П1.5 Настройка средства защиты от воздействий вредоносного кода «Dr Web Enterprise Security Suite» (версия 10.01.0) 43](#_Toc496019749)

[ПРИЛОЖЕНИЕ 2 НАСТРОЙКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «АККОРД» 58](#_Toc496019750)

[П2.1 Подготовка компьютера к установке комплекса 59](#_Toc496019753)

[П2.2 Установка в компьютер АМДЗ «Аккорд-5МХ/5.5/5.5е» 62](#_Toc496019754)

[П2.3 Установка драйверов комплекса Аккорд 62](#_Toc496019755)

[П2.4 Установка СПО «Аккорд-Win32/64» 63](#_Toc496019756)

[П2.5 Настройка комплекса Аккорд 64](#_Toc496019757)

[П2.5.1 Настройка синхронизации комплекса Аккорд 64](#_Toc496019758)

[П2.5.2 Настройка редактора прав доступа (ACED32) 64](#_Toc496019759)

[П2.5.2.1 Настройка параметров входа в систему 64](#_Toc496019760)

[П2.5.2.2 Настройка параметров программной среды 66](#_Toc496019761)

[П2.5.2.3 Настройка раздела «Опции» 67](#_Toc496019762)

[П2.5.2.4 Настройка раздела «Результаты И/А» 68](#_Toc496019763)

[П2.5.2.5 Настройка правил разграничения доступа 69](#_Toc496019764)

[П2.5.2.6 Регистрация пользователей комплекса Аккорд 70](#_Toc496019765)

[П2.5.2.7 Настройка привилегий пользователей комплекса Аккорд 71](#_Toc496019766)

[П2.5.2.8 Настройка стартовых задач для пользователей комплекса Аккорд 72](#_Toc496019767)

[П2.5.3 Настройка конфигурационных файлов комплекса Аккорд 72](#_Toc496019768)

[П2.5.4 Активация комплекса Аккорд 73](#_Toc496019769)

[П2.5.5 Настройка комплекса СЗИ от НСД «Аккорд-Win32/64» 73](#_Toc496019770)

[П2.5.6 Настройка механизма КЦ комплекса Аккорд 77](#_Toc496019771)

[П2.5.6.1 Настройка механизма КЦ на аппаратном уровне 77](#_Toc496019772)

[П2.5.6.2 Настройка механизма КЦ на программном уровне 78](#_Toc496019773)

[П2.5.6.3 Минимальные настройки механизма КЦ на программном уровне 79](#_Toc496019774)

[П2.5.7 Настройка политики безопасности 80](#_Toc496019775)

[П2.5.8 Рекомендации по настройке СЗ от ВВК 82](#_Toc496019776)

[П2.5.9 Обеспечение совместной работы комплекса и подсистемы Паспорт АРМ УОС. 82](#_Toc496019777)

[П2.5.10 Обеспечение совместной работы комплекса и ЕСМИБ ТУ 83](#_Toc496019778)

[П2.5.11 Примечания 84](#_Toc496019779)

[П2.5.12 Сообщения об ошибках 85](#_Toc496019780)

[ПРИЛОЖЕНИЕ 3 Настройка СЗИ от НСД «Secret Net» на рабочих станциях и серверах (контроллерах домена) 86](#_Toc496019781)

[П3.1 Значения параметров СЗИ от НСД «Secret Net 6.5» для всех применяемых версий операционных систем (Windows XP/7/2003/2008 (x32/x64)). 86](#_Toc496019785)

[П3.2 Значения параметров СЗИ от НСД «Secret Net 7.6» для всех применяемых версий операционных систем Windows XP/7/2003/2008 (x32/x64)). 93](#_Toc496019786)

[П3.3 Построение модели замкнутой программной среды (ЗПС) и контроля целостности (КЦ) 100](#_Toc496019787)

[П3.3.1 Модель ЗПС для 32-х разрядных операционных систем Windows XP/7 101](#_Toc496019788)

[П3.3.2 Модель контроля целостности файлов для 32-хразрядных операционных систем Windows XP/7 111](#_Toc496019789)

[П3.3.3 Модель ЗПС для 64-х разрядных операционных систем Windows XP/7 114](#_Toc496019790)

[П3.3.4 Модель контроля целостности файлов для 64х разрядных операционных систем Windows XP/7 125](#_Toc496019791)

[П3.3.5 Разграничение доступа к каталогам и файлам, обеспечивающее защиту от подмены или модификации программного обеспечения 128](#_Toc496019792)

[ПРИЛОЖЕНИЕ 4 Настройки ОС на рабочих станциях и серверах (контроллерах домена) при использовании СЗИ от НСД «SecretNet» и «Аккорд» (при функционировании рабочих станций c ОС Windows XP/7 под управлением контроллеров домена c ОС Windows Server 2003 129](#_Toc496019793)

[П4.1 Настройка BIOS/UEFI 129](#_Toc496019798)

[П4.2 Регистрация попыток входа в систему и доступа к критичным объектам локальной файловой системы. 129](#_Toc496019799)

[П4.3 Рекомендации по настройке политик безопасности для контроллеров домена, АРМ и пользователей при использовании СЗИ от НСД «SecretNet» 129](#_Toc496019800)

[П4.4 Рекомендации по настройке политик безопасности для серверов и АРМ платежной системы при использовании СЗИ от НСД «Аккорд» 187](#_Toc496019801)

[ПРИЛОЖЕНИЕ 5 Настройки ОС на рабочих станциях и серверах (контроллерах домена) при использовании СЗИ от НСД «SecretNet» и «Аккорд» при функционировании рабочих станций c ОС Windows XP/7 под управлением контроллеров домена c ОС Windows Server 2008 189](#_Toc496019802)

[П5.1 Параметры групповой политики для пользователей СВТ при использовании СЗИ от НСД Secret Net 191](#_Toc496019808)

[П5.2 Параметры групповой политики для АРМ при использовании СЗИ от НСД Secret Net 213](#_Toc496019809)

[П5.3 Параметры групповой политики для рядовых серверов и контролллеров домена при использовании СЗИ от НСД Secret Net 255](#_Toc496019810)

[П5.4 Настройки СЗИ от НСД «Аккорд» на рабочих станциях и серверах (контроллерах домена) (при функционировании рабочих станций c ОС Windows 2000/XP/7 под управлением контроллеров домена c ОС Windows Server 2008. 305](#_Toc496019811)

[ПРИЛОЖЕНИЕ 6 Настройка системы «Контроль-ПУ» 307](#_Toc496019812)

[ПРИЛОЖЕНИЕ 7 Настройка системы паспортизации 312](#_Toc496019813)

[П7.1 Настройка зарегистрированных компьютеров 313](#_Toc496019821)

[П7.2 Настройка параметров контроля состава ПО 314](#_Toc496019822)

[П7.3 Настройка списка программного обеспечения 315](#_Toc496019823)

**Перечень рисунков**

[*Рисунок 1 – Настройки параметров экранной заставки* 60](#_Toc494109042)

[*Рисунок 2 – Настройка параметров плана электропитания* 60](#_Toc494109043)

[*Рисунок 3 – Настройка параметров экранной заставки* 61](#_Toc494109044)

[*Рисунок 4 – Настройка схемы управления электропитанием* 61](#_Toc494109045)

[*Рисунок 5 – Параметры настройки спящего режима* 62](#_Toc494109046)

[*Рисунок 6 –Установка драйвера PCI-устройства (плата АМДЗ «Аккорд-5MX/5.5/5.5e»)* 63](#_Toc494109047)

[*Рисунок 7 –Настройка параметров синхронизации комплекса Аккорд* 64](#_Toc494109048)

[*Рисунок 8 – Настройка параметров пароля для группы пользователей «Администраторы»* 65](#_Toc494109049)

[*Рисунок 9 – Настройка параметров пароля для группы пользователей «Обычные»* 66](#_Toc494109050)

[*Рисунок 10 – Настройка параметров Программной среды* 66](#_Toc494109051)

[*Рисунок 11 – Настройка параметров гашения экрана* 67](#_Toc494109052)

[*Рисунок 12 – Настройка Опции для группы Обычные* 68](#_Toc494109053)

[*Рисунок 13 – Настройка Результатов И/А для всех групп* 69](#_Toc494109054)

[*Рисунок 14 – Настройка атрибутов доступа к объектам* 70](#_Toc494109055)

[*Рисунок 15 – Настройка и регистрация пользователей комплекса* 71](#_Toc494109056)

[*Рисунок 16 – Настройка привилегий для администраторов комплекса* 72](#_Toc494109057)

[*Рисунок 17 – Параметры Настройки комплекса Аккорд* 74](#_Toc494109058)

[*Рисунок 18 – Параметры дополнительных опций Комплекса, вкладка Контроль* 74](#_Toc494109059)

[*Рисунок 19 – Параметры дополнительных опций Комплекса, вкладка Режим сессии* 75](#_Toc494109060)

[*Рисунок 20 – Параметры дополнительных опций Комплекса, вкладка Разное* 76](#_Toc494109061)

[*Рисунок 21 – Параметры дополнительных опций Комплекса, вкладка Данные конфигурации* 77](#_Toc494109062)

[*Рисунок 22 – Описание данных АРМ пользователя РАБИС и АС ЭКР 2.0* 314](#_Toc494109063)

[*Рисунок 23 – Настройка параметров контроля целостности ПО* 315](#_Toc494109064)

[*Рисунок 24 – Настройка описания программного обеспечения* 316](#_Toc494109065)

[*Рисунок 25 – Настройка перечня программного обеспечения* 316](#_Toc494109066)

**Перечень таблиц**

[Таблица 1. Параметры политик СЗ от ВВК Антивирус «Kaspersky Endpoint Security 10» SP 1 MR 2 (версия 10.2.4.674) для рабочих станций пользователей РАБИС-НП и АС ЭКР 2.0 23](#_Toc495338138)

[Таблица 2 Параметры задачи поиска вирусов 28](#_Toc495338139)

[Таблица 3 Параметры настройки задачи обновления сигнатурных баз 28](#_Toc495338140)

[Таблица 4 Параметры настройки задачи "Загрузка обновлений в хранилище" 29](#_Toc495338141)

[Таблица 5 Параметры настройки политики Агента администрирования 29](#_Toc495338142)

[Таблица 6. Параметры политик СЗ от ВВК Антивирус «Kaspersky Endpoint Security 10» SP 1 MR 4 (версия 10.2.6.3733) для рабочих станций пользователей РАБИС-НП и АС ЭКР 2.0 под управлением ОС Windows XP SP3 RUS. 31](#_Toc495338143)

[Таблица 7. Параметры политик СЗ от ВВК Антивирус «Kaspersky Endpoint Security 10» SP 2 (версия 10.3.0.6294) для рабочих станций пользователей РАБИС-НП и АС ЭКР 2.0 под управлением ОС Windows 7 SP1 RUS. 35](#_Toc495338144)

[Таблица 8 Параметры задачи поиска вирусов 40](#_Toc495338145)

[Таблица 9 Параметры настройки задачи обновления сигнатурных баз 40](#_Toc495338146)

[Таблица 10 Параметры настройки задачи "Загрузка обновлений в хранилище" 41](#_Toc495338147)

[Таблица 11 Параметры настройки политики Агента администрирования. 41](#_Toc495338148)

[Таблица 12 Параметры настройки «Репозиторий - Общая конфигурация репозитория» 43](#_Toc495338149)

[Таблица 13 Параметры настройки «Конфигурация - Конфигурация Сервера Dr.Web» 43](#_Toc495338150)

[Таблица 14 Параметры настройки «Администрирование → Конфигурация оповещений» 46](#_Toc495338151)

[Таблица 15 Параметры настройки «Конфигурация → Планировщика заданий Сервера Dr.Web» 48](#_Toc495338152)

[Таблица 16. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Права» 49](#_Toc495338153)

[Таблица 17. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Планировщик заданий» 50](#_Toc495338154)

[Таблица 18. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Устанавливаемые компоненты» 51](#_Toc495338155)

[Таблица 19. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Windows» 52](#_Toc495338156)

[Таблица 20. Рекомендуемые к применению на сервере приложений АС ЭКР 2.0 настройки исключений компонеты "SplDer Guard для серверов" ПО СЗ от ВВК "Dr.Web 10" 55](#_Toc495338157)

[Таблица 21. Рекомендуемые к применению на сервере ЕСМИБ ТУ настройки исключений компонет "Сканер", "SplDer Guard для серверов" ПО СЗ от ВВК "Dr.Web 10" 56](#_Toc495338158)

[Таблица 22. Настройка политик безопасности 80](#_Toc495338159)

[Таблица 23. Значения параметров СЗИ от НСД Secret Net 6.5, общие для серверов и ПЭВМ 86](#_Toc495338160)

[Таблица 24. Параметры настройки защитных механизмов Secret Net 6 92](#_Toc495338161)

[Таблица 25. Привилегии доменных групп в системе Secret Net 6 92](#_Toc495338162)

[Таблица 26. Значения параметров ПО СЗИ от НСД Secret Net 7.6, общие для серверов и АРМ 93](#_Toc495338163)

[Таблица 27. Параметры настройки защитных механизмов Secret Net 7 99](#_Toc495338164)

[Таблица 28. Задания/задачи ЗПС 101](#_Toc495338165)

[Таблица 29. Ресурсы для основных ресурсов компьютера – задача MS Windows 107](#_Toc495338166)

[Таблица 30. Ресурсы основных ресурсов компьютера – задача СЗИ Secret Net. 109](#_Toc495338167)

[Таблица 31. Параметры создаваемых Заданий контроля целостности 111](#_Toc495338168)

[Таблица 32. Перечень заданий контроля целосности 112](#_Toc495338169)

[Таблица 33. Контроль целостности критичных ресурсов системного реестра ОС Windows 113](#_Toc495338170)

[Таблица 34. Задания/задачи ЗПС (пример настройки для 64-разрядных операционных систем) 114](#_Toc495338171)

[Таблица 35. Задача "MS Windows: основные ресурсы" 119](#_Toc495338172)

[Таблица 36. Ресурсы основных ресурсов компьютера – задача СЗИ Secret Net 123](#_Toc495338173)

[Таблица 37. Задача КЦ "MS Windows: критичные ресурсы реестра" 125](#_Toc495338174)

[Таблица 38. Настройки при установке ПО ОС Windows XP 132](#_Toc495338175)

[Таблица 39. Настройки параметров групповой политики, применяемой для пользователей, работающих на АРМ платежной системы при использовании СЗИ от НСД «SecretNet» 132](#_Toc495338176)

[Таблица 40. Настройки параметров групповой политики, применяемой для АРМ платежной системы при использовании СЗИ от НСД «SecretNet» 146](#_Toc495338177)

[Таблица 41. Настройки параметров групповой политики, применяемой для файловых серверов и контроллеров платежного домена при использовании СЗИ от НСД «SecretNet» 166](#_Toc495338178)

[Таблица 42. Настройки параметров групповой политики, применяемой для серверов и ПЭВМ платежной системы при использовании СЗИ от НСД «Аккорд» 187](#_Toc495338179)

[Таблица 43 Параметры групповой политики для пользователей СВТ при использовании СЗИ от НСД Secret Net 191](#_Toc495338180)

[Таблица 44. Параметры групповой политики для АРМ при использовании СЗИ от НСД Ssecret Net 213](#_Toc495338181)

[Таблица 45. Параметры групповой политики для рядовых серверов и контролллеров домена при использовании СЗИ от НСД Secret Net 255](#_Toc495338182)

[Таблица 46. Настройки параметров групповой политики для серверов и АРМ при использовании СЗИ от НСД Аккорд 305](#_Toc495338183)

[Таблица 47. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ», применяемые для АРМ РАБИС-НП и АС ЭКР 2.0 307](#_Toc495338184)

[Таблица 48. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части аудита и теневого копирования 308](#_Toc495338185)

[Таблица 49. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части алертинга 309](#_Toc495338186)

[Таблица 50. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования Анти-кейлогера 309](#_Toc495338187)

[Таблица 51. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования устройств 310](#_Toc495338188)

[Таблица 52. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части безопасности устройств 310](#_Toc495338189)

[Таблица 53. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования протоколов 311](#_Toc495338190)

**Перечень сокращений**

|  |  |  |
| --- | --- | --- |
| АМДЗ | – | аппаратный модуль доверенной загрузки |
| АРМ | – | автоматизированное рабочее место |
| АРМ УОС ТУ | – | АРМ учетно-операционной системы ТУ |
| АС ЭКР | – | автоматизированная система эмиссионно-кассовых работ |
| ГУБиЗИ | – | главное управление безопасности и защиты информации |
| ДИТ | – | департамент информационных технологий |
| ЕСМИБ | – | единая система мониторинга информационной безопасности |
| ПАК | – | программно-аппаратный комплекс |
| ПО | – | программное обеспечение |
| РАБИС | – | региональная автоматизированная банковская информационная система |
| СВТ | – | средство вычислительной техники |
| СЗИ | – | средство защиты информации |
| СЗ от ВВК | – | средство защиты от воздействия вредоносного кода |
| СЗИ от НСД | – | средство защиты информации от несанкционированного доступа |
| СКАД | – | система криптографической авторизации электронных документов |
| СПО | – | специальное программное обеспечение |
| СУБД | – | система управления базой данных |
| ТУ | – | территориальное учреждение |

# Общие положения

Настоящий Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации (далее – СЗИ) Территориальных учреждений Банка России для РАБИС-НП и АС ЭКР 2.0 (в дальнейшем – Порядок) разработан с целью выработки и поддержания в актуальном состоянии единой технической политики использования средств обеспечения информационной безопасности на рабочих местах и серверах платёжной системы в Территориальных учреждений Банка России при обеспечении выполнения требований нормативных документов Банка России в части обеспечения информационной безопасности.

Настоящий Порядок включает в себя перечень параметров настройки СЗИ, входящих в состав унифицированных конфигураций СЗИ для АРМ и серверов РАБИС-НП и АС ЭКР 2.0. (далее – Унифицированные конфигурации). Необходимо отметить, что требования к настройкам, содержащиеся в документации на СКАД «Сигнатура» версии 5, имеют приоритет по отношению к рекомендованным настройкам унифицированных конфигураций (письмо ГУБиЗИ 23-4-5/183 от 27.01.2016).

# Область применения

Положения данного Порядка перевода распространяются на участников и объекты взаимодействия:

* ГУБиЗИ как координатора и регулятора работ по обеспечению единой технической политики использования технических средств обеспечения информационной безопасности на рабочих местах и серверах платёжной системы в Территориальных учреждениях Банка России при выполнении требований нормативных документов в части обеспечения информационной безопасности;
* ТУ Банка России - Опорные объекты информатизации Банка России, выполняющие работы по обновлению технорабочей документации РАБИС-НП и АС ЭКР 2.0 в части использования и рекомендованных настроек средств защиты информации в соответствии с вышеприведёнными организационно-распорядительными документами Банка России;
* ТУ Банка России, эксплуатирующие РАБИС-НП и АС ЭКР 2.0;
* Разработчиков РАБИС-НП и АС ЭКР 2.0 в части внесения изменений в технорабочую документацию.
* Ответственные ТУ Банка России.

# Описание плана обновления (актуалиазации) унифицированныХ конфигурациЙ сзи для РАБИС-нп, арм ас экр 2.0 территориальных учреждений банка россии

### Подготовительные работы

### Проверка технологических карт обновлений версий СЗИ

Первым этапом мероприятий по обновлению (актуализации) унифицированных конфигураций является проведение Ответственными ТУ тестирования обновленных унифицированных конфигураций с подготовленными настройками на совместимость с РАБИС-НП и АС ЭКР 2.0, при необходимости взаимодействуя по перечню настроек с Внешней организацией.

По результатам работ тестирования Ответственные ТУ направляют в адрес ГУБиЗИ и опорного объекта по информационной безопасности отчет о проверке документа «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России» на стендах тестирования, включающий замечания и предложения по доработке состава или настроек унифицируемых конфигураций.

### Доработка унифицированных конфигураций и технологических карт обновлений версий СЗИ для РАБИС-НП, АРМ АС ЭКР 2.0

На данном этапе ГУБиЗИ организует доработку типовых конфигураций и технологических карт обновлений версий СЗИ для РАБИС-НП, АС ЭКР 2.0 по замечаниям, полученным от Ответственных ТУ в ходе тестирования унифицированных конфигураций и их настроек, совместимости используемых в них технических и программных средств.

### Принятие решения и направление письма о переводе ТУ на унифицированные конфигурации, направление решения в ТУ

Главное управление безопасности и защиты информации Банка России осуществляет:

* Планирование, организацию и координацию работ по обновлению (актуализации) унифицированных конфигураций в Территориальных учреждениях Банка России;
* Согласование с Департаментом информационных технологий Банка России (далее – ДИТ) и утверждение состава унифицированных конфигураций и их обновлений.
* Направление Письма об обновлении (актуализации) унифицированных конфигураций в Территориальные учреждения Банка России.

### Установка унифицированных конфигураций на стендах тестирования территориальных учреждений

Установка унифицированных конфигураций на стендах тестирования территориальных учреждений Банка России проводится со следующими целями:

* Приведение типов и версий средств информационной безопасности на стендах тестирования к типовым, определённым в унифицированных конфигурациях.
* Практическое ознакомление персонала территориальных учреждений, занятых в процессах эксплутации средств защиты информации с порядком и особенностями установки и дальнейшей эксплуатации типовых типов и версий средств защиты информации из состава унифицированных конфигураций.
* Подготовка к установке данных типов и версий средств информационной безопасности в платёжных сегментах территориальных учреждений Банка России.

Установку унифицированных конфигураций на стендах тестирования необходимо выполнить до их установки в платёжном сегменте ТУ Банка России. При проведении настроек средств защиты информации на стендах тестирования целесообразно руководствоваться требованиями настоящего документа. Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ. Согласование должно быть оформлено документально и утверждено руководством ТУ.

### Настройка доменной структуры на стенде

Применение доменной структуры Active Directory является обязательным условием использования унифицированных конфигураций средств защиты информации для РАБИС-НП и АС ЭКР. К указанным серверам необходимо применить политики и настройки, рекомендованные документами УК.

Необходимые настройки доменной структуры Active Directory для использования унифицированных конфигураций приведены в приложениях (ПРИЛОЖЕНИЕ 4 и ПРИЛОЖЕНИЕ 5) данного документа.

### Установка и настройка унифицированных версий СЗ от ВВК на стенде

При наличии на стендах тестирования ТУ версий СЗ от ВВК, отличных от приведенных в документе «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России», необходимо провести их обновление. Порядок установки и обновления СЗ от ВВК описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

В качестве решений по защите ресурсов УОС ТУ Банка России от разрушающих и иных воздействий вредоносного кода должно использоваться программное обеспечение с учётом эшелонирования защиты согласно требованиям п.2.2 Положения Банка России № 327-П от 01.11.2008 «Об организации защиты информационно-вычислительных ресурсов Банка России от воздействий вредоносного кода» для Уровня серверов и Уровня рабочих станций (далее – АРМ).

В соответствии с документом «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России» для обеспечения многоуровневой системы защиты от воздействия вредоносного кода (далее – СЗ от ВВК) рекомендуется установка двух различных средств защиты от ВВК. Согласно данному документу:

* для Уровня серверов определено использование «Dr.Web»:
  + серверная часть (управляющий компонент) Dr.Web Enterprise Security Suite (версия 10.01.0);
  + клиентская часть (агент) Agent for Windows (версия 11.0.1.05150)[[1]](#footnote-2) – при установке агента с помощью Центра управления;
  + клиентская часть (агент) Agent for Windows supporting Active Directory (версия 11.00.05180)1 – при установке агента с помощью службы Active Directory;
* для Уровня рабочих станций (АРМ) – СЗ от ВВК семейства «Антивирус Касперского»:
  + серверная часть (управляющий компонент) Kaspersky Security Center 10 Service Pack 2 (версия 10.3.407);
  + клиентская часть Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 2 (версия 10.2.4.674).

Рекомендованные настройки СЗ от ВВК унифицированных версий описаны в приложении (ПРИЛОЖЕНИЕ 1) в разделах П1.1 и П1.2 для антивируса Kaspersky, в разделе П1.5 для антивируса Dr.Web. Обновление СЗ от ВВК на АРМ и серверах должно выполняться в период времени, когда данные АРМ и сервера не задействованы в обработке платежной информации.

Дополнительно в приложении (ПРИЛОЖЕНИЕ 1) в разделах П1.3 и П1.4 приведены настройки СЗ от ВВК обновленных версий семейства «Антивирус Касперского» для Уровня рабочих станций (АРМ):

* + серверная часть (управляющий компонент) Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (версия 10.4.343);
  + клиентская часть Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294) – для АРМ с ОС Windows 7;
* клиентская часть Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 4 (версия 10.2.6.3733) – АРМ с ОСWindows XP SP3.

Контроль/защита от воздействия вредоносного кода ПО агента ЕСМИБ ТУ и серверов ЕСМИБ ТУ выполняется встроенными механизмами защиты ЕСМИБ ТУ в соответствии с типовыми решениями ЕСМИБ ТУ.

Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в Территориальных учреждениях Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Установка и настройка средств защиты информации от несанкционированного доступа на стенде

При наличии на стендах тестирования ТУ версий СЗИ от НСД, отличных от приведенных в документе «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России», необходимо провести их обновление. Порядок установки и обновления СЗИ от НСД описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

В соответствии с документом «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России» в качестве унифицированных версий СЗИ от НСД в ТУ Банка России рекомендуется применять:

* «Secret Net» (сетевой вариант) версия 6.5 или версия 7.6:
  + совместно с платой Secret Net Card или ПАК Соболь версии 3.0;
  + с использованием входящего в его состав механизма защиты дисков совместно с аппаратным средством защиты RuToken S.
* СПО Аккорд (автономный вариант): «Аккорд-Win32» версии 4.0.9.43 (актуальная 4.0.9.50) или «Аккорд-Win64» версии 5.0.9.43 (актуальная 5.0.9.50) совместно с системным ПО контроллеров «Аккорд-5MX», «Аккорд-5.5», «Аккорд-5.5е» версии 02.01.015.

Порядок обновления СЗИ от НСД, включая средства централизованного управления, описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

Требования к версиям программной части и встроенного программного обеспечения контроллеров приведены в документе «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России».

Настройки СЗИ от НСД унифицированных версий описаны в приложениях (ПРИЛОЖЕНИЕ 2 и ПРИЛОЖЕНИЕ 3) к настоящему документу.

Контроль/защита от несанкционированных изменений ПО агента ЕСМИБ ТУ и серверов ЕСМИБ ТУ выполняется встроенными механизмами защиты, блокирующими попытки доступа на запись со стороны стороннего ПО, в соответствии с типовыми решениями ЕСМИБ ТУ.

Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Установка и настройка унифицированной версии системы «Контроль-ПУ»

В соответствии с документом «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России» для организации блокировки и контроля доступа к коммуникационным портам и устройствам ввода-вывода на средствах вычислительной техники стендов сопровождения и тестирования РАБИС-НП и АС ЭКР 2.0 рекомендуется применять систему «Контроль-ПУ» на основе программного комплекса DeviceLock (актуальная версия 8.2.69641) в ТУ Банка России.

Требования к версии программной части приведены в документе «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России».

Настройки системы «Контроль-ПУ» на основе ПК DeviceLock унифицированной версии описаны в приложении (ПРИЛОЖЕНИЕ 6) к настоящему документу. В целях  создания на стендах тестирования РАБИС-НП и АС ЭКР 2.0 условий, идентичных промышленной среде (платежному сегменту) функционирования РАБИС-НП и АС ЭКР 2.0 применение системы «Контроль-ПУ» на основе программного комплекса DeviceLock может быть опциональным при условии, что функционал данной системы (контроль портов и ведение журналов событий) осуществляется механизмами защиты СЗИ от НСД Secret Net.

Рекомендованные настройки и опциональное использование системы «Контроль-ПУ» на основе ПК DeviceLock могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

При наличии на стендах тестирования ТУ версий системы «Контроль-ПУ», отличных от приведенных в документе «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России», необходимо провести их обновление. Порядок установки и обновления системы «Контроль-ПУ» описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

### Установка и настройка унифицированной версии системы паспортизации

При наличии на стендах тестирования ТУ версий системы паспортизации, отличных от приведенных в документе «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России», необходимо провести их обновление. Порядок установки и обновления системы паспортизации описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

В соответствии с документом «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России» в качестве системы паспортизации на основе программного комплекса «Паспорт автоматизированных рабочих мест учетно-операционной системы» (далее – ПК «Паспорт АРМ УОС») в ТУ Банка России рекомендуется применять версию не ниже 5.17.х.х (рекомендованная и протестированная версия 5.17.8.4). Порядок обновления системы паспортизации на основе ПК «Паспорт АРМ УОС» описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

Настройки системы паспортизации на основе ПК «Паспорт АРМ УОС» унифицированной версии описаны в приложении (ПРИЛОЖЕНИЕ 7) к настоящему документу.

Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Установка унифицированных конфигураций в платежном сегменте территориальных учреждений

### Настройка доменной структуры в платёжном сегменте ТУ Банка России

Применение доменной структуры Active Directory является обязательным условием использования унифицированных конфигураций средств защиты информации для РАБИС-НП и АС ЭКР. К указанным серверам необходимо применить политики и настройки, рекомендованные документами УК.

Необходимые настройки доменной структуры Active Directory для использования унифицированных конфигураций приведены в приложениях (ПРИЛОЖЕНИЕ 4 и ПРИЛОЖЕНИЕ 5) данного документа.

Для обеспечения взаимодействия СВТ, установленных в различных сегментах платежной сети, с серверами централизованного управления средствами защиты информации, мониторинга информационной безопасности и инфраструктурной компонентой:

* СЗ от ВВК «Антивирус Касперского»,
* СЗ от ВВК «Dr.Web»,
* СЗИ от НСД Secret Net,
* СЗИ от НСД «Аккорд»,
* Система паспортизации «Паспорт АРМ УОС»,
* IBM WebSphere MQSeries (WMQ),
* Единая система мониторинга информационной безопасности территориального учреждения Банка России (ЕСМИБ),
* Региональное звено интегрированной системы управления телекоммуникационными и информационными ресурсами (РЗ ИСУТИР),
* Региональная система сегмента распространения программных средств (РС СРПС),
* Система резервного копирования (СРК),
* доменные службы DNS,
* службы единого времени,

необходимо обеспечить их сквозное сетевое взаимодействие. Приведенный перечень программных средств и системных компонент может быть изменен или дополнен в рамках перечня разрешенных протоколов и портов, указанных в документации производителя программного обеспечения по согласованию с подразделением безопасности и защиты информации. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Установка и настройка СЗ от ВВК в платёжном сегменте ТУ Банка России

В соответствии с документом «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России» для обеспечения многоуровневой системы защиты от воздействия вредоносного кода (далее – СЗ от ВВК) рекомендуется установка двух различных средств защиты от ВВК. Согласно данному документу:

* для Уровня серверов определено использование «Dr.Web»:
  + серверная часть (управляющий компонент) Dr.Web Enterprise Security Suite (версия 10.01.0);
  + клиентская часть (агент) Agent for Windows (версия 11.0.1.05150)1 – при установке агента с помощью Центра управления;
  + клиентская часть (агент) Agent for Windows supporting Active Directory (версия 11.00.05180)1 – при установке агента с помощью службы Active Directory;
* для Уровня рабочих станций (АРМ) – СЗ от ВВК семейства «Антивирус Касперского»:
  + серверная часть (управляющий компонент) Kaspersky Security Center 10 Service Pack 2 (версия 10.3.407);
  + клиентская часть Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 2 (версия 10.2.4.674).

Рекомендованные настройки СЗ от ВВК унифицированных версий описаны в приложении (ПРИЛОЖЕНИЕ 1) в разделах П1.1 и П1.2 для антивируса Kaspersky, в разделе П1.5 для антивируса Dr.Web. Обновление СЗ от ВВК на АРМ и серверах должно выполняться в период времени, когда данные АРМ и сервера не задействованы в обработке платежной информации.

Дополнительно в приложении (ПРИЛОЖЕНИЕ 1) в разделах П1.3 и П1.4 приведены настройки СЗ от ВВК обновленных версий семейства «Антивирус Касперского» для Уровня рабочих станций (АРМ):

* + серверная часть (управляющий компонент) Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 (версия 10.4.343);
  + клиентская часть Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294) – для АРМ с ОС Windows 7;
  + клиентская часть Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 4 (версия 10.2.6.3733) – АРМ с ОСWindows XP SP3.

Контроль/защита от воздействия вредоносного кода ПО агента ЕСМИБ ТУ и серверов ЕСМИБ ТУ выполняется встроенными механизмами защиты ЕСМИБ ТУ в соответствии с типовыми решениями ЕСМИБ ТУ.

Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Установка и настройка СЗИ от НСД в платёжном сегменте ТУ Банка России

В соответствии с документом «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России» в качестве унифицированных версий СЗИ от НСД в ТУ Банка России рекомендуется применять:

* «Secret Net» (сетевой вариант) версия 6.5 или версия 7.6:
  + совместно с платой Secret Net Card или ПАК Соболь версии 3.0;
  + с использованием входящего в его состав механизма защиты дисков совместно с аппаратным средством защиты RuToken S.
* СПО Аккорд (автономный вариант): «Аккорд-Win32» версии 4.0.9.43 (актуальная 4.0.9.50) или «Аккорд-Win64» версии 5.0.9.43 (актуальная 5.0.9.50) совместно с системным ПО контроллеров «Аккорд-5MX», «Аккорд-5.5», «Аккорд-5.5е» версии 02.01.015.

Требования к версиям программной части и встроенного программного обеспечения контроллеров приведены в документе «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России».

Настройки СЗИ от НСД унифицированных версий описаны в приложениях (ПРИЛОЖЕНИЕ 2 и ПРИЛОЖЕНИЕ 3) к настоящему документу.

Контроль/защита от несанкционированных изменений ПО агента ЕСМИБ ТУ и серверов ЕСМИБ ТУ выполняется встроенными механизмами защиты, блокирующими попытки доступа на запись со стороны стороннего ПО, в соответствии с типовыми решениями ЕСМИБ ТУ.

Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Установка и настройка системы паспортизации в платёжном сегменте ТУ Банка России

В соответствии с документом «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России» в качестве системы паспортизации на основе ПК «Паспорт АРМ УОС» в ТУ Банка России рекомендуется применять версию не ниже 5.17.х.х (рекомендованная и протестированная версия 5.17.8.4). Порядок обновления системы паспортизации на основе ПК «Паспорт АРМ УОС» описан в документе «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России».

Требования к версии программной части приведены в документе «Перечень унифицированных конфигураций СЗИ для использования в РАБИС-НП и АС ЭКР 2.0 территориальных учреждений Банка России».

Настройки системы паспортизации на основе ПК «Паспорт АРМ УОС» унифицированной версии описаны в приложении (ПРИЛОЖЕНИЕ 7) к настоящему документу.

Рекомендованные настройки могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

### Доработка технорабочих проектов на РАБИС-НП и АС ЭКР 2.0 ТУ БР

Специалистами ТУ Банка России или специалистами подрядной организации в установленном порядке вносятся изменения в технорабочую документацию РАБИС-НП и АС ЭКР 2.0 Территориального учреждения Банка России в соответствии с актуализированной и утвержденной ДИТ и ГУБиЗИ типовой технорабочей документацией на РАБИС–НП и АС ЭКР 2.0.

### НАСТРОЙКА СЗ ОТ ВВК

### Параметры настройки СЗ от ВВК «Kaspersky Security Center 10.3.407»

Ниже приведены рекомендованные настройки для средств защиты от воздействия вредоносного кода (СЗ от ВВК). Данные настройки, при необходимости, могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

Внимание: Настройка параметра политики для программного обеспечения системы защиты от воздействия вредоносного кода «Kaspersky Endpoint Security 10» для Windows на рабочих станциях (далее - ПО СЗ от ВВК KES 10) "Отображать интерфейс программы" (в разделе "Дополнительные параметры – Интерфейс - Взаимодействие с пользователем") является элементом настройки механизма замкнутой программной среды для пользователя. Установка параметра "Отображать интерфейс программы" в значение "Выключен" предотвращает несанкционированный доступ пользователя к проводнику Windows через интерфейс ПО СЗ от ВВК KES 10.

Для выполнения требования, указанного в пункте 3.6 Положения Банка России от 01.11.2008 № 327-П "Об организации защиты информационно-вычислительных ресурсов Банка России от воздействия вредоносного кода" (с учетом изменений и дополнений), необходимо выполнить настройку уведомлений в разделе "Дополнительные параметры – Интерфейс - Уведомления" в соответствии с таблицей (Таблица 1):

Таблица 1. Параметры политик СЗ от ВВК Антивирус «Kaspersky Endpoint Security 10» SP 1 MR 2 (версия 10.2.4.674) для рабочих станций пользователей РАБИС-НП и АС ЭКР 2.0

| **Раздел** | **Параметр (группа параметров)** | | | | | | | **Значение  параметра** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Контроль рабочего места | Контроль активности программ  (Заблокировать изменение параметра – З) | | | | | | | Выключен |
| Антивирусная защита - основные параметры защиты | Основные параметры | Запускать Kaspersky Endpoint Security 10 для Windows при включении компьютера | | | | | | √ |
| Применять технологию лечения активного заражения | | | | | | √ |
| Объекты для обнаружения (З) | Объекты для обнаружения (Настройка) | | | | Вредоносные  программы | | √ Вирусы, черви |
| √ Троянские программы |
| √ Вредоносные утилиты |
| Реклама, автодозвон, другие программы | | √ Рекламные программы |
| √ Программы автодозвона |
| √ Другие |
| Упаковщики | | √ Упакованные файлы, которые могут нанести вред |
| √ Многократно упакованные файлы |
| Исключения и доверенная зона (З)[[2]](#footnote-3) | Доверенная зона | | | | | | Рекомендуется исключить из проверки компонентом "Файловый антивирус":  1) каталоги с ПО СЗИ от НСД. Например, для Secret Net (включая подкаталоги):  C:\Program Files\Infosec\\*.\*;  C:\Program Files\Secret Net\\*.\*;  2) файлы агента ОС Windows ЕСМИБ ТУ:  c:\Windows\AGENT\mailaudt.la;  3) файлы облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\ Agents\\*\Data\mailaudt.la;  4) каталог агентской платформы ЕСМИБ ТУ (включая вложенные подкаталоги):  c:\Program Files (x86)\Crystall\Misc \AgentPlatform\\*.\*.  Рекомендуется добавить в перечень доверенных программ:  1) процессы агента ОС Windows ЕСМИБ ТУ:  c:\Windows\AGENT\sthl.exe;  c:\Windows\AGENT\dskappl.dll;  c:\Windows\AGENT\explorer.exe  c:\Windows\AGENT \sthl.dll;  2) процесс облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\liteagent.exe**;**  3) процесс агентской платформы:  C:\Program Files (x86)\Crystall\Misc\ AgentPlatform\AgentPlatform.exe |
| Контролируемые порты (З) | Контролировать только  выбранные порты | | | | | | Список портов формируется автоматически:  √ SMTP(25)  √ HTTP(80,81,82,83)  √ POP3(110)  √ IRC(113)  √ NNTP(119)  √ IMAP(143)  √ IRC(194)  √ HTTPS(443)  √ SMTP SSL(465)  √ NNTP SSL(563)  √ IMAP SSL (993)  √ POP3 SSL(995)  √HTTP(1080,3128,7900,8000,8080, 8088,8888,11523). |
| Антивирусная защита -Файловый  антивирус | Файловый антивирус (З) | | | | | | | √ |
| Уровень  безопасности (З) | | Общие | | | | Типы файлов | Все файлы |
| Область  защиты | Все съемные диски |
| Все жесткие диски |
| Производительность | | | | Методы  проверки | √ Сигнатурный,  √ Эвристический анализ  (поверхностный) |
| Оптимизация проверки | √ Проверять только новые и измененные файлы |
| Проверка  составных  файлов | √ Проверять архивы,  √ Проверять установочные пакеты,  √ Проверять вложенные  OLE-объекты |
| Производительность  (Дополнительно) | | | | Составные файлы  (Фоновая  проверка) | √ Распаковывать составные файлы в фоновом режиме;  Минимальный размер файла:  0 Мб |
| Составные файлы  (Ограничение по размеру) | Не распаковывать составные файлы большого размера - Выключен; |
| Дополнительно | | | | Режим проверки | Интеллектуальный |
| Технологии  проверки | √ Технология iSwift |
| √ Технология iChecker |
| Действие при обнаружении угрозы (З) | | Выполнять действие: | | | | | √ Лечить |
| √ Удалять, если лечение невозможно[[3]](#footnote-4) |
| Антивирусная защита - Почтовый Антивирус | Почтовый Антивирус (З) | | | | | | | Выключен |
| Антивирусная защита – Веб-Антивирус | Веб-Антивирус (З) | | | | | | | Выключен |
| Антивирусная защита – IM-Антивирус | IM-Антивирус (З) | | | | | | | Выключен |
| Антивирусная защита - Сетевой экран | Сетевой экран (З) | | | | | | | Выключен |
| Антивирусная защита – Защита от сетевых атак | Защита от сетевых атак (З) | | | | | | | Выключен |
| Мониторинг системы | Мониторинг системы (З) | | | | | | | Включен[[4]](#footnote-5) |
| Общие параметры (З) | | | | Включить защиту от  эксплойтов | | | √ |
| Хранить историю активности программ для базы BSS | | | √ |
| Не контролировать активность программ, имеющих цифровую подпись | | | √ |
| Откат действий вредоносных программ (З) | | | | Выполнять откат действий вредоносных программ при лечении | | | √ |
| Проактивная защита (З) | | | | √ Использовать обновляемые шаблоны опасного поведения(BSS) | | | Выбирать действие автоматически |
| Дополнительные параметры -Параметры программы | Параметры самозащиты (З) | | | Включить самозащиту | | | | √ |
| Выключить внешнее управление системной службой | | | | √ |
| Режимы работы (З) | | | Не запускать задачи по расписанию при работе от аккумулятора | | | | √ |
| Уступать ресурсы другим программам | | | | √ |
| Разрешать отображение и управление локальными задачами (за исключением выборочной проверки) | | | | Выключен |
| Разрешать управление групповыми задачами | | | | Выключен |
| Использовать KSC в качестве прокси-сервера для активации | | | | Выключен |
| Включить запись дампов | | | | Выключен |
| Параметры прокси-сервера | | | Использовать прокси-сервер | | | | Выключен |
| Дополнительные параметры – Параметры защиты | Фоновая проверка (3) | | | Выполнять проверку во время простоя компьютера | | | | Выключен |
| Проверка съемных дисков при подключении (З) | | | Действия при подключении съемного диска | | | | Быстрая проверка |
| Максимальный размер съемного диска | | | | Не определено |
| Защита от атак BadUSB (З) | | | Запрашивать авторизацию USB-клавиатур при подключении | | | | √ |
| Разрешать использование экранной клавиатуры при авторизации | | | | Выключен |
| Дополнительные параметры -Отчеты и хранилища | Параметры отчетов (З) | | | Хранить отчеты не более | | | | √  90 дней |
| Максимальный размер файла | | | | 100 Мб |
| Карантин и  резервное  хранилище (З) | | | Проверять файлы на карантине после обновления | | | | √ |
| Хранить объекты не более | | | | √  90 дней |
| Максимальный размер хранилища | | | | 100 Мб |
| Информировать Сервер администрирования (З) | | | О файлах на карантине | | | | √ |
| О файлах резервного  хранилища | | | | √ |
| О необработанных файлах | | | | √ |
| О найденных уязвимостях | | | | Выключен |
| Об установленных устройствах | | | | Выключен |
| О запускаемых программах | | | | Выключен |
| Об ошибках шифрования файлов | | | | Выключен |
| Уведомление о состоянии локальных антивирусных баз | | | Отправить уведомление "Базы устарели", если обновление баз не выполнялось | | | | 3 дня |
| Отправить уведомление "Базы сильно устарели", если обновление баз не выполнялось | | | | 7 дней |
| Параметры KSN | Параметры KSN | | | Принимаю условия Положения и участвую в KSN | | | | Выключен |
| Дополнительные параметры -Интерфейс | Взаимодействие с пользователем (З) | | | Отображать интерфейс программы | | | | Выключен[[5]](#footnote-6) |
| Отображать "Protected be Kaspersky Lab" поверх экрана приветствия Windows | | | | √ |
| Защита паролем (З) | | | Включить защиту паролем | | | | √  Через кнопку "Настройка" задать пароль[[6]](#footnote-7) |
| Уведомления (З) (настроить дополнительно к параметрам по умолчанию) | | | Системный аудит – Уведомлять на экране | | | | Включить все критические события и события, связанные со сбоями в работе программы |
| Антивирусная защита - Файловый антивирус – Уведомлять на экране | | | | Включить все критические события |
| Антивирусная защита – Мониторинг системы – Уведомлять на экране | | | | Включить все критические события |
| Задачи по расписанию – Обновления – Уведомлять на экране | | | | Включить все критические события |

### Параметры настройки задач СЗ от ВВК Kaspersky Security Center 10.3.407

Таблица 2 Параметры задачи поиска вирусов

| **Раздел** | **Параметр (группа параметров)** | | | **Значение параметра** |
| --- | --- | --- | --- | --- |
| Уведомление | √ На Сервере администрирования в течение (дней) | | | 90 |
| В журнале событий ОС на клиентском компьютере | | | √ |
| В журнале событий ОС на Сервере администрирования | | | √ |
| Сохранять все события | | | + |
| Расписание[[7]](#footnote-8) | Запуск по расписанию | | | Еженедельно |
| Каждый | | | День недели ТУ определяет самостоятельно |
| Время запуска | | | Время запуска ТУ определяет самостоятельно |
| Запускать пропущенные задачи | | | √ |
| Распределять запуск задачи случайным образом в интервале (мин.) | | | 5 |
| Параметры | Уровень  безопасности | Область  действия | Типы файлов | Все файлы |
| Проверка  составных  файлов | √ Проверять все архивы |
| √ Проверять все установочные пакеты |
| √ Проверять все вложенные OLE-объекты |
| Дополнительно | Методы  проверки | √ Эвристический анализ (глубокий) |
| Технологии  проверки | √ Технологий iSwift |
| √ Технология iChecker |
| Область проверки (Настройка) | Область проверки | | √ Системная память,  √ Объекты автозапуска,  √ Загрузочные секторы,  √ Системное резервное хранилище,  √ Все съемные диски,  √ Все жесткие диски  (√ включая вложенные папки) |
| Действие при обнаружении угрозы | Выполнять действие: Лечить. Удалять, если лечение невозможно | | |
| Лечить | | √ |
| Удалять, если лечение невозможно | | √[[8]](#footnote-9) |
| Учетная запись | Автоматически созданная учетная запись | | | + |

Таблица 3 Параметры настройки задачи обновления сигнатурных баз

| **Наименование параметра** | **Значение параметра** | | |
| --- | --- | --- | --- |
| Общие | | | |
| Наименование | Задача обновления | | |
| Уведомления | | | |
| Сохранять  информацию о результатах | На сервере администрирования в течение (дней): | | 90 |
| Сохранять все события | | + |
| Расписание | | | |
| Запуск по  расписанию | При загрузке обновлений в хранилище | | |
| Запускать пропущенные задачи | | + |
| Автоматически определять интервал для распределения запуска задачи | | + |
| Параметры обновления баз и модулей программы | | | |
| Параметры обновления в локальном  режиме | Источник обновлений | Kaspersky Security Center 10.х | + |
| Региональные параметры | Определять автоматически |
| Загружать обновления модулей программы – Устанавливать критические и одобренные обновления[[9]](#footnote-10) | | + |
| Учетная запись | | | |
| Автоматически созданная учетная запись | | | + |

Таблица 4 Параметры настройки задачи "Загрузка обновлений в хранилище"[[10]](#footnote-11)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Раздел** | **Значение параметра** | | | | | |
| Уведомление | Сохранять информацию о результатах | | На сервере администрирования в течение (дней): | | | 90 |
| Сохранять все события | | | + |
| Расписание | Запуск по расписанию | | | | Ежедневно | |
| Каждый | | | | 1 день | |
| Время запуска | | | | Время запуска ТУ определяет самостоятельно | |
| Запускать пропущенные задачи | | | | + | |
| Параметры | Источник  обновлений | Локальная или  сетевая папка | | Указать источник в соответствии с принятым в ТУ порядком | | |
| Состав  обновлений | Определять состав загружаемых обновлений автоматически | | | | + |
| Прочие  параметры | Обновлять модули Серверов администрирования | | | | + |
| Обновлять модули Агентов администрирования | | | | + |

Таблица 5 Параметры настройки политики Агента администрирования[[11]](#footnote-12)

| **Раздел  политики** | **Параметр (группа параметров)** | | **Значение  параметра** |
| --- | --- | --- | --- |
| Параметры | Скачивать обновления только через агенты обновлений (З) | | √ |
| Максимальный размер очереди событий (МБ): (З) | | 2 |
| Использовать пароль деинсталляции | | √[[12]](#footnote-13) |
| Хранилища | Информация об установленных программах (З) | | √ |
| Информация об обновлениях MS Windows (З) | | √ |
| Информация об уязвимостях ПО (З) | | √ |
| Информация о реестре оборудования (З) | | √ |
| Управление перезагрузкой | Не перезагружать ОС | | + |
| Общий доступ к РС | Включить аудит | | Выключен |
| Сеть | Подключение к Серверу администрирования (З) | Период синхронизации (мин.) | 15 |
| Сжимать сетевой трафик | √ |
| Использовать  SSL-соединение | √ |
| Использовать UDP-порт (З) | | √ |
| Номер UDP-порта | | 15000 |
| Сеть-Менеджер соединений | Подключаться при необходимости | | + |

### Параметры настройки СЗ от ВВК «Kaspersky Security Center 10.4.343»

Ниже приведены рекомендованные настройки для СЗ от ВВК обновленных версий семейства «Антивирус Касперского» для Уровня рабочих станций (АРМ). Данные настройки, при необходимости, могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

Внимание: Настройка параметра политики для программного обеспечения системы защиты от воздействия вредоносного кода «Kaspersky Endpoint Security 10» для Windows на рабочих станциях (далее - ПО СЗ от ВВК KES 10) "Отображать интерфейс программы" (в разделе "Дополнительные параметры – Интерфейс - Взаимодействие с пользователем") является элементом настройки механизма замкнутой программной среды для пользователя. Установка параметра "Отображать интерфейс программы" в значение "Выключен" предотвращает несанкционированный доступ пользователя к проводнику Windows через интерфейс ПО СЗ от ВВК KES 10.

Для выполнения требования, указанного в пункте 3.6 Положения Банка России от 01.11.2008 № 327-П "Об организации защиты информационно-вычислительных ресурсов Банка России от воздействия вредоносного кода" (с учетом изменений и дополнений), необходимо выполнить настройку уведомлений в разделе "Дополнительные параметры – Интерфейс - Уведомления" в соответствии с таблицами (Таблица 6 и Таблица 7):

Таблица 6. Параметры политик СЗ от ВВК Антивирус «Kaspersky Endpoint Security 10» SP 1 MR 4 (версия 10.2.6.3733) для рабочих станций пользователей РАБИС-НП и АС ЭКР 2.0 под управлением ОС Windows XP SP3 RUS.

| **Раздел** | **Параметр (группа параметров)** | | | | | | **Значение  параметра** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Контроль рабочего места | Контроль активности программ  (Заблокировать изменение параметра - З) | | | | | | Выключен |
| Антивирусная защита - основные параметры защиты | Основные параметры | Запускать Kaspersky Endpoint Security 10 для Windows при включении компьютера | | | | | √ |
| Применять технологию лечения активного заражения | | | | | √ |
| Объекты для обнаружения (З) | Объекты для обнаружения (Настройка) | | | Вредоносные  программы | | √ Вирусы, черви |
| √ Троянские программы |
| √ Вредоносные утилиты |
| Реклама, автодозвон, другие программы | | √ Рекламные программы |
| √ Программы автодозвона |
| √ Другие |
| Упаковщики | | √ Упакованные файлы, которые могут нанести вред |
| √ Многократно упакованные файлы |
| Исключения и доверенная зона (З)[[13]](#footnote-14) | Доверенная зона | | | | | Рекомендуется исключить из проверки компонентом "Файловый антивирус":  1) каталоги с ПО СЗИ от НСД. Например, для Secret Net (включая подкаталоги):  C:\Program Files\Infosec\\*.\*;  C:\Program Files\Secret Net\\*.\*;  2) файлы агента ОС Windows ЕСМИБ ТУ:  c:\Windows\AGENT\mailaudt.la;  3) файлы облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\ Agents\\*\Data\mailaudt.la;  4) каталог агентской платформы ЕСМИБ ТУ (включая вложенные подкаталоги):  c:\Program Files (x86)\Crystall\Misc \AgentPlatform\\*.\*.  Рекомендуется добавить в перечень доверенных программ:  1) процессы агента ОС Windows ЕСМИБ ТУ:  c:\Windows\AGENT\sthl.exe;  c:\Windows\AGENT\dskappl.dll;  c:\Windows\AGENT\>\explorer.exe  c:\Windows\AGENT \sthl.dll;  2) процесс облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\liteagent.exe**;**  3) процесс агентской платформы:  C:\Program Files(x86)\Crystall\Misc\ AgentPlatform\AgentPlatform.exe |
| Контролируемые порты (З) | Контролировать только  выбранные порты | | | | | Список портов формируется автоматически:  √ SMTP(25)  √ HTTP(80,81,82,83)  √ POP3(110)  √ IRC(113)  √ NNTP(119)  √ IMAP(143)  √ IRC(194)  √ HTTPS(443)  √ SMTP SSL(465)  √ NNTP SSL(563)  √ IMAP SSL (993)  √ POP3 SSL(995)  √HTTP(1080,3128,7900,8000,8080, 8088,8888,11523). |
| Антивирусная защита -Файловый  антивирус | Файловый антивирус (З) | | | | | | √ |
| Уровень  безопасности (З) | | Общие | | | Типы файлов | Все файлы |
| Область  защиты | √ Все съемные диски |
| √ Все жесткие диски |
| Производительность | | | Методы  проверки | √ Сигнатурный,  √ Эвристический анализ  (поверхностный) |
| Оптимизация проверки | √ Проверять только новые и измененные файлы |
| Проверка  составных  файлов | √ Проверять архивы,  √ Проверять установочные пакеты,  √ Проверять вложенные  OLE-объекты |
| Производительность  (Дополнительно) | | | Составные файлы  (Фоновая  проверка) | √ Распаковывать составные файлы в фоновом режиме;  Минимальный размер файла:  0 Мб |
| Составные файлы  (Ограничение по размеру) | Не распаковывать составные файлы большого размера - Выключен; |
| Дополнительно | | | Режим проверки | Интеллектуальный |
| Технологии  проверки | √ Технология iSwift |
| √ Технология iChecker |
| Действие при обнаружении угрозы (З) | | Выполнять действие: | | | | √ Лечить |
| √ Удалять, если лечение невозможно[[14]](#footnote-15) |
| Антивирусная защита - Почтовый Антивирус | Почтовый Антивирус (З) | | | | | | Выключен |
| Антивирусная защита – Веб-Антивирус | Веб-Антивирус (З) | | | | | | Выключен |
| Антивирусная защита – IM-Антивирус | IM-Антивирус (З) | | | | | | Выключен |
| Антивирусная защита - Сетевой экран | Сетевой экран (З) | | | | | | Выключен |
| Антивирусная защита – Защита от сетевых атак | Защита от сетевых атак (З) | | | | | | Выключен |
| Мониторинг системы | Мониторинг системы (З) | | | | | | Включен[[15]](#footnote-16) |
| Общие параметры (З) | | | Включить защиту от  эксплойтов | | | √ |
| Хранить историю активности программ для базы BSS | | | √ |
| Не контролировать активность программ, имеющих цифровую подпись | | | √ |
| Откат действий вредоносных программ (З) | | | Выполнять откат действий вредоносных программ при лечении | | | √ |
| Проактивная защита (З) | | | √ Использовать обновляемые шаблоны опасного поведения(BSS) | | | Выбирать действие автоматически |
| Дополнительные параметры -Параметры программы | Параметры самозащиты (З) | | | Включить самозащиту | | | √ |
| Выключить внешнее управление системной службой | | | √ |
| Режимы работы (З) | | | Не запускать задачи по расписанию при работе от аккумулятора | | | √ |
| Уступать ресурсы другим программам | | | √ |
| Разрешить отображение и управление локальными задачами (за исключением выборочной проверки) | | | Выключен |
| Разрешить управление групповыми задачами | | | Выключен |
| Использовать KSC в качестве прокси-сервера для активации | | | Выключен |
| Включить запись дампов | | | Выключено |
| Отсылать файлы дампов и файлов трассировки в "Лабораторию Касперского" | | | Выключен |
| Дополнительные параметры – Параметры защиты | Фоновая проверка (3) | | | Выполнять проверку во время простоя компьютера | | | Выключен |
| Проверка съемных дисков при подключении (З) | | | Действия при подключении съемного диска | | | Быстрая проверка |
| Максимальный размер съемного диска | | | Не определено |
| Защита от атак BadUSB (З) | | | Запрашивать авторизацию USB-клавиатур при подключении | | | √ |
| Разрешать использование экранной клавиатуры при авторизации | | | Выключен |
| Дополнительные параметры -Отчеты и хранилища | Параметры отчетов (З) | | | Хранить отчеты не более | | | √  90 дней |
| Максимальный размер файла | | | 100 Мб |
| Карантин и  резервное  хранилище (З) | | | Проверять файлы на карантине после обновления | | | √ |
| Хранить объекты не более | | | √  90 дней |
| Максимальный размер хранилища | | | 100 Мб |
| Информировать Сервер администрирования (З) | | | О файлах на карантине | | | √ |
| О файлах резервного  хранилища | | | √ |
| О необработанных файлах | | | √ |
| О найденных уязвимостях | | | √ |
| Об установленных устройствах | | | √ |
| О запускаемых программах | | | √ |
| Об ошибках шифрования файлов | | | Выключен |
| Уведомление о состоянии локальных антивирусных баз | | | Отправить уведомление "Базы устарели", если обновление баз не выполнялось | | | 3 дня |
| Отправить уведомление "Базы сильно устарели", если обновление баз не выполнялось | | | 7 дней |
| Параметры KSN | Параметры KSN | | | Принимаю условия Положения и участвую в KSN | | | Выключен |
| Дополнительные параметры -Интерфейс | Взаимодействие с пользователем (З) | | | Отображать интерфейс программы | | | Выключен[[16]](#footnote-17) |
| Отображать "Protected be Kaspersky Lab" поверх экрана приветствия Windows | | | √ |
| Защита паролем (З) | | | Включить защиту паролем | | | √  Через кнопку "Настройка" задать пароль[[17]](#footnote-18) |
| Уведомления (З) (настроить дополнительно к параметрам по умолчанию) | | | Системный аудит – Уведомлять на экране | | | Включить все критические события и события, связанные со сбоями в работе программы |
| Антивирусная защита - Файловый антивирус – Уведомлять на экране | | | Включить все критические события |
| Антивирусная защита – Мониторинг системы – Уведомлять на экране | | | Включить все критические события |
| Задачи по расписанию – Обновления – Уведомлять на экране | | | Включить все критические события |
| Поддержка пользователей  (Настройка) | | | Информация о поддержке | | |  |

Таблица 7. Параметры политик СЗ от ВВК Антивирус «Kaspersky Endpoint Security 10» SP 2 (версия 10.3.0.6294) для рабочих станций пользователей РАБИС-НП и АС ЭКР 2.0 под управлением ОС Windows 7 SP1 RUS.

| **Раздел** | **Параметр (группа параметров)** | | | | | | **Значение  параметра** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Контроль рабочего места | Контроль активности программ  (Заблокировать изменение параметра - З) | | | | | | Выключен |
| Антивирусная защита - основные параметры защиты | Основные параметры | Запускать Kaspersky Endpoint Security 10 для Windows при включении компьютера | | | | | √ |
| Применять технологию лечения активного заражения | | | | | √ |
| Объекты для обнаружения (З) | Объекты для обнаружения (Настройка) | | | Вредоносные  программы | | √ Вирусы, черви |
| √ Троянские программы |
| √ Вредоносные утилиты |
| Реклама, автодозвон, другие программы | | √ Рекламные программы |
| √ Программы автодозвона |
| √ Другие |
| Упаковщики | | √ Упакованные файлы, которые могут нанести вред |
| √ Многократно упакованные файлы |
| Исключения и доверенная зона (З)[[18]](#footnote-19) | Доверенная зона | | | | | Рекомендуется исключить из проверки компонентом "Файловый антивирус":  1) каталоги с ПО СЗИ от НСД. Например, для Secret Net (включая подкаталоги):  C:\Program Files\Infosec\\*.\*;  C:\Program Files\Secret Net\\*.\*;  2) файлы агента ОС Windows ЕСМИБ ТУ:  c:\Windows\AGENT\mailaudt.la;  3) файлы облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\ Agents\\*\Data\mailaudt.la;  4) каталог агентской платформы ЕСМИБ ТУ (включая вложенные подкаталоги):  c:\Program Files (x86)\Crystall\Misc \AgentPlatform\\*.\*.  Рекомендуется добавить в перечень доверенных программ:  1) процессы агента ОС Windows ЕСМИБ ТУ:  c:\Windows\AGENT\sthl.exe;  c:\Windows\AGENT\dskappl.dll;  c:\Windows\AGENT\>\explorer.exe  c:\Windows\AGENT \sthl.dll;  2) процесс облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\liteagent.exe**;**  3) процесс агентской платформы:  C:\Program Files(x86)\Crystall\Misc\ AgentPlatform\AgentPlatform.exe |
| Контролируемые порты (З) | Контролировать только  выбранные порты | | | | | Список портов формируется автоматически:  √ SMTP(25)  √ HTTP(80,81,82,83)  √ POP3(110)  √ IRC(113)  √ NNTP(119)  √ IMAP(143)  √ IRC(194)  √ HTTPS(443)  √ SMTP SSL(465)  √ NNTP SSL(563)  √ IMAP SSL (993)  √ POP3 SSL(995)  √HTTP(1080,3128,7900,8000,8080, 8088,8888,11523),  √ TCP (135, 139),  √ UDP (137, 138). |
| Антивирусная защита -Файловый  антивирус | Файловый антивирус (З) | | | | | | √ |
| Уровень  безопасности (З) | | Общие | | | Типы файлов | Все файлы |
| Область  защиты | Все съемные диски |
| Все жесткие диски |
| Производительность | | | Методы  проверки | √ Сигнатурный,  √ Эвристический анализ  (поверхностный) |
| Оптимизация проверки | √ Проверять только новые и измененные файлы |
| Проверка  составных  файлов | √ Проверять архивы,  √ Проверять установочные пакеты,  √ Проверять файлы офисных форматов |
| Производительность  (Дополнительно) | | | Составные файлы  (Фоновая  проверка) | √ Распаковывать составные файлы в фоновом режиме;  Минимальный размер файла:  0 Мб |
| Составные файлы  (Ограничение по размеру) | Не распаковывать составные файлы большого размера - Выключен; |
| Дополнительно | | | Режим проверки | Интеллектуальный |
| Технологии  проверки | √ Технология iSwift |
| √ Технология iChecker |
| Действие при обнаружении угрозы (З) | | Выполнять действие: | | | | √ Лечить |
| √ Удалять, если лечение невозможно[[19]](#footnote-20) |
| Антивирусная защита - Почтовый Антивирус | Почтовый Антивирус (З) | | | | | | Выключен |
| Антивирусная защита – Веб-Антивирус | Веб-Антивирус (З) | | | | | | Выключен |
| Антивирусная защита – IM-Антивирус | IM-Антивирус (З) | | | | | | Выключен |
| Антивирусная защита - Сетевой экран | Сетевой экран (З) | | | | | | Выключен |
| Антивирусная защита – Защита от сетевых атак | Защита от сетевых атак (З) | | | | | | Выключен |
| Мониторинг системы | Мониторинг системы (З) | | | | | | Включен[[20]](#footnote-21) |
| Общие параметры (З) | | | Включить защиту от  эксплойтов | | | √ |
| Режим работы (З) | | | Не контролировать активность программ, имеющих цифровую подпись | | | √ |
| Действие при обнаружении угрозы (З) | | | При обнаружении вредоносной активности программы: Выбирать действие автоматически | | | √ |
| Откат действий вредоносных программ (З) | | | Выполнять откат действий вредоносных программ при лечении | | | √ |
| Дополнительные параметры -Параметры программы | Параметры самозащиты (З) | | | Включить самозащиту | | | √ |
| Выключить внешнее управление системной службой | | | √ |
| Режимы работы (З)  (Настройка) | | | Откладывать задачи по расписанию при работе от аккумулятора | | | √ |
| Уступать ресурсы другим программам | | | √ |
| Разрешить использование локальных задач | | | Выключен |
| Разрешить отображение групповых задач | | | Включен |
| Разрешить управление групповыми задачами | | | Выключен |
| Использовать KSC в качестве прокси-сервера для активации | | | Выключен |
| Включить запись дампов | | | Выключен |
| Отсылать файлы дампов и файлы трассировки в «Лабораторию Касперского» | | | Выключен |
| Включить защиту файлов дампов и файлов трассировки | | | Выключен |
| Параметры прокси-сервера (Настройка) | | | Использовать прокси-сервер | | | Выключен |
| Защита паролем (З) | | | Включить защиту паролем | | | √  Через кнопку "Настройка" задать пароль[[21]](#footnote-22) |
| Фоновая проверка (3) | | | Выполнять проверку во время простоя компьютера | | | Выключен |
| Проверка съемных дисков при подключении (З) | | | Действие при подключении съемного диска | | | Быстрая проверка |
| Максимальный размер съемного диска | | | Не определено |
| Дополнительные параметры -Отчеты и хранилища | Параметры отчетов (З) | | | Хранить отчеты не более | | | √  90 дней |
| Максимальный размер файла | | | 100 Мб |
| Параметры карантина и резервного  хранилища (З) | | | Проверять файлы на карантине после обновления | | | √ |
| Хранить объекты не более | | | √  90 дней |
| Максимальный размер хранилища | | | 100 Мб |
| Уведомления | | | Обнаружен вредоносный объект | | | √ |
| Обнаружен возможно зараженный объект | | | √ |
| Лечение невозможно | | | √ |
| Невозможно удалить объект | | | √ |
| Ошибка обработки | | | √ |
| Невозможно поместить объект на карантин | | | √ |
| Объект удален | | | √ |
| Уведомление о состоянии локальных антивирусных баз | | | Отправить уведомление "Базы устарели", если обновление баз не выполнялось | | | 3 дня |
| Отправить уведомление "Базы сильно устарели", если обновление баз не выполнялось | | | 7 дней |
| Параметры KSN | Параметры KSN | | | Принимаю условия Положения и участвую в KSN | | | Выключен |
| Дополнительные параметры -Интерфейс | Взаимодействие с пользователем (З) | | | Отображать интерфейс программы | | | Выключен[[22]](#footnote-23) |
| Предупреждения | | | Наличие необработанных файлов | | | Включен |
| Необходимость перезагрузки компьютера | | | Включен |
| Проблемы с антивирусными базами | | | Включен |
| Проблемы с уровнем защиты | | | Включен |
| Проблемы с лицензией | | | Включен |
| Наличие обновлений | | | Включен |
| Поддержка пользователей  (Настройка) | | | Информация о поддержке | | |  |
| |KATA Endpoint Sensor | Выключен | | | | | | |

### Параметры настройки задач СЗ от ВВК Kaspersky Security Center 10.4.343

Таблица 8 Параметры задачи поиска вирусов

| **Раздел** | **Параметр (группа параметров)** | | | **Значение параметра** |
| --- | --- | --- | --- | --- |
| Уведомление | √ На Сервере администрирования в течение (дней) | | | 90 |
| В журнале событий ОС на клиентском компьютере | | | √ |
| В журнале событий ОС на Сервере администрирования | | | √ |
| Сохранять все события | | | + |
| Расписание[[23]](#footnote-24) | Запуск по расписанию | | | Еженедельно |
| Каждый | | | День недели ТУ определяет самостоятельно |
| Время запуска | | | Время запуска ТУ определяет самостоятельно |
| Запускать пропущенные задачи | | | √ |
| Распределять запуск задачи случайным образом в интервале (мин.) | | | 5 |
| +Параметры | Уровень  безопасности | Область  действия | Типы файлов | Все файлы |
| Проверка  составных  файлов | √ Проверять все архивы |
| √ Проверять все установочные пакеты |
| √ Проверять все вложенные OLE-объекты |
| Дополнительно | Методы  проверки | √ Эвристический анализ (глубокий) |
| Технологии  проверки | √ Технологий iSwift |
| √ Технология iChecker |
| Область проверки (Настройка) | Область проверки | | √ Системная память,  √ Объекты автозапуска,  √ Загрузочные секторы,  √ Системное резервное хранилище,  √ Все съемные диски,  √ Все жесткие диски  (√ включая вложенные папки) |
| Действие при обнаружении угрозы | Выполнять действие: Лечить. Удалять, если лечение невозможно | | |
| Лечить | | √ |
| Удалять, если лечение невозможно | | √[[24]](#footnote-25) |
| Учетная запись | Автоматически созданная учетная запись | | | + |

Таблица 9 Параметры настройки задачи обновления сигнатурных баз

| **Наименование параметра** | **Значение параметра** | | | |
| --- | --- | --- | --- | --- |
| Общие | | | | |
| Наименование | | Задача обновления | | |
| Уведомления | | | | |
| Сохранять  информацию о результатах | На сервере администрирования в течение (дней): | | | 90 |
| Сохранять все события | | | + |
| Расписание | | | | |
| Запуск по  расписанию | При загрузке обновлений в хранилище | | | |
| Запускать пропущенные задачи | | | + |
| Автоматически определять интервал для распределения запуска задачи | | | + |
| Параметры обновления баз и модулей программы | | | | |
| Параметры обновления в локальном  режиме | | Источник обновлений | Kaspersky Security Center 10.х | + |
| Региональные параметры | Определять автоматически |
| Загружать обновления модулей программы – Устанавливать критические и одобренные обновления[[25]](#footnote-26) | | + |
| Учетная запись | | | | |
| Автоматически созданная учетная запись | | | | + |

Таблица 10 Параметры настройки задачи "Загрузка обновлений в хранилище"[[26]](#footnote-27)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Раздел** | **Значение параметра** | | | | | |
| Уведомление | Сохранять информацию о результатах | | На сервере администрирования в течение (дней): | | | 90 |
| Сохранять все события | | | + |
| Расписание | Запуск по расписанию | | | | Ежедневно | |
| Каждый | | | | 1 день | |
| Время запуска | | | | Время запуска ТУ определяет самостоятельно | |
| Запускать пропущенные задачи | | | | + | |
| Параметры | Источник  обновлений | Локальная или  сетевая папка | | Указать источник в соответствии с принятым в ТУ порядком | | |
| Состав  обновлений | Определять состав загружаемых обновлений автоматически | | | | + |
| Прочие  параметры | Обновлять модули Серверов администрирования | | | | + |
| Обновлять модули Агентов администрирования | | | | + |
| Учетная запись | Автоматически созданная учетная запись | | | | | + |

Таблица 11 Параметры настройки политики Агента администрирования[[27]](#footnote-28).

| **Раздел  политики** | **Параметр (группа параметров)** | | **Значение  параметра** |
| --- | --- | --- | --- |
| Параметры | Скачивать обновления только через агенты обновлений (З) | | √ |
| Максимальный размер очереди событий (МБ): (З) | | 2 |
| Использовать пароль деинсталляции | | √[[28]](#footnote-29) |
| Хранилища | Информация об установленных программах (З) | | √ |
| Информация об обновлениях MS Windows (З) | | √ |
| Информация об уязвимостях ПО (З) | | √ |
| Информация о реестре оборудования (З) | | √ |
| Управление перезагрузкой | Не перезагружать ОС | | + |
| Общий доступ к РС | Включить аудит | | Выключен |
| Сеть | Подключение к Серверу администрирования (З) | Период синхронизации (мин.) | 15 |
| Сжимать сетевой трафик | √ |
| Использовать  SSL-соединение | √ |
| Использовать UDP-порт (З) | | √ |
| Номер UDP-порта | | 15000 |
| Сеть-Менеджер соединений | Подключаться при необходимости | | + |

### Настройка средства защиты от воздействий вредоносного кода «Dr Web Enterprise Security Suite» (версия 10.01.0)

С использованием расширения Центр управления безопасности Dr.Web Enterprise Security Suite (далее – Dr.Web ESS) в разделе "Администрирование" выполнить настройки сервера средств защиты от воздействия вредоносного кода Dr.Web Security Server в соответствии с таблицами (Таблица 12 – Таблица 15):

Таблица 12 Параметры настройки «Репозиторий - Общая конфигурация репозитория»

|  |  |  |
| --- | --- | --- |
| **Группа параметров** | **Параметр** | **Значение параметра** |
| ВСО Dr.Web | Базовый URI | Настраивается в соответствии с принятым в ТУ порядком обновления сигнатурных баз. |
| Использовать CDN |  |
| Использовать SSL |  |
| Список серверов Всемирной системы обновления Dr.Web | Настраивается в соответствии с принятым в ТУ порядком обновления сигнатурных баз. |
| **F** Агент Dr.Web для Windows**tyА** | Обновлять только вирусные базы | Включено |
| Агент Dr.Web для UNIX |  |  |
| **С** Сервер Dr.Web **е** | Windows NT x64 (AMD/EM64T) | Включить для соответствующей серверной платформы (x64 или x86). |
| Windows NT x86 (32bit) |
| Новости компании Dr.Web | Русский | √ |
| Языки Агента Dr.Web для Windows | English | √ |
| Русский | √ |

Таблица 13 Параметры настройки «Конфигурация - Конфигурация Сервера Dr.Web»

| **Группа параметров** | | **Параметр** | | **Значение параметра** |
| --- | --- | --- | --- | --- |
| Общие | | Название Сервера Dr.Web | | Внутреннее наименование сервера |
| Язык Сервера | | Русский |
| Количество параллельных запросов от клиентов | | 5 |
| Ограничить трафик обновлений | |  |
| Режим регистрации новичков | | Подтверждать доступ вручную |
| Первичная группа по умолчанию | | Everyone |
| Переводить неавторизованных новичков | | √ |
| Допустимая разница между временем Сервера и Агента | | 3 (минуты) |
| Заменять IP-адреса | |  |
| Заменять NetBIOS-имена | |  |
| Синхронизировать описания станций | | √ |
| Синхронизировать географическое положение | | √ |
| Стартовая синхронизация | | 0 |
| Сеть | DNS | Тайм-аут для DNS-запросов (c) | | 5 |
| Количество повторных DNS-запросов | | 3 |
| Задать время хранения ответов от DNS-сервера | Для положительных ответов (мин.) |  |
| Для отрицательных ответов (мин.) |  |
| Серверы DNS | |  |
| Домены DNS | |  |
| Прокси | Использовать прокси-сервер | | Настраивается в соответствии с принятым в ТУ порядком |
| Транспорт | Шифрование | | Возможно |
| Сжатие | | Возможно |
| Уровень сжатия | | 8(оптимальный) |
| Адрес | | IP адрес сервера Dr.Web |
| Порт | | 2193 |
| Обнаружение | | √ |
| Multicasting | | √ |
| Multicast-группа | |  |
| Название | |  |
| Кластер |  | |  |
| Загрузка | Адрес сервера Dr.Web | | NetBIOS-имя сервера |
| Порт | | 2193 |
| Групповые обновления | Включить групповые обновления | |  |
| Статистика | | Состояние карантина | | √ |
| Состав оборудования и программ | | √ |
| Список модулей станций | | √ |
| Список установленных компонентов | | √ |
| Сессии пользователей станций | | √ |
| Запуск/Завершение компонентов | | √ |
| Обнаруженные угрозы безопасности | | √ |
| Отслеживание эпидемии | Период (с) | 300 |
| Количество сообщений | 100 |
| Отправлять статистику в компанию «Доктор Веб» | |  |
| Ошибки сканирования | | √ |
| Статистика сканирования | | √ |
| Инсталляции Агентов | | √ |
| Журнал выполнения заданий на станции | | √ |
| Состояние станций | | √ |
| Состояние вирусных баз | | √ |
| Безопасность | | Аудит операций администратора | | √ |
|  | | Аудит внутренних операций сервера | | √ |
|  | | Аудит операций Web API | | √ |
| Кэш | | Период очистки кэша (час) | | 1 |
|  | | Файлы в карантине (нед.) | | 1 |
|  | | Инсталляционные пакеты (нед.) | | 1 |
|  | | Файлы репозитория (с) | | 90 |
| База данных[[29]](#footnote-30) | | Количество соединений с БД | | 2 |
| База данных | | ODBC |
| Имя DSN | | Имя источника данных ODBC |
| Имя пользователя | | Регистрационное имя пользователя БД |
| Пароль | | Пароль пользователя БД |
| Еще раз пароль | | Пароль пользователя БД |
| Уровень изоляции транзакций | | По умолчанию |
| Модули | | Расширение Центра управления безопасностью Dr.Web | | √ |
| Расширение Dr.Web Server FrontDoor | |  |
| Протокол Агента Dr.Web | | √ |
| Протокол Microsoft NAP Health Validator | | √ |
| Протокол инсталлятора Агента Dr.Web | | √ |
| Протокол кластера серверов Dr.Web | |  |
| Протокол сервера Dr.Web | | √[[30]](#footnote-31) |
| Расположение | | Организация | |  |
| Подразделение | |  |
| Страна или регион | |  |
| Область | |  |
| Город | |  |
| Улица | |  |
| Этаж | |  |
| Помещение | |  |
| Широта | |  |
| Долгота | |  |
| Лицензии | | Срок действия выдаваемых лицензий (час.) | | 24 |
| Период для продления получаемых лицензий (час.) | | 1 |
| Период синхронизации лицензий (час.) | | 24 |

Таблица 14 Параметры настройки «Администрирование → Конфигурация оповещений»

| **Группа параметров / Параметр** | | **Значение параметра** |
| --- | --- | --- |
| Метод отправки оповещений | | Веб-консоль |
| Администраторы | Неизвестный администратор | √ |
| Ошибка авторизации администратора | √ |
| Другое | Ошибка записи журнала | √ |
| Ошибка ротации журнала | √ |
| Периодический отчет | √ |
| Соседний сервер давно не подключался | √ |
| Тестовое сообщение | √ |
| Эпидемия | √ |
| Новичок | Ожидание подтверждения | √ |
| Станция отклонена автоматически | √ |
| Станция отклонена админстратором | √ |
| Ограничение лицензии | Истек срок выдачи лицензий | √ |
| Количество станций приближается к максимально допустимому | √ |
| Окончание срока действия агентского ключа | √ |
| Превышено допустимое количество лицензий | √ |
| Превышено допустимое количество станций | √ |
| Превышено допустимое количество станций в базе данных | √ |
| Репозиторий | Актуальное состояние продукта | √ |
| Запущено обновление репозитория | √ |
| Мало свободного места на диске | √ |
| Ошибка обновления продукта | √ |
| Продукт заморожен из-за ошибки обновления | √ |
| Продукт обновлен | √ |
| Станция | Неизвестная станция | √ |
| Необходима перезагрузка станции | √ |
| Обнаружена инфекция | √ |
| Обрыв соединения | √ |
| Ошибка авторизации станции | √ |
| Ошибка в процессе сканирования |  |
| Ошибка обновления станции | √ |
| Ошибка создания учетной записи станции | √ |
| Станция давно не подключалась к серверу | √ |
| Станция допущена | √ |
| Станция допущена автоматически | √ |
| Станция уже зарегистрирована | √ |
| Статистика сканирования |  |
| Установка | Установка выполнена успешно | √ |
| Установка не выполнена | √ |
| Метод отправки оповещений | | Веб-консоль |
| Количество повторных отправок | | 10 |
| Тайм-аут повторной отправки | | 300 |
| Время хранения оповещения (дней) | | 10 |
| Администраторы | Неизвестный администратор | √ |
| Ошибка авторизации администратора | √ |
| Другое | Ошибка записи журнала Сервера | √ |
| Ошибка ротации журнала Сервера | √ |
| Соседний сервер давно не подключался | √ |
| Статистический отчет | √ |
| Тестовое сообщение | √ |
| Эпидемия в сети | √ |
| Лицензии | Достигнуто ограничение по переданным лицензиям | √ |
| Достигнуто ограничение по станциям в сети | √ |
| Истек срок передачи лицензий | √ |
| Лицензионный ключ автоматически обновлен |  |
| Лицензионный ключ не может быть автоматически обновлен |  |
| Окончание срока действия лицензионного ключа | √ |
| Превышено ограничение по станциям в группе | √ |
| Приближается ограничение по станциям в группе | √ |
| Новички | Станция ожидает подтверждения | √ |
| Станция отклонена автоматически | √ |
| Станция отклонена администратором | √ |
| Репозиторий | Актуальное состояние продукта в репозитории | √ |
| Запущено обновление продукта в репозитории | √ |
| Недостаточно свободного места на диске | √ |
| Обновление продукта в репозитории заморожено | √ |
| Ошибка обновления продукта в репозитории | √ |
| Продукт в репозитории обновлен | √ |
| Станции | Аварийный разрыв соединения | √ |
| Критическая ошибка обновления станции | √ |
| Неизвестная станция | √ |
| Обнаружена угроза безопасности | √ |
| Ошибка авторизации станции | √ |
| Ошибка сканирования |  |
| Ошибка создания учетной записи станции | √ |
| Станция давно не подключалась к Серверу | √ |
| Станция подтверждена автоматически | √ |
| Станция подтверждена администратором | √ |
| Станция уже зарегистрирована | √ |
| Статистика сканирования | √ |
| Требуется перезагрузка станции | √ |
| Установки | Установка на станции не выполнена | √ |
| Установка на станции успешно завершена | √ |

Таблица 15 Параметры настройки «Конфигурация → Планировщика заданий Сервера Dr.Web»

| **Группа параметров** | | **Параметр** | **Значение параметра** |
| --- | --- | --- | --- |
| Резервное копирование критичных данных сервера (Backup sensitive date) | Общие | Название | Резервное копирование критичных данных сервера (Backup sensitive date) |
| Разрешить выполнение | √ |
| Критическое задание | √ |
| Действие | Действие | Резервное копирование критичных данных сервера |
| Путь | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком |
| Максимальное количество копий |
| Время | Периодичность |
| Запретить после первого выполнения |
| Время |
| Очистка неотправленных событий (Purge unsent IS events) | Общие | Название | Очистка неотправленных событий (Purge unsent IS events) |
| Разрешить выполнение | √ |
| Критическое задание |  |
| Действие | Действие | Очистка неотправленных событий |
| Часов | 12 |
| Время | Периодичность | Ежедневно |
| Запретить после первого выполнения | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком |
| Минута |
| Очистка старых записей (Purge old data) | Общие | Название | Очистка старых записей (Purge old data) |
| Разрешить выполнение | √ |
| Критическое задание |  |
| Действие | Действие | Очистка старых записей |
| Данные соседних серверов | 90 |
| События, неотправленные родительским серверам | 90 |
| События, полученные от подчиненных серверов | 90 |
| Журнал выполнения заданий Сервером | 90 |
| Журнал выполнения заданий станциями | 90 |
| Журнал аудита | 90 |
| Журнал карантина | 90 |
| Удаленные станции | 90 |
| Состояния станций | 90 |
| Инсталляции Агентов | 90 |
| Статистика сканирования | 90 |
| Инфекции | 90 |
| Ошибки сканирования | 90 |
| Запуск/Завершение компонентов | 90 |
| Обмен ключами | 90 |
| Временные таблицы | 1 |
| Время | Периодичность | Ежедневно |
| Запретить после первого выполнения | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком |
| Время |
| Обновление репозитория: вирусные базы | Общие | Название | Обновление репозитория: вирусные базы |
| Разрешить выполнение | √ |
| Критическое задание | √ |
| Действие | Действие | Обновление репозитория |
| Продукт | √ Вирусные базы Dr.Web |
| Время | Периодичность | Ежедневно |
| Запретить после первого выполнения | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком |
| Время |
| Обновление репозитория: программная часть | Общие | Название | Обновление репозитория: программная часть |
| Разрешить выполнение | √ |
| Критическое задание | √ |
| Действие | Действие | Обновление репозитория |
| Продукт | √ Вирусные базы Dr.Web |
| √ Модуль обновления Dr.Web |
| √ Агент Dr.Web для Windows |
| √ Сервер DDDr.Web |
| Время | Периодичность | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком. |
| Запретить после первого выполнения |
| Время |
|  |  |  |  |

Для централизованного распространения настроек СЗ от ВВК на сервере СЗ от ВВК Dr.Web необходимо:

1. В оснастке Центр управления безопасности Dr.Web ESS в разделе «Антивирусная сеть» создать группу, в которой будут размещены серверы платежной системы, оснащенные ПО СЗ от ВВК Dr.Web.
2. Для созданной группы выполнить настройки в соответствии с таблицами (Таблица 16 – Таблица 19):

Таблица 16. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Права»

|  |  |  |  |
| --- | --- | --- | --- |
| **Группа параметров** | | **Параметр** | **Значение параметра** |
| Windows | Компоненты | Запуск Сканера | √ |
| Изменение конфигурации Сканера |  |
| Запуск SpIDer Guard для рабочих станций |  |
| Изменение конфигурации SpIDer Guard для рабочих станций |  |
| Останов SpIDer Guard для рабочих станций |  |
| Запуск SpIDer Guard для серверов |  |
| Изменение конфигурации SpIDer Guard для серверов | √ |
| Останов SpIDer Guard для серверов |  |
| Запуск SpIDer Gate |  |
| Изменение конфигурации SpIDer Gate |  |
| Останов SpIDer Gate |  |
| Запуск SpIDer Mail |  |
| Изменение конфигурации SpIDer Mail |  |
| Останов SpIDer Mail |  |
| Запуск Офисного контроля Dr.Web |  |
| Изменение конфигурации Офисного контроля Dr.Web |  |
| Останов Офисного контроля Dr.Web |  |
| Запуск Dr.Web для Microsoft Outlook |  |
| Изменение конфигурации Dr.Web для Microsoft Outlook |  |
| Запуск превентивной защиты | √ |
| Изменение конфигурации превентивной защиты |  |
| Останов превентивной защиты |  |
| Общие | Запуск в мобильном режиме |  |
| Изменение режима работы |  |
| Изменение конфигурации Агента Dr.Web |  |
| Отключение самозащиты |  |
| Деинсталляция Агента Dr.Web |  |

Таблица 17. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Планировщик заданий»

|  |  |  |  |
| --- | --- | --- | --- |
| **Группа параметров\Параметр** | | | **Значение  параметра** |
| Общие | Название | | Еженедельное сканирование |
| Разрешить выполнение | | √ |
| Критическое задание | | √ |
| Действие | Действие | | Сканер Dr.Web. Полное сканирование |
| Действия | Инфицированные | Лечить |
| Подозрительные | Перемещать в карантин |
| Неизлечимые | Перемещать в карантин |
| Инфицированные инсталляционные пакеты | Перемещать в карантин |
| Инфицированные архивы | Перемещать в карантин |
| Инфицированные почтовые файлы | Перемещать в карантин |
| Инфицированные загрузочные секторы | Лечить |
| Рекламные программы | Перемещать в карантин |
| Программы дозвона | Перемещать в карантин |
| Программы-шутки | Перемещать в карантин |
| Потенциально опасные | Перемещать в карантин |
| Программы взлома | Перемещать в карантин |
| Приоритет сканирования | Обычный |
| Уровень загрузки ресурсов компьютера | Оптимальный (рекомендуется) |
| Действия после сканирования | ничего не делать |
| Перезагружать компьютер автоматически |  |
| Ограничения | Максимальное время сканирования (мс) | 0 |
| Максимальный уровень вложенности в архив | 5 |
| Максимальный размер архива (КБ) | 0 |
| Максимальный коэффициент сжатия архива | 1000 |
| Максимальный размер распакованного объекта (КБ) | 524288 |
| Порог проверки уровня сжатия (КБ) | 1024 |
| Время | Периодичность | | Еженедельно |
| Запретить после первого выполнения | | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком |
| Запускать задание по UTC | |
| День | |
| Время | |
|  | Действия |  |  |
|  | Действия |  |  |
|  | Действия |  |  |
|  | Действия |  |  |
|  | Действия |  |  |

Таблица 18. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Устанавливаемые компоненты»

| **Параметр** | **Значение параметра** |
| --- | --- |
| Агент Dr.Web для Windows | Должен быть установлен (по умолчанию) |
| Сканер Dr.Web | Должен быть установлен (по умолчанию) |
| Сканер Dr.Web для Windows | Должен быть установлен |
| SpIDer Guard для рабочих станций Windows | Не может быть установлен |
| SpIDer Guard для серверов Windows | Должен быть установлен |
| SpIDer Mail для Windows | Не может быть установлен |
| SpIDer Gate для рабочих станций Windows | Не может быть установлен |
| Офисный контроль Dr.Web | Не может быть установлен |
| Dr.Web для Microsoft Outlook | Не может быть установлен |
| Антиспам Dr.Web | Не может быть установлен |
| Брандмауэр Dr.Web | Не может быть установлен |

Таблица 19. Параметры настройки «Антивирусная сеть → Группа «Наименование группы» → Windows»

| **Компонент** | **Группа параметров** | **Параметр** | **Значение** |
| --- | --- | --- | --- |
| Сканер | Общие | Проигрывать звуки |  |
| Автоматически применять действия к угрозам | √ |
| Прерывать проверку при переходе на питание от аккумулятора |  |
| Уровень загрузки ресурсов компьютера | Оптимальный (рекомендуется) |
| Действия | Инфицированные | Лечить |
| Подозрительные | Перемещать в карантин |
| Неизлечимые | Перемещать в карантин |
| Инфицированные инсталляционные пакеты | Перемещать в карантин |
| Инфицированные архивы | Перемещать в карантин |
| Инфицированные почтовые файлы | Перемещать в карантин |
| Рекламные программы | Перемещать в карантин |
| Программы дозвона | Перемещать в карантин |
| Программы-шутки | Перемещать в карантин |
| Потенциально опасные | Перемещать в карантин |
| Программы взлома | Перемещать в карантин |
| Действие, когда необходима перезагрузка | Предлагать перезагрузку |
| Исключения | Исключаемые пути и файлы [[31]](#footnote-32) | Исключаемые пути и файлы:  каталог агентской платформы ЕСМИБ ТУ (включая вложенные подкаталоги):  1) файлы агентской платформы:  c:\Program Files (x86)\Crystall\Misc\ AgentPlatform\\*.\*;  2) файлы облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\Data \mailaudit.la |
| Проверять содержимое следующих файлов | √ Архивы |
| √ Почтовые файлы |
| √ Инсталляционные пакеты |
| Журнал | Вести подробный журнал |  |
| SplDer Guard для серверов | Общие | Режим проверки | Оптимальный |
| Использовать эвристический анализ | √ |
| Проверять на наличие руткитов | √ |
| Проверять загружаемые программы и модули | √ |
| Проверять инсталляционные пакеты | √ |
| Проверять объекты в локальной сети |  |
| Проверять объекты на съемных носителях | √ |
| Проверять архивы |  |
| Проверять почтовые файлы |  |
| Блокировать автозапуск со сменных носителей | √ |
| Действия | Инфицированные | Лечить |
| Подозрительные | Перемещать в карантин |
| Неизлечимые | Перемещать в карантин |
| Инфицированные инсталляционные пакеты | Перемещать в карантин |
| Инфицированные архивы | Перемещать в карантин |
| Инфицированные почтовые файлы | Перемещать в карантин |
| Рекламные программы | Перемещать в карантин |
| Программы дозвона | Перемещать в карантин |
| Программы-шутки | Перемещать в карантин |
| Потенциально опасные | Перемещать в карантин |
| Программы взлома | Перемещать в карантин |
| Исключения | Исключать из сканирования системные файлы | √ |
| Исключать файлы БД Prefetcher | √ |
| Исключать файлы БД Windows поиска | √ |
| Исключаемые пути и файлы[[32]](#footnote-33) | C:\Program Files\Infosec\\*.\*;  C:\Program Files\Secret Net\\*.\*,  C:\Rabis-np\kernel\srvany.exe,  каталог агентской платформы ЕСМИБ ТУ (включая вложенные подкаталоги):  c:\Program Files (x86)\Crystall\Misc\ AgentPlatform\\*.\*,  файлы облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\Data \mailaudit.l |
| Исключения | Исключаемые процессы | \\SERVER\RABIS-NP\kernel\load.exe, \\SERVER\RABIS-NP\kernel\task992.ovl,  процесс облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\ liteagent.exe;  процесс агентской платформы:  C:\Program Files(x86)\Crystall\Misc\AgentPlatform\ AgentPlatform.exe |
| Журнал | Вести подробный журнал |  |
| Агент Dr.Web | Общие | Задержка запуска Планировщика заданий (мин.) | 1 |
| Периодичность отправки статистики (мин.) | 360 |
| Язык | Русский |
| Включить Microsoft Network Access Protection |  |
| Разрешить удаленное управление карантином | √ |
| Собирать информацию о станциях: Период сбора информации о станциях (мин.) |  |
| Синхронизировать время |  |
| Запрещать изменение даты и времени системы |  |
| Запрещать эмуляцию действий пользователя |  |
| Включить поддержку аппаратной виртуализации |  |
| Сеть | Открытый ключ | Генерируется во время установки сервера |
| Разрешить работу без открытого ключа |  |
| Разрешить работу при неверном открытом ключе |  |
| Сервер |  |
| Количество повторений поиска | 3 |
| Тайм-аут поиска (сек.) | 5 |
| Режим сжатия | Возможно |
| Режим шифрования | Возможно |
| Параметры прослушивания сети | udp/:2193 |
| Мобильность | Периодичность обновления | 30 минут |
| Использовать прокси-сервер | Настраивается эксплуатирующим подразделением в соответствии с принятым в ТУ порядком |
| Журнал | Уровень детализации журнала Агента | Трассировка |
| Уровень детализации журнала движка | Ошибка |
| Уровень детализации журнала обновлений | Информация |
| Дополнительно: Создавать дампы памяти при ошибках проверки |  |
| Интерфейс | Отображать значок на панели задач |  |
| Отображать запрос на перезагрузку при обновлении компонентов | √ |
| Критические оповещения | √ |
| Оповещения об угрозах | √ |
| Важные оповещения | √ |
| Малозначительные оповещения |  |
| Дополнительно: Не показывать уведомления в полноэкранном режиме | √ |
| Дополнительно: Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме | √ |
| Превентивная защита | Защита от эксплойтов | | Блокировать использование неавторизованного кода |
| Уровень блокировки подозрительных действий | | Оптимальный |
| Целостность запущенных приложений | | Запрещать |
| Целостность файлов пользователей | | Запрещать |
| HOSTS файл | | Запрещать |
| Низкоуровневый доступ к диску | | Запрещать |
| Загрузка драйверов | | Разрешать |
| Image File Execution Options | | Разрешать |
| User Drivers | | Разрешать |
| Параметры оболочки Winlogon | | Запрещать |
| Нотификаторы Winlogon | | Разрешать |
| Автозапуск оболочки Windows | | Запрещать |
| Ассоциации исполняемых файлов | | Запрещать |
| Политики ограничения запуска программ (SRP) | | Запрещать[[33]](#footnote-34) |
| Плагины Internet Explorer (BHO) | | Разрешать |
| Автозапуск программ | | Разрешать |
| Автозапуск политик | | Разрешать |
| Конфигурация безопасного режима | | Запрещать |
| Параметры Session Manager | | Запрещать |
| Системные службы | | Разрешать |

Таблица 20. Рекомендуемые к применению на сервере приложений АС ЭКР 2.0 настройки исключений компоненты "SplDer Guard для серверов" ПО СЗ от ВВК "Dr.Web 10"

|  |  |
| --- | --- |
| **Параметр** | **Значение параметра** |
| Исключаемые пути | C:\mq\_deb.log  C:\windows\shadow\cache\cache\*.dat  C:\windows\security\templates\policies\tmpgptfl.inf  C:\windows\security\templates\policies\gpt\*.dom  C:\windows\security\logs\\*.log  C:\windows\security\database\secedit.sdb  C:\windows\system32\wbem\logs\framework.log  C:\windows\temp\stderr\_\*.txt  C:\pasportclient\spclient.log  C:\usr\ov\data\tmp\opc\proc\*.\*  C:\usr\ov\data\tmp\opc\moa3  C:\usr\ov\data\tmp\opc\moa4  C:\usr\ov\data\wasspi\wbs\log\errorlog  C:\usr\ov\data\wasspi\wbs\log\config.log  C:\usr\ov\data\wasspi\wbs\datalog\tempgraph.spi.dat  C:\asekr\home\asekrsd\workspace\.metadata\.log |
| Исключаемые процессы | C:\program files\ibm\websphere\appserver\java\bin\java.exe  C:\program files\ibm\websphere mq\bin\amqzmuc0.exe  C:\program files\ibm\websphere mq\bin\amqzlaa0.exe  C:\program files\ibm\websphere mq\bin\amqrrmfa.exe  C:\program files\ibm\websphere mq\bin\amqzmur0.exe  C:\program files\ibm\websphere mq\bin\amqzmgr0.exe  C:\program files\ibm\websphere mq\bin\amqzxma0.exe  C:\program files\ibm\websphere mq\bin\amqfqpub.exe  C:\program files\ibm\websphere mq\bin\amqmtbrn.exe  C:\program files\ibm\websphere mq\bin\mqexplorer.exe  C:\program files\ibm\websphere mq\bin\amqzfuma.exe  C:\program files\ibm\websphere mq\bin\amqzmuf0.exe  C:\program files\ibm\websphere mq\bin\amqfcxba.exe  C:\program files\ibm\websphere mq\bin\amqzlsa0.exe  C:\program files\ibm\websphere mq\bin\amqsvc.exe C:\program files\ibm\websphere mq\bin\runmqchi.exe  C:\program files\ibm\websphere mq\bin\strmqm.exe C:\ism\asekr\_spi2\ism\_spi2.exe  C:\ism\mqs\_conf\ism\_mqs\_conf.exe  C:\ism\mqs\_mon\ism\_mqs\_mon.exe  C:\usr\ov\lbin\eaagt\opcacta.exe  C:\usr\ov\data\bin\instru~1\itoprocs.exe  C:\program files\crystall\zobserver\asekr\liteagent.exe  C:\program files\crystall\zobserver\agents\evtlog\liteagent.exe  C:\Program Files\Crystall\ZObserver\Agents\\*\Data\mailaudit.la  C:\Program Files\Crystall\AgentPlatform\AgentPlatform.exe |

Таблица 21. Рекомендуемые к применению на сервере ЕСМИБ ТУ настройки исключений компонент "Сканер", "SplDer Guard для серверов" ПО СЗ от ВВК "Dr.Web 10"

|  |  |
| --- | --- |
| **Параметр** | **Значение параметра** |
| Исключаемые пути | Каталоги серверных компонентов ПО ЕСМИБ ТУ (включая вложенные подкаталоги):  C:\Program Files (x86)\Crystall\ZObserver\Audit, включая номерные каталоги агентов Audit\<№ агента>\\*.\*;  C:\Program Files (x86)\Crystall\ZObserver\Log;  C:\Program Files (x86)\Crystall\ZObserver\Contexts\\*.\*;  C:\Program Files (x86)\Crystall\ZObserver\TmpUser;  C:\Program Files (x86)\Crystall\ZObserver\Executable\\*.\*;  C:\Program Files (x86)\Crystall\ZObserver\Agent.Distrib (включая номерные каталоги агентов Agent.Distrib \<№ агента>\\*.\*);  C:\Program Files (x86)\Crystall\ZObserver\System.Private\Global;  C:\Program Files (x86)\Crystall\ZObserver\System\Global;  c:\Program Files (x86)\Microsoft SQL Server\MSSQL10\_50.SQL2008\MSSQL\DATA\\*.\*;  C:\Program Files (x86)\Crystall\Monitor\DataBases\DBIdentity;  C:\Program Files (x86)\Crystall\Monitor\DataBases\DBIncident.  Каталог агентской платформы ЕСМИБ ТУ (включая вложенные подкаталоги):  c:\Program Files (x86)\Crystall\Misc\AgentPlatform\\*.\*.  Файлы облегченного агента ЕСМИБ ТУ и агентов, построенных на базе облегченного:  C:\Program Files\Crystall\ZObserver\Agents\\*\Data\mailaudit.la |
| Исключаемые процессы | Исполняемые модули процессов ЕСМИБ ТУ:  C:\Program Files (x86)\Crystall\ZObserver\ntsm.exe;  C:\Program Files (x86)\Crystall\ZObserver\Audit\_Parser.exe;  C:\Program Files (x86)\Crystall\Monitor\Monitor\Services\OperSignService.exe;  C:\Program Files (x86)\Crystall\Monitor\Monitor\Services\ScenSignService.exe;  C:\Program Files\Crystall\ZObserver\Agents\\*\liteagent.exe;  C:\Program Files(x86)\Crystall\Misc\AgentPlatform\AgentPlatform.exe |

### НАСТРОЙКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «АККОРД»

Настоящие рекомендации предназначены для установки и настройки программно-аппаратного комплекса СЗИ от НСД на базе контроллеров АМДЗ "Аккорд-Win32/Win64", далее – комплекса, на рабочие станции и серверные вычислительные установки систем РАБИС-НП и АС ЭКР 2.0, используемые для подготовки, обработки, передачи и хранения электронных платёжных документов, под управлением операционных систем Windows XP/7/2003/2008 и распространяются только на технические средства из состава РАБИС-НП и АС ЭКР 2.0 ТУ. Настройка средств защиты от НСД для других технических средств платёжного сегмента (ЕС МИБ, ТУз ТСЭР и т.п.) регламентируется соответствующей документацией на эти системы.

Версии специального программного обеспечения (далее – СПО) «Аккорд-Win32/64» должны быть не ниже v.4.0.9.43 и v.5.0.9.43, актуальные – v.4.0.9.50 и v.5.0.9.50, соответственно.

Версии встроенного программного обеспечения должны быть не ниже 02.01.015 для контроллеров плат «Аккорд-5MX», «Аккорд-5.5», «Аккорд-5.5е».

Установку и настройку комплекса производить в соответствии с эксплуатационной документацией после установки и настройки системного и прикладного ПО АРМ.

Не упомянутые в рекомендациях режимы и опции оставить в первоначальном, после инсталляции СПО, состоянии.

Во время установки и настройки комплекса, при выходе из окон все изменения сохранять.

Некоторые опции: – «Спрашивать разрешение», «Переключение монитора в текстовый режим при старте», «Включить контроль печати» и т.д., в зависимости от использованных: – операционной системы, – версии СПО, – типа платы АМДЗ, состояния - активированного или нет, а также режимов настройки, могут быть недоступными для изменений.

Состав контролируемых файлов на отдельных АРМ может отличаться от приведённого в настоящих рекомендациях перечнях, в зависимости от состава и версий установленного системного и прикладного программного обеспечения, а также применённых обновлений.

Параметры паролей для доступа к ресурсам учетной операционной системы должны удовлетворять требованиям документов: Положения Банка России № 410-П от 13.12.2013 «Об обеспечении информационной безопасности при физическом и логическом доступе к объектам и ресурсам информационно-телекоммуникационной системы Банка России» и «Временные требования по обеспечению технологий обработки электронных платёжных документов в системе Центрального банка Российской Федерации» № 60 от 03.04.1997.

Данные настройки при необходимости, могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в Территориальных учреждениях Банка России по согласованию с подразделением информационной безопасности ТУ. Согласование должно быть оформлено документально и утверждено руководством ТУ.

В настоящих рекомендациях учтены требования к обеспечению информационной безопасности, при эксплуатации средства криптографической защиты информации СКАД «Сигнатура» версии 5.

Комплекс настраивается одинаково для всех операционных систем, если иное не оговорено отдельно.



### Подготовка компьютера к установке комплекса

Файловая система компьютера, на который устанавливается комплекс, должна быть NTFS.

Необходимо удалить не используемы компоненты Windows:

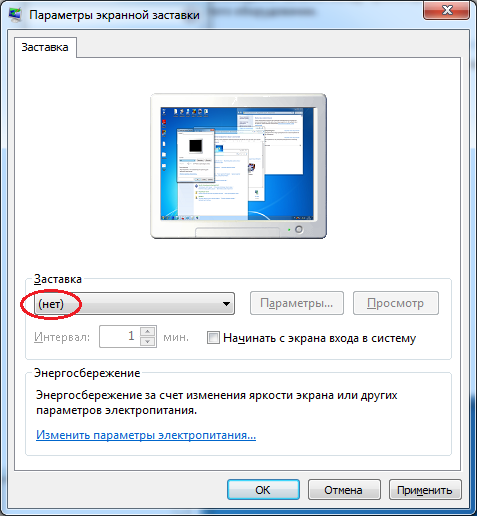
* для ОС Windows XP выбрать Панель управления → Установка и удаление программ → Установка компонентов Windows. В Мастере компонентов Windows снять флажок со следующих компонент:
* Outlook Express;
* Проигрыватель Windows Media.
* Для ОС Windows 7 выбрать Панель управления → Программы и компоненты → Включение или отключение компонентов Windows. В Мастере компонентов Windows снять флажок со следующих компонент:
* Компоненты для работы с мультимедиа (для ОС Windows 7);

После снятия флажка нажать клавишу Далее, дождаться завершения настройки компонент и нажать клавишу Готово.

Для исключения возможных конфликтов комплекса с операционной системой, при функционировании в режим экономии энергии необходимо отключить системный хранитель экрана и энергосберегающие режимы:

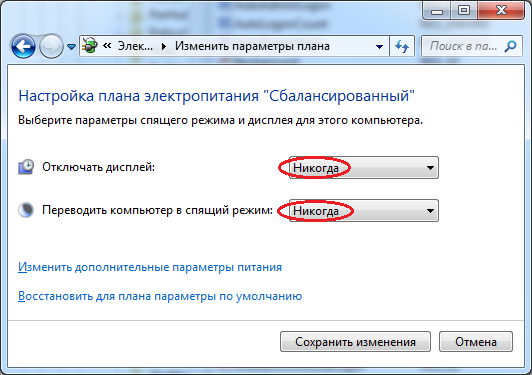
1. **Для Windows 7/2008:**

Панель управления → Оформление и персонализация → Персонализация → Изменение заставки → Заставка (установить в состояние «Нет»).



*Рисунок 1 – Настройки параметров экранной заставки*

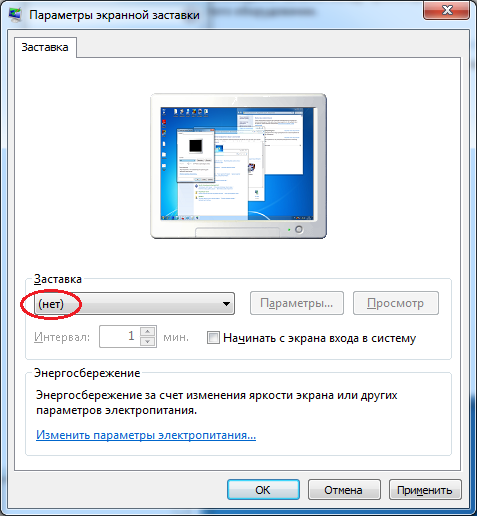
Панель управления → Оборудование и звук → Электропитание → Настройка отключения дисплея: параметры «Отключать дисплей» и «Переводить компьютер в спящий режим» (установить в состояние: – «Никогда»).



*Рисунок 2 – Настройка параметров плана электропитания*

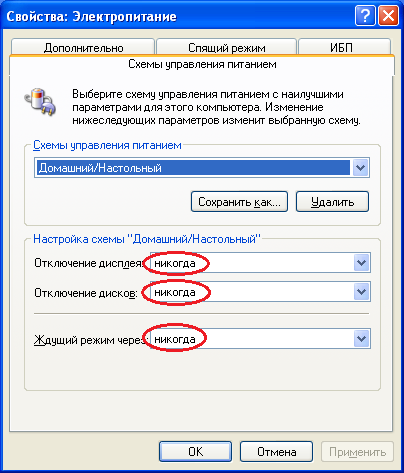
1. **для Windows XP/2003:**

Панель управления → Экран → Заставка – установить в состояние: – «Нет».



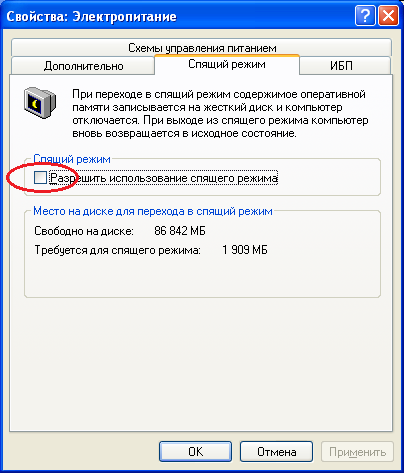
*Рисунок 3 – Настройка параметров экранной заставки*

Панель управления Электропитание → Свойства → Схемы управления питанием → Настройка схемы – «Отключение дисплея» («Отключение дисков» и «Ждущий режим» установить в состояние: – «Никогда»).



*Рисунок 4 – Настройка схемы управления электропитанием*

Панель управления → Электропитание → Свойства → Спящий режим (отключить режим «Разрешить использование спящего режима»).



*Рисунок 5 – Параметры настройки спящего режима*

### Установка в компьютер АМДЗ «Аккорд-5МХ/5.5/5.5е»

Для установки платы АМДЗ «Аккорд-5MX/5.5/5.5e» в компьютер необходимо:

1. выключить компьютер и вставить плату в свободный слот PCI/PCI-express компьютера;
2. подсоединить считыватель/съемник информации (ТМ идентификаторов);
3. включить компьютер и в стартовом меню АМДЗ «Аккорд-5MX/5.5/5.5e» в разделе «Администрирование» зарегистрировать администратора информационной безопасности (ИБ), назначив ему идентификатор[[34]](#footnote-35).

После успешного выполнения процедуры регистрации администратора ИБ (супервизора комплекса Аккорд) следует: перезагрузить компьютер; убедиться в том, что в процессе загрузки появляется сообщение «Предъявите идентификатор»; после успешного прохождения процедуры идентификации и аутентификации в стартовом меню АМДЗ «Аккорд-5MX/5.5/5.5e» выполнить загрузку ОС.

### Установка драйверов комплекса Аккорд

Для дальнейшей настройки комплекса Аккорд необходимо загрузить ОС с правами Администратора. Система обнаружит новое PCI-устройство (плата АМДЗ «Аккорд-5MX/5.5/5.5e») и предложит установить драйвер.



*Рисунок 6 –Установка драйвера PCI-устройства (плата АМДЗ «Аккорд-5MX/5.5/5.5e»)*

Для установки драйвера следует указать папку \Drivers\Win\_32 (для 32х битной версии ОС) или папку \Drivers\Win\_32 (для 64х битной версии ОС), которая находится на компакт-диске «Аккорд- АМДЗ», поставляемом в составе комплекса Аккорд.

По окончанию установки драйверов в «Диспетчере устройств» ОС появится новая группа «Аппаратная защита от НСД», а в этой группе устройства «Аккорд–5MX/5.5/5.5e».

### Установка СПО «Аккорд-Win32/64»

Для установки СПО «Аккорд-Win32/64» необходимо запустить программу AccordSetupWin64.exe (для 64х битной версии ОС Windows) или AccordSetupWin32.exe (для 32х битной версии ОС Windows), следовать инструкциям установщика и использовать каталог для размещения файлов по умолчанию.

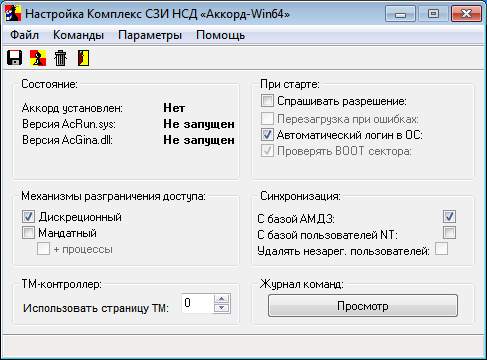
По окончанию завершения работы мастера установки запустите утилиту Редактор прав доступа (ACED32)[[35]](#footnote-36) или запустите файл Aced32.exe установочного каталога, не регистрируйте никаких новых пользователей, выполните сохранение базы и завершите работу Редактора прав доступа[[36]](#footnote-37).

### Настройка комплекса Аккорд

Дальнейшая настройка комплекса выполняется последовательно в соответствии с пунктами данного раздела. Часть настроек комплекса Аккорд становятся доступными после выполнения активации Комплекса (см. раздел П2.5.4) и перезагрузки компьютера.

### Настройка синхронизации комплекса Аккорд

Для выполнения настройки синхронизации комплекса Аккорд необходимо запустить утилиту Настройка комплекса Аккорд (файл acsetup.exe установочного каталога)[[37]](#footnote-38), снять синхронизацию с базой пользователей NT, сохранить изменения и выйти из утилиты.



*Рисунок 7 –Настройка параметров синхронизации комплекса Аккорд*

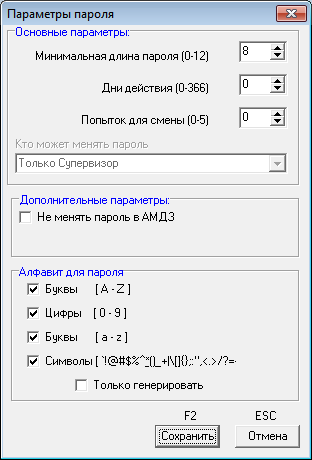
### Настройка редактора прав доступа (ACED32)

Для настройки редактора прав доступа запустите утилиту Редактор прав доступа или запустите файл Aced32.exe установочного каталога.

### Настройка параметров входа в систему

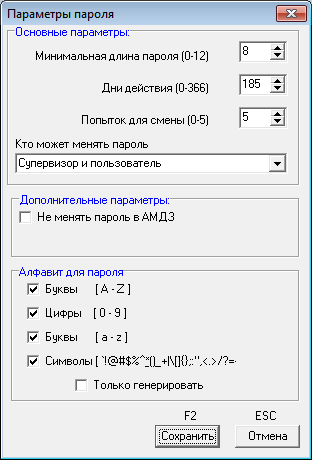
Для настройки параметров входа в систему необходимо зайти в раздел «Вход в систему» → «Параметры пароля» и настроить:

* для группы пользователей «Администраторы»:
  + установить – «Минимальная длина пароля» = 8;
  + установить – «Дни действия» = 0;
  + установить – «Попыток смены» = 0;
  + установить – «Кто может менять пароль» = только Супервизор;
  + снять – «Не менять пароль в АМДЗ»;
  + установить – «Алфавит для пароля» – «Цифры, прописные и строчные буквы, символы»;
  + снять – «Только генерировать».



*Рисунок 8 – Настройка параметров пароля для группы пользователей «Администраторы»*

* для группы пользователей «Обычные»:
  + установить – «Минимальная длина пароля» = 8;
  + установить – «Дни действия» = 185;
  + установить – «Попыток для смены» = 5;
  + установить – «Кто может менять пароль» = Супервизор и пользователь;
  + снять – «Не менять пароль в АМДЗ»;
  + установить – «Алфавит для пароля» – «Цифры, прописные и строчные буквы, символы»;
  + снять – «Только генерировать».

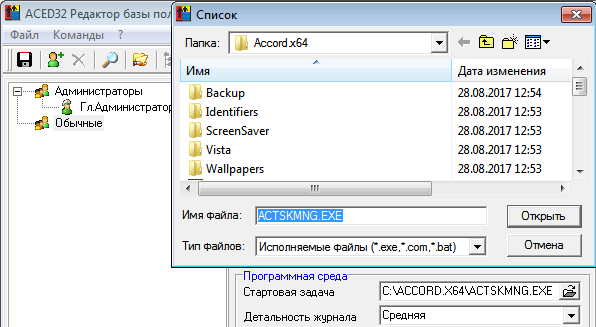


*Рисунок 9 – Настройка параметров пароля для группы пользователей «Обычные»*

### Настройка параметров программной среды

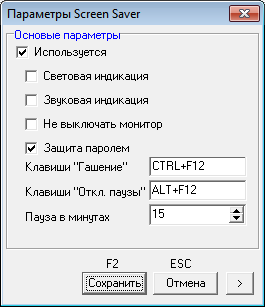
Для настройки параметров программной среды необходимо зайти в раздел «Программная среда».

* установить стартовую задачу для группы пользователей «Обычные»: - «C:\Accord.NT\AcTaskMng.exe»;
* установить детальность журнала для групп пользователей «Администраторы» и «Обычные»: – «Средняя».



*Рисунок 10 – Настройка параметров Программной среды*

* настроить «Гашение экрана» (Параметры Screen Saver) для групп пользователей «Администраторы» и «Обычные»:
  + «Используется»;
  + «Пауза в минутах» – не более 15;
  + «Защита паролем».



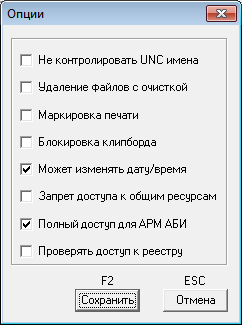
*Рисунок 11 – Настройка параметров гашения экрана*

На рабочих местах, используемых для мониторинга процессов приёма-передачи и обработки информации, допускается устанавливать опцию «Не выключать монитор».

### Настройка раздела «Опции»

Для группы пользователей «Обычные» необходимо настроить следующие параметры:

* снять – «Не контролировать UNC имена»;
* снять – «Удаление файлов с очисткой»;
* снять – «Маркировка печати»;
* снять – «Блокировка клипборда»;
* установить - «Может изменять дату/время»;
* снять – «Запрет доступа к общим ресурсам»;
* установить - «Полный доступ для АРМ АБИ»;
* снять – «Проверять доступ к реестру».

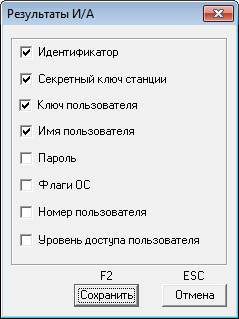


*Рисунок 12 – Настройка Опции для группы Обычные*

### Настройка раздела «Результаты И/А»

Для групп пользователей «Администраторы» и «Обычные» необходимо настроить следующие параметры:

* установить - «Идентификатор»;
* установить - «Секретный ключ станции»;
* установить - «Секретный ключ пользователя»;
* установить - «Имя пользователя»;
* снять - «Пароль»;
* снять – «Флаги ОС»;
* снять – «Номер пользователя»;
* снять – «Уровень доступа пользователя».

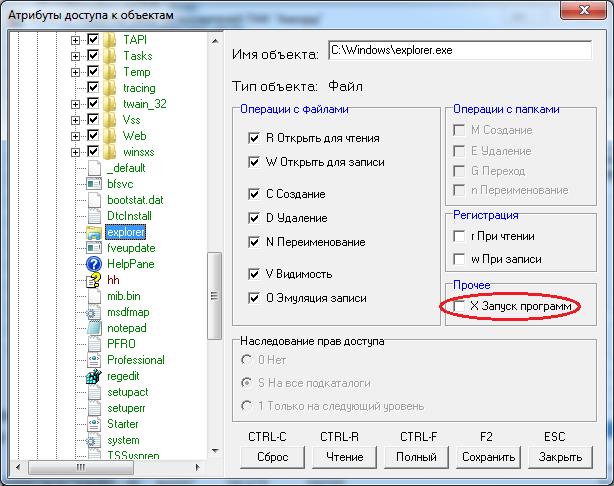


*Рисунок 13 – Настройка Результатов И/А для всех групп*

### Настройка правил разграничения доступа

В разделе «Разграничение доступа» для групп пользователей «Обычные» необходимо настроить следующие правила разграничения:

* установить запрет на выполнение программных файлов:
  + C:\Windows\explorer.exe;
  + C:\Windows\hh.exe;
  + C:\Windows\notepad.exe;
  + C:\Windows\winhelp.exe;
  + C:\Windows\winhlp32.exe;
  + C:\Windows\System32\calc.exe
  + C:\Windows\System32\cmd.exe
  + C:\Windows\System32\help.exe;
  + C:\Windows\System32\hhctrl.ocx;
  + C:\Windows\System32\mspaint.exe;
  + C:\Windows\System32\notepad.exe;
  + C:\Windows\System32\sethc.exe;
  + C:\WINDOWS\system32\tourstart.exe (только для Windows XP);
  + C:\Windows\System32\utilman.exe;
  + C:\Program Files\Internet Explorer\iexplore.exe (за исключением АРМ персонала ЕСМИБ ТУ);
  + C:\Program Files\Outlook Express\msimn.exe, (только для Windows XP);
  + C:\Program Files (x86)\Internet Explorer\iexplore.exe, (только для Windows 7/2008);
  + C:\Program Files (x86)\Windows NT\Accessories\wordpad.exe (только для Windows 7/2008);
  + C:\Program Files\Windows NT\Accessories\wordpad.exe
  + C:\Windows\SysWOW64\calc.exe, (только для Windows 7/2008);
  + C:\Windows\SysWOW64\cmd.exe, (только для Windows 7/2008);
  + C:\Windows\SysWOW64\explorer.exe, (только для Windows 7/2008);
  + C:\Windows\SysWOW64\help.exe, (только для Windows 7/2008);
  + C:\Windows\SysWOW64\hh.exe, (только для Windows 7/2008);
  + C:\Windows\SysWOW64\hhctrl.ocx, (только для Windows 7/2008);
  + C:\Windows\SysWOW64\mspaint.exe, (только для Windows 7/2008);
  + C:\Windows\ SysWOW64\notepad.exe, (только для Windows 7/2008).



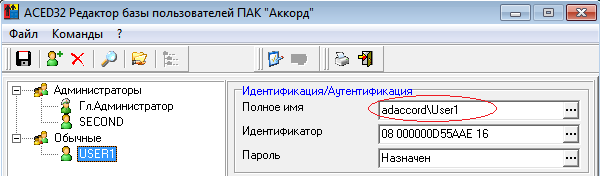
*Рисунок 14 – Настройка атрибутов доступа к объектам*

* установить запрет на выполнение программ (все exe-файлы) в каталоге C:\Program Files\MSN Gaming Zone\ (только для ОС Windows XP);
* установить запрет на выполнение программ, имеющих собственный файловый менеджер: таких как Far manager, Winrar, WinZip, и т. п.;
* на компьютерах с интегрированными видеоадаптерами на базе Intel Graphics Media Accelerator установить запрет на выполнение программных файлов – hkcmd.exe, igfxpers.exe, igfxrun.exe, igfxtray.exe;
* установить полный доступ на объект «\\» с подкаталогами»;
* установить полный доступ на объект «\device\»;
* установить необходимые правила доступа к портам и устройствам ввода-вывода информации;
* установить атрибут «Видимость» (v) для папок C:\Accord.NT\, C:\Accord.х64 и C:\Accord.RAU\, с наследованием прав, установить атрибута «Видимость» (v) на файлы скрытого раздела на компьютере с ОС Windows7 и другие файлы, к которым производится обращение перечисленных выше программ и процессов[[38]](#footnote-39).

### Регистрация пользователей комплекса Аккорд

В комплексе Аккорд необходимо зарегистрировать следующих пользователей:

* резервного администратора ИБ в группе «Администраторы»;
* пользователей компьютера в группе «Обычные».



*Рисунок 15 – Настройка и регистрация пользователей комплекса*

В группу «Обычные» должны включаться только доменные пользователи, при этом в окне «Идентификация/Аутентификация» следует указывать полные доменные имена. При использовании в качестве резервных администраторов на рабочих станциях и серверах (не контроллерах домена) учётных записей обычных доменных пользователей ввести их в группу локальных администраторов.

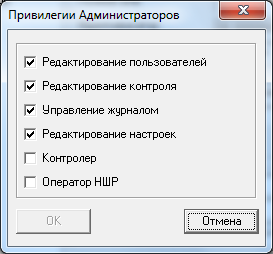
Учетные записи доменных пользователей, используемых в качестве резервных администраторов и введенных в группу локальных администраторов, запрещается использовать для целей, отличных от администрирования комплекса Аккорд.

Настроить доступ к портам и устройствам ввода–вывода информации для пользователей, если их правила отличаются от групповых (см. предыдущий раздел П2.5.2.5).

### Настройка привилегий пользователей комплекса Аккорд

Для пользователей группы «Администраторы» проверить настройки привилегий: «Команды» → «Привилегии Администраторов»:

* установить - «Редактирование пользователей»;
* установить - «Редактирование контроля»;
* установить - «Управление журналом»;
* установить - «Редактирование контроля»;
* снять - «Контролёр»;
* снять - «Оператор НШР».



*Рисунок 16 – Настройка привилегий для администраторов комплекса*

В группу «Обычные» должны включаться только доменные пользователи, при этом в окне «Идентификация/Аутентификация» следует указывать полные доменные имена. При использовании в качестве резервных администраторов на рабочих станциях и серверах (не контроллерах домена) учётных записей обычных доменных пользователей ввести их в группу локальных администраторов.

Учетные записи доменных пользователей, используемых в качестве резервных администраторов и введенных в группу локальных администраторов, запрещается использовать для целей, отличных от администрирования комплекса Аккорд.

Выполнить сохранение изменений в базе Редактора и закрыть его.

### Настройка стартовых задач для пользователей комплекса Аккорд

Установить стартовую задачу для пользователей, одну или несколько. Для этого, в каталоге «C:\Accord.NT\х64» создать текстовые файлы «<имя\_пользователя>.act», в соответствии с разделом 6.9 «Установка стартовой задачи пользователя» документа «ПАК СЗИ от НСД Аккорд. Установка правил разграничения доступа. Программа ACED32»: 11443195.4012-036 97 (для Win-32) и 11443195.4012-037 97 (для Win-64), для каждого пользователя, включая пользователей группы «Администраторы», с перечнем необходимых программ. Для пользователей группы «Администраторы» установить стартовую задачу explorer.exe и (или) far.exe. Пути в файлах \*.act указывать в WIN-кодировке.

### Настройка конфигурационных файлов комплекса Аккорд

В файле accord.ini установочного каталога СПО «Аккорд-Win32/64» необходимо установить значение параметра WriteNsdOnFind равным No26.

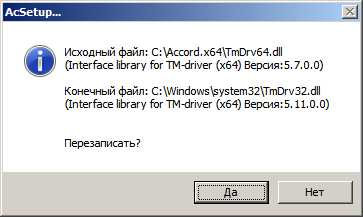
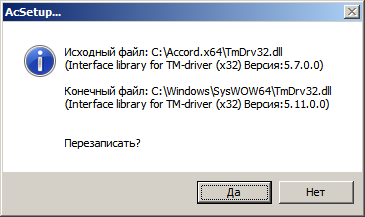
Для установки запрета на отображение в панели Менеджера задач иконок программ в файле actskmng.ini установочного каталога СПО «Аккорд-Win32/64» необходимо установить значение параметра ShowTrayIcons равным No. Иконки языка раскладки, подключенных USB устройств и менеджера задач Аккорда останутся доступными.

Состояние антивирусной защиты на рабочих станциях контролировать через консоль управления СЗ от ВВК.

### Активация комплекса Аккорд

Для выполнения активации комплекса Аккорд необходимо запустить утилиту «Настройка комплекса Аккорд», выбрать Команды → Активация.

В информационных окнах о перезаписи файлов TmDrv нажать клавишу Да.

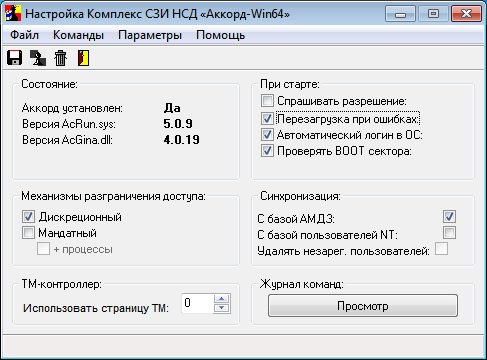


В информационном окне «Система успешно установлена» нажать **ОК** и выполнить перезагрузку компьютера.

### Настройка комплекса СЗИ от НСД «Аккорд-Win32/64»

Запустить утилиту «Настройка комплекса Аккорд»:

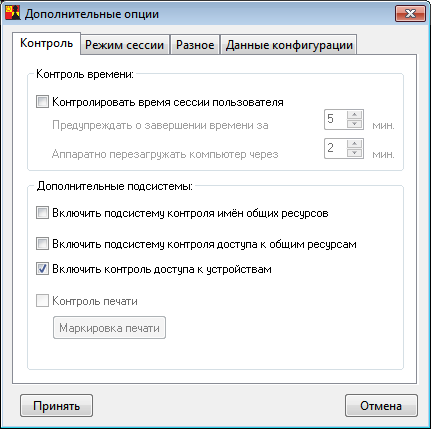
* В главном окне утилиты настройки Комплекса:
  + установить механизм разграничения доступа - «Дискреционный»;
  + снять механизм разграничения доступа - «Мандатный»;
  + установить страницу в идентификаторе - «0»;
  + снять при старте «Спрашивать разрешение»;
  + установить при старте - «Перезагрузка при ошибках» - можно только после активации;
  + установить при старте - «Автоматический логин в ОС»;
  + установить при старте - «Проверять BOOT сектора»;
  + установить при старте - «Поддержка USB клавиатуры»;
  + установить синхронизацию «С базой АМДЗ»;
  + снять синхронизацию «С базой пользователей NT»;
  + снять «Удалять незарегистрированных пользователей».



*Рисунок 17 – Параметры Настройки комплекса Аккорд*

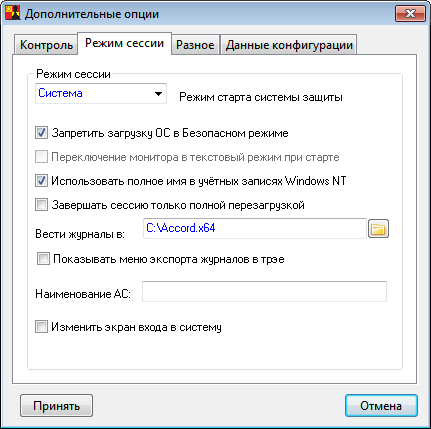
Настроить дополнительные опции Комплекса: «Параметры» → «Дополнительные опции».

* Вкладка «Контроль»:
  + снять – «Контролировать время сессии пользователя»;
  + снять – «Включить подсистему контроля общих имён»;
  + снять – «Включить подсистему контроля доступа к общим ресурсам»;
  + установить – «Включить контроль доступа к устройствам»;
  + снять – «Включить контроль печати».



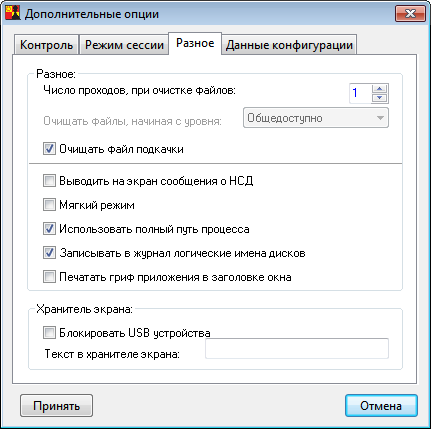
*Рисунок 18 – Параметры дополнительных опций Комплекса, вкладка Контроль*

* Вкладка «Режим сессии».
  + установить режим старта системы защиты – «Система»;
  + установить - «Запретить загрузку ОС в безопасном режиме»;
  + установить - «Переключение монитора в текстовый режим при старте»;
  + установить - «Использовать полное имя в учётных записях Windows NT»;
  + снять - «Завершать сессию только полной перезагрузкой»;
  + в поле «Вести журналы» указать каталог для ведения журналов: C:\Accord.NT; C:\Accord.NT\AссLog или другой;
  + снять - «Показывать меню экспорта в трее»;
  + заполнить, при необходимости, поле: – «Наименование АС:», содержимое этого поля будет заносится в журнал комплекса.



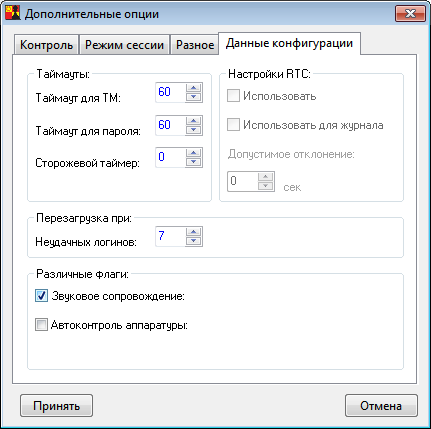
*Рисунок 19 – Параметры дополнительных опций Комплекса, вкладка Режим сессии*

* Вкладка «Разное»:
  + оставить число проходов при очистке файлов = «1»;
  + установить – «Очищать файл подкачки»;
  + снять – «Очищать сетевые файлы»;
  + снять – «Выводить на экран сообщения об НСД»;
  + снять – «Мягкий режим»;
  + установить – «Использовать полный путь процесса»;
  + установить – «Записывать в журнал логические имена дисков»;
  + снять – «Печатать гриф приложения в заголовке окна»;
  + снять – «Блокировать USB устройства»;
  + заполнить, при необходимости, поле – «Текст в хранителе экрана».



*Рисунок 20 – Параметры дополнительных опций Комплекса, вкладка Разное*

* Вкладка «Данные конфигурации»:
  + установить значение - «Таймаут для идентификатора:» = 60;
  + установить значение - «Таймаут пароля:» = 60;
  + установить «Сторожевой таймер:» = «0»;
  + снять «Использовать» – в «Настройки RTC:»;
  + снять «Использовать для журнала» – в «Настройки RTC:»;
  + установить «Допустимое отклонение:» = «0»
  + установить в – «Перезагрузка при:» «Неудачных логинов:» = 7;
  + установить при необходимости в – «Различные флаги:» - «Звуковое сопровождение:»;
  + снять - «Автоконтроль аппаратуры:».



*Рисунок 21 – Параметры дополнительных опций Комплекса, вкладка Данные конфигурации*

Сохранить изменения нажатием кнопки «Принять» в «Дополнительных опциях», а затем сохранить изменения в настройках комплекса и закрыть утилиту настройки.

### Настройка механизма КЦ комплекса Аккорд

### Настройка механизма КЦ на аппаратном уровне

Настройка механизма контроля целостности (КЦ) на аппаратном уровне выполняется в стартовом меню АМДЗ «Аккорд-5MX/5.5/5.5e» в разделе «Администрирование».

В разделе «Аппаратура» необходимо исключить контроль параметров раздела BIOS.

В разделе «Файлы» необходимо сформировать перечень файлов для КЦ, включив в него:

* файлы, перечисленные в приложении 2 документа ПАК СЗИ от НСД для ПЭВМ (PC) «Аккорд–АМДЗ» (Аппаратный модуль доверенной загрузки) Руководство администратора», 11443195.4012.038 90;
* файлы, перечисленные в приложениях 6, 7 и 8 документа «ПАК СЗИ от НСД «Аккорд-Win32» (версия 4.0). Руководство администратора», 11443195.4012-036 90 – для 32х разрядных версий ОС Windows;
* файлы, перечисленные в приложениях 6, 7 и 8 документа «ПАК СЗИ от НСД «Аккорд-Win64» (версия 5.0). Руководство администратора», 11443195.4012-037 90 – для 64х разрядных версий ОС Windows;
* исполняемый файл hashfilе.exe СКАД «Сигнатура».

### Настройка механизма КЦ на программном уровне

Настройка механизма контроля целостности (КЦ) на аппаратном уровне выполняется с помощью утилиты «Редактор прав доступа» (ACED32) в разделе «Контроль целостности» для группы «Обычные», включив в него:

* файлы, перечисленные в приложениях 7 и 8 документов:
  + «ПАК СЗИ от НСД «Аккорд-Win32» (версия 4.0). Руководство администратора», 11443195.4012-036 90 – для 32х разрядных версий ОС Windows;
  + «ПАК СЗИ от НСД «Аккорд-Win64» (версия 5.0). Руководство администратора», 11443195.4012-037 90 – для 64х разрядных версий ОС Windows;
* файлы \*.exe, \*.dll, \*.act из каталога C:\Accord.NT;
* файлы, перечни которых находятся на передаточном носителе в архиве \Средство КЗИ\00107 Setup.zip в виде отдельных файлов с расширением \*.hsh для каждой поддерживаемой операционной системы, входящего в состав дистрибутив СКАД Сигнатура версия 5;
* файлы \*.exe, \*.dll из каталога C:\Program Files\MDPREI и его подкаталогов;
* файлы \*.exe, \*.dll, \*.sys из каталога C:\Program Files\Validata и его подкаталогов;
* исполняемый файл программы hashfile.exe и эталон верификации в соответствии с документом «СКАД «Сигнатура» версия 5. Программа контроля целостности. Руководство администратора информационной безопасности» ВАМБ.00107-01 93 02;
* файлы из системного каталога %system%, в соответствии с документом «СКАД «Сигнатура» версия 5. Программа контроля целостности. Руководство администратора информационной безопасности» ВАМБ.00107-01 93 02:
  + atl80.dll;
  + gdbm8.dll;
  + iconv8.dll;
  + intl8.dll;
  + libpki1.dll;
  + libxml28.dll;
  + mfc80.dll;
  + msvcm80.dll;
  + msvcp80.dll;
  + msvcr80.dll;
  + rpcrt4.dll;
  + scertui.dll;
  + scrypt.dll;
  + spki.dll;
  + spki1.dll;
  + spki1jni.dll;
  + spkicom.dll;
  + spkissl.dll;
  + vcertmsg.dll;
  + vdmondll.dll;
  + vdcngl.dll;
  + zlib1.dll;
  + \drivers\vdcngdrv.sys;
  + \drivers\vdcrydrv.sys;
  + \drivers\vdmondrv.sys;
* файлы в соответствии с письмом Отделения по Рязанской обл. ГУ Банка России по СФО № 70-17-15/5474 от 27.05.2016 «О контроле целостности программных файлов СКАД «Сигнатура»:
  + Для 32-битных ОС Windows XP, Windows Server 2003:

%WINDIR%\WinSxS\x86\_Microsoft.VC80.ATL\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_cbb27474\ATL80.dll

%WINDIR%\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6b128700\msvcm80.dll

%WINDIR%\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6b128700\msvcp80.dll

%WINDIR%\WinSxS\x86\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6b128700\msvcr80.dll

%WINDIR%\WinSxS\x86\_Microsoft.VC80.MFC\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_3bf8fa05\mfc80.dll

* + Для 64-битных ОС Windows XP, Windows Server 2003:

%WINDIR%\WinSxS\amd64\_Microsoft.VC80.ATL\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_fdbc5a54\ATL80.dll

%WINDIR%\WinSxS\amd64\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_9d1c6ce0\msvcm80.dll

%WINDIR%\WinSxS\amd64\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_9d1c6ce0\msvcp80.dll

%WINDIR%\WinSxS\amd64\_Microsoft.VC80.CRT\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_9d1c6ce0\msvcr80.dll

%WINDIR%\WinSxS\amd64\_Microsoft.VC80.MFC\_1fc8b3b9a1e18e3b\_8.0.50727.762\_x-ww\_6e02dfe5\mfc80.dll

* + Для всех остальных 32-битных ОС Windows, на которых функционируют СКАД «Сигнатура» версия 5 и СКЗИ «Янтарь» версия 5:

%WINDIR%\WinSxS\x86\_microsoft.vc80.atl\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_11ecb0ab9b2caf3c\ATL80.dll

%WINDIR%\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_10b2f55f9bffb8f8\msvcm80.dll

%WINDIR%\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_10b2f55f9bffb8f8\msvcp80.dll

%WINDIR%\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_10b2f55f9bffb8f8\msvcr80.dll

%WINDIR%\WinSxS\x86\_microsoft.vc80.mfc\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_0c178a139ee2a7ed\mfc80.dll

* + Для всех остальных 64-битных ОС Windows, на которых функционируют СКАД «Сигнатура» версия 5 и СКЗИ «Янтарь» версия 5:

%WINDIR%\WinSxS\amd64\_microsoft.vc80.atl\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_ca3f79d486b08636\ATL80.dll

%WINDIR%\WinSxS\amd64\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_c905be8887838ff2\msvcm80.dll

%WINDIR%\WinSxS\amd64\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_c905be8887838ff2\msvcp80.dll

%WINDIR%\WinSxS\amd64\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_c905be8887838ff2\msvcr80.dll

%WINDIR%\WinSxS\amd64\_microsoft.vc80.mfc\_1fc8b3b9a1e18e3b\_8.0.50727.762\_none\_c46a533c8a667ee7\mfc80.dll

После завершения создания списка контролируемых объектов отметить в «Параметрах проверки» пункт «До запуска системы», произвести расчёт контрольных сумм и сохранить настройки.

### Минимальные настройки механизма КЦ на программном уровне

В данном разделе приведен минимальный перечень файлов (каталогов) АРМ и серверов, целостность которых должна контролироваться СЗИ от НСД Аккорд. Перечень контролируемых файлов необходимо обновлять после обновления версий программного обеспечения.

1. Программные файлы из каталога C:\Accord.NT\х64\RAU.
2. Системные файлы, конкретный перечень которых приведён в дистрибутиве в файле «Средство КЗИ\00107 Setup.zip».
3. Системные файлы, конкретный перечень которых приведён в документе «СКАД «Сигнатура» Версия 5. Программа контроля целостности. Руководство администратора информационной безопасности. Раздел 5. Рекомендуемые списки контролируемых модулей. ВАМБ.00107-01 93 02.
4. Программные файлы из каталогов с программным прикладным обеспечением РАБИС-НП и АС ЭКР 2.0 в соответствии с технорабочей документацией на РАБИС-НП и АС ЭКР 2.0.
5. Программные файлы из каталога с подкаталогами C:\Program Files\MDPREY.
6. Программные файлы из каталога с подкаталогами C:\Program Files\Validata.
7. Программные файлы из каталога с подкаталогами C:\Program Files\Java\jre6.

### Настройка политики безопасности

Таблица . Настройка политик безопасности

|  |  |
| --- | --- |
| **Параметры безопасности\Локальные политики\Политика паролей** | |
| Вести журнал паролей | 10 сохранённых паролей |
| Минимальная длина пароля | 8 |
| Максимальный срок действия пароля | 185 дней |
| Минимальный срок действия пароля | 3 |
| **Параметры безопасности\Локальные политики\Политика блокировки учётных записей** | |
| Время до сброса счётчика блокировки | 5 мин. |
| Пороговое значение блокировки | 5 ошибок входа в систему |
| Продолжительность блокировки учётной записи | 5 мин. |
| **Параметры безопасности\Параметры безопасности\Локальные политики\Политика аудита** | |
| Аудит входа в систему | Успех, Отказ |
| Аудит изменения политики | Успех, Отказ |
| Аудит использования привилегий | Отказ |
| Аудит событий входа в систему | Успех, Отказ |
| Аудит управления учетными записями | Успех, Отказ |
| **Параметры безопасности\Локальные политики\Параметры безопасности** | |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | 0 - входов в систему |
| Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера | Включен |
| Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности | Включен |
| Учетные записи: Состояние учетной записи 'Администратор' | Включен |
| Учетные записи: Состояние учетной записи 'Гость' | Отключен |
| Завершение работы: очистка файла подкачки виртуальной памяти | Включен |

Для отключения:

* кэширования информации о регистрации пользователей в сети;
* автоматической регистрации в системе;
* сохранения сетевых паролей;
* сохранения паролей или учётных данных для сетевой проверки подлинности;
* действий функциональных клавиш клавиатуры «Menu» и «Windows» (за исключением АРМ персонала ЕСМИБ ТУ);
* отключения общих системных папок: – ADMIN$, C$, D$,

Необходимо создать и выполнить скрипт – в виде текстового файла с расширением – reg, например – «set\_policies.reg»:

*; отключить запрет кэширования информации о регистрации пользователей в сети*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]*

*"cachedlogonscount"="10"*

*; запретить автоматическую регистрацию в системе*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]*

*"AutoAdminLogon"="0"*

*; отключить запрет сохранения сетевых паролей*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\network]*

*"DisablePwdCaching"=dword:00000000*

*; запретить сохранение паролей или учётных данных для сетевой проверки подлинности*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]*

*"disabledomaincreds"=dword:00000001*

*; отключить действие функциональных клавиш клавиатуры «Menu» и «Windows»*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]*

*"Scancode Map"=hex:00,00,00,00,00,00,00,00,04,00,00,00,00,00,5B,E0,00,00,5C,E0,00,00,5D,E0,00,00,00,00*

*; отключить общие системные папки ADMIN$, C$, D$ для северов*

*; [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters]*

*;"AutoShareServer"=dword:00000000*

*; отключить общие системные папки ADMIN$, C$, D$ для рабочих станций*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters]*

*"AutoShareWks"=dword:00000000*

-- конец скрипта «set\_policies.reg» на установку ограничений через реестр Windows --

Для отмены изменений создать и выполнить скрипт – текстовый файл – «restore\_policies.reg»:

-- начало скрипта «restore\_policies.reg» для отмены ограничений через реестр Windows ––

*Windows Registry Editor Version 5.00*

*; отключить запрет кэширования информации о регистрации пользователей в сети*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]*

*"cachedlogonscount"="10"*

*; запретить автоматическую регистрацию в системе*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]*

*"AutoAdminLogon"=-*

*; отключить запрет сохранения сетевых паролей*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\network]*

*"DisablePwdCaching"=-*

*; запретить сохранение паролей или учётных данных для сетевой проверки подлинности*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]*

*"disabledomaincreds"=-*

*; отключить действие функциональных клавиш клавиатуры «Menu» и «Windows»*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]*

*"Scancode Map"=-*

*; отключить общие системные папки ADMIN$, C$, D$ для северов*

*; [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters]*

*;"AutoShareServer"=-*

*; отключить общие системные папки ADMIN$, C$, D$ для рабочих станций*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters]*

*"AutoShareWks"=-*

-- конец скрипта «restore\_policies.reg» для отмены ограничений через реестр Windows --

### Рекомендации по настройке СЗ от ВВК

Включить в доверенную зону СЗ от ВВК каталоги C:\Accord.NT, C:\Accord.x64, C:\Accord.RAU, каталог для ведения журналов Аккорда, в случае, если он вынесен из каталога с СПО, а также программные модули комплекса, которые после установки и активации комплекса копируются в системные каталоги. Список файлов, включаемых в доверенную зону СЗ от ВВК, приведен ниже (его состав может отличаться, в зависимости от используемой версии СПО):

\Windows\**System32**\accord.scr

\Windows\**System32**\acgina.dll

\Windows\**System32**\acnp.dll

\Windows\**System32**\acrunnt.exe

\Windows\**System32**\acrunvdd.dll

\Windows\**System3**2\acrunvdd.exe

\Windows\**System32**\acusrm64.dll

\Windows\**System32**\autoexec.nt

\Windows\**System32**\aziah64.dll

\Windows\**System32**\tmattach.dll

\Windows\**System32**\tmatt64.dll

\Windows\**System32**\tmdrv32.dll

\Windows\**System32**\tmdrv64.dll

\Windows\System32\**Drivers**\acboot.sys

\Windows\System32\**Drivers**\aclock2k.sys

\Windows\System32\**Drivers**\acrun.sys

\Windows\System32\**Drivers**\acxallow.sys

\Windows\System32\**Drivers**\acxlmsrv.sys

\Windows\System32\**Drivers**\tmac5.sys

\Windows\System32\**Drivers**\tmac5w.sys

\Windows\System32\**Drivers**\tmac5xw.sys

\Windows\System32\**Drivers**\tmac5\_64.sys

\Windows\System32\**Drivers**\tmac5x64.sys

\Windows\System32\**Drivers**\tmac55.sys

\Windows\System32\**Drivers**\tmac55w.sys

\Windows\System32\**Drivers**\tmac5564.sys

\Windows\System32\**Drivers**\tmacgx32.sys

\Windows\System32\**Drivers**\tmacgx64.sys

\Windows\System32\**Drivers**\macu32.sys

\Windows\System32\**Drivers**\tmacu64.sys

\Windows\**SysWOW\**acusrmod.dll

\Windows\**SysWOW**\azIahlp.dll

\Windows\**SysWOW**\tmattach.dll

\Windows\**SysWOW**\tmdrv32.dll

### Обеспечение совместной работы комплекса и подсистемы Паспорт АРМ УОС.

Исключить из состава ПО контролируемого подсистемой Паспорт АРМ УОС файлы комплекса, размещённые в каталогах C:\Accord.NT, C:\Accord.x64 и C:\Accord.RAU, а также файлы скрытого раздела на компьютере с ОС Windows7/2008.

### Обеспечение совместной работы комплекса и ЕСМИБ ТУ

Для обеспечения совместной работы АРМ персонала ЕСМИБ ТУ и ПАК СЗИ от НСД Аккорд необходимо при выполнении настройкой комплекса Аккорд руководствоваться следующими изменениями:

1. Стартовая задача на АРМ персонала ЕСМИБ ТУ не устанавливается и замкнутая программная среда не создаётся.
2. Запрет на выполнение программных файлов на АРМ персонала ЕСМИБ ТУ, перечисленных в разделе П2.5.2.5 не устанавливается.
3. Действие функциональных клавиш клавиатуры «Menu» и «Windows» не отключается (см. раздел П2.5.7).
4. Перечень файлов для контроля формируется из:

* файлов, перечисленных в разделе П2.5.6;
* файлов, перечни которых находятся на передаточном носителе в архиве \Средство КЗИ\00107 Setup.zip в виде отдельных файлов с расширением \*.hsh для каждой поддерживаемой ОС;

1. Для пользователей группы администраторов необходимо наличие файлов с описаниями стартовых задач «explorer» и (или) «far manager» (см. раздел П2.5.2.8).
2. Для обеспечения совместной работы агента ЕСМИБ ТУ и СЗИ от НСД при завершении ОС Windows в конфигурационном файле AcTskMng.ini, который находится в каталоге установки СЗИ, установить параметр WaitEndTask в значение No.
3. После установки компонентов ПО ЕСМИБ ТУ необходимо исключить из-под контроля СЗИ от НСД каталоги, используемые данными компонентами. Для каждого пользователя, не обладающего административными полномочиями в СЗИ от НСД, устанавливаются права доступа, необходимые для функционирования компонентов ЕСМИБ ТУ:

* C:\ – чтение, переход, видимость (полное наследование);
* D:\ – чтение, переход, видимость (полное наследование);
* C:\Windows\System32 – выполнение (наследование на 1 уровень);
* C:\Windows\AGENT – полный доступ (полное наследование) – для подконтрольных объектов с агентом ОС Windows;
* C:\Program Files\Crystall\ZObserver\Agents\<Путь для инсталляции агента> – полный доступ (полное наследование) – для объектов функционирования облегченного агента ОС Windows и агентов, построенных на его базе;
* C:\Program Files (x86)\Crystall\Misc\AgentPlatform – полный доступ (полное наследование) – для объектов функционирования агентов;
* C:\Program Files (x86)\Crystall\Misc – полный доступ (полное наследование) – для компьютеров с утилитами ЕСМИБ ТУ;
* C:\Program Files (x86)\Crystall\SecAdmin Workshop – полный доступ (полное наследование) – для АРМ персонала ЕСМИБ ТУ;
* C:\Program Files (x86)\Crystall\Common – полный доступ (полное наследование) – для компьютеров с утилитами ЕСМИБ ТУ и АРМ персонала ЕСМИБ ТУ;
* C:\Program Files (x86)\Crystall – полный доступ (полное наследование) – для сервера с ПО серверных компонентов ПО ЕСМИБ ТУ;
* C:\Program Files\Internet Explorer – выполнение (полное наследование) – для АРМ персонала ЕСМИБ ТУ;
* \*Microsoft Silverlight\* – выполнение (полное наследование) – для АРМ персонала ЕСМИБ ТУ;
* %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files – чтение, переход, видимость (полное наследование) – для АРМ персонала ЕСМИБ ТУ, работающих под управлением ОС Windows 7;
* C:\Documents and Settings – чтение, переход, видимость (полное наследование) – для АРМ персонала ЕСМИБ ТУ, работающих под управлением ОС Windows XP;
* C:\Windows\Microsoft.NET – выполнение (полное наследование) – для сервера с ПО идентификации и обработки КСИБ;
* C:\Windows\assembly – выполнение (полное наследование) – для сервера с ПО идентификации и обработки КСИБ;
* С:\Windows\System32\inetsrv\ – выполнение (полное наследование) – для сервера с ПО идентификации и обработки КСИБ.

1. Для обеспечения функционирования агента ЕСМИБ ТУ, выполняющего чтение журналов СЗИ от НСД, установить доступ на просмотр содержимого и чтение файлов из каталога, хранящего файлы журналов СЗИ от НСД, заданного в настройках СЗИ, для всех учетных записей пользователей.

Приведенные выше настройки являются минимально необходимыми для работы ПО ЕСМИБ ТУ. Если это необходимо, возможно применение настроек, устанавливающих права доступа на файловую систему в объеме большем, чем указано в приведенных настройках.

### Примечания

1. При организации доступа к внешним носителям, подключаемым через USB порты, необходимо сначала разрешить подключение устройства, а после подключения дать доступ к файловой структуре устройства.
2. Организация доступа к внешним носителям, подключаемым через USB порты, выполняется корректно только в том случае, если устройство подключено до запуска редактора прав доступа и остаётся подключенным до его завершения.
3. При изменении пароля в аппаратной части комплекса на стадии включения питания компьютера, до загрузки операционной системы, например, при окончании срока его действия, произойдёт его смена только в комплексе, в операционной системе пароль не поменяется.
4. При изменении пароля после входа в систему – по трём клавишам (ctrl + alt + del), пароль поменяется и в операционной системе и в комплексе, при условии, что на момент смены пароли в комплексе и в операционной системе совпадают. При несовпадении паролей система выдаст запрос на смену пароля в комплексе.
5. Использовать для пароля в аппаратной части только разрешённые символы.
6. Использовать пароль длиной не более 12 знаков.
7. Параметр «Корректировать переключение раскладки клавиатуры» в файле actskmng.ini, при использовании менеджера задач - actskmng.exe, заменой «NO» на «YES» только в случае, когда переключение раскладки клавиатуры не происходит.
8. Для восстановления реакции системы на прикосновение идентификатора к считывателю, при использовании модификации с USB, необходимо переинициализировать устройство переподключив соединительный кабель считывателя к компьютеру.

### Сообщения об ошибках

Коды ошибок, возникающих при выполнении задач из пунктов меню Аккорда:

1. код ошибки [2] – системе не удаётся найти указанный файл;
2. код ошибки [3] – системе не удаётся найти указанный путь;
3. код ошибки [5] – к указанному файлу нет доступа;
4. код ошибки [193] – в файле actskmng.ini установлен режим ожидания завершения задачи – WaitEndTask=Yes, перевести в режим - WaitEndTask=No.
5. код ошибки [c0000128] – добавить в act-файл пользователя параметр WaitEndTask=No следующим образом:

[Task11.1]

DisplayName=РАБИС-НП

ImagePath=\\lc009\tk\xpress\rkc.lnk

WaitEndTask=No

### Настройка СЗИ от НСД «Secret Net» на рабочих станциях и серверах (контроллерах домена)

Ниже приведены рекомендованные настройки для СЗИ от НСД «SecretNet» версий 6.5 и 7.6.  Данные настройки при необходимости  могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

**Внимание**: до применения групповых политик с настройками СЗИ от НСД "Secret Net" на АРМ и серверах, необходимо предварительно зарегистрировать на них все используемые (планируемые к использованию) устройства (ключевые носители, внешние жесткие диски и т.д.).



### Значения параметров СЗИ от НСД «Secret Net 6.5» для всех применяемых версий операционных систем (Windows XP/7/2003/2008 (x32/x64)).

Таблица 23. Значения параметров СЗИ от НСД Secret Net 6.5, общие для серверов и ПЭВМ

| **Раздел/параметр групповой политики** | **Значение** |
| --- | --- |
| **Конфигурация Windows — Параметры безопасности — Параметры Secret Net — Настройки подсистем** |  |
| Вход в систему: Запрет вторичного входа в систему | отключен |
| Вход в систему: Количество неудачных попыток аутентификации | 3 |
| Вход в систему: Максимальный период неактивности до блокировки экрана | Для серверов ТПК РАБИС-НП, АРМ МИБ АС ЭКР 2.0 – отключена.[[39]](#footnote-40) Для остальных – 15 минут |
| Вход в систему: Разрешить интерактивный вход только доменным пользователям | отключена |
| Вход в систему: Режим аутентификации пользователя | стандартная аутентификация |
| Вход в систему: Режим входа пользователя | Только по идентификатору |
| Журнал: Максимальный размер журнала системы защиты | 50494 Кб |
| Журнал: Политика перезаписи событий | Затирать события по мере необходимости |
| Запрет использования сетевых интерфейсов | Беспроводное соединение (WiFi),  Соединение BlueTooth,  Соединение 1394(FireWire),  Инфракрасное соединение (IrDA) |
| Затирание данных: Количество циклов затирания конфиденциальной информации | 0 (отключено) |
| Затирание данных: Количество циклов затирания на локальных дисках | 1 (0 - для АРМ Администратора модификаций АС ЭКР 2.0, серверов приложений АС ЭКР 2.0) |
| Затирание данных: Количество циклов затирания на сменных носителях | 1 |
| Контроль устройств: Режим работы | Жесткий |
| Полномочное управление доступом: Гриф конфиденциальности для Microsoft Excel | не определено |
| Полномочное управление доступом: Гриф конфиденциальности для Microsoft Word | не определено |
| Полномочное управление доступом: Названия уровней конфиденциальности | не определено |
| Полномочное управление доступом: Режим контроля печати конфиденциальных документов | Отключен |
| Полномочное управление доступом: Режим работы | контроль потоков отключен |
| Разграничение доступа к устройствам: Режим работы | Жесткий |
| **Параметры Secret Net — Ключи пользователя** |  |
| Максимальный срок действия ключа | 360 дней |
| Минимальный срок действия ключа | 30 дней |
| Предупреждение об истечении срока действия ключа | 30 дней |
| **Параметры Secret Net — Привилегии** |  |
| Журнал: Просмотр журнала системы защиты | <имя\_домена>[[40]](#footnote-41)\SecretNetAdmins[[41]](#footnote-42),  <имя\_домена>\Auditors[[42]](#footnote-43),  <имя\_домена>\SPOAdmins[[43]](#footnote-44) |
| Журнал: Управление журналом системы защиты | <имя\_домена>\Auditors |
| Замкнутая программная среда: Не действует | <имя\_домена>\SecretNetAdmins,  <имя\_домена>\SPOAdmins  <имя\_домена>\ModifyAdmins[[44]](#footnote-45) |
| **Параметры Secret Net — Регистрация событий** |  |
| Администрирование: Добавлен пользователь | включена |
| Администрирование: Изменен ключ пользователя | включена |
| Администрирование: Изменены параметры действующей политики безопасности | включена |
| Администрирование: Изменены параметры пользователя | включена |
| Администрирование: Удален пользователь | включена |
| Администрирование: Удаление ключа пользователя | включена |
| Вход/выход: Вход пользователя в систему | включена |
| Вход/выход: Завершение работы пользователя | включена |
| Вход/выход: Запрет входа пользователя | включена |
| Вход/выход: Компьютер заблокирован системой защиты | включена |
| Вход/выход: Компьютер разблокирован | включена |
| Вход/выход: Ошибка выполнения функционального контроля | включена |
| Вход/выход: Пользователь возобновил сеанс работы на компьютере | включена |
| Вход/выход: Пользователь приостановил сеанс работы на компьютере | включена |
| Вход/выход: Успешное завершение функционального контроля | включена |
| Вход/выход: Электронный идентификатор не зарегистрирован | включена |
| Замкнутая программная среда: Загрузка библиотеки | включена |
| Замкнутая программная среда: Запрет загрузки библиотеки | включена |
| Замкнутая программная среда: Запрет запуска программы | включена |
| Замкнутая программная среда: Запрет исполнения неизвестного скрипта | включена |
| Замкнутая программная среда: Запрет исполнения скрипта | включена |
| Замкнутая программная среда: Запуск программы | включена |
| Замкнутая программная среда: Исполнение скрипта | включена |
| Контроль аппаратной конфигурации: Изменены параметры устройства | включена |
| Контроль аппаратной конфигурации: Контроль аппаратной конфигурации завершен с ошибками | включена |
| Контроль аппаратной конфигурации: Контроль аппаратной конфигурации успешно завершен | включена |
| Контроль аппаратной конфигурации: Обнаружено новое устройство | включена |
| Контроль аппаратной конфигурации: Устройство удалено из системы | включена |
| Контроль аппаратной конфигурации: Утверждение аппаратной конфигурации компьютера | включена |
| Контроль печати: Запрет печати конфиденциального документа | отключена |
| Контроль печати: Запрет прямого обращения к принтеру | отключена |
| Контроль печати: Печать документа | отключена |
| Контроль печати: Печать конфиденциального документа | отключена |
| Контроль печати: Прямое обращение к принтеру | отключена |
| Контроль целостности: Для ресурса отсутствует эталонное значение | включена |
| Контроль целостности: Добавление учетной записи к заданию ЗПС | включена |
| Контроль целостности: Завершение обработки задания на контроль целостности | включена |
| Контроль целостности: Завершение проверки целостности ресурса | включена |
| Контроль целостности: Завершение проверки целостности ресурса с ошибкой | включена |
| Контроль целостности: Завершение с ошибкой обработки задания на контроль целостности | включена |
| Контроль целостности: Изменение группы ресурсов | включена |
| Контроль целостности: Изменение задания | включена |
| Контроль целостности: Изменение задачи | включена |
| Контроль целостности: Исправление ошибок в базе данных | включена |
| Контроль целостности: Начало обработки задания на контроль целостности | включена |
| Контроль целостности: Ошибка при восстановлении ресурса по эталонному значению | включена |
| Контроль целостности: Ошибка при открытии базы данных контроля целостности | включена |
| Контроль целостности: Ошибка при попытке принять текущее значение ресурса в качестве эталонного | включена |
| Контроль целостности: Ошибка синхронизации локальной базы данных с центральной | включена |
| Контроль целостности: Принятие текущего значения в качестве эталонного | включена |
| Контроль целостности: Ресурс восстановлен по эталонному значению | включена |
| Контроль целостности: Синхронизация локальной базы данных с центральной | включена |
| Контроль целостности: Снятие задания КЦ с контроля | включена |
| Контроль целостности: Создание группы ресурсов | включена |
| Контроль целостности: Создание задания | включена |
| Контроль целостности: Создание задачи | включена |
| Контроль целостности: Удаление группы ресурсов | включена |
| Контроль целостности: Удаление задания | включена |
| Контроль целостности: Удаление задачи | включена |
| Контроль целостности: Удаление устаревших эталонных значений | включена |
| Контроль целостности: Удаление учетной записи из задания ЗПС | включена |
| Контроль целостности: Установка задания КЦ на контроль | включена |
| Общие события: Несанкционированное действие | включена |
| Общие события: Отладочное событие | включена |
| Общие события: Ошибка | включена |
| Общие события: Предупреждение | отключена |
| Общие события: Событие | отключена |
| Полномочное управление доступом: Вывод конфиденциальной информации на внешний носитель | отключена |
| Полномочное управление доступом: Доступ к конфиденциальному документу | отключена |
| Полномочное управление доступом: Запрет вывода конфиденциальной информации на внешний носитель | отключена |
| Полномочное управление доступом: Запрет доступа к конфиденциальному документу | отключена |
| Полномочное управление доступом: Запрет изменения параметров конфиденциальности ресурса | отключена |
| Полномочное управление доступом: Изменение категории конфиденциальности | отключена |
| Полномочное управление доступом: Изменение признака наследования | отключена |
| Разграничение доступа к устройствам: Доступ к устройству | включена |
| Разграничение доступа к устройствам: Запрет доступа к устройству | включена |
| Разграничение доступа к устройствам: Запрет подключения устройства | включена |
| Разграничение доступа к устройствам: К системе подключено устройство | включена |
| Разграничение доступа к устройствам: Несанкционированное отключение устройства | включена |
| Разграничение доступа к устройствам: Устройство отключено от системы | включена |
| Расширение групповой политики: Групповые политики успешно применены | включена |
| Расширение групповой политики: Ошибка применения групповых политик | включена |
| Расширение групповой политики: Предупреждение при применении групповых политик | включена |
| Сеть: Запрет сетевого подключения под другим именем | включена |
| Служба репликации: Ошибка создания контекста пользователя | включена |
| ЦУ КЦ-ЗПС: Добавление субъекта | включена |
| ЦУ КЦ-ЗПС: Добавление учетной записи к заданию ЗПС | включена |
| ЦУ КЦ-ЗПС: Изменение группы ресурсов | включена |
| ЦУ КЦ-ЗПС: Изменение задания | включена |
| ЦУ КЦ-ЗПС: Изменение задачи | включена |
| ЦУ КЦ-ЗПС: Изменение субъекта | включена |
| ЦУ КЦ-ЗПС: Снятие задания КЦ с контроля | включена |
| ЦУ КЦ-ЗПС: Создание группы ресурсов | включена |
| ЦУ КЦ-ЗПС: Создание задания | включена |
| ЦУ КЦ-ЗПС: Создание задачи | включена |
| ЦУ КЦ-ЗПС: Удаление группы ресурсов | включена |
| ЦУ КЦ-ЗПС: Удаление задания | включена |
| ЦУ КЦ-ЗПС: Удаление задачи | включена |
| ЦУ КЦ-ЗПС: Удаление субъекта | включена |
| ЦУ КЦ-ЗПС: Удаление учетной записи из задания ЗПС | включена |
| ЦУ КЦ-ЗПС: Установка задания КЦ на контроль | включена |
| **Параметры Secret Net — Устройства** |  |
| **Локальные устройства** | Задать настройки контроля;  Разрешить подключение устройства;  Разрешить отключение устройства;  Регистрировать подключение и отключение устройства. |
| Последовательные порты | Использовать заданные здесь настройки |
| Параллельные порты | Использовать заданные здесь настройки |
| Сменные диски | Наследовать настройки контроля от родительского объекта |
| Оптические диски | Наследовать настройки контроля от родительского объекта |
| Логические диски | Наследовать настройки контроля от родительского объекта |
| Физические диски | Наследовать настройки контроля от родительского объекта |
| Процессоры | Наследовать настройки контроля от родительского объекта |
| Оперативная память | Наследовать настройки контроля от родительского объекта |
| Системная плата | Наследовать настройки контроля от родительского объекта |
| Сетевые платы | Наследовать настройки контроля от родительского объекта |
| Аппаратная поддержка | Наследовать настройки контроля от родительского объекта |
| **Устройства USB** | Задать настройки контроля;  Разрешить подключение устройства;  Разрешить отключение устройства;  Регистрировать подключение и отключение устройства. |
| Звук | Наследовать настройки контроля от родительского объекта |
| Соединения | Наследовать настройки контроля от родительского объекта |
| Устройства интерфейса с пользователем | Наследовать настройки контроля от родительского объекта |
| Мониторинг | Наследовать настройки контроля от родительского объекта |
| Аппаратный интерфейс | Наследовать настройки контроля от родительского объекта |
| Устройства захвата изображений | Наследовать настройки контроля от родительского объекта |
| Принтер | Наследовать настройки контроля от родительского объекта |
| Хранение данных | Наследовать настройки контроля от родительского объекта |
| Универсальный концентратор для USB | Наследовать настройки контроля от родительского объекта |
| Управление данными | Наследовать настройки контроля от родительского объекта |
| Микросхема(Смарт-карта) | Наследовать настройки контроля от родительского объекта |
| Устройства защиты данных | Наследовать настройки контроля от родительского объекта |
| Видео | Наследовать настройки контроля от родительского объекта |
| Диагностические устройства | Наследовать настройки контроля от родительского объекта |
| Контроллер беспроводного доступа | Наследовать настройки контроля от родительского объекта |
| Определяемые приложением | Наследовать настройки контроля от родительского объекта |
| Прочие | Наследовать настройки контроля от родительского объекта |
| **Устройства PCMCI** | Задать настройки контроля;  Разрешить подключение устройства;  Разрешить отключение устройства;  Регистрировать подключение и отключение устройства. |
| Многофункциональное устройство | Наследовать настройки контроля от родительского объекта |
| Память | Наследовать настройки контроля от родительского объекта |
| Последовательные Порты | Наследовать настройки контроля от родительского объекта |
| Параллельные Порты | Наследовать настройки контроля от родительского объекта |
| Физические диски | Наследовать настройки контроля от родительского объекта |
| Видео | Наследовать настройки контроля от родительского объекта |
| Сетевые платы | Наследовать настройки контроля от родительского объекта |
| AIMS | Наследовать настройки контроля от родительского объекта |
| SCSI | Наследовать настройки контроля от родительского объекта |
| Устройства защиты данных | Наследовать настройки контроля от родительского объекта |
| Прочие | Наследовать настройки контроля от родительского объекта |
| **Устройства IEEE1394** | Задать настройки контроля;  Разрешить подключение устройства;  Разрешить отключение устройства;  Регистрировать подключение и отключение устройства. |
| Системные устройства | Наследовать настройки контроля от родительского объекта |
| Устройства SBP-2 | Наследовать настройки контроля от родительского объекта |
| Мультимедиа устройства | Наследовать настройки контроля от родительского объекта |
| Сетевые устройства | Наследовать настройки контроля от родительского объекта |
| Прочие | Наследовать настройки контроля от родительского объекта |
| **Устройства Secure Digital** | Задать настройки контроля;  Разрешить подключение устройства;  Разрешить отключение устройства;  Регистрировать подключение и отключение устройства. |
| Карточки памяти | Наследовать настройки контроля от родительского объекта |
| Прочие | Наследовать настройки контроля от родительского объекта |

Таблица 24. Параметры настройки защитных механизмов Secret Net 6

(Пуск → Панель управления → Управление Secret Net 6 → Защитные механизмы Secret Net)

|  |  |
| --- | --- |
| **Параметр** | **Значение** |
| Защитный механизм | Использование |
| Затирание данных | Включен |
| Контроль устройств | Включен |
| Полномочное управление доступом | Отключен |
| Замкнутая программная среда | Включен |
| Шифровать управляющий сетевой трафик | Отключен |

Таблица 25. Привилегии доменных групп в системе Secret Net 6

| **Группа** | **Привилегии** | **Значение** |
| --- | --- | --- |
| SecretNetAdmins | Просмотр информации ОУ | Включен |
| Выполнение оперативных команд | Включен |
| Архивирование журналов | Отключен |
| Auditors | Просмотр информации ОУ | Включен |
| Выполнение оперативных команд | Отключен |
| Архивирование журналов | Включен |
| SPOAdmins | Просмотр информации ОУ | Включен |
| Выполнение оперативных команд | Включен |
| Архивирование журналов | Отключен |

### Значения параметров СЗИ от НСД «Secret Net 7.6» для всех применяемых версий операционных систем Windows XP/7/2003/2008 (x32/x64)).

Таблица 26. Значения параметров ПО СЗИ от НСД Secret Net 7.6, общие для серверов и АРМ

| **Раздел/параметр групповой политики** | | **Значение** |
| --- | --- | --- |
| **Конфигурация Windows — Параметры безопасности — Параметры Secret Net — Настройки подсистем** | |  |
| Администрирование: Локальное оповещение об НСД | | включено |
| Вход в систему: Запрет вторичного входа в систему | | отключен |
| Вход в систему: Количество неудачных попыток аутентификации | | 3 |
| Вход в систему: Максимальный период неактивности до блокировки экрана | | Для серверов ТПК РАБИС-НП[[45]](#footnote-46), АРМ МИБ АС ЭКР 2.0 – отключена. Для остальных – 15 минут |
| Вход в систему: Разрешить интерактивный вход только доменным пользователям | | отключена |
| Вход в систему: Реакция на изъятие идентификатора | | нет |
| Вход в систему: Режим аутентификации пользователя | | стандартная аутентификация |
| Вход в систему: Режим идентификации пользователя | | Только по идентификатору |
| Журнал: Максимальный размер журнала системы защиты | | 50494 Кб |
| Журнал: Политика перезаписи событий | | Затирать события по мере необходимости |
| Затирание данных: Количество циклов затирания конфиденциальной информации | | 0 (отключено) |
| Затирание данных: Количество циклов затирания на локальных дисках | | 1 (0 - для АРМ Администратора модификаций АС ЭКР 2.0) |
| Затирание данных: Количество циклов затирания на сменных носителях | | 1 |
| Контроль печати: Маркировка документов | | отключена |
| Контроль печати: Перенаправление принтеров в RDP-подключениях | | запрещено |
| Контроль печати: Теневое копирование | | отключено для всех принтеров |
| Контроль приложений: Перенаправление буфера обмена в RDP-подключениях | | запрещено |
| Контроль приложений: Режим аудита | | аудит пользовательских приложений |
| Контроль устройств: Перенаправление устройств в RDP-подключениях | | Перенаправление COM-портов – запрещено только входящее,  Перенаправление LPT-портов – запрещено только входящее,  Перенаправление дисков – запрещено только входящее,  Перенаправление устройств Plug and Play – запрещено только входящее. |
| Контроль устройств: Теневое копирование | | отключено для всех устройств |
| Полномочное управление доступом: Названия уровней конфиденциальности | | Не конфиденциально, Конфеденциально, Строго конфиденциально |
| Полномочное управление доступом: Режим работы | | контроль потоков отключен |
| Теневое копирование: Размер хранилища | | размер:5%, автоматическая перезапись отключена |
| **Параметры Secret Net — Ключи пользователя** | |  |
| Максимальный срок действия ключа | | 360 дней |
| Минимальный срок действия ключа | | 30 дней |
| Предупреждение об истечении срока действия ключа | | 30 дней |
| **Параметры Secret Net — Привилегии** | |  |
| Дискреционное управление доступом: Управление правами доступа | | <имя\_домена>[[46]](#footnote-47)\SecretNetAdmin\_Forest, SecretNetAdmin\_Domain[[47]](#footnote-48), |
| Журнал: Просмотр журнала системы защиты | | <имя\_домена>\SecretNetAdmin\_Forest, SecretNetAdmin\_Domain,  <имя\_домена>\Auditors[[48]](#footnote-49),  <имя\_домена>\SPOAdmins[[49]](#footnote-50) |
| Журнал: Управление журналом системы защиты | | <имя\_домена>\Auditors, SecretNetAdmin\_Forest, SecretNetAdmin\_Domain |
| Замкнутая программная среда: Не действует | | <имя\_домена>\ SecretNetAdmin\_Forest, SecretNetAdmin\_Domain,  <имя\_домена>\SPOAdmins;  <имя\_домена>\ModifyAdmins[[50]](#footnote-51) |
| **Параметры Secret Net — Регистрация событий** | |  |
| Trust Access: Ошибка синхронизации учетной информации с Trust Access | | отключена |
| Trust Access: Синхронизация учетной информации с Trust Access | | отключена |
| Администрирование: Включена защитная подсистема | | включена |
| Администрирование: Добавлен пользователь | | включена |
| Администрирование: Изменен ключ пользователя | | включена |
| Администрирование: Изменен пароль пользователя | | включена |
| Администрирование: Изменены параметры действующей политики безопасности | | включена |
| Администрирование: Изменены параметры пользователя | | включена |
| Администрирование: Отключена защита для диска | | включена |
| Администрирование: Отключена защитная подсистема | | включена |
| Администрирование: Удален ключ пользователя | | включена |
| Администрирование: Удален пользователь | | включена |
| Администрирование: Установлена защита для диска | | включена |
| Вход/выход: Вход пользователя в систему | | включена |
| Вход/выход: Завершение работы пользователя | | включена |
| Вход/выход: Запрет входа пользователя | | включена |
| Вход/выход: Идентификатор не зарегистрирован | | включена |
| Вход/выход: Компьютер заблокирован системой защиты | | включена |
| Вход/выход: Компьютер разблокирован | | включена |
| Вход/выход: Ошибка выполнения функционального контроля | | включена |
| Вход/выход: Пароль пользователя не соответствует требованиям безопасности | | включена |
| Вход/выход: Пользователь возобновил сеанс работы на компьютере | | включена |
| Вход/выход: Пользователь приостановил сеанс работы на компьютере | | включена |
| Вход/выход: Система защиты инициировала блокировку сессии пользователя | | включена |
| Вход/выход: Успешное завершение функционального контроля | | включена |
| Дискреционное управление доступом: Доступ к файлу и каталогу | | отключена |
| Дискреционное управление доступом: Запрет доступа к файлу и каталогу | | отключена |
| Дискреционное управление доступом: Изменение прав доступа | | отключена |
| Замкнутая программная среда: Загрузка библиотеки | | включена |
| Замкнутая программная среда: Запрет загрузки библиотеки | | включена |
| Замкнутая программная среда: Запрет запуска программы | | включена |
| Замкнутая программная среда: Запрет исполнения неизвестного скрипта | | включена |
| Замкнутая программная среда: Запуск программы | | включена |
| Замкнутая программная среда: Исполнение скрипта | | включена |
| Контроль конфигурации: Выход из спящего режима | | включена |
| Контроль конфигурации: Изменены параметры устройства | | включена |
| Контроль конфигурации: Обнаружено новое устройство | | включена |
| Контроль конфигурации: Обнаружены изменения в процессе контроля аппаратной конфигурации | | включена |
| Контроль конфигурации: Переход в спящий режим | | включена |
| Контроль конфигурации: Успешное завершение контроля аппаратной конфигурации | | включена |
| Контроль конфигурации: Устройство удалено из системы | | включена |
| Контроль конфигурации: Утверждение аппаратной конфигурации компьютера | | включена |
| Контроль печати: Запрет печати конфиденциального документа | | отключена |
| Контроль печати: Запрет прямого обращения к принтеру | | отключена |
| Контроль печати: Начало печати документа | | отключена |
| Контроль печати: Начало печати экземпляра документа | | отключена |
| Контроль печати: Ошибка при печати документа | | отключена |
| Контроль печати: Ошибка при печати экземпляра документа | | отключена |
| Контроль печати: Печать документа | | отключена |
| Контроль печати: Сохранение копии напечатанного документа | | отключена |
| Контроль печати: Успешное завершение печати документа | | отключена |
| Контроль печати: Успешное завершение печати экземпляра документа | | отключена |
| Контроль приложений: Завершение процесса | | включена |
| Контроль приложений: Запуск процесса | | включена |
| Контроль целостности: Для ресурса отсутствует эталонное значение | | включена |
| Контроль целостности: Добавление учетной записи к заданию ЗПС | | включена |
| Контроль целостности: Изменение группы ресурсов | | включена |
| Контроль целостности: Изменение задания | | включена |
| Контроль целостности: Изменение задачи | | включена |
| Контроль целостности: Исправление ошибок в базе данных | | включена |
| Контроль целостности: Нарушение целостности ресурса | | включена |
| Контроль целостности: Начало обработки задания на контроль целостности | | включена |
| Контроль целостности: Обнаружено нарушение целостности при обработке задания | | включена |
| Контроль целостности: Ошибка при восстановлении ресурса по эталонному значению | | включена |
| Контроль целостности: Ошибка при открытии базы данных контроля целостности | | включена |
| Контроль целостности: Ошибка при принятии текущего значения ресурса в качестве эталонного | | включена |
| Контроль целостности: Ошибка при расчете эталона | | включена |
| Контроль целостности: Ошибка синхронизации локальной базы данных с центральной | | включена |
| Контроль целостности: Ресурс восстановлен по эталонному значению | | включена |
| Контроль целостности: Синхронизация локальной базы данных с центральной | | включена |
| Контроль целостности: Снятие задания КЦ с контроля | | включена |
| Контроль целостности: Создание группы ресурсов | | включена |
| Контроль целостности: Создание задания | | включена |
| Контроль целостности: Создание задачи | | включена |
| Контроль целостности: Текущее значение ресурса принято в качестве эталонного | | включена |
| Контроль целостности: Удаление группы ресурсов | | включена |
| Контроль целостности: Удаление задания | | включена |
| Контроль целостности: Удаление задачи | | включена |
| Контроль целостности: Удаление устаревших эталонных значений | | включена |
| Контроль целостности: Удаление учетной записи из задания ЗПС | | включена |
| Контроль целостности: Успешная проверка целостности ресурса | | включена |
| Контроль целостности: Успешное завершение задания на контроль целостности | | включена |
| Контроль целостности: Установка задания КЦ на контроль | | включена |
| Общие события: Информационное событие | | включена |
| Общие события: Несанкционированное действие | | включена |
| Общие события: Ошибка | | включена |
| Общие события: Предупреждение | | отключена |
| Общие события: Событие | | отключена |
| Полномочное управление доступом: Вывод конфиденциальной информации на внешний носитель | | отключена |
| Полномочное управление доступом: Доступ к конфиденциальному ресурсу | | отключена |
| Полномочное управление доступом: Запрет вывода конфиденциальной информации на внешний носитель | | отключена |
| Полномочное управление доступом: Запрет доступа к конфиденциальному ресурсу | | отключена |
| Полномочное управление доступом: Запрет изменения параметров конфиденциальности ресурса | | отключена |
| Полномочное управление доступом: Запрет перемещения конфиденциального ресурса | | отключена |
| Полномочное управление доступом: Изменение параметров конфиденциальности ресурса | | отключена |
| Полномочное управление доступом: Использование механизма исключений | | отключена |
| Полномочное управление доступом: Конфликт категорий конфиденциальности | | отключена |
| Полномочное управление доступом: Перемещение конфиденциального ресурса | | отключена |
| Полномочное управление доступом: Удаление конфиденциального ресурса | | отключена |
| Разграничение доступа к устройствам: Доступ к устройству | | включена |
| Разграничение доступа к устройствам: Запрет доступа к устройству | | включена |
| Разграничение доступа к устройствам: Запрет подключения устройства | | включена |
| Разграничение доступа к устройствам: Несанкционированное отключение устройства | | включена |
| Разграничение доступа к устройствам: Отключение устройства | | включена |
| Разграничение доступа к устройствам: Подключение устройства | | включена |
| Расширение групповой политики: Групповые политики успешно применены | | включена |
| Расширение групповой политики: Ошибка применения групповых политик | | включена |
| Расширение групповой политики: Предупреждение при применении групповых политик | | включена |
| Сеть: Запрет сетевого подключения под другим именем | | включена |
| Служба репликации: Ошибка создания контекста пользователя | | включена |
| Теневое копирование: Завершена запись на сменный диск | | отключена |
| Теневое копирование: Завершена запись образа CD/DVD/BD | | отключена |
| Теневое копирование: Запрет записи на сменный диск | | отключена |
| Теневое копирование: Запрет записи образа CD/DVD/BD | | отключена |
| Теневое копирование: Начата запись на сменный диск | | отключена |
| Теневое копирование: Начата запись образа CD/DVD/BD | | отключена |
| Теневое копирование: Ошибка записи на сменный диск | | отключена |
| Теневое копирование: Ошибка записи образа CD/DVD/BD | | отключена |
| ЦУ КЦ-ЗПС: Добавление субъекта | | включена |
| ЦУ КЦ-ЗПС: Добавление учетной записи к заданию ЗПС | | включена |
| ЦУ КЦ-ЗПС: Изменение группы ресурсов | | включена |
| ЦУ КЦ-ЗПС: Изменение задания | | включена |
| ЦУ КЦ-ЗПС: Изменение задачи | | включена |
| ЦУ КЦ-ЗПС: Изменение субъекта | | включена |
| ЦУ КЦ-ЗПС: Снятие задания КЦ с контроля | | включена |
| ЦУ КЦ-ЗПС: Создание группы ресурсов | | включена |
| ЦУ КЦ-ЗПС: Создание задания | | включена |
| ЦУ КЦ-ЗПС: Создание задачи | | включена |
| ЦУ КЦ-ЗПС: Удаление группы ресурсов | | включена |
| ЦУ КЦ-ЗПС: Удаление задания | | включена |
| ЦУ КЦ-ЗПС: Удаление задачи | | включена |
| ЦУ КЦ-ЗПС: Удаление субъекта | | включена |
| ЦУ КЦ-ЗПС: Удаление учетной записи из задания ЗПС | | включена |
| ЦУ КЦ-ЗПС: Установка задания КЦ на контроль | | включена |
| **Параметры Secret Net — Устройства** | |  |
| **Локальные устройства** | Устройство постоянно подключено к компьютеру (Блокировать компьютер при изменении устройства – Включено) | |
| Последовательные порты | Наследовать настройки контроля от родительского объекта | |
| Параллельные порты | Наследовать настройки контроля от родительского объекта | |
| Сменные диски | Подключение устройства запрещено | |
| Оптические диски | Подключение устройства запрещено[[51]](#footnote-52) | |
| Физические диски | Подключение устройства разрешено | |
| Процессоры | Наследовать настройки контроля от родительского объекта | |
| Оперативная память | Наследовать настройки контроля от родительского объекта | |
| Системная плата | Наследовать настройки контроля от родительского объекта | |
| Аппаратная поддержка | Устройство постоянно подключено к компьютеру (Блокировать компьютер при изменении устройства – Включено) | |
| Программно-реализуемые диски | Подключение устройства разрешено | |
| **Устройства USB** | Подключение устройства запрещено | |
| Сетевые платы и модемы | Наследовать настройки контроля от родительского объекта | |
| Интерфейсные устройства (мышь, клавиатура, ИБП и др) | Подключение устройства разрешено | |
| Сканеры и цифровые фотоаппараты | Наследовать настройки контроля от родительского объекта | |
| Принтеры | Подключение устройства разрешено | |
| Устройства хранения | Наследовать настройки контроля от родительского объекта[[52]](#footnote-53) | |
| Bluetooth адаптеры | Наследовать настройки контроля от родительского объекта | |
| Сотовые телефоны (Смартфоны, КПК) | Наследовать настройки контроля от родительского объекта | |
| Электронные идентификаторы и считыватели | Наследовать настройки контроля от родительского объекта | |
| Прочие | Подключение устройства разрешено[[53]](#footnote-54) | |
| **Устройства PCMCI** | Подключение устройств запрещено | |
| Последовательные Порты и модемы | Наследовать настройки контроля от родительского объекта | |
| Параллельные Порты |
| Устройства хранения |
| Сетевые платы |
| Прочие |
| **Устройства IEEE1394** | Подключение устройств запрещено | |
| Устройства хранения | Наследовать настройки контроля от родительского объекта | |
| Принтеры |
| Сканеры и цифровые фотоаппараты |
| Сетевые устройства |
| Цифровые видеокамеры |
| Прочие |
| **Устройства Secure Digital** | Подключение устройств запрещено | |
| Карточки памяти | Наследовать настройки контроля от родительского объекта | |
| **Сеть** | Устройство постоянно подключено к компьютеру. | |
| Соединение Ethernet | Наследовать настройки контроля от родительского объекта | |
| Беспроводное соединение (WiFi) | Подключение устройств запрещено | |
| Соединение Bluetooth | Подключение устройств запрещено | |
| Соединение 1394 (FireWire) | Подключение устройств запрещено | |
| Инфракрасное соединение (IrDA) | Подключение устройств запрещено | |
| **Параметры Secret Net - Принтеры** | | |
| Настройки по умолчанию | Категория конфиденциальности - Любой категории конфиденциальности | |

Таблица 27. Параметры настройки защитных механизмов Secret Net 7

(Пуск → Панель управления → Управление Secret Net 7 → Защитные механизмы Secret Net)

|  |  |
| --- | --- |
| **Параметр** | **Значение** |
| Защитный механизм | Использование |
| Затирание данных | Включен |
| Контроль устройств | Включен |
| Полномочное управление доступом | Отключен |
| Замкнутая программная среда | Включен |
| Контроль печати | Отключен |
| Шифровать управляющий сетевой трафик | Отключен |
| Дискреционное управление доступом | Отключен |

Общие рекомендации по установке клиента «Secret Net» 7.6:

* защитный механизм Secret Net 7.6 "Защита дисков" не устанавливать;
* после завершения установки на АРМ клиента «Secret Net» 7.6, в оснастке Панели управления "Установка и удаление программ" удалить ПО "Windows Search".

**Примечание**: удаление выполняется только для ОС Windows XP/2003. При возникновении ошибок инициализации защитных подсистем Secret Net при загрузке ОС на СВТ (после удаления) требуется выполнить повторный запуск инсталляции Secret Net в режиме исправления ошибок).

### Построение модели замкнутой программной среды (ЗПС) и контроля целостности (КЦ)

Настройка механизма ЗПС и КЦ выполняется централизовано из программы "Контроль программ и данных (централизованный режим)" в несколько этапов:

* с помощью ручного метода сценариев формируются задачи ЗПС ресурсов (или групп ресурсов), которые описываются в редакторе сценария,
* создаются задания ЗПС и к ним добавляются задачи ЗПС,
* создаются задания КЦ и к ним добавляются задачи КЦ,
* субъектам "компьютер" назначаются задания ЗПС и КЦ.

ПО СЗИ от НСД «Secret Net» версий 6.5 и 7.6 располагает централизованным способом настройки механизма ЗПС и КЦ. Для централизованной настройки используется программа «Контроль программ и данных (централизованный режим)». Задания ЗПС и КЦ создаются добавлением к ним задач ручным методом сценариев, при этом для ресурсов, расположенных локально на АРМ, создаются нетиражируемые задания, для ресурсов, расположенных на серверах в локальной вычислительной сети, создаются тиражируемые задания. Задания ЗПС назначаются субъектам "компьютер" ("группа" компьютеров). Для централизованной настройки механизма ЗПС и контроля целостности используются одни и те же ресурсы и группы ресурсов. В таблицах (Таблица 28 – Таблица 30) приведены наименования параметров для SecretNet версии 7.6. Для версии 6.5 имеются отличия: параметр «Подготовить для ЗПС» именуется «Вместе с зависимыми модулями».

С целью запрета возможности запуска стандартного средства ОС Windows "Проводник" при двойном клике мыши на пункте меню ОС Windows "Пуск – Программы", в системном реестре рекомендуется удалить ключ [HKEY\_CLASSES\_ROOT\Folder\shell\open\command] (Только для Windows XP, для Windows 7 не применять).

В случае появления после настройки ЗПС на СВТ событий НСД в программе "Монитор" средства управления СЗИ от НСД «SecretNet», необходимо выяснить к запуску какого ПО относятся данные события НСД. Для разрешения запуска этого ПО на СВТ дополнительно в программе «Контроль программ и данных (централизованный режим)»:

* создать задачу, сформировав ее ручным методом сценариев, описав в ней разрешённые к загрузке ресурсы данного ПО, используя данные журнала НСД на СВТ;
* создать нетиражируемое задание, добавить в него созданную задачу;
* субъекту "компьютер" назначить созданное задание ЗПС.

Контроль целостности файлов производится в режиме «по расписанию» при загруженной ОС.

### Модель ЗПС для 32-х разрядных операционных систем Windows XP/7

Таблица 28. Задания/задачи ЗПС

| **Наименование контролируемых ресурсов** | | **Тип** | | **Каталоги/Путь/Имя** | | **Игнорировать объекты реестра(И), Рекурсия(Р)/Подготовить для ЗПС (П)** | | **Файлы/Переменные** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Задание ЗПС для ОС и СЗИ (нетиражируемое)- СЗИ Secret Net 7 (задача) | | | | | | | | |
| Ресурсы задачи приведены в таблице (Таблица 30) | | | | | | | | |
| Задание ЗПС для ОС и СЗИ (нетиражируемое) - MS Windows: основные ресурсы (задача) | | | | | | | | |
| Файловые ресурсы задачи приведены в Таблице (Таблица 29) | | | | | | | | |
| Задание ЗПС для KES10 (нетиражируемое) – KES10 (задача по сценарию) | | | | | | | | |
| KES10 | | Установленные программы (MSI) | | \*Kaspersky Endpoint Security 10\* | | И/П | | \*.dll;\*.ppl;\*.com;\*.exe;\*.tbp;\*.sys |
| Agent | | Установленные программы (MSI) | | \*Агент администрирования Kaspersky\* | | И/П | | \*.exe;\*.dll |
| Задание ЗПС для DRWEB (нетиражируемое) – DRWEB 10 (задача) | | | | | | | | |
| Исполняемые модули DRWEB | Файлы по каталогу | | C:\Program Files\DrWeb | | -/П | | \*.exe;\*.dll | |
| Задание ЗПС для СКАД Сигнатура 5 (нетиражируемое) - СКАД Сигнатура 5 (задача) | | | | | | | | |
| Исполняемые модули СКАД Сигнатура | Установленные программы (MSI) | | \*СКАД Сигнатура\* | | -/П | | \*.exe;\*.dll | |
| Validata | Каталоги с файлами | | c:\Program Files\Validata\VDCSP | | -/П | | \*.exe;\*.dll | |
| env\_util\_hashfile | Файлы по каталогу | | c:\Program Files\mdprei\spki | | -/П | | env\_util.exe;  hashfile.exe | |
| Задание ЗПС для Паспорт 12 (нетиражируемое) – ПК Паспорт 12 (задача) | | | | | | | | |
| spchange | Файлы по каталогу | | c:\Program Files\Passport | | -/П | | \*.exe;\*.dll | |
| Задание ЗПС для Паспорт на Server (нетиражируемое)– Группа ресурсов для Паспорт на Server (задача) | | | | | | | | |
| Passport | Каталоги с файлами | | c:\Program Files\Passport | | -/П | | \*.exe;\*.dll | |
| Задача ЗПС для eToken PKI (нетиражируемое) – eToken PKI (задача) | | | | | | | | |
| Исполняемые модули | Установленные программы (MSI) | | \*eToken PKI\* | | -/П | | \*.exe;\*.dll | |
| dll | Каталоги с файлами | | c:\Program Files\Aladdin\eToken\PKIClient\x32 | | Р/П | | \*.dll | |
| PKIMonitor | Файлы по каталогу | | c:\Program Files\Aladdin\eToken\PKIClient\x32 | | -/П | | PKIMonitor.exe | |
| Задание ЗПС для JAVA (нетиражируемое) – JAVA 6 (задача) | | | | | | | | |
| Исполняемые модули | Установленные программы (MSI) | | Java\* | | -/П | | \*.exe;\*.dll | |
| Доп.модули | Файлы по каталогу | | c:\Program Files\Java\jre6\bin | | -/П | | \*.exe;\*.dll | |
| Задание ЗПС для JAVA (нетиражируемое) – Журнал JAVA 6 (группа ресурсов) | | | | | | | | |
|  |  | | c:\Program Files\Java\jre6\bin\client\ | |  | | jvm.dll | |
|  |  | | c:\Program Files\Java\jre6\lib\deploy\jqs\ie\ | |  | | jqs\_plugin.dll | |
|  |  | | c:\Program Files\Common Files\Java\Java update\ | |  | | jusched.exe | |
|  |  | | c:\Program Files\Common Files\Java\Java update\ | |  | | jaucheck.exe | |
| Задание ЗПС для печати (нетиражируемое) – Печать РАБИС-НП (задача) | | | | | | | | |
| Исполняемые модули | Каталоги с файлами | | %SystemRoot%\system32\spool\drivers\w32x86\ | | Р/П | | \*.dll;\*.exe | |
| Задание ЗПС старт ЛТС (нетиражируемое) – Локальный запуск ЛТС (задача) | | | | | | | | |
| Доп.модули | Каталоги с файлами | | c:\Program Files\Common Files\system | | Р/П | | \*.dll;\*.rll | |
| kernel\bpldll | Файлы по каталогу | | d:\rabis-np\kernel\bpldll | | -/П | | \*.dll;\*.bpl | |
| xpress,load | Файлы по каталогу | | d:\rabis-np\kernel | | -/П | | xpress.exe;  load.exe | |
| start\_lts | Файлы по каталогу | | d:\rabis-np\xpress\config\ | | -/П | | start\_lts.bat | |
| kernel | Файлы по каталогу | | d:\rabis-np\kernel | | -/П | | \*.ovl | |
| Задание ЗПС старт ЛТС (нетиражируемое) – Журнал РАБИС-НП (локальный запуск) (группа ресурсов) | | | | | | | | |
|  |  | | d:\rabis-np\kernel\bpldll\ | |  | | Rar.exe | |
| Задание ЗПС для РАБИС-НП на SERVER (тиражируемое) – Группа ресурсов РАБИС-НП на SERVER (группа ресурсов).  Прмечание: Ресурсы добавляются не через сценарии, а вручную по указанным маскам файлов. | | | | | | | | |
|  |  | | \\SERVER\Rabis-np\kernel\ | |  | | \*.exe;\*.ovl;\*.bat | |
|  |  | | \\ SERVER\Rabis-np\tools\ | |  | | \*.exe;\*.dll;\*.bat | |
|  |  | | \\ SERVER\Rabis-np\xpress\config\ | |  | | \*.bat | |
|  |  | | \\ SERVER\Rabis-np\kernel\bpldll\ | |  | | \*.dll;\*.bpl | |
|  |  | | \\ SERVER\Rabis-np\kernel\bpldll\ | |  | | rar.exe  vcl35.ru | |
| Задание ЗПС для РАБИС-НП на SERVER (нетиражируемое) – Задача РАБИС-НП на SERVER | | | | | | | | |
| Дополнительные модули | Каталоги с файлами | | c:\Program Files\Common Files\system | | Р/П | | \*.dll;\*.rll | |
| Задание ЗПС для АС ЭКР 2.0 (тиражируемое) - АС ЭКР 2.0 (группа ресурсов) | | | | | | | | |
| Модули клиентской части | Файлы по каталогу | | \\Server\arm\asekr2\asekr\_rcp\_client2,  \\Server\arm\asekr2\dll, | | Р/П | | \*\*.dll;\*.exe | |
| Дополнительные модули для взаимодействия с ТСД | Файлы по каталогу | | C:\Windows\WindowsMobile\  C:\Program Files\Microsoft ActiveSync\ | | Р/П | | \*.exe;\*.dll | |
| Задание ЗПС для АС ЭКР 2.0 (нетиражируемое) - АС ЭКР 2.0 дополнительные модули (группа ресурсов) | | | | | | | | |
| Дополнительные модули |  | | Файлы, согласно приложению 12 документа «ЦБРФ.4257101.521-01 90 08-1. Типовая автоматизированная система эмиссионных и кассовых работ в трехзвенной архитектуре (АС ЭКР 2.0). Руководство по установке и настройке» | | -/П | |  | |
| Задание ЗПС для Altiris (нетиражируемое) – Группа ресурсов для Altiris | | | | | | | | |
|  |  | | %SystemRoot%\system32\ | |  | | AmInit32.dll | |
|  |  | | %SystemRoot%\system32\ | |  | | AeXSystemPerformance.dll | |
|  |  | | c:\Program Files\Altiris\Altiris Agent\Application Metering Agent\ | |  | | AmAgent.dll | |
|  |  | | c:\Windows\WinSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_x-ww\_31a54e43\ | |  | | msvcm90.dll | |
|  |  | | c:\Windows\WinSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_x-ww\_31a54e43\ | |  | | msvcp90.dll | |
|  |  | | c:\Windows\WinSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_x-ww\_31a54e43\ | |  | | msvcr90.dll | |
| Задание ЗПС для Altiris (нетиражируемое) – Altiris (задача) | | | | | | | | |
| Altiris Agent | Каталоги с файлами | | c:\Program Files\Altiris\Altiris Agent | | Р/П | | \*.exe;\*.dll | |
| Common Files | Файлы по каталогу | | c:\Program Files\Common Files\Altiris | | -/- | | \*.dll | |
| Задание ЗПС для ЭЛФОР на SERVER (нетиражируемое) – ЭЛФОР (задача)  **Примечание**: Приведены параметры задания ЗПС при функционировании ПО ЭЛФОР под ОС Windows 7 64-разрядной. | | | | | | | | |
| dll1 | Файлы по каталогу | | c:\Program Files (x86)\sybase\dddk8\deployment dlls | | -/П | | \*.dll | |
| dll2 | Файлы по каталогу | | c:\Program Files (x86)\sybase\shared\merantodbc | | -/П | | \*.dll | |
| assembly | Каталоги с файлами | | c:\windows\assembly | | Р/П | | \*.dll | |
| Задание ЗПС для ЭЛФОР на SERVER (нетиражируемое) – ЭЛФОР (группа ресурсов) | | | | | | | | |
|  |  | | c:\windows\ | |  | | splwow64.exe | |
|  |  | | c:\windows\Microsoft.Net\assembly\GAC\_64\CustomMarshalers\v4.0\_4.0.0.0\_b03f5f7f11d50a3a\ | |  | | CustomMarshalers.dll | |
| Задание ЗПС для ЭЛФОР на SERVER (тиражируемое) – Группа ресурсов ЭЛФОР на SERVER (группа ресурсов) | | | | | | | | |
|  |  | | \\Server\hellarc\modif\ | |  | | \*.exe;\*.dll | |
|  |  | | \\Server\hellarc\ARM\ | |  | | \*.exe;\*.dll | |
|  |  | | \\Server\hellarc\ARM\plg\ | |  | | \*.exe;\*.dll;\*.plg | |
|  |  | | \\Server\hellarc\ARM\hviewer\ | |  | | \*.exe;\*.dll | |
|  |  | | \\Server\hellarc\ARM\efrburn\ | |  | | \*.exe | |
| Задание ЗПС для Криптоцентр-авизо (нетиражируемое) – Криптоцентр-авизо (задача) | | | | | | | | |
| Исп.модуль | Каталог с файлами | | c:\program files\ancort\cryptocenter-avizo | | -/П | | \*.exe;\*.dll | |
| Доп.модуль 1 | Файлы по каталогу | | c:\program files\microsoft office\office | | -/П | | osa.exe | |
| Доп.модуль 2 | Файлы по каталогу | | c:\program files\common files\microsoft shared\dao | | -/П | | dao350.dll | |
| Задание ЗПС для ЕСМИБ ТУ – Агент ОС Windows (задача) | | | | | | | | |
| Исполняемые модули | Файлы по каталогу | | c:\Windows\AGENT | | Р/П | | \*.exe, \*.dll | |
| Агентская платформа | Файлы по каталогу | | C:\Program Files\Crystall\Misc\AgentPlatform | | Р/П | | \*.exe, \*.dll | |
| Задание ЗПС для ЕСМИБ ТУ – Облегченный агент ОС Windows (задача) | | | | | | | | |
| Исполняемые модули | Файлы по каталогу | | C:\Program Files\Crystall\ZObserver\Agents\\* | | Р/П | | \*.exe, \*.dll | |
| Агентская платформа | Файлы по каталогу | | C:\Program Files\Crystall\Misc\AgentPlatform | | Р/П | | \*.exe, \*.dll | |
| Задание ЗПС ЕСМИБ ТУ – МБ (задача) | | | | | | | | |
| Исполняемые модули | Файлы по каталогу | | C:\Program Files\Crystall\ZObserver | | Р/П | | \*.exe, \*.dll | |
| Вспомогательные библиотеки | Файлы по каталогу | | C:\Program Files\Crystall\Common | | Р/П | | \*.dll | |
| Задание ЗПС для ЕСМИБ ТУ – ПО обработки и идентификации КСИБ | | | | | | | | |
| Службы и веб-сервисы | Файлы по каталогу | | C:\Program Files\Crystall | | Р/П | | \*.exe, \*.dll | |
| Net.Framework 4.0. | Файлы по каталогу | | C:\Windows\Microsoft.NET  C:\Windows\assembly | | Р/П | | \*.exe, \*.dll | |
| InternetInformationServices | Файлы по каталогу | | c:\Windows\System32\inetsrv\ | | Р/П | | \*.exe, \*.dll, \*.msc | |
| Задание ЗПС для ЕСМИБ ТУ – ПО АРМ персонала системы (задача) | | | | | | | | |
| Исполняемые модули | Файлы по каталогу | | C:\Program Files\Crystall\SecAdmin Workshop | | Р/П | | \*.exe, \*.dll, \*.bat | |
| Вспомогательные библиотеки | Файлы по каталогу | | C:\Program Files\Crystall\Common | | Р/П | | \*.dll, \*.rll | |
| Интернет-браузер | Файлы по каталогу | | C:\Program Files\Internet Explorer | | Р/П | | \*.exe, \*.dll | |
| Microsoft Silverlight | Установленные программы | | \*Microsoft Silverlight\* | | Р/П | | \*.exe, \*.dll | |
| Клиентские библиотеки | Файлы по каталогу | | %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files (для ОС Windows 7)  C:\Documents and Settings (для ОС Windows XP) | | Р/П | | \*.xap | |
| Задание ЗПС для ЕСМИБ ТУ – Утилиты (задача) | | | | | | | | |
| Исполняемые модули | Файлы по каталогу | | C:\Program Files\Crystall\Misc | | Р/П | | \*.exe, \*.dll | |
| Вспомогательные библиотеки | Файлы по каталогу | | C:\Program Files\Crystall\Common | | Р/П | | \*.dll | |
| Задание ЗПС для ЕСМИБ ТУ – ЕСМИБ по журналу (группа ресурсов) | | | | | | | | |
|  |  | | С:\Windows\System32\WindowsPowershell\v1.0\ | |  | | pwrshsip.dll | |
|  | |  | |  | |  | |  |

**Примечание**: Перечень заданий и задач, приведенных в таблице (Таблица 28), не является окончательным и зависит от условий функционирования ТПК РАБИС-НП, АС ЭКР 2.0 и связанного с ним ПО в конкретном ТУ.

Таблица 29. Ресурсы для основных ресурсов компьютера – задача MS Windows

| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги/Путь** | **Рекурсия(Р)/**  **Подготовить для ЗПС (П)** | **Файлы/Переменные** |
| --- | --- | --- | --- | --- |
| Модули в каталоге Windows | Файлы по каталогу | %SystemRoot%\ | -/П | explorer.exe |
| Модули в каталоге System32 | Файлы по каталогу | %SystemRoot%\System32\ | -/П | \*.exe;\*.dll;\*.cpl,  \*.drv;\*.sys;\*.ocx,  \*.vbs;\*.scr;\*.rll,  \*.ime;\*.bpl;\*.ax,  \*.acm;\*.ppl |
| WinSXS | Файлы по каталогу | %SystemRoot%\WinSxS | Р/П | \*.dll |
| PowerShell | Файлы по каталогу | %SystemRoot%\System32\windowspowershell | Р/П | \*.dll |
| apppatch | Файлы по | %SystemRoot%\apppatch | Р/П | \*.dll |
| ime | Файлы по каталогу | %SystemRoot%\ime | Р/П | \*.dll |
| Manifest | Файлы по каталогу | %SystemRoot%\ | -/П | WindowsShell.Manifest |
| Модули, запускаемые при загрузке Windows | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx | Р/- | \* |
| Службы Windows | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services | Р/- | DependOnGroup;DependOnService;Group;ImagePath;Type |
| Active setup | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components | Р/- | \* |
| ShellServiceObjectDelayLoad | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad | Р/- | \* |
| ShellIconOverlayIdentifiers | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers | Р/- | (Default) |
| Classes\PROTOCOLS\Filter | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Filter | Р/- | CLSID |
| Classes\PROTOCOLS\Handler | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler | Р/- | CLSID |
| Extensions | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions | Р/- | \* |
| Print\Monitors | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors | Р/- | Driver |
| Utility Manager | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Accessibility\Utility Manager | Р/- | Application\* |
| BootExecute | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ |  | BootExecute |
| StartupPrograms | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\ |  | StartupPrograms |
| GinaDll | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon |  | GinaDll |
| AutoRun | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor |  | AutoRun |
| AlternateShell | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\ |  | AlternateShell |
| Common Startup | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\ |  | Common\* |
| Wbem | Файлы по каталогу | %SystemRoot%\System32\wbem | -/П | \*.exe;\*.dll |
| Запрет запуска cmd | Файлы по каталогу | %SystemRoot%\ system32 | Действие-Удалять | CMD.EXE[[54]](#footnote-55) |
| Запрет запуска 1 | Файлы по каталогу | %SystemRoot%\ | Действие-Удалять | hh.exe |
| Запрет запуска 2 | Файлы по каталогу | %SystemRoot%\ | Действие-Удалять | winhlp32.exe |
| Запрет запуска 3 | Файлы по каталогу | %SystemRoot%\ system32 | Действие-Удалять | winhlp32.exe |
| Запрет запуска 4 | Файлы по каталогу | %SystemRoot%\ | Действие-Удалять | notepad.exe |
| Запрет запуска 5 | Файлы по каталогу | %SystemRoot%\ system32 | Действие-Удалять | notepad.exe |

Таблица 30. Ресурсы основных ресурсов компьютера – задача СЗИ Secret Net.

| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги/Путь/Имя** | **Рекурсия(Р)/Подготовить для ЗПС (П)** | **Файлы/Переменные** |
| --- | --- | --- | --- | --- |
| Генерация задачи | Установленные программы (MSI) | Secret Net \* | -/П | \* |
| Службы Secret Net-FSManager | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\FSManager | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net-HWManager | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HWManager | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- Sn5CrPack | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Sn5CrPack | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- Sn5Crypto | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Sn5Crypto | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnAgent | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnAgent | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnCC0 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnCC0 | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnDaCs | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnDaCs | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnEFS | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnEFS | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnEraser | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnEraser | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnExeQuota | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnExeQuota | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnHwSrv | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnHwSrv | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnicheckService | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnicheckService | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnMC5xx | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnMC5xx | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnSrvService | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnSrvService | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnTmCard5 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnTmCard5 | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Исключаемые 1 | Каталоги с файлами | c:\program files\infosec\secretnet5\client\icheck | Действие-Удалять | \* |
| Исключаемые 2 | Каталоги с файлами | c:\program files\secret net\client\icheck | Действие-Удалять | \* |
| Исключаемые 3 | Каталоги с файлами | c:\program files\secret net\client\etalons | Действие-Удалять | \* |

### Модель контроля целостности файлов для 32-хразрядных операционных систем Windows XP/7

Для каждого СВТ рекомендуется создать два задания на контроль целостности ресурсов:

1. Задание на контроль целостности основных ресурсов компьютера (ПО ОС Windows и ПО СЗИ от НСД) должно включать в себя две задачи: "MS Windows: основные ресурсы" и "СЗИ Secret Net".

2. Задание на контроль целостности важных ресурсов ОС Windows должно включать в себя задачу "MS Windows: критичные ресурсы реестра".

В таблице (Таблица 31) приведены параметры создаваемых Заданий контроля целостности. Таблица 32 содержит перечень заданий контроля целостности.

Таблица 31. Параметры создаваемых Заданий контроля целостности

| **Наименование параметра задания на контроль целостности** | **Значения параметра задания на контроль целостности** |
| --- | --- |
| Тиражируемое | Отключен |
| Метод контроля ресурсов | Содержимое (для Задания на КЦ основных ресурсов компьютера),  Содержимое (для Задания на КЦ важных ресурсов системного реестра) |
| Алгоритм | CRC7 (для Задания на КЦ основных ресурсов компьютера),  Полное совпадение (для Задания на КЦ важных ресурсов системного реестра) |
| Успех завершения | Да |
| Ошибка завершения | Да |
| Успех проверки | Нет |
| Ошибка проверки | Да |
| Реакция на отказ | |
| Действия | Заблокировать компьютер |
| Расписание | |
| При загрузке ОС | Отключен |
| При входе | Отключен (для Задания на КЦ основных ресурсов компьютера),  Включен (для Задания на КЦ важных ресурсов системного реестра) |
| После входа | Отключен (для Задания на КЦ важных ресурсов системного реестра),  Включен (для Задания на КЦ основных ресурсов компьютера) |

Таблица 32. Перечень заданий контроля целостности

| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги/Путь/Имя** | **Игнорировать объекты реестра(И), Рекурсия(Р)/Подготовить для ЗПС (П)** | **Файлы/Переменные** |
| --- | --- | --- | --- | --- |
| Задание на КЦ основных ресурсов компьютера - MS Windows: основные ресурсы (задача) | | | | |
| Ресурсы задачи приведены в таблице (Таблица 29) | | | | |
| Задание на КЦ основных ресурсов компьютера – СЗИ Secret Net 7 (задача) | | | | |
| Ресурсы задачи приведены в таблице (Таблица 30) | | | | |
| Задание на КЦ важных ресурсов системного реестра Windows – MS Windows: критичные ресурсы реестра (задача) | | | | |
| Ресурсы задачи приведены в таблице (Таблица 33). | | | | |
| Задание на КЦ файлов ПО СКАД Сигнатура 5 – Файлы ПО СКАД Сигнатура 5 (группа ресурсов) | | | | |
|  |  | c:\Program Files\mdprei\spki\ (для 32-разрядных систем),  (c:\Program Files (x86)\Validata\VDCSP (для 64-разрядных систем) |  | hashfile.exe  Файл верификации (например, hash.out) |
| Задание на КЦ файлов ПО СКАД Сигнатура 5 – Задача КЦ эталона верификации Сигнатура 5 (задача) | | | | |
| signatura | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Validata\Hashfile | -/- | \*/\* |

Таблица 33. Контроль целостности критичных ресурсов системного реестра ОС Windows

| **Наименование контролируемых ресурсов** | **Тип** | **Путь/Имя** | **Рекурсия(Р)/Подготовить для ЗПС (П)** | **Файлы/Переменные** |
| --- | --- | --- | --- | --- |
| PackedCatalogItem | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol\_Catalog9\Catalog\_Entries | Р/- | PackedCatalogItem |
| KnownDlls | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ KnownDlls | Р/- | \* |
| Image File Execution Options | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options | Р/- | \* |
| Notify | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify | Р/- | Dllname |
| GPExtensions | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ GPExtensions | Р/- | Dllname |
| AppInit\_Dlls | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ |  | AppInit\_Dlls |
| Security Packages | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\ |  | Security\* |
| Notification Packages | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\ |  | Notification\* |
| Authentication Packages | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\ |  | Authentication\* |
| VmApplet | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | VmApplet |
| System | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | System |
| Shell | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon |  | Shell |
| Userinit | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | Userinit |
| Taskman | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | Taskman |
| UIhost | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | UIhost |
| SnIcon | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ |  | SnIcon |

### Модель ЗПС для 64-х разрядных операционных систем Windows XP/7

Таблица 34. Задания/задачи ЗПС (пример настройки для 64-разрядных операционных систем)

| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги/Путь/Имя** | **Игнорировать объекты реестра(И), Рекурсия(Р)/Подготовить для ЗПС (П)** | **Файлы/Переменные** | | |
| --- | --- | --- | --- | --- | --- | --- |
| Задание ЗПС для ОС и СЗИ (нетиражируемое) - СЗИ Secret Net (задача) | | | | | | |
| Ресурсы задачи приведены в таблице (Таблица 36) | | | | | | |
| Задание ЗПС для ОС и СЗИ (нетиражируемое) - MS Windows: основные ресурсы (задача) | | | | | | |
| Ресурсы задачи приведены в таблице (Таблица 35) | | | | | | |
| Задание ЗПС для KES10 (нетиражируемое) – KES10 (задача по сценарию) | | | | | | |
| KES10 | Установленные программы (MSI) | \*Kaspersky Endpoint Security 10\* | И/П | \*.dll;\*.ppl;\*.com;\*.exe;\*.tbp;\*.sys | | |
| Agent | Установленные программы (MSI) | \*Агент администрирования Kaspersky\* | И/П | \*.exe;\*.dll | | |
| Задание ЗПС для DRWEB (нетиражируемое) – DRWEB 10 (задача) | | | | | | |
| Исполняемые модули DRWEB | Файлы по каталогу | C:\Program Files\DrWeb | -/В | \*.exe;\*.dll | | |
| Задание ЗПС для СКАД Сигнатура 5 (нетиражируемое) - СКАД Сигнатура 5 (задача) | | | | | | |
| Исполняемые модули СКАД Сигнатура | Установленные программы (MSI) | \*СКАД Сигнатура\* | -/П | \*.exe;\*.dll | | |
| Validata | Файлы по каталогу | c:\Program Files (x86)\Validata\VDCSP | -/П | \*.exe;\*.dll | | |
| Validata2 | Файлы по каталогу | c:\Program Files\Validata\VDCSP | -/П | \*.exe;\*.dll | | |
| env\_util\_hashfile | Файлы по каталогу | c:\Program Files\mdprei\spki | -/П | env\_util.exe:  hashfile.exe | | |
| Задание ЗПС для Паспорт 12 (нетиражируемое) – ПК Паспорт 12 (задача) | | | | | | |
| spchange | Файлы по каталогу | spchange | -/П | \*.exe;\*.dll | | |
| Задание ЗПС для Паспорт на Server (нетиражируемое)– Группа ресурсов для Паспорт на Server (задача) | | | | | | |
| Passport | Каталоги с файлами | c:\Program Files\Passport | -/П | \*.exe;\*.dll | | |
| Задача ЗПС для eToken PKI (нетиражируемое) – eToken PKI (задача) | | | | | | |
| Исполняемые модули | Установленные программы (MSI) | \*eToken PKI\* | -/П | \*.exe;\*.dll | | |
| dll | Каталоги с файлами | c:\Program Files\Aladdin\eToken\PKIClient\x64 | Р/П | \*.dll | | |
| PKIMonitor | Файлы по каталогу | c:\Program Files\Aladdin\eToken\PKIClient\x64 | -/П | PKIMonitor.exe | | |
| Задание ЗПС для JAVA (нетиражируемое) – JAVA 6 (задача) | | | | | | |
| Исполняемые модули | Установленные программы (MSI) | Java\* | -/П | \*.exe;\*.dll | | |
| Доп. модули | Файлы по каталогу | c:\Program Files (x86)\Java\jre6\bin | -/П | \*.exe;\*.dll | | |
| Задание ЗПС для JAVA (нетиражируемое) – Журнал JAVA 6 (группа ресурсов) | | | | | | |
|  |  | c:\Program Files (x86)\Java\jre6\bin\client\ |  | jvm.dll | | |
|  |  | c:\Program Files (x86)\Java\jre6\lib\deploy\jqs\ie\ |  | jqs\_plugin.dll | | |
|  |  | c:\Program Files (x86)\Common Files\Java\Java update\ |  | jusched.exe | | |
|  |  | c:\Program Files (x86)\Common Files\Java\Java update\ |  | jaucheck.exe | | |
| Задание ЗПС для печати (нетиражируемое) – Печать РАБИС-НП (задача) | | | | | | |
| Исполняемые модули | Каталоги с файлами | %SystemRoot%\system32\spool\drivers\ x64\3\ | Р/П | \*.dll;\*.exe | | |
| Задание ЗПС для Windows 7 (нетиражируемое) – Журнал Windows 7 (группа ресурсов)  **Примечание**: Приведены параметры задания ЗПС для Windows 7 64-разрядной (формируется по журналу НСД, в модель обязательно включаются библиотеки из каталога WinSxS, перечень которых определяется по журналу). | | | | | | |
|  |  | C:\Windows\winSxS\ amd64\_microsoft.vc90.mfcloc\_1fc8b3b9a1e18e3b\_9.0.30729.1\_none\_92995f253c01eddb\ |  | MFC90RUS.DLL | | |
|  |  | C:\Windows\winSxS\x86\_microsoft.windows.common-controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2\ |  | comctl32.dll | | |
|  |  | C:\Windows\winSxS\ amd64\_microsoft.windows.common-controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_fa396087175ac9ac\ |  | comctl32.dll | | |
|  |  | C:\Windows\winSxS\x86\_microsoft.vc90.mfcloc\_1fc8b3b9a1e18e3b\_9.0.30729.1\_none\_da4695fc507e16e1\ |  | MFC90RUS.DLL | | |
|  |  | C:\Windows\winSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_none\_50934f2ebcb7eb57 |  | msvcp90.dll | | |
|  |  | C:\Windows\AppPatch\ |  | AcLayers.dll | | |
|  |  | C:\Windows\AppPatch\ |  | acwow64.dll | | |
|  |  | C:\Windows\AppPatch\ |  | AcRes.dll | | |
|  |  | C:\Windows\AppPatch\ |  | AcGeneral.dll | | |
|  |  | C:\Windows\AppPatch\AppPatch64\ |  | AcGenrall.dll | | |
|  |  | C:\Windows\system32\wbem\ |  | wbemsvc.dll | | |
|  |  | C:\Windows\system32\wbem\ |  | fastprox.dll | | |
|  |  | C:\Windows\system32\wbem\ |  | wbemprox.dll | | |
|  |  | C:\Windows\SysWOW64\wbem\ |  | fastprox.dll | | |
|  |  | C:\Windows\SysWOW64\wbem\ |  | wbemprox.dll | | |
|  |  | C:\Windows\SysWOW64\wbem\ |  | wbemsvc.dll | | |
|  |  | C:\Program Files\Internet Explorer\ |  | ieproxy.dll | | |
|  |  | C:\Program Files (x86)\Internet Explorer\ |  | ieproxy.dll | | |
|  |  | C:\Windows\ |  | splwow64.exe | | |
| Задание ЗПС старт ЛТС (нетиражируемое) – Локальный запуск ЛТС (задача) | | | | | | |
| Доп. модули | Каталоги с файлами | c:\Program Files (x86)\Common Files\system | Р/П | \*.dll;\*.rll | | |
| kernel\bpldll | Файлы по каталогу | d:\rabis-np\kernel\bpldll | -/П | \*.dll;\*.bpl | | |
| xpress,load | Файлы по каталогу | d:\rabis-np\kernel | -/П | xpress.exe;  load.exe | | |
| start\_lts | Файлы по каталогу | d:\rabis-np\xpress\config | -/П | start\_lts.bat | | |
| kernel | Файлы по каталогу | d:\rabis-np\kernel | -/П | \*.ovl | | |
| Задание ЗПС для РАБИС-НП на SERVER (тиражируемое) – Группа ресурсов РАБИС-НП на SERVER (группа ресурсов).  Примечание: Ресурсы добавляются не через сценарии, а вручную по указанным маскам файлов. | | | | | | |
|  |  | \\SERVER\Rabis-np\kernel\ |  | | \*.exe;\*.ovl;\*.bat | |
|  |  | \\SERVER\Rabis-np\tools\ |  | | \*.exe;\*.dll;\*.bat | |
|  |  | \\SERVER\Rabis-np\xpress\config\ |  | | \*.bat | |
|  |  | \\SERVER\Rabis-np\kernel\bpldll\ |  | | \*.dll;\*.bpl | |
|  |  | \\SERVER\Rabis-np\kernel\bpldll\ |  | | rar.exe  vcl35.ru | |
| Задание ЗПС для РАБИС-НП на SERVER (нетиражируемое) – Задача РАБИС-НП на SERVER | | | | | |
| Дополнительные модули | Каталоги с файлами | c:\Program Files (x86)\Common Files\System | Р/П | | \*.dll;\*.rll | |
| Задание ЗПС для АС ЭКР 2.0 (тиражируемое)- АС ЭКР 2.0 (группа ресурсов) | | | | | | |
| Модули клиентской части | Файлы по каталогу | \\Server\arm\asekr2\asekr\_rcp\_client2,  \\Server\arm\asekr2\dll, | Р/П | | \*.dll;\*.exe | |
| Дополнительные модули для взаимодействия с ТСД | Файлы по каталогу | C:\Windows\WindowsMobile\  C:\Program Files\Microsoft ActiveSync\ | Р/П | | \*.exe;\*.dll | |
| Задание ЗПС для АС ЭКР 2.0 (нетиражируемое) - АС ЭКР 2.0 дополнительные модули (группа ресурсов) | | | | | | |
| Дополнительные модули |  | Файлы, согласно приложению 12 документа «ЦБРФ.4257101.521-01 90 08-1. Типовая автоматизированная система эмиссионных и кассовых работ в трехзвенной архитектуре (АС ЭКР 2.0). Руководство по установке и настройке» | -/П | |  | |
| Задание ЗПС для Altiris (нетиражируемое) – Группа ресурсов для Altiris | | | | | | |
|  |  | c:\Windows\SysWoW64\ |  | | AmInit32.dll | |
|  |  | c:\Windows\system32\ |  | | AmInit32.dll | |
|  |  | c:\Windows\SysWoW64\ |  | | AmInit64.dll | |
|  |  | c:\Windows\system32\ |  | | AmInit64.dll | |
|  |  | c:\Program Files\Altiris\Altiris Agent\Agents\ Application Metering Agent\ |  | | AmAgent.dll | |
|  |  | %SystemRoot%\system32\ |  | | AeXSystemPerformance.dll | |
|  |  | c:\Windows\WinSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_x-ww\_31a54e43\ |  | | msvsm90.dll | |
|  |  | c:\Windows\WinSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_x-ww\_31a54e43\ |  | | msvsp90.dll | |
|  |  | c:\Windows\WinSxS\x86\_microsoft.vc90.crt\_1fc8b3b9a1e18e3b\_9.0.30729.6161\_x-ww\_31a54e43\ |  | | msvsr90.dll | |
|  |  | c:\Program Files\Altiris\Altiris Agent\ |  | | AexAgentPages.dll | |
|  |  | c:\Program Files\Altiris\Altiris Agent\ |  | | AexAgentUI.dll | |
| Задание ЗПС для Altiris (нетиражируемое) – Altiris (задача) | | | | | | |
| Altiris Agent | Каталоги с файлами | c:\Program Files\Altiris\Altiris Agent | Р/П | | \*.exe;\*.dll | |
| Common Files | Файлы по каталогу | c:\Program Files\Common Files\Altiris | -/- | | \*.dll | |
| Задание ЗПС для ЭЛФОР на SERVER (нетиражируемое) – ЭЛФОР (задача)  **Примечание**: Приведены параметры задания ЗПС при функционировании ПО ЭЛФОР под ОС Windows 7 64-разрядной. | | | | | | |
| dll1 | Файлы по каталогу | c:\Program Files (x86)\sybase\dddk8\deployment dlls | -/П | | \*.dll | |
| dll2 | Файлы по каталогу | c:\Program Files (x86)\sybase\shared\merantodbc | -/П | | \*.dll | |
| assembly | Каталоги с файлами | c:\windows\assembly | Р/П | | \*.dll | |
| Задание ЗПС для ЭЛФОР на SERVER (нетиражируемое) – ЭЛФОР (группа ресурсов) | | | | | | |
|  |  | c:\windows\ |  | | splwow64.exe | |
|  |  | c:\wimdows\Microsoft.Net\assembly\GAC\_64\CustomMarshalers\v4.0\_4.0.0.0\_b03f5f7f11d50a3a\ |  | | CustomMarshalers.dll | |
|  |  | c:\Program Files\mdprei\spki\ |  | | spki1utl.exe | |
| Задание ЗПС для ЭЛФОР на SERVER (тиражируемое) – Группа ресурсов ЭЛФОР на SERVER (группа ресурсов) | | | | | | |
|  |  | \\Server\hellarc\modif\ |  | | \*.exe;\*.dll | |
|  |  | \\Server\hellarc\ARM\ |  | | \*.exe;\*.dll | |
|  |  | \\Server\hellarc\ARM\plg\ |  | | \*.exe;\*.dll;\*.plg | |
|  |  | \\Server\hellarc\ARM\hviewer\ |  | | \*.exe;\*.dll | |
|  |  | \\Server\hellarc\ARM\efrburn\ |  | | \*.exe | |
| Задание ЗПС для ЕСМИБ ТУ – Облегченный агент ОС Windows (задача) | | | | | | |
| Исполняемые модули | Файлы по каталогу | C:\Program Files\Crystall\ZObserver\Agents\\* | Р/П | | \*.exe, \*.dll | |
| Агентская платформа | Файлы по каталогу | C:\Program Files (x86)\Crystall\Misc\AgentPlatform | Р/П | | \*.exe, \*.dll | |
| Задание ЗПС ЕСМИБ ТУ – МБ (задача) | | | | | | |
| Исполняемые модули | Файлы по каталогу | C:\Program Files (x86)\Crystall\ZObserver | Р/П | | \*.exe, \*.dll | |
| Вспомогательные библиотеки | Файлы по каталогу | C:\Program Files (x86) \Crystall\Common | Р/П | | \*.dll | |
| Задание ЗПС для ЕСМИБ ТУ – ПО обработки и идентификации КСИБ | | | | | | |
| Службы и веб-сервисы | Файлы по каталогу | C:\Program Files (x86)\Crystall | Р/П | | \*.exe, \*.dll | |
| Net.Framework 4.0. | Файлы по каталогу | C:\Windows\Microsoft.NET  C:\Windows\assembly | Р/П | | \*.exe, \*.dll | |
| InternetInformationServices | Файлы по каталогу | c:\Windows\System32\inetsrv\ | Р/П | | \*.exe, \*.dll, \*.msc | |
| Задание ЗПС для ЕСМИБ ТУ – ПО АРМ персонала системы (задача) | | | | | | |
| Исполняемые модули | Файлы по каталогу | C:\Program Files (x86)\Crystall\SecAdmin Workshop | Р/П | | \*.exe, \*.dll, \*.bat | |
| Вспомогательные библиотеки | Файлы по каталогу | C:\Program Files (x86)\Crystall\Common | Р/П | | \*.dll, \*.rll | |
| Интернет-браузер | Файлы по каталогу | C:\Program Files\Internet Explorer | Р/П | | \*.exe, \*.dll | |
| Интернет-браузер | Файлы по каталогу | C:\Program Files (x86)\Internet Explorer | Р/П | | \*.exe, \*.dll | |
| Microsoft Silverlight | Установленные программы | \*Microsoft Silverlight\* | Р/П | | \*.exe, \*.dll | |
| Клиентские библиотеки | Файлы по каталогу | %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files (для ОС Windows 7)  C:\Documents and Settings (для ОС Windows XP) | Р/П | | \*.xap | |
| Задание ЗПС для ЕСМИБ ТУ – Утилиты (задача) | | | | | | |
| Исполняемые модули | Файлы по каталогу | C:\Program Files (x86)\Crystall\Misc | Р/П | | \*.exe, \*.dll | |
| Вспомогательные библиотеки | Файлы по каталогу | C:\Program Files (x86)\Crystall\Common | Р/П | | \*.dll | |
| Задание ЗПС для ЕСМИБ ТУ – ЕСМИБ по журналу (группа ресурсов) | | | | | | |
|  |  | С:\Windows\System32\WindowsPowershell\v1.0\ |  | | pwrshsip.dll | |

**Примечание**: Перечень заданий и задач, приведенных в таблице (Таблица 34), не является окончательным и зависит от условий функционирования ТПК РАБИС-НП, АС ЭКР 2.0 и связанного с ним ПО в конкретном ТУ.

Таблица 35. Задача "MS Windows: основные ресурсы"

| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги / Путь** | **Рекурсия (Р) / Подготовить для ЗПС (П)** | **Файлы / Переменные** |
| --- | --- | --- | --- | --- |
| Модули в каталоге Windows | Файлы по каталогу | %SystemRoot%\ | -/П | explorer.exe |
| Модули в каталоге System32 | Файлы по каталогу | %SystemRoot%\System32\ | -/П | \*.exe;\*.dll;\*.cpl,  \*.drv;\*.sys;\*.ocx,  \*.vbs;\*.scr;\*.rll,  \*.ime;\*.bpl;\*.ax,  \*.acm;\*.ppl |
| Модули в каталоге SysWOW64 | Файлы по каталогу | %SystemRoot%\SysWOW64\ | -/П | \*.exe;\*.dll;\*.cpl,  \*.drv;\*.sys;\*.ocx,  \*.vbs;\*.scr;\*.rll,  \*.ime;\*.bpl;\*.ax,  \*.acm;\*.ppl |
| Модули, запускаемые при загрузке оболочки Windows | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | Р/- | \* |
| Run WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run | Р/- | \* |
| Модули, запускаемые при загрузке оболочки Windows | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce | Р/- | \* |
| RunOnce WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce | Р/- | \* |
| Модули, запускаемые при загрузке оболочки Windows | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx | Р/- | \* |
| RunOnceEx WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx | Р/- | \* |
| Службы Windows | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services | Р/- | DependOnGroup;DependOnService;Group;ImagePath;Type |
| Active setup | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components | Р/- | \* |
| Active setup WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Active Setup\Installed Components | Р/- | \* |
| Shared Task Scheduler | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler |  |  |
| SharedTaskScheduler WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler |  |  |
| ShellServiceObjectDelayLoad | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad | Р/- | \* |
| ShellServiceObjectDelayLoad WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad | Р/- | \* |
| ShellExecuteHooks | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks |  |  |
| ShellExecuteHooks WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks |  |  |
| ShellIconOverlayIdentifiers | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers | Р/- | (Default) |
| ShellIconOverlayIdentifiers WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers | Р/- | (Default) |
| Shell Extension\Approved | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extension\Approved |  |  |
| Shell Extension\Approved WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\ Shell Extension\Approved |  |  |
| Classes\Folder\shellex\ColumnHandlers | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Folder\shellex\ColumnHandlers |  |  |
| Classes\Folder\shellex\ColumnHandlers WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Classes\Folder\shellex\ColumnHandlers |  |  |
| Classes\PROTOCOLS\Filter | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Filter | Р/- | CLSID |
| Classes\PROTOCOLS\Filter WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Classes\PROTOCOLS\Filter | Р/- | CLSID |
| Classes\PROTOCOLS\Handler | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler | Р/- | CLSID |
| Classes\PROTOCOLS\Handler WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Classes\PROTOCOLS\Handler | Р/- | CLSID |
| Browser Helper Object | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Object |  |  |
| Browser Helper Object WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Object |  |  |
| Extensions | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions | Р/- | \* |
| Extensions WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Internet Explorer\Extensions | Р/- | \* |
| Print\Monitors | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors | Р/- | Driver |
| Toolbar | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ |  |  |
| Toolbar WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ |  |  |
| Utility Manager | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility\Utility Manager | Р/- | Application\* |
| Utility Manager WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Accessibility\Utility Manager | Р/- | Application\* |
| BootExecute | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ |  | BootExecute |
| StartupPrograms | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\ |  | StartupPrograms |
| GinaDll | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon |  | GinaDll |
| GinaDll WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon |  | GinaDll |
| AutoRun | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Command Processor\ |  | AutoRun |
| AutoRun WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Command Processor\ |  | AutoRun |
| AlternateShell | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\ |  | AlternateShell |
| PendingFileRenameOperations | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\ |  | PendingFileRenameOperations |
| Common Startup | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\ |  | Common\* |
| Common Startup WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\ |  | Common\* |
| Services\_Start | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\seclogon\Start[[55]](#footnote-56) | Р/-, Действие-Удалять | \* |
| Запрет запуска 1 | Файлы по каталогу | %SystemRoot%\ | Действие-Удалять | hh.exe |
| Запрет запуска 2 | Файлы по каталогу | %SystemRoot%\ | Действие-Удалять | winhlp32.exe |
| Запрет запуска 3 | Файлы по каталогу | %SystemRoot%\ | Действие-Удалять | notepad.exe |
| Запрет запуска 4 | Файлы по каталогу | %SystemRoot%\system32 | Действие-Удалять | notepad.exe |
| Запрет запуска 5 | Файлы по каталогу | %SystemRoot%\SysWOW64 | Действие-Удалять | notepad.exe |
| Запрет запуска cmd | Файлы по каталогу | %SystemRoot%\system32,%SystemRoot%\sysWoW64 | Действие-Удалять | CMD.EXE**[[56]](#footnote-57)** |

Таблица 36. Ресурсы основных ресурсов компьютера – задача СЗИ Secret Net

| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги/Путь/Имя** | **Рекурсия(Р)/Подготовить для ЗПС (П)** | **Файлы/Переменные** |
| --- | --- | --- | --- | --- |
| Генерация задачи SN 7 | Установленные программы (MSI) | Secret Net\* | -/П | \* |
| Генерация задачи Secret Net Prequisites | Установленные программы (MSI) | Secret Net Prequisites | -/П | \* |
| Службы Secret Net-FSManager | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\FSManager | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net-HWManager | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HWManager | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- Sn5CrPack | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Sn5CrPack | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- Sn5Crypto | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Sn5Crypto | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnAgent | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnAgent | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnCC0 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnCC0 | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnDaCs | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnDaCs | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnEFS | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnEFS | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnEraser | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnEraser | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnExeQuota | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnExeQuota | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnHwSrv | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnHwSrv | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnicheckService | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnicheckService | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnMC5xx | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnMC5xx | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnSrvService | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnSrvService | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| Службы Secret Net- SnTmCard5 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnTmCard5 | Р/- | DependOnGroup;  DependOnService;  Group;ImagePath;  Start;Type |
| GroupPolicy | Каталоги с файлами | c:\Program Files\Secret Net\Client\GroupPolicy | Действие-Удалять | \* |

### Модель контроля целостности файлов для 64х разрядных операционных систем Windows XP/7

Настройка механизма производится в соответствии с разделом П3.3.2, с учетом таблиц (Таблица 34 – Таблица 36).

Особенности настройки задачи КЦ "MS Windows: критичные ресурсы реестра" приведены в таблице (Таблица 37):

Таблица 37. Задача КЦ "MS Windows: критичные ресурсы реестра"

| **Наименование контролируемых ресурсов** | **Тип** | **Путь/Имя** | **Рекурсия(Р)/Подготовить для ЗПС (П)** | **Файлы/Переменные** |
| --- | --- | --- | --- | --- |
| PackedCatalogItem | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol\_Catalog9\Catalog\_Entries | Р/- | PackedCatalogItem |
| KnownDlls | Ключи с переменными | HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\ KnownDlls | Р/- | \* |
| Image File Execution Options | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options | Р/- | \* |
| Image File Execution Options WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options | Р/- | \* |
| Notify | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify | Р/- | DllName |
| Notify WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify | Р/- | DllName |
| GPExtensions | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions | Р/- | DllName |
| GPExtensions WOW64 | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions | Р/- | DllName |
| Catalog\_Entries (ключ) | Ключи с переменными | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol\_Catalog9\Catalog\_Entries |  |  |
| AppInit\_Dlls | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ |  | AppInit\_Dlls |
| AppInit\_Dlls WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\ |  | AppInit\_Dlls |
| Security Packages | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ |  | Security\* |
| Notification Packages | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ |  | Notification\* |
| Authentication Packages | Переменные по ключу | HKEY\_L  OCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ |  | Authentication\* |
| VmApplet | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | VmApplet |
| VmApplet WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | VmApplet |
| System | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | System |
| System WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | System |
| Shell | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon |  | Shell |
| Shell WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon |  | Shell |
| Userinit | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | Userinit |
| Userinit WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | Userinit |
| Taskman | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | Taskman |
| Taskman WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | Taskman |
| UIhost | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | UIhost |
| UIhost WOW64 | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\ |  | UIhost |
| SnIcon | Переменные по ключу | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ |  | SnIcon |

### Разграничение доступа к каталогам и файлам, обеспечивающее защиту от подмены или модификации программного обеспечения

Разграничение доступа к каталогам и файлам, обеспечивающее защиту от подмены или модификации программного обеспечения обеспечивается применением двух способов:

* включение дополнительного параметра в механизме замкнутой программной среды «Secret Net» – «Проверять целостность модулей перед запуском» (контроль целостности запускаемых пользователем приложений);
* использование задания контроля целостности ресурсов "Задание на КЦ основных ресурсов компьютера" (Таблица 29 и Таблица 30) (контроль целостности основных файлов операционной системы Windows и ПО СЗИ от НСД «Secret Net»).

**Примечание**: Подмена или модификация ресурса, для которого выполнен расчет эталонного значения для ЗПС, делает невозможным запуск данного ресурса в "жёстком" режиме работы ЗПС. Об этом будут свидетельствовать записи об НСД в журнале событий НСД «Secret Net». Необходимо учитывать, что в "мягком" режиме работы ЗПС запуск подменённого или модифицированного ресурса блокироваться не будет.

### Настройки ОС на рабочих станциях и серверах (контроллерах домена) при использовании СЗИ от НСД «SecretNet» и «Аккорд» (при функционировании рабочих станций c ОС Windows XP/7 под управлением контроллеров домена c ОС Windows Server 2003

Ниже приведены рекомендованные настройки ОС на рабочих станциях.  Данные настройки, при необходимости,  могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.



### Настройка BIOS/UEFI

Запретить доступ пользователя к программе SETUP BIOS/UEFI материнской платы путем установки администраторского пароля на вход в SETUP BIOS. Должно быть установлено разрешение на загрузку только с ЖМД (диск С) и установлен запрет на загрузку с альтернативных носителей (гибкие диски, CD-ROM, USB, Ethernet и другие).

### Регистрация попыток входа в систему и доступа к критичным объектам локальной файловой системы.

Регистрация попыток входа в систему и доступа к критичным объектам локальной файловой системы настраивается включением соответствующих политик аудита в ОС Windows локально с помощью оснастки Local Security Policy, либо централизованно, с использованием механизма доменных групповых политик.

### Рекомендации по настройке политик безопасности для контроллеров домена, АРМ и пользователей при использовании СЗИ от НСД «SecretNet»

Значения настроек параметров групповых политик приведены для русскоязычной ОС Windows 2003 Server.

В таблице (Таблица 39) приведены настройки параметров групповой политики, применяемой для пользователей, работающих на АРМ ТПК РАБИС-НП платежной системы при использовании СЗИ от НСД «SecretNet».

Внимание:

1. Политики для пользователей, АРМ, контроллеров домена и серверов, перенаправления папки не применять к доменным группам Domain Admins, Enterprise Admins, SecretNetAdmins и локальной группе администраторов;
2. В соответствии с параметром настройки групповой политики для пользователей "Главное меню" (Таблица 39) рекомендуется меню запуска только необходимых пользователю приложений формировать с использованием механизма перенаправления папок:

|  |  |
| --- | --- |
| **Наименование раздела/параметра групповой политики** | **Значение параметра** |
| Конфигурация Windows — Перенаправление папки |  |
| Главное меню | Устанавливается в отдельном объекте групповой политики. |

Для организации замкнутой программной среды и запрета возможности запуска "Проводника" необходимо дополнительно выполнить следующие требования:

1. В реестре ОС Windows XP АРМ пользователей удалить ключ [HKEY\_CLASSES\_ROOT\Folder\shell\open\command].

2. В папке перенаправления:

* создать пустую подпапку "Программы", запретить доступ к ней всем пользователям и группам;
* не создавать другие подпапки (кроме пустой подпапки "Программы").

3. Необходимые ярлыки запуска приложений пользователя размещать в папке перенаправления.

1. Для обеспечения доступа к ресурсам файловой системы через графический интерфейс прикладного программного обеспечения, а также с целью выполнения регламентных операций для отдельных категорий пользователей подсистем ТПК РАБИС-НП, требуется разрешить отображение в диалоговых окнах "Открыть/сохранить файл" локальных ресурсов файловой системы и сетевого окружения.

Для отображения локальных (сетевых) ресурсов при функционировании рабочих станций с ОС Windows 2000/ХР/7 (RUS) под управлением контроллеров домена с ОС Windows 2003 Server (RUS) необходимо в политике пользователей установить в значение "Отключена" следующие параметры групповой политики:

* "Конфигурация пользователя – Административные шаблоны – Рабочий стол –Удалить значок "Мой компьютер" с рабочего стола";
* "Конфигурация пользователя – Административные шаблоны – Рабочий стол –Убрать значок "Сетевое окружение" и рабочего стола";
* "Конфигурация пользователя – Административные шаблоны – Компоненты Windows – Проводник – Скрыть значок "Вся сеть" в папке "Сетевое окружение".

1. Все изменения в профиль пользователя (в том числе настройку принтера) рекомендуется вносить до перемещения учетной записи пользователя под действие пользовательской политики.
2. Настройки параметров групповых политик в соответствии с данными рекомендациями скрывают языковую панель от пользователя. Установка параметра "Не отображать панели инструментов в панели задач" в значение "Включена" предотвращает несанкционированный доступ пользователя к проводнику Windows через интерфейс одной из панели инструментов - языковой панели. Переключение между языками ввода должно осуществляться настроенными сочетаниями клавиш.

В некоторых случаях для того чтобы переключение языков ввода функционировало корректно нужно дополнительно:

* вывести учетную запись пользователя из-под действия политики пользователей;
* войти пользователем в операционную систему АРМ и в контекстном меню появившейся языковой панели выполнить пункт "Закрыть языковую панель", проверить работу механизма переключения языков – механизм должен функционировать корректно;
* ввести учетную запись пользователя под действие политики пользователей;
* войти пользователем, проверить работу механизма переключения языков – языковая панель должна быть скрыта, механизм функционировать корректно.

1. Терминальный вход пользователя в соответствии с документацией к ПО СЗИ от НСД «Secret Net» обеспечивается "пробросом" TM-идентификатора на удаленный сервер за счет настройки соответствующих параметров в разделах:

1. Конфигурация компьютера – Административные шаблоны – Система – Удалённый вызов процедур (RPC) – Ограничения для не прошедших проверку RPC-клиентов.

2. Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Локальные политики – Параметры безопасности – Разрешать анонимный доступ к именованным каналам.

1. Рекомендации по дополнительной настройке механизма ЗПС на АРМ пользователей при использовании ПО СЗИ от НСД «Secret Net»:
2. Рекомендация по настройке запрета использования пользователем "горячих клавиш" Windows+X в ОС Windows XP.

На АРМ платежной сети в системном реестре добавить ключ [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]

"Scancode Map"=hex:00,00,00,00,00,00,00,00,03,00,00,00,00,00,5B,E0,00,00,5C,E0,00,00,00,00

1. Рекомендации по установке драйверов видео и аудио устройств.

При установке драйверов видео и аудио устройств (при наличии технической возможности) не устанавливать программные расширения, позволяющие изменять параметры звука, графики и т.д. при помощи настраиваемых «горячих» клавиш, через иконки в панели задач.

1. Рекомендации по установке компонентов ОС Windows XP.

При установке ПО операционной системы Windows XP на АРМ платежной сети не устанавливать компоненты ОС "Громкость" и "Звукозапись" или установить запрет на их запуск пользователям средствами ПО СЗИ от НСД Secret Net - дополнить задачу «MS Windows: основные ресурсы» (Таблица 29, Таблица 35):

Таблица 38. Настройки при установке ПО ОС Windows XP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование контролируемых ресурсов** | **Тип** | **Каталоги/Путь/Имя** | **Действие** | **Файлы** |
| Запрет запуска 6 | Файлы по каталогу | %SystemRoot%\ system32 | Действие-Удалять | sndvol32.exe |
| Запрет запуска 7 | Файлы по каталогу | %SystemRoot%\ system32 | Действие-Удалять | sndrec32.exe |

Таблица 39. Настройки параметров групповой политики, применяемой для пользователей, работающих на АРМ платежной системы при использовании СЗИ от НСД «SecretNet»

| **Наименование раздела/параметра групповой политики** | **Значение параметра** | **Примечание** |
| --- | --- | --- |
| **Конфигурация программ** | |  |
| **Конфигурация программ — Установка программ** | |  |
| **Конфигурация Windows — Сценарии (вход/выход из системы)** | |  |
| Вход в систему |  |  |
| Выход из системы |  |  |
| **Конфигурация Windows — Параметры безопасности — Политики открытого ключа** |  |  |
| Доверительные отношения в предприятии |  |  |
| Параметры автоматической подачи заявок |  |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ — Уровни безопасности** |  |  |
| Не разрешено |  |  |
| Неограниченный |  |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ — Дополнительные правила** |  |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ — Принудительный** |  |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ — Назначенные типы файлов** |  |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ — Доверенные издатели** |  |  |
| **Конфигурация Windows — Перенаправление папки** |  |  |
| Application Data | Не задана |  |
| Рабочий стол | Не задана |  |
| Мои документы | Не задана |  |
| Главное меню | Устанавливается в отдельном объекте групповой политики. |  |
| **Конфигурация Windows — Настройка Internet Explorer — Пользовательский интерфейс обозревателя — Заголовки, картинки, значки и т.д.** |  |  |
| Заголовок обозревателя |  |  |
| Эмблема |  |  |
| Настройка панели инструментов обозревателя |  |  |
| **Конфигурация Windows — Настройка Internet Explorer — Подключение — Параметры подключения, прокси и автонастройки** |  |  |
| Параметры подключения |  |  |
| Автоматическая настройка обозревателя |  |  |
| Параметры прокси-сервера |  |  |
| Строка обозревателя |  |  |
| **Конфигурация Windows — Настройка Internet Explorer — URL-адреса — Избранное, ссылки и важнейшие адреса URL** |  |  |
| Избранное и ссылки |  |  |
| Важные URL-адреса |  |  |
| **Конфигурация Windows — Настройка Internet Explorer — Безопасность — Зоны, оценки и Authenticode** |  |  |
| Зоны безопасности и оценка содержимого | Выставить признак «Импортировать текущие параметры безопасности и конфиденциальности. Добавить все серверы ТПК РАБИС-НП и АС ЭКР в формате \\<имя\_сервера> |  |
| Параметры Authenticode |  |  |
| **Конфигурация Windows — Настройка Internet Explorer — Программы — Параметры программ по умолчанию и внешних программ** |  |  |
| Программы |  |  |
| **Административные шаблоны — Компоненты Windows — NetMeeting** |  |  |
| Включить автоматическую настройку | Отключена |  |
| Отключение службы каталога NetMeeting | Включена |  |
| Запрещение добавления серверов каталога | Включена |  |
| Запрещение просмотра веб-каталогов | Включена |  |
| Указание веб-страницы, поддерживающей интрасеть | Отключена |  |
| Указание параметров безопасности вызовов | Отключена |  |
| Запретить изменение метода выполнения вызова | Включена |  |
| Запретить автоматический прием вызовов | Включена |  |
| Разрешить устойчивый автоматический прием вызовов | Отключена |  |
| Запретить отправку файлов | Включена |  |
| Запретить получение файлов | Включена |  |
| Ограничить размер отправляемых файлов | Отключена |  |
| Запретить разговор | Включена |  |
| Запретить доску NetMeeting 2.x | Включена |  |
| Запретить использование доски | Включена |  |
| **Административные шаблоны — Компоненты Windows — NetMeeting — Общий доступ к приложениям** |  |  |
| Отключить общий доступ к приложениям | Включена |  |
| Запретить предоставление общего доступа | Включена |  |
| Запретить предоставление общего доступа к рабочему столу | Включена |  |
| Запретить предоставление общего доступа к командной строке | Включена |  |
| Запретить предоставление общего доступа к окнам Проводника | Включена |  |
| Запретить управление | Включена |  |
| Запретить общий доступ к приложениям в режиме True Color | Включена |  |
| **Административные шаблоны — Компоненты Windows — NetMeeting — Аудио и видео** |  |  |
| Ограничить использование пропускной способности для звука и видео | Отключена |  |
| Отключить звук | Включена |  |
| Отключить полный дуплекс для звука | Включена |  |
| Запретить изменение параметра DirectSound | Включена |  |
| Запретить передачу видео | Включена |  |
| Запретить получение видео | Включена |  |
| **Административные шаблоны — Компоненты Windows — NetMeeting — Страница параметров** |  |  |
| Скрыть страницу "Общие" | Включена |  |
| Отключить кнопку "Расширенный вызов" | Включена |  |
| Скрыть страницу безопасности | Включена |  |
| Скрыть страницу "Звук" | Включена |  |
| Скрыть страницу "Видео" | Включена |  |
| **Административные шаблоны — Компоненты Windows — Internet Explorer[[57]](#footnote-58)** |  |  |
| **Административные шаблоны — Компоненты Windows — Совместимость приложений** |  |  |
| Предотвращение доступа к 16-разрядным приложениям | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Диспетчер вложений** |  |  |
| Уровень риска по умолчанию для вложенных файлов | Отключена |  |
| Список исключений для типов файлов высокого риска | Отключена |  |
| Список исключений для типов файлов умеренного риска | Отключена |  |
| Список исключений для типов файлов низкого риска | Отключена |  |
| Логика доверия для вложенных файлов | Отключена |  |
| Не сохранять сведения о зоне во вложенных файлах | Отключена |  |
| Скрыть возможности для удаления сведений о зоне | Отключена |  |
| Уведомлять антивирусную программу при открытии вложений | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Проводник — Общее диалоговое окно открытия файлов** |  |  |
| Элементы, отображаемые в панели мест | Отключена |  |
| Скрыть панель мест из общих диалогов открытия файлов | Включена |  |
| Скрыть кнопку "Назад" в общих диалогах открытия файлов | Включена |  |
| Скрыть раскрывающийся список недавно открывавшихся файлов | Включена |  |
| **Административные шаблоны — Компоненты Windows — Проводник** |  |  |
| Использовать классический стиль оболочки | Включена |  |
| Удалить команду "Свойства папки" из меню "Сервис" | Включена |  |
| Удалить меню "Файл" из проводника Windows | Включена |  |
| Удалить команды "Подключение сетевого диска" и "Отключение сетевого диска" | Включена |  |
| Удалить кнопку "Поиск" из проводника Windows | Включена |  |
| Запретить вывод контекстного меню по умолчанию для проводника Windows | Включена | ЗПС |
| Скрыть команду "Управление" из контекстного меню Проводника | Включена |  |
| Разрешить использование только пользовательских или зарегистрированных расширений | Отключена |  |
| Не отслеживать ярлыки оболочки при перемещении | Включена |  |
| Скрыть выбранные диски из окна "Мой компьютер" | Отключена |  |
| Запретить доступ к дискам через "Мой компьютер" | Отключена |  |
| Удалить вкладку "Оборудование" | Включена |  |
| Удалить вкладку DFS | Включена |  |
| Удалить вкладку "Безопасность" | Включена |  |
| Запретить изменение видеоэффектов для меню | Включена |  |
| Запретить изменение вывода при работе с клавиатурой | Включена |  |
| Скрыть значок "Соседние компьютеры" в папке "Сетевое окружение" | Включена |  |
| Скрыть значок "Вся сеть" в папке "Сетевое окружение" | Включена |  |
| Максимальная длина списка "Недавние документы" | Включена (1) |  |
| Не запрашивать другие имя пользователя и пароль | Включена |  |
| Запрашивать имя пользователя и пароль при установке по сети | Отключена |  |
| Удалить возможности записи компакт-дисков | Включена |  |
| Не перемещать удаляемые файлы в "Корзину" | Включена |  |
| Запрашивать подтверждение при удалении файлов | Включена |  |
| Максимально допустимый размер "Корзины" | Отключена |  |
| Удалить "Общие документы" из окна "Мой компьютер" | Включена |  |
| Отключить кэширование эскизов изображений | Включена |  |
| Отключить сочетания клавиш Windows+X | Включена |  |
| Отключить защищенный режим протокола оболочки | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Консоль управления Microsoft** |  |  |
| Запретить пользователям использовать авторский режим | Отключена |  |
| Ограничить использование оснасток списком явно разрешенных оснасток | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Консоль управления Microsoft — Запрещенные или разрешенные оснастки — Оснастки расширений** |  |  |
| AppleTalk-маршрутизация | Отключена |  |
| Диспетчер авторизации | Отключена |  |
| Параметры политики центра сертификации | Отключена |  |
| Совместное использование подключения (NAT) | Отключена |  |
| Расширение настройки DCOM | Отключена |  |
| Диспетчер устройств | Отключена |  |
| Управление DHCP-ретрансляцией | Отключена |  |
| Просмотр событий | Отключена |  |
| Расширенный вид (веб-вид) | Отключена |  |
| Ведение журнала IAS | Отключена |  |
| IGMP-маршрутизация | Отключена |  |
| IP-маршрутизация | Отключена |  |
| IPX-маршрутизация RIP | Отключена |  |
| IPX-маршрутизация | Отключена |  |
| IPX-маршрутизация SAP | Отключена |  |
| Логические и подключенные диски | Отключена |  |
| OSPF-маршрутизация | Отключена |  |
| Политики открытых ключей | Отключена |  |
| RAS-доступ - узел пользователя | Отключена |  |
| Удаленный доступ | Отключена |  |
| Съемные ЗУ | Отключена |  |
| RIP-маршрутизация | Отключена |  |
| Маршрутизация | Отключена |  |
| Расширение общих папок | Отключена |  |
| Отправка сообщения консоли | Отключена |  |
| Зависимости служб | Отключена |  |
| Протокол SMTP | Отключена |  |
| SNMP | Отключена |  |
| Свойства системы | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Консоль управления Microsoft — Запрещенные или разрешенные оснастки — Групповая политика — Расширения оснастки групповой политики** |  |  |
| Административные шаблоны (компьютеры) | Отключена |  |
| Административные шаблоны (пользователи) | Отключена |  |
| Перенаправление папок | Отключена |  |
| Настройка Internet Explorer | Отключена |  |
| Службы удаленной установки | Отключена |  |
| Сценарии (вход/выход из системы) | Отключена |  |
| Сценарии (запуск/завершение) | Отключена |  |
| Параметры безопасности | Отключена |  |
| Установка программ (компьютеры) | Отключена |  |
| Установка программ (пользователи) | Отключена |  |
| Политики беспроводной сети (IEEE 802.11) | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Консоль управления Microsoft — Запрещенные или разрешенные оснастки — Групповая политика — Расширения оснастки результирующей политики (RSoP)** |  |  |
| Административные шаблоны (компьютеры) | Отключена |  |
| Административные шаблоны (пользователи) | Отключена |  |
| Перенаправление папок | Отключена |  |
| Настройка Internet Explorer | Отключена |  |
| Сценарии (вход/выход из системы) | Отключена |  |
| Сценарии (запуск/завершение) | Отключена |  |
| Параметры безопасности | Отключена |  |
| Установка программ (компьютеры) | Отключена |  |
| Установка программ (пользователи) | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Консоль управления Microsoft — Запрещенные или разрешенные оснастки — Групповая политика** |  |  |
| Управление групповой политикой | Отключена |  |
| Редактор объектов групповой политики | Отключена |  |
| Вкладка групповой политики для средств Active Directory | Отключена |  |
| Оснастка результирующей политики (RSoP) | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Консоль управления Microsoft — Запрещенные или разрешенные оснастки** |  |  |
| Active Directory - пользователи и компьютеры | Отключена |  |
| Active Directory - домены и доверие | Отключена |  |
| Active Directory - сайты и службы | Отключена |  |
| Редактирование ADSI | Отключена |  |
| Элемент управления ActiveX | Отключена |  |
| Сертификаты | Отключена |  |
| Центр сертификации | Отключена |  |
| Шаблоны сертификатов | Отключена |  |
| Беспроводной монитор | Отключена |  |
| Службы компонентов | Отключена |  |
| Управление компьютером | Отключена |  |
| Диспетчер устройств | Отключена |  |
| Управление дисками | Отключена |  |
| Дефрагментация диска | Отключена |  |
| Распределенная файловая система DFS | Отключена |  |
| Просмотр событий | Отключена |  |
| Служба факсов | Отключена |  |
| Расширения сервера FrontPage | Отключена |  |
| Служба индексирования | Отключена |  |
| Конфигурация .Net Framework | Отключена |  |
| Служба проверки подлинности в Интернете (IAS) | Отключена |  |
| Службы IIS | Отключена |  |
| Управление политикой IP-безопасности | Отключена |  |
| Диспетчер IP-безопасности | Отключена |  |
| Ссылка на веб-адрес | Отключена |  |
| Локальные пользователи и группы | Отключена |  |
| Оповещения и журналы производительности | Отключена |  |
| Контроль допуска QoS | Отключена |  |
| Удаленные рабочие столы | Отключена |  |
| Управление съемными носителями | Отключена |  |
| Маршрутизация и удаленный доступ | Отключена |  |
| Анализ и настройка безопасности | Отключена |  |
| Шаблоны безопасности | Отключена |  |
| Службы | Отключена |  |
| Общие папки | Отключена |  |
| Сведения о системе | Отключена |  |
| Телефония | Отключена |  |
| Настройка служб терминалов | Отключена |  |
| Элемент управления WMI | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Планировщик заданий** |  |  |
| Скрывать страницы свойств | Отключена |  |
| Запретить запуск и завершение задач | Отключена |  |
| Запретить перетаскивание с помощью мыши | Отключена |  |
| Запретить создание новых заданий | Отключена |  |
| Запретить удаление заданий | Отключена |  |
| Скрыть флажок дополнительных свойств в мастере планирования заданий | Отключена |  |
| Запретить обзор | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Клиент** |  |  |
| Запретить сохранение паролей | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Сеансы** |  |  |
| Задать ограничение по времени для отключенных сеансов | Отключена |  |
| Задать ограничение по времени для активных сеансов | Отключена |  |
| Задать ограничение по времени для бездействующих сеансов | Отключена |  |
| Разрешать переподключение только от исходного клиента | Отключена |  |
| Завершать сеанс при достижении ограничения по времени | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Службы терминалов** |  |  |
| Запускать программу при подключении | Отключена |  |
| Устанавливает правила удаленного управления для сеансов пользователей служб терминалов | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Установщик Windows** |  |  |
| Всегда производить установку с повышенными привилегиями | Отключена |  |
| Порядок поиска установочных файлов | Отключена |  |
| Запретить откат | Отключена |  |
| Запретить использование съемных носителей при установке | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Windows Messenger** |  |  |
| Запретить выполнение Windows Messenger | Включена |  |
| Не запускать автоматически Windows Messenger при входе | Включена |  |
| **Административные шаблоны — Компоненты Windows — Windows Update** |  |  |
| Удалить доступ к возможностям Windows Update | Включена | ЗПС |
| Не отображать параметр "Установить обновления и завершить работу" в диалоговом окне завершения работы Windows | Включена |  |
| Не настраивать параметр "Установить обновления и завершить работу" в диалоговом окне завершения работы Windows в качестве параметра по умолчанию | Включена |  |
| **Административные шаблоны — Компоненты Windows — Windows Movie Maker** |  |  |
| Запретить выполнение программы Windows Movie Maker | Включена |  |
| **Административные шаблоны — Компоненты Windows — Проигрыватель Windows Media — Интерфейс пользователя** |  |  |
| Скрыть вкладку "Конфиденциальность" | Отключена |  |
| Скрыть вкладку "Безопасность" | Отключена |  |
| Задать и закрепить обложку | Отключена |  |
| Не отображать закрепленное окно | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Проигрыватель Windows Media — Воспроизведение** |  |  |
| Запретить загрузку кодеков | Отключена |  |
| Разрешить отображение заставки | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Проигрыватель Windows Media — Сеть** |  |  |
| Скрыть вкладку "Сеть" | Отключена |  |
| Протоколы потоков мультимедиа | Отключена |  |
| Настройка HTTP-прокси | Отключена |  |
| Настройка MMS-прокси | Отключена |  |
| Настройка RTSP-прокси | Отключена |  |
| Настройка сетевой буферизации | Отключена |  |
| **Административные шаблоны — Компоненты Windows — Проигрыватель Windows Media** |  |  |
| Запретить получение сведений о компакт-диске и диске DVD | Отключена |  |
| Запретить получение сведений о диске с музыкальными файлами | Отключена |  |
| Запретить получение списка радиостанций из Интернета | Отключена |  |
| **Административные шаблоны — Панель задач и меню "Пуск"** |  |  |
| Удалить папки пользователя из главного меню | Отключена |  |
| Удалить ссылки и запретить использование Windows Update | Включена | ЗПС |
| Скрыть общие группы программ в меню "Пуск" | Включена | ЗПС |
| Удалить значок "Мои документы" из главного меню | Включена | ЗПС |
| Удалить меню "Документы" из главного меню | Включена | ЗПС |
| Отключить папки программ в меню "Настройка" | Включена | ЗПС |
| Удалить "Сетевые подключения" из меню "Пуск" | Включена |  |
| Удаляет меню "Избранное" из главного меню | Включена | ЗПС |
| Удалить меню "Найти" из главного меню | Включена | ЗПС |
| Удалить справку из главного меню | Включена | ЗПС |
| Удалить команду "Выполнить" из меню "Пуск" | Включена | ЗПС |
| Удалить значок "Мои рисунки" из главного меню | Включена | ЗПС |
| Удалить значок "Моя музыка" из главного меню | Включена | ЗПС |
| Удалить значок "Сетевое окружение" из меню "Пуск" | Включена | ЗПС |
| Добавить пункт выхода из системы в главное меню | Отключена |  |
| Удалить "Завершение сеанса" из меню "Пуск" | Отключена |  |
| Удалить и запретить доступ к команде "Завершение работы" | Отключена |  |
| Удалить контекстные меню перетаскивания для элементов меню "Пуск" | Включена | ЗПС |
| Запретить изменение параметров панели задач и меню "Пуск" | Включена | ЗПС |
| Запретить доступ к контекстному меню для панели задач | Включена | ЗПС |
| Не хранить сведения о недавно открывавшихся документах | Включена |  |
| Очищать список недавно открывавшихся документов при выходе | Включена |  |
| Отключить сокращенные меню | Включена |  |
| Отключить слежение за действиями пользователя | Включена |  |
| Добавить флажок "Запустить в отдельной области памяти" в окно команды "Выполнить" | Отключена |  |
| Не использовать сопоставление ярлыков оболочки на основе поиска | Включена |  |
| Не использовать метод на основе отслеживания для сопоставления ярлыков | Включена |  |
| Затенить ярлыки меню "Пуск" на не полностью установленные программы | Отключена |  |
| Запретить группировку элементов панели задач | Включена |  |
| Отключить очистку области уведомлений | Включена |  |
| Зафиксировать положение панели задач | Включена |  |
| Форсировать классическое меню Пуск | Включена |  |
| Удалить всплывающие подсказки для элементов главного меню | Включена |  |
| Удалить список программ, закрепленных в меню "Пуск" | Включена | ЗПС |
| Удалить список часто используемых программ в меню "Пуск" | Включена | ЗПС |
| Удалить список всех программ в меню "Пуск" | Включена | ЗПС |
| Удалить кнопку ''Отстыковка ПК'' из меню ''Пуск'' | Включена |  |
| Удалить имя пользователя из меню "Пуск" | Включена |  |
| Удалить часы из системной области уведомлений | Отключена |  |
| Скрыть область уведомлений | Отключена |  |
| Не отображать панели инструментов в панели задач | Включена |  |
| Удаление значка доступа к программам и параметров по умолчанию из меню "Пуск" | Включена | ЗПС |
| **Административные шаблоны — Рабочий стол** |  |  |
| Скрыть и отключить все значки на рабочем столе | Включена[[58]](#footnote-59) | ЗПС |
| Удалить значок "Мои документы" с рабочего стола | Включена | ЗПС |
| Удалить значок "Мой компьютер" с рабочего стола | Включена | ЗПС |
| Удалить значок "Корзины" с рабочего стола | Включена | ЗПС |
| Удалить команду "Свойства" из контекстного меню папки "Мои документы" | Включена | ЗПС |
| Удалить команду ''Свойства'' из контекстного меню объекта ''Мой компьютер'' | Включена | ЗПС |
| Удалить команду "Свойства" из контекстного меню "Корзины" | Включена | ЗПС |
| Убрать значок "Сетевое окружение" и рабочего стола | Включена | ЗПС |
| Не показывать значок Internet Explorer | Включена | ЗПС |
| Не добавлять общие папки, из которых открыты документы в "Сетевое окружение" | Включена | ЗПС |
| Запретить пользователям изменять путь папки "Мои документы" | Включена | ЗПС |
| Запретить перетаскивание и закрытие всех панелей инструментов на панели задач | Включена | ЗПС |
| Запретить изменение расположения панелей инструментов рабочего стола | Включена | ЗПС |
| Не сохранять параметры настройки при выходе | Включена |  |
| Удалить мастер очистки рабочего стола | Включена |  |
| **Административные шаблоны — Рабочий стол — Active Desktop** |  |  |
| Включить Active Desktop | Отключена |  |
| Отключить Active Desktop | Включена |  |
| Отключить все элементы веб-содержимого | Включена |  |
| Запретить изменения | Включена |  |
| Запретить добавление элементов веб-содержимого | Включена |  |
| Запретить удаление элементов веб-содержимого | Включена |  |
| Запретить редактирование элементов веб-содержимого | Включена |  |
| Запретить закрытие элементов веб-содержимого | Включена |  |
| Добавление или удаление элементов | Отключена |  |
| Рисунок рабочего стола Active Desktop | Отключена |  |
| Разрешить использование только точечных фоновых рисунков | Отключена |  |
| **Административные шаблоны — Рабочий стол — Active Directory** |  |  |
| Максимальный размер поиска в Active Directory | Отключена |  |
| Задействовать фильтр в диалоговом окне поиска | Отключена |  |
| Скрыть папку Active Directory | Включена |  |
| **Административные шаблоны — Панель управления** |  |  |
| Запретить доступ к панели управления | Включена | ЗПС |
| Скрыть указанные элементы панели управления | Отключена |  |
| Отображать только указанные элементы панели управления | Отключена |  |
| Форсировать классический стиль панели управления | Включена |  |
| **Административные шаблоны — Панель управления — Установка и удаление программ** |  |  |
| Удалить окно установки и удаления программ | Отключена |  |
| Скрыть страницу "Замена или удаление программ" | Отключена |  |
| Скрыть страницу установки программ | Отключена |  |
| Скрыть страницу "Добавление и удаление компонентов Windows" | Отключена |  |
| Скрытие страницы доступа к программам и параметров по умолчанию | Отключена |  |
| Скрыть пункт "Установка программы с компакт-диска или с дискет" | Отключена |  |
| Скрыть пункт "Установка программ от Майкрософт" | Отключена |  |
| Скрыть пункт "Установка программ из локальной сети" | Отключена |  |
| Перейти сразу на страницу мастера компонентов | Отключена |  |
| Не выводить информацию о поддержке | Отключена |  |
| Указать категорию по умолчанию для страницы "Установка новой программы" | Отключена |  |
| **Административные шаблоны — Панель управления — Экран — Темы оформления рабочего стола** |  |  |
| Отключить настройку тем оформления | Отключена |  |
| Запретить выбор стиля оформления окон и кнопок | Отключена |  |
| Запретить выбор размера шрифта темы оформления | Отключена |  |
| Запретить выбор цвета темы оформления | Отключена |  |
| Загрузить конкретный файл оформления или зафиксировать классический стиль | Отключена |  |
| **Административные шаблоны — Панель управления — Экран** |  |  |
| Удалить значок "Экран" из панели управления | Отключена |  |
| Скрыть вкладку рабочего стола | Отключена |  |
| Запретить изменение фонового рисунка | Отключена |  |
| Скрыть вкладку выбора тем оформления | Отключена |  |
| Скрыть вкладку установки параметров | Отключена |  |
| Скрыть вкладку выбора заставки | Отключена |  |
| Использовать экранные заставки | Отключена |  |
| Имя исполняемого файла экранной заставки | Отключена |  |
| Использовать парольную защиту для экранных заставок | Отключена |  |
| Таймаут экранной заставки | Отключена |  |
| **Административные шаблоны — Панель управления — Принтеры** |  |  |
| Разрешить обзор общего веб-узла с целью поиска принтеров | Отключена |  |
| Разрешить обзор сети для поиска принтеров | Отключена |  |
| Путь поиска принтеров Active Directory по умолчанию | Отключена |  |
| Ограничения указания и печати | Отключена |  |
| Запретить добавление принтеров | Отключена |  |
| Запретить удаление принтеров | Отключена |  |
| **Административные шаблоны — Панель управления — Язык и стандарты** |  |  |
| Ограничить выбор языка для меню и диалогов Windows | Отключена |  |
| **Административные шаблоны — Общие папки** |  |  |
| Разрешить публикацию общих ресурсов | Отключена |  |
| Разрешить публикацию DFS-корней | Отключена |  |
| **Административные шаблоны — Сеть — Автономные файлы** |  |  |
| Запретить пользовательскую настройку автономных файлов | Включена |  |
| Синхронизовать автономные файлы при входе в систему | Отключена |  |
| Синхронизация всех автономных файлов перед выходом из системы | Отключена |  |
| Синхронизовать автономные файлы перед приостановкой | Отключена |  |
| Действия при отключении от сервера | Отключена |  |
| Нестандартные действия при отключении от сервера | Отключена |  |
| Удалить "Сделать доступными автономно" | Включена |  |
| Запретить использование папки "Автономные файлы" | Включена |  |
| Административно назначенные автономные файлы | Отключена |  |
| Отключить всплывающие напоминания | Включена |  |
| Частота появления всплывающих напоминаний | Отключена |  |
| Длительность отображения первого всплывающего напоминания | Отключена |  |
| Длительность отображения всплывающих напоминаний | Отключена |  |
| Уровень регистрации событий | Отключена |  |
| Запретить применение "Сделать доступными автономно" для этих файлов и папок | Отключена |  |
| Не делать перенаправляемые папки доступными в автономном режиме автоматически | Включена |  |
| **Административные шаблоны — Сеть — Сетевые подключения** |  |  |
| Способность переименовывать LAN-подключения и общие подключения удаленного доступа | Отключена |  |
| Запретить доступ к свойствам компонентов подключений по локальной сети | Включена |  |
| Запретить доступ к свойствам компонентов подключений удаленного доступа | Включена |  |
| Запретить дополнительную настройку TCP/IP | Включена |  |
| Запретить доступ к команде 'Дополнительные параметры' в меню 'Дополнительно' | Включена |  |
| Запретить добавление и удаление компонентов для подключений LAN или удаленного доступа | Включена |  |
| Запретить доступ к свойствам подключений по локальной сети | Включена |  |
| Запретить включение и отключение компонентов подключений по локальной сети | Включена |  |
| Способность изменения свойств общих подключений удаленного доступа | Отключена |  |
| Запретить изменение свойств личных подключений удаленного доступа | Включена |  |
| Запретить удаление подключений удаленного доступа | Включена |  |
| Способность удалять общие подключения удаленного доступа | Включена |  |
| Запретить подключение и отключение для подключений удаленного доступа | Включена |  |
| Способность подключать и отключать подключения по локальной сети | Отключена |  |
| Запретить доступ к мастеру новых подключений | Включена |  |
| Способность переименовывать подключения по локальной сети | Отключена |  |
| Способность переименовывать общие подключения удаленного доступа | Отключена |  |
| Запретить переименование личных подключений удаленного доступа | Включена |  |
| Запретить доступ к команде 'Параметры удаленного доступа' в меню 'Дополнительно' | Включена |  |
| Запретить просмотр состояния для активного подключения | Включена |  |
| Включить политики сетевых подключений Windows 2000 для администраторов | Отключена |  |
| Отключить уведомления при ограниченном или отсутствующем подключении | Отключена |  |
| **Административные шаблоны — Система — Профили пользователей** |  |  |
| Подключить домашнюю папку к корню общего ресурса | Отключена |  |
| Ограничить размер профиля | Отключена |  |
| Исключить папки из перемещаемого профиля | Отключена |  |
| **Административные шаблоны — Система — Сценарии** |  |  |
| Синхронное выполнение сценариев входа в систему | Включена |  |
| Выполнять сценарии входа прежних версий без отображения команд | Отключена |  |
| Выполнять сценарии входа с отображением команд | Включена |  |
| Выполнять сценарии выхода с отображением команд | Включена |  |
| **Административные шаблоны — Система — Возможности Ctrl+Alt+Del** |  |  |
| Удалить диспетчер задач | Включена |  |
| Запретить блокировку компьютера | Отключена |  |
| Запретить изменение пароля | Отключена |  |
| Запретить завершение сеанса | Отключена |  |
| **Административные шаблоны — Система — Вход в систему** |  |  |
| Запускать указанные программы при входе в систему | Отключена |  |
| Не обрабатывать список автозапуска программ, выполняемых однажды | Отключена |  |
| Не обрабатывать список автозапуска для старых версий | Отключена |  |
| **Административные шаблоны — Система — Групповая политика** |  |  |
| Интервал обновления групповой политики для пользователей | Отключена |  |
| Обнаружение медленных подключений для групповой политики | Отключена |  |
| Выбор контроллера домена групповой политики | Отключена |  |
| Создание ссылок объектов групповой политики по умолчанию запрещено | Отключена |  |
| Имя по умолчанию для новых объектов групповой политики | Отключена |  |
| Вывод пункта "Показывать только политики" | Отключена |  |
| Отключить автоматическое обновление ADM-файлов | Отключена |  |
| Запретить интерактивным пользователям создавать данные результирующей политики (RSoP) | Отключена |  |
| **Административные шаблоны — Система — Управление электропитанием** |  |  |
| Запрашивать пароль при выходе из спящего или ждущего режима | Включена |  |
| **Административные шаблоны — Система — Управление связью через Интернет — Параметры связи через Интернет** |  |  |
| Отключить веб-публикацию в списке задач для файлов и папок | Включена |  |
| Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков | Включена |  |
| Отключить заказ отпечатков через Интернет в списке задач для изображений | Включена |  |
| Отключить участие в программе улучшения поддержки пользователей Windows Messenger | Включена |  |
| Отключить службу сопоставления файлов Интернета | Включена |  |
| Отключить выполнение печати через HTTP-протокол | Включена |  |
| Отключить загрузку драйверов печати через HTTP-протокол | Включена |  |
| Отключить автоматическую загрузку кодеков для Windows Movie Maker | Включена |  |
| Отключить веб-ссылки в Windows Movie Maker | Включена |  |
| Отключить сохранение видео на веб-узлах поставщиков видеохостинга в Windows Movie Maker | Включена |  |
| **Административные шаблоны — Система — Управление связью через Интернет** |  |  |
| Ограничить связь через Интернет | Включена |  |
| **Административные шаблоны — Система** |  |  |
| Не отображать окно "Первое знакомство" при входе в систему | Включена |  |
| Интерпретация столетия для 2000 года | Отключена |  |
| Выбор мест для поиска драйверов | Отключена |  |
| Подписывание драйверов устройств | Отключена |  |
| Особый интерфейс пользователя | Отключена | ЗПС |
| Запретить использование командной строки | Отключена |  |
| Сделать недоступными средства редактирования реестра | Включена | ЗПС |
| Выполнять только разрешенные приложения для Windows | Отключена |  |
| Не запускать указанные приложения Windows[[59]](#footnote-60) | Включена (explorer.exe, cmd.exe, iexplore.exe[[60]](#footnote-61)) | ЗПС |
| Отключить автозапуск | Включена (все диски) | ЗПС |
| Запретить запуск из Справки перечисленных программ | Включена (\*.\*) | ЗПС |
| Загружать отсутствующие COM-компоненты | Включена |  |
| Автоматическое обновление Windows | Отключена |  |
| Отключить запрос на использование Windows Update при поиске драйверов | Включена |  |

**Примечание**. Параметры групповой политики, отмеченные в таблице (Таблица 39) в столбце «Примечание» как «ЗПС» реализуют дополнительные (дополнительно к механизму СЗИ от НСД «Secret Net») мероприятия по организации замкнутой программной среды (скрытию элементов интерфейса) для пользователей на АРМ и серверах платежной системы.

Таблица (Таблица 40) содержит настройки параметров групповой политики, применяемой для АРМ платежной системы при использовании СЗИ от НСД «SecretNet».

Таблица 40. Настройки параметров групповой политики, применяемой для АРМ платежной системы при использовании СЗИ от НСД «SecretNet»

| **Наименование раздела/параметра групповой политики** | **Значение параметра** |
| --- | --- |
| **Конфигурация программ** |  |
| **Конфигурация Windows — Сценарии (запуск/завершение)** |  |
| **Конфигурация Windows — Параметры безопасности — Политики учетных записей — Политика паролей [[61]](#footnote-62)** |  |
| Макс. срок действия пароля | 180 дней |
| Мин. длина пароля | 8 символов |
| Мин. срок действия пароля | 0 дней |
| Пароль должен отвечать требованиям сложности | Включен |
| Требовать неповторяемости паролей | 5 хранимых паролей |
| Хранить пароли всех пользователей в домене, используя обратимое шифрование | Отключен |
| **Конфигурация Windows — Параметры безопасности — Политики учетных записей — Политика блокировки учетной записи** |  |
| Блокировка учетной записи на | 0 |
| Пороговое значение блокировки | 3 ошибок входа в систему |
| Сброс счетчика блокировки через | 30 минут |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Политика аудита** |  |
| Аудит входа в систему | Успех, Отказ |
| Аудит доступа к объектам | Нет аудита |
| Аудит доступа к службе каталогов | Отказ |
| Аудит изменения политики | Успех, Отказ |
| Аудит использования привилегий | Нет аудита |
| Аудит отслеживания процессов | Нет аудита |
| Аудит системных событий | Успех, Отказ |
| Аудит событий входа в систему | Успех, Отказ |
| Аудит управления учетными записями | Успех, Отказ |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Назначение прав пользователя** |  |
| Архивирование файлов и каталогов | Администраторы |
| Восстановление файлов и каталогов | Администраторы |
| Вход в качестве пакетного задания | Локальная система |
| Вход в качестве службы | [[62]](#footnote-63) |
| Добавление рабочих станций к домену | Администраторы |
| Доступ к компьютеру из сети | Прошедшие проверку |
| Завершение работы системы | Администраторы, Пользователи |
| Загрузка и выгрузка драйверов устройств | Администраторы |
| Закрепление страниц в памяти |  |
| Замена маркера уровня процесса | Локальная система, Сетевая служба |
| Запретить вход в систему через службу терминалов |  |
| Запуск операций по обслуживанию тома | Администраторы |
| Извлечение компьютера из стыковочного узла | Администраторы |
| Изменение параметров среды оборудования | Администраторы |
| Изменение системного времени | Администраторы |
| Локальный вход в систему[[63]](#footnote-64) | Администраторы, Пользователи |
| Настройка квот памяти для процесса | Администраторы |
| Обход перекрестной проверки | Прошедшие проверку |
| Овладение файлами или иными объектами | Администраторы |
| Олицетворение клиента после проверки подлинности | СЛУЖБА, Администраторы |
| Отказ в доступе к компьютеру из сети | loser |
| Отказ во входе в качестве пакетного задания |  |
| Отказать во входе в качестве службы |  |
| Отклонить локальный вход |  |
| Отладка программ | Администраторы |
| Принудительное удаленное завершение | Администраторы |
| Профилирование загруженности системы | Администраторы |
| Профилирование одного процесса | Администраторы |
| Работа в режиме операционной системы | Локальная система |
| Разрешать вход в систему через службу терминалов | Администраторы |
| Разрешение доверия к учетным записям при делегировании | Администраторы |
| Синхронизация данных службы каталогов |  |
| Создание глобальных объектов | Администраторы |
| Создание журналов безопасности | Локальная система, Сетевая служба |
| Создание маркерного объекта | Локальная система |
| Создание постоянных объектов совместного использования | Локальная система |
| Создание страничного файла | Администраторы |
| Увеличение приоритета диспетчирования | Администраторы |
| Управление аудитом и журналом безопасности[[64]](#footnote-65) | <имя\_домена>\Auditors |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Назначение прав пользователя (для АРМ с Windows 7 в Active Directory необходимо создать отдельный OU и применить к нему GPO с нижеприведёнными параметрами)** |  |
| Вход в качестве пакетного задания | LOCAL SERVICE |
| Замена маркера уровня процесса | LOCAL SERVICE, NETWORK SERVICE |
| Профилирование загруженности системы | Администраторы, LOCAL SERVICE |
| Работа в режиме операционной системы | LOCAL SERVICE |
| Синхронизация данных службы каталогов | Администраторы |
| Создание маркерного объекта | LOCAL SERVICE |
| Создание постоянных объектов совместного использования | LOCAL SERVICE |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Параметры безопасности** |  |
| DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language) | Не определено |
| DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language) | Не определено |
| Аудит: аудит доступа глобальных системных объектов | Отключен |
| Аудит: аудит прав на архивацию и восстановление | Отключен |
| Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности | Отключен |
| Доступ к сети: Разрешить трансляцию анонимного SID в имя | Отключен |
| Завершение работы: очистка страничного файла виртуальной памяти | Включен |
| Завершение работы: разрешить завершение работы системы без выполнения входа в систему | Включен |
| Интерактивный вход в систему: поведение при извлечении смарт-карты | Блокировка рабочей станции |
| Интерактивный вход в систему: требовать смарт-карту | Отключен |
| Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему | Не определено |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | 0 Входы в систему |
| Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее | 5 дн. |
| Интерактивный вход в систему: не отображать последнего имени пользователя | Включен |
| Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL | Отключен |
| Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован | Не определено |
| Интерактивный вход в систему: текст сообщения для пользователей при входе в систему | Не определено |
| Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (всегда) | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) | Включен |
| Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам | Отключен |
| Консоль восстановления: разрешить автоматический вход администратора | Отключен |
| Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам | Отключен |
| Контроллер домена: запретить изменение пароля учетных записей компьютера | Отключен |
| Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию | Отключен |
| Контроллер домена: требования подписывания для LDAP сервера | Не определено |
| Сервер сети Microsoft: Длительность простоя перед отключением сеанса | 15 мин. |
| Сервер сети Microsoft: использовать цифровую подпись (всегда) | Отключен |
| Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента) | Включен |
| Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа | Отключен |
| Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC) | Не определено |
| Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC) | Не определено |
| Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля | Включен |
| Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы | Отключен |
| Сетевая безопасность: требования подписывания для LDAP клиента | Не определено |
| Сетевая безопасность: уровень проверки подлинности LAN Manager | Отправлять только NTLMv2 ответ |
| Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей | Не определено |
| Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями | Включен |
| Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями | Включен |
| Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя | Отключен |
| Сетевой доступ: пути в реестре доступны через удаленное подключение | Не определено |
| Сетевой доступ: разрешать анонимный доступ к именованным каналам | Не определено |
| Сетевой доступ: разрешать анонимный доступ к общим ресурсам | Не определено |
| Сетевой доступ: разрешать применение разрешений для всех к анонимным пользователям | Отключен |
| Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания | Не определено |
| Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов | Группа администраторов |
| Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок) | Включен |
| Системные объекты: учитывать регистр для подсистем, отличных от Windows | Включен |
| Устройства: запретить пользователям установку драйверов принтера | Включен |
| Устройства: поведение при установке неподписанного драйвера | Предупреждать, но разрешать установку |
| Устройства: разрешать отстыковку без входа в систему | Включен |
| Устройства: разрешено форматировать и извлекать съемные носители | Администраторы |
| Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям | Включен |
| Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям | Включен |
| Учетные записи: ограничить использование пустых паролей только для консольного входа | Включен |
| Учетные записи: Переименование учетной записи администратора | adm |
| Учетные записи: Переименование учетной записи гостя | loser |
| Учетные записи: Состояние учетной записи 'Администратор' | Отключен[[65]](#footnote-66) |
| Учетные записи: Состояние учетной записи 'Гость' | Отключен |
| Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала | Отключен |
| Член домена: максимальный срок действия пароля учетных записей компьютера | 180 дн. |
| Член домена: отключить изменение пароля учетных записей компьютера | Отключен |
| Член домена: требует стойкого ключа сеанса (Windows 2000 или выше) | Отключен |
| Член домена: цифровая подпись данных безопасного канала, когда это возможно | Включен |
| Член домена: шифрование данных безопасного канала, когда это возможно | Включен |
| **Конфигурация Windows — Параметры безопасности — Журнал событий** |  |
| Запретить доступ локальной группы гостей к журналу безопасности | Включен |
| Запретить доступ локальной группы гостей к журналу приложений | Включен |
| Запретить доступ локальной группы гостей к системному журналу | Включен |
| Максимальный размер журнала безопасности | 81920 КБ |
| Максимальный размер журнала приложений | 32768 КБ |
| Максимальный размер системного журнала | 32768 КБ |
| Сохранение событий в журнале безопасности | Не определено |
| Сохранение событий в журнале безопасности | По мере надобности |
| Сохранение событий в журнале приложений | Не определено |
| Сохранение событий в журнале приложений | По мере надобности |
| Сохранение событий в системном журнале | Не определено |
| Сохранение событий в системном журнале | По мере надобности |
| **Конфигурация Windows — Параметры безопасности — Группы с ограниченным доступом[[66]](#footnote-67)** |  |
| **Конфигурация Windows — Параметры безопасности — Системные службы[[67]](#footnote-68)** |  |
| ASP.NET State Service | Отключено |
| DHCP-клиент | Авто |
| DNS-клиент | Авто |
| Kaspersky Endpoint Security Service | Не определено |
| MS Software Shadow Copy Provider | Отключено |
| NetMeeting Remote Desktop Sharing | Отключено |
| Plug and Play | Авто |
| QoS RSVP | Отключено |
| Secret Net 5 Hardware Support System | Авто |
| Secret Net Agent | Авто |
| Secret Net Core Service | Авто |
| Secret Net Integrity Check Service | Авто |
| Telnet | Вручную |
| Windows Audio | Авто |
| Windows CardSpace | Отключено |
| Windows Installer | Вручную |
| Windows Presentation Foundation Font Cache 3.0.0.0 | Отключено |
| Автоматическое обновление | Отключено |
| Автонастройка проводного доступа | Отключено |
| Агент защиты доступа к сети | Отключено |
| Адаптер производительности WMI | Вручную |
| Беспроводная настройка | Отключено |
| Брандмауэр Windows/Общий доступ к Интернету (ICS) | Отключено |
| Веб-клиент | Отключено |
| Вторичный вход в систему | Вручную |
| Диспетчер авто-подключений удаленного доступа | Вручную |
| Диспетчер логических дисков | Авто |
| Диспетчер очереди печати | Авто |
| Диспетчер подключений удаленного доступа | Вручную |
| Диспетчер сеанса справки для удаленного рабочего стола | Отключено |
| Диспетчер сетевого DDE | Вручную |
| Диспетчер учетных записей безопасности | Авто |
| Доступ к HID-устройствам | Вручную |
| Журнал событий | Авто |
| Журналы и оповещения производительности | Вручную |
| Запуск серверных процессов DCOM | Авто |
| Защищенное хранилище | Авто |
| Инструментарий управления Windows | Вручную |
| Источник бесперебойного питания | Вручную |
| Клиент отслеживания изменившихся связей | Авто |
| Клиент Паспорт АРМ УОС | Авто |
| Координатор распределенных транзакций | Авто |
| Локатор удаленного вызова процедур (RPC) | Вручную |
| Маршрутизация и удаленный доступ | Отключено |
| Модуль поддержки NetBIOS через TCP/IP | Авто |
| Обозреватель компьютеров | Отключено |
| Оповещатель | Вручную |
| Определение оборудования оболочки | Вручную |
| Планировщик заданий | Отключено. Для ПЭВМ "АРМ Администратора ПО", находящиеся в ТУ установить Авто |
| Поставщик поддержки безопасности NT LM | Вручную |
| Протокол HTTP SSL | Вручную |
| Рабочая станция | Авто |
| Расширения драйверов WMI (Windows Management Instrumentation) | Авто |
| Сервер | Отключено[[68]](#footnote-69) |
| Сервер папки обмена | Вручную |
| Сетевой вход в систему | Авто |
| Сетевые подключения | Авто |
| Система событий COM+ | Вручную |
| Системное приложение COM+ | Вручную |
| Служба COM записи компакт-дисков IMAPI | Отключено[[69]](#footnote-70) |
| Служба администрирования диспетчера логических дисков | Вручную |
| Служба восстановления системы | Отключено |
| Служба времени Windows | Авто |
| Служба загрузки изображений (WIA) | Отключено |
| Служба индексирования | Отключено |
| Служба обеспечения сети | Вручную |
| Служба обнаружения SSDP | Вручную |
| Служба протокола EAP | Вручную |
| Служба регистрации ошибок | Авто |
| Служба серийных номеров переносных устройств мультимедиа | Вручную |
| Служба сетевого DDE | Вручную |
| Служба сетевого расположения (NLA) | Авто |
| Служба сообщений | Авто |
| Служба управления сертификатами и ключами работоспособности | Вручную |
| Служба шлюза уровня приложения | Отключено |
| Службы IPSEC | Авто |
| Службы криптографии | Авто |
| Службы терминалов | Отключено |
| Смарт-карты | Авто |
| Совместимость быстрого переключения пользователей | Отключено |
| Справка и поддержка | Отключено |
| Съемные ЗУ | Авто |
| Телефония | Отключено |
| Темы | Отключено |
| Теневое копирование тома | Отключено |
| Уведомление о системных событиях | Авто |
| Удаленный вызов процедур (RPC) | Авто |
| Удаленный реестр | Отключено |
| Узел универсальных PnP-устройств | Авто |
| Управление приложениями | Вручную |
| Фоновая интеллектуальная служба передачи (BITS) | Вручную |
| Центр обеспечения безопасности | Отключено |
| **Конфигурация Windows — Параметры безопасности — Реестр** |  |
| **Конфигурация Windows — Параметры безопасности — Файловая система** |  |
| **Конфигурация Windows — Параметры безопасности — Политики открытого ключа** |  |
| Файловая система EFS |  |
| Параметры автоматического запроса сертификатов |  |
| Доверенные корневые центры сертификации |  |
| Доверительные отношения в предприятии |  |
| Параметры автоматической подачи заявок |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ** |  |
| Политики безопасности IP на "Служба каталогов Active Directory" |  |
| Client (Respond Only) | Нет |
| Secure Server (Require Security) | Нет |
| Server (Request Security) | Нет |
| **Административные шаблоны — Компоненты Windows — NetMeeting** |  |
| Запретить удаленное управление рабочим столом | Включена |
| **Административные шаблоны — Компоненты Windows — Internet Explorer[[70]](#footnote-71)** |  |
| **Административные шаблоны — Компоненты Windows — Совместимость приложений** |  |
| Выключить обработчик совместимости приложений | Отключена |
| Выключить мастер совместимости программ | Отключена |
| Удалить страницу свойств совместимости программ | Отключена |
| Выключить журнал событий справки приложения | Отключена |
| Предотвращение доступа к 16-разрядным приложениям | Отключена |
| **Административные шаблоны — Компоненты Windows — Просмотр событий** |  |
| URL-адрес EVENTS.ASP | Отключена |
| Программа EVENTS.ASP | Отключена |
| Параметры командной строки программы EVENTS.ASP | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы IIS (Internet Information Services)** |  |
| Запрет установки IIS | Отключена |
| **Административные шаблоны — Компоненты Windows — Центр обеспечения безопасности** |  |
| Включить "Центр обеспечения безопасности" (только для компьютеров в домене) | Отключена |
| **Административные шаблоны — Компоненты Windows — Планировщик заданий** |  |
| Скрывать страницы свойств | Включена |
| Запретить запуск и завершение задач | Включена |
| Запретить перетаскивание с помощью мыши | Включена |
| Запретить создание новых заданий | Включена |
| Запретить удаление заданий | Включена |
| Скрыть флажок дополнительных свойств в мастере планирования заданий | Включена |
| Запретить обзор | Включена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов** |  |
| Подключения, проверяемые на активность | Отключена |
| Автоматическое переподключение | Отключена |
| Ограничить пользователей службы терминалов одним удаленным сеансом | Отключена |
| Принудительная отмена фонового рисунка удаленного рабочего стола | Отключена |
| Запретить завершение консольного сеанса администратора | Отключена |
| Ограничить количество подключений | Отключена |
| Ограничить максимальную глубину цвета | Отключена |
| Разрешать удаленное подключение с использованием служб терминалов | Отключена |
| Не разрешать локальным администраторам настраивать разрешения | Отключена |
| Удалить элемент "Безопасность Windows" из меню Пуск | Отключена |
| Удалить элемент 'Отключение сеанса' из диалога завершения работы | Отключена |
| Задать путь для перемещаемых профилей TS | Отключена |
| Домашняя папка пользователя сервера терминалов | Отключена |
| Устанавливает правила удаленного управления для сеансов пользователей служб терминалов | Отключена |
| Запускать программу при подключении | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Перенаправление данных клиент/сервер** |  |
| Разрешить перенаправление часового пояса | Отключена |
| Не разрешать перенаправление буфера обмена | Отключена |
| Не разрешать перенаправление устройства чтения смарт-карт | Отключена |
| Разрешить перенаправление звука | Отключена |
| Не разрешать перенаправление COM-портов | Отключена |
| Не разрешать перенаправление клиентских принтеров | Отключена |
| Не разрешать перенаправление LPT-портов | Отключена |
| Не разрешать перенаправление дисков | Отключена |
| Не устанавливать используемый по умолчанию принтер клиента в качестве принтера для сеанса | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Шифрование и безопасность — Политика RPC-безопасности** |  |
| Безопасный сервер (требовать безопасность) | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Шифрование и безопасность** |  |
| Всегда запрашивать у клиента пароль при подключении | Отключена |
| Установить уровень шифрования для клиентских подключений | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Лицензирование** |  |
| Группа безопасности сервера лицензий | Отключена |
| Запретить повышение лицензий | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Временные папки** |  |
| Не использовать временные папки для сеанса | Отключена |
| Не удалять временные папки при выходе | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Клиент** |  |
| Запретить сохранение паролей | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Каталог сеансов** |  |
| Перенаправление IP-адреса сервера терминалов | Отключена |
| Сводный каталог сеансов | Отключена |
| Сервер каталога сеансов | Отключена |
| Имя кластера каталога сеансов | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Сеансы** |  |
| Задать ограничение по времени для отключенных сеансов | Отключена |
| Задать ограничение по времени для активных сеансов | Отключена |
| Задать ограничение по времени для бездействующих сеансов | Отключена |
| Разрешать переподключение только от исходного клиента | Отключена |
| Завершать сеанс при достижении ограничения по времени | Отключена |
| **Административные шаблоны — Компоненты Windows — Проводник** |  |
| Отключить защищенный режим протокола оболочки | Отключена |
| **Административные шаблоны — Компоненты Windows — Установщик Windows** |  |
| Запретить использование установщика Windows | Включена (никогда) |
| Всегда производить установку с повышенными привилегиями | Отключена |
| Запретить откат | Отключена |
| Удалить диалоговое окно обзора нового источника | Отключена |
| Запретить применение пакетов исправлений | Включена |
| Отключить запрос безопасности IE для сценариев Windows Installer | Отключена |
| Разрешить пользователям изменять параметры установки | Отключена |
| Разрешить обзор источника при повышенных привилегиях | Отключена |
| Разрешить использование носителей при повышенных привилегиях | Отключена |
| Разрешить применение пакетов исправлений во время привилегированных установок | Отключена |
| Разрешить администраторам выполнение установки в сеансе сервера терминалов | Отключена |
| Кэшировать файлы трансформации в безопасном месте на рабочей станции | Отключена |
| Ведение журнала | Включена |
| Запретить установки для пользователей | Отключена |
| Отключить создание контрольных точек восстановления системы | Включена |
| Запретить удаление обновлений | Отключена |
| Задать обязательные правила обновления компонентов | Отключена |
| Запретить пользователям, не являющимися администраторами, устанавливать обновления, подписанные изготовителем программ | Отключена |
| Максимальный размер кэша базисных файлов | Отключена |
| **Административные шаблоны—— Компоненты Windows — Windows Messenger** |  |
| Запретить выполнение Windows Messenger | Включена |
| Не запускать автоматически Windows Messenger при входе | Включена |
| **Административные шаблоны — Компоненты Windows — Управление цифровыми правами Windows Media (DRM)** |  |
| Запретить доступ к Интернету для Windows Media DRM | Включена |
| **Административные шаблоны — Компоненты Windows — Windows Movie Maker** |  |
| Запретить выполнение программы Windows Movie Maker | Включена |
| **Административные шаблоны — Компоненты Windows — Windows Update** |  |
| Не отображать параметр "Установить обновления и завершить работу" в диалоговом окне завершения работы Windows | Включена |
| Не настраивать параметр "Установить обновления и завершить работу" в диалоговом окне завершения работы Windows в качестве параметра по умолчанию | Включена |
| Настройка автоматического обновления | Отключена |
| Указать размещение службы обновлений Microsoft в интрасети | Отключена |
| Разрешить клиенту присоединение к целевой группе | Отключена |
| Перенос запланированных автоматических установок обновлений | Отключена |
| Не выполнять автоматический повторный запуск для автоматических установок обновлений | Включена |
| Частота поиска автоматических обновлений | Отключена |
| Разрешить немедленную установку автоматических обновлений | Отключена |
| Задержка перезагрузки при запланированных установках | Отключена |
| Повторный запрос для перезагрузки при запланированных установках | Отключена |
| **Административные шаблоны — Компоненты Windows — Проигрыватель Windows Media** |  |
| Не отображать диалоговые окна первого использования | Включена |
| Не создавать ярлык на рабочем столе | Включена |
| Не создавать ярлык на панели быстрого запуска | Включена |
| Запретить автоматические обновления | Включена |
| Запретить сглаживание изображения | Включена |
| **Secret Net Integrity Check settings (Добавляется в соответствии с разделом «Централизованное управление списком расширений**  **исполняемых файлов» документа СЗИ от НСД SecretNet 7 Руководство администратора. Управление. Основные механизмы защиты)** |  |
| Extension Executive [[71]](#footnote-72) | Включена (.exe;.dll;.cpl;.drv;.sys;.ocx;.vbs;.scr; .rll;.ime;.bpl;.ax;.acm;.com;.ppl;.cmd;.bat;.ovl;.tbp;.lnk, .manifest;.mui) [[72]](#footnote-73) |
| **Административные шаблоны — Система** |  |
| Предотвращение доступа к потенциально небезопасным функциям справки HTML для указанных папок | Включена (пустой список) |
| Не отображать страницу "Управление данным сервером" при входе | Включена |
| Отображать диалог слежения за завершением работы | Отключена |
| Включить свойство данных состояния системы слежения за завершением работы | Отключена |
| Включить постоянную временную метку | Включена (60 сек.) |
| Указать расположение установочных файлов Windows | Отключена |
| Указать размещение установочных файлов пакета обновления Windows | Отключена |
| Отключить сообщения о состоянии загрузки, завершения работы, входа и выхода из сети | Отключена |
| Подробные сообщения о состоянии | Отключена |
| Запретить запуск из Справки перечисленных программ | Включена (\*.\*) |
| Отключить автозапуск | Включена (все диски) |
| Не выполнять автоматическое шифрование файлов, перемещаемых в зашифрованные папки | Отключена |
| Загружать отсутствующие COM-компоненты | Включена |
| Разрешить клиентам отслеживания изменившихся связей использовать ресурсы домена | Отключена |
| Не выключайте питание компьютера после завершения работы Windows. | Отключена |
| Отключить запрос на использование Windows Update при поиске драйверов | Включена |
| **Административные шаблоны — Система — Профили пользователей** |  |
| Не проверять собственность пользователя перемещаемого профиля | Отключена |
| Удалять кэшированные копии перемещаемых профилей | Отключена |
| Не определять медленные подключения | Отключена |
| Таймаут для профилей пользователей для медленных сетевых подключений | Отключена |
| Дождаться загрузки перемещаемого пользовательского профиля | Отключена |
| Выдавать запрос пользователю при обнаружении медленного подключения | Отключена |
| Таймаут диалоговых окон | Отключена |
| Завершать сеанс пользователя в случае ошибки перемещаемого профиля | Отключена |
| Максимальное число повторов попыток выгрузки и обновления профиля пользователя | Отключена |
| Добавлять группу администраторов для перемещаемых профилей пользователя | Отключена |
| Запретить распространение изменений в перемещаемом профиле на сервер | Включена |
| Разрешать использование только локальных профилей | Отключена |
| Оставить установочные данные установщика Windows и групповой политики | Отключена |
| **Административные шаблоны — Система — Сценарии** |  |
| Синхронное выполнение сценариев входа в систему | Включена |
| Асинхронное выполнение сценариев загрузки | Отключена |
| Выполнять сценарии загрузки с отображением команд | Отключена |
| Выполнять сценарии завершения работы с отображением команд | Отключена |
| Максимальное время выполнения сценариев групповой политики | Отключена |
| **Административные шаблоны — Система — Вход в систему** |  |
| Не отображать окно "Первое знакомство" при входе в систему | Отключена |
| Всегда использовать классический вход в систему | Включена,  Отключена для АРМ Инкассатора АС ЭКР 2.0 и АРМ Заведующего кладовой АС ЭКР 2.0 |
| Запускать указанные программы при входе в систему | Отключена |
| Не обрабатывать список автозапуска программ, выполняемых однажды | Отключена |
| Не обрабатывать список автозапуска для старых версий | Отключена |
| Всегда ожидать инициализации сети при загрузке и входе в систему | Включена |
| **Административные шаблоны — Система — Дисковые квоты** |  |
| Включить дисковые квоты | Отключена |
| Задать предел дисковой квоты | Отключена |
| Предел квоты по умолчанию и уровень предупреждения | Отключена |
| Вести журнал даже при превышении предела квоты | Отключена |
| Заносить событие превышение уровня предупреждения квоты | Отключена |
| Применять политику к съемным носителям | Отключена |
| **Административные шаблоны — Система — Сетевой вход в систему** |  |
| Ожидаемая задержка при удаленном входе | Отключена |
| Имя сайта | Не задана [[73]](#footnote-74) |
| Кэш-параметр негативного обнаружения контроллеров домена | Отключена |
| Начальный интервал попыток обнаружения контроллеров домена для фоновых клиентов | Отключена |
| Максимальный интервал повторных попыток обнаружения контроллера домена для фоновых клиентов | Отключена |
| Окончательный интервал попыток обнаружения контроллера домена для фоновых клиентов | Отключена |
| Положительное периодическое обновление кэша DC для фонового вызова | Отключена |
| Положительное периодическое обновление кэша DC для не фонового вызова | Отключена |
| Интервал очистки | Отключена |
| Обращение к PDC в случае неудачи входа в систему | Отключена |
| Уровень отладки файла журнала | Отключена |
| Максимальный размер файла журнала | Отключена |
| Совместимость общего ресурса Sysvol | Отключена |
| Совместимость общего сетевого доступа | Отключена |
| **Административные шаблоны — Система — Сетевой вход в систему — DNS-записи локатора контроллеров домена** [[74]](#footnote-75) |  |
| Динамическая регистрация DNS-записей локатора контроллеров домена | Не задана |
| DNS-записи локатора контроллеров домена, не регистрируемые контроллерами доменов | Не задана |
| Интервал обновления DNS-записей локатора контроллеров домена | Не задана |
| Набор весов DNS SRV-записей локатора контроллеров домена | Не задана |
| Приоритет, установленный в DNS SRV-записях локатора контроллеров домена | Не задана |
| Набор TTL DNS-записей локатора контроллеров домена | Не задана |
| Автоматическое обслуживание сайта DNS SRV-записями локатора контроллеров домена | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора контроллеров домена | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора глобального каталога | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора раздела каталога приложений | Не задана |
| Обнаружение DC, несущих домен с однокомпонентным DNS-именем | Не задана |
| **Административные шаблоны — Система — Групповая политика** |  |
| Отключить фоновое обновление групповой политики | Отключена |
| Интервал обновления групповой политики для компьютеров | Отключена |
| Интервал обновления групповой политики для контроллеров домена | Отключена |
| Режим обработки замыкания пользовательской групповой политики | Отключена. Для ПЭВМ «Криптоцентр-Авизо» - включена. |
| Включить политику пользователя перекрестного леса и перемещаемые профили пользователя | Отключена |
| Разрешить выполнение сценариев входа в систему при отключенной службе NetBIOS | Включена |
| Обнаружение медленных подключений для групповой политики | Отключена |
| Отключить протоколирование RSoP | Отключена |
| Запретить пользователям вызывать обновление политики компьютера | Включена |
| Запретить интерактивным пользователям создавать данные результирующей политики (RSoP) | Включена |
| Обработка политики реестра | Отключена |
| Обработка политики настройки Internet Explorer | Отключена |
| Обработка политики установки программ | Отключена |
| Обработка политики перенаправления папки | Отключена |
| Обработка политики сценариев | Отключена |
| Обработка политики безопасности | Отключена |
| Обработка политики IP-безопасности | Отключена |
| Обработка беспроводной политики | Отключена |
| Обработка политики восстановления EFS | Отключена |
| Обработка политики дисковой квоты | Отключена |
| Всегда использовать локальные файлы ADM для редактора объектов групповой политики | Отключена |
| **Административные шаблоны — Система — Удаленный помощник** |  |
| Запрошенная удаленная помощь | Отключена |
| Разрешить предложение удаленной помощи | Отключена |
| **Административные шаблоны — Система — Восстановление системы** |  |
| Отключить восстановление системы | Включена |
| Отключить конфигурацию | Включена |
| **Административные шаблоны — Система — Отчет об ошибках** |  |
| Отображать уведомления об ошибках | Отключена |
| Настроить отчеты об ошибках | Отключена |
| **Административные шаблоны — Система — Отчет об ошибках — Параметры расширенного отчета об ошибках** |  |
| Параметры по умолчанию отчета об ошибках приложений | Отключена |
| Список приложений, для которых нужно отправлять отчет об ошибках | Отключена |
| Список приложений, для которых не нужно отправлять отчет об ошибках | Отключена |
| Сообщать о системных ошибках | Отключена |
| Отправлять отчет о незапланированном завершении работы | Отключена |
| **Административные шаблоны — Система — Защита файлов Windows** |  |
| Установить частоту сканирования защиты файлов Windows | Отключена |
| Скрывать окно индикации сканирования файлов | Включена |
| Ограничить размер кэша защиты файлов Windows | Отключена |
| Укажите размещение кэша для защиты файлов Windows | Отключена |
| **Административные шаблоны — Система — Удаленный вызов процедур (RPC)** |  |
| Диагностическая информация состояния RPC | Отключена |
| Передача расширенных сведений об ошибках | Отключена |
| Пропустить сбой делегирования | Отключена |
| Минимальный таймаут простаивающих подключений для RPC/HTTP-подключений | Отключена |
| Ограничения для не прошедших проверку подлинности RPC-клиентов | Отключена |
| Проверка RPC-клиентов сопоставителя конечных точек | Отключена |
| **Административные шаблоны — Система — Служба времени Windows** |  |
| Глобальные параметры конфигурации | Отключена |
| **Административные шаблоны — Система — Служба времени Windows — Поставщики времени** |  |
| Включить Windows NTP-клиента | Включена |
| Настроить Windows NTP-клиента | Отключена |
| Включить Windows NTP-сервер | Отключена |
| **Административные шаблоны — Система — Управление связью через Интернет** |  |
| Ограничить связь через Интернет | Включена |
| **Административные шаблоны — Система — Управление связью через Интернет — Параметры связи через Интернет** |  |
| Отключить веб-публикацию в списке задач для файлов и папок | Включена |
| Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков | Включена |
| Отключить заказ отпечатков через Интернет в списке задач для изображений | Включена |
| Отключить участие в программе улучшения поддержки пользователей Windows Messenger | Включена |
| Отключить отображение раздела "Знаете ли вы?" в окне "Центра справки и поддержки" | Включена |
| Отключить поиск в базе знаний Майкрософт в окне "Центра справки и поддержки" | Включена |
| Отключить отчеты об ошибках Windows | Включена |
| Отключить службу сопоставления файлов Интернета | Включена |
| Отключить мастер подключения к Интернету, если URL-адрес ссылается на MICROSOFT.COM | Включена |
| Отключить ссылки EVENTS.ASP в программе "Просмотр событий" | Включена |
| Отключить автоматическое обновление корневых сертификатов | Включена |
| Отключить регистрацию, если URL-адрес ссылается на MICROSOFT.COM | Включена |
| Отключить обновление информационных файлов "Помощника по поиску" | Включена |
| Отключить выполнение печати через HTTP-протокол | Включена |
| Отключить загрузку драйверов печати через HTTP-протокол | Включена |
| Отключить использование Windows Update при поиске драйверов | Включена |
| Отключить доступ ко всем возможностям Windows Update | Включена |
| Отключить автоматическую загрузку кодеков для Windows Movie Maker | Включена |
| Отключить веб-ссылки в Windows Movie Maker | Включена |
| Отключить сохранение видео на веб-узлах поставщиков видеохостинга в Windows Movie Maker | Включена |
| **Административные шаблоны — Система — DCOM — Параметры совместимости приложений** |  |
| Разрешать локальные исключения проверки безопасности при активации | Отключена |
| Задать исключения проверки безопасности при активации | Отключена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft — PNRP-протокол (Peer Name Resolution Protocol) — Глобальные облака** |  |
| Задать сервер инициализации | Отключена |
| Отключить многоадресную загрузку | Включена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft — PNRP-протокол (Peer Name Resolution Protocol) — Локальные облака сайта** |  |
| Задать сервер инициализации | Отключена |
| Отключить многоадресную загрузку | Включена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft — PNRP-протокол (Peer Name Resolution Protocol) — Локальные облака связи** |  |
| Задать сервер инициализации | Отключена |
| Отключить многоадресную загрузку | Включена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft** |  |
| Отключить службы одноранговых сетей Microsoft | Включена |
| **Административные шаблоны — Сеть — DNS-клиент** |  |
| Основной DNS суффикс | Отключена |
| Динамическое обновление | Включена |
| Порядок просмотра суффиксов DNS | Отключена |
| Регрессирование основного DNS-суффикса | Включена |
| Регистрация PTR-записей | Включена (регистрация только если A-запись успешно зарегистрирована) |
| Интервал обновления регистрации | Включена (1800 сек.) |
| Замена адресов в случае конфликтов | Отключена |
| DNS-серверы | Отключена |
| DNS-суффикс этого подключения | Отключена |
| Регистрировать DNS-записи с DNS-суффиксом подключения | Включена |
| Установить TTL для A- и PTR-записей | Отключена |
| Уровень безопасности обновлений | Отключена |
| Обновлять зоны доменов верхнего уровня | Отключена |
| **Административные шаблоны — Сеть — Автономные файлы** |  |
| Разрешить или запретить использование автономных файлов | Отключена |
| Запретить пользовательскую настройку автономных файлов | Включена |
| Синхронизовать автономные файлы при входе в систему | Отключена |
| Синхронизация всех автономных файлов перед выходом из системы | Отключена |
| Синхронизовать автономные файлы перед приостановкой | Отключена |
| Размер кэша по умолчанию | Отключена |
| Действия при отключении от сервера | Отключена |
| Нестандартные действия при отключении от сервера | Отключена |
| Удалить "Сделать доступными автономно" | Включена |
| Запретить использование папки "Автономные файлы" | Включена |
| Некэшируемые файлы | Отключена |
| Административно назначенные автономные файлы | Отключена |
| Отключить всплывающие напоминания | Включена |
| Частота появления всплывающих напоминаний | Отключена |
| Длительность отображения первого всплывающего напоминания | Отключена |
| Длительность отображения всплывающих напоминаний | Отключена |
| При выходе из системы удалять локальную копию автономных файлов пользователя | Включена |
| Уровень регистрации событий | Отключена |
| Сделать подпапки всегда доступными в автономном режиме | Отключена |
| Шифровать кэш автономных файлов | Отключена |
| Запретить применение "Сделать доступными автономно" для этих файлов и папок | Отключена |
| Настроить скорость медленного подключения | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения — Брандмауэр Windows — Профиль домена** |  |
| Брандмауэр Windows: Защитить все сетевые подключения | Отключена |
| Брандмауэр Windows: Не разрешать исключения | Отключена |
| Брандмауэр Windows: Задать исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного управления | Отключена |
| Брандмауэр Windows: Разрешать исключения для общего доступа к файлам и принтерам | Отключена |
| Брандмауэр Windows: Разрешать исключения ICMP | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного рабочего стола | Отключена |
| Брандмауэр Windows: Разрешать исключения для UPnP-инфраструктуры | Отключена |
| Брандмауэр Windows: Запретить уведомления | Отключена |
| Брандмауэр Windows: Разрешать ведение журнала | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | Отключена |
| Брандмауэр Windows: Задать исключения для портов | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для портов | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения — Брандмауэр Windows — Стандартный профиль** |  |
| Брандмауэр Windows: Защитить все сетевые подключения | Отключена |
| Брандмауэр Windows: Не разрешать исключения | Отключена |
| Брандмауэр Windows: Задать исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного управления | Отключена |
| Брандмауэр Windows: Разрешать исключения для общего доступа к файлам и принтерам | Отключена |
| Брандмауэр Windows: Разрешать исключения ICMP | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного рабочего стола | Отключена |
| Брандмауэр Windows: Разрешать исключения для UPnP-инфраструктуры | Отключена |
| Брандмауэр Windows: Запретить уведомления | Отключена |
| Брандмауэр Windows: Разрешать ведение журнала | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | Отключена |
| Брандмауэр Windows: Задать исключения для портов | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для портов | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения — Брандмауэр Windows** |  |
| Брандмауэр Windows: Разрешать обход для прошедших проверку IPSec | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения** |  |
| Запретить использование общего доступа к подключению Интернета в сети DNS-домена | Включена |
| Запретить использование брандмауэра подключения к Интернету в сети DNS-домена | Отключена |
| Запретить установку и настройку сетевых мостов в вашей сети DNS-доменов | Отключена |
| IEEE 802.1x Центр Сертификации для проверки подлинности компьютеров | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS — Значение DSCP для соответствующих пакетов** |  |
| Тип службы "Best effort" | Отключена |
| Тип службы "Controlled load" | Отключена |
| Тип службы "Guaranteed" | Отключена |
| Тип службы "Network control" | Отключена |
| Тип службы "Qualitative" | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS — Значение DSCP для не соответствующих пакетов** |  |
| Тип службы "Best effort" | Отключена |
| Тип службы "Controlled load" | Отключена |
| Тип службы "Guaranteed" | Отключена |
| Тип службы "Network control" | Отключена |
| Тип службы "Qualitative" | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS — Значение приоритета второго уровня** |  |
| Не соответствующие пакеты | Отключена |
| Тип службы "Best effort" | Отключена |
| Тип службы "Controlled load" | Отключена |
| Тип службы "Guaranteed" | Отключена |
| Тип службы "Network control" | Отключена |
| Тип службы "Qualitative" | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS** |  |
| Ограничить резервируемую пропускную способность | Отключена |
| Ограничение ожидающих обработки пакетов | Отключена |
| Задать разрешение таймера | Отключена |
| **Административные шаблоны — Сеть — SNMP** |  |
| Сообщества | Отключена |
| Разрешенные диспетчеры | Отключена |
| Ловушки только для публичного сообщества | Отключена |
| **Административные шаблоны — Сеть — Фоновая интеллектуальная служба передачи (BITS)** |  |
| Максимальная пропускная способность сети, используемая BITS | Отключена |
| Таймаут (в днях) для неактивных заданий | Отключена |
| **Административные шаблоны — Сеть** |  |
| Частота выполнения обнаружения контроллеров домена клиентом DFS | Отключена |
| **Административные шаблоны — Принтеры** |  |
| Разрешить публикацию принтеров | Включена |
| Разрешить очистку опубликованных принтеров | Включена |
| Автоматическая публикация новых принтеров в Active Directory | Отключена |
| Проверять состояние публикации | Отключена |
| Размещение компьютера | Отключена |
| Особый URL-адрес службы поддержки в левой панели папки принтеров | Отключена |
| Интервал очистки Active Directory | Отключена |
| Приоритет потока при очистке Active Directory | Отключена |
| Повторы при очистке Active Directory | Отключена |
| Запретить установку принтеров, использующих работающие в режиме ядра драйверы | Отключена |
| Записывать события контакта службы очистки каталогов | Отключена |
| Заполнение строки поиска принтеров | Отключена |
| Обзор принтеров | Включена |
| Удалять принтеры, которые не были автоматически повторно опубликованы | Отключена |
| Разрешить диспетчеру печати добавление новых клиентских подключений | Включена |
| Печать на основе использования веба | Отключена |

Таблица (Таблица 41) содержит настройки параметров групповой политики, применяемой для файловых серверов и контроллеров платежного домена при использовании СЗИ от НСД «SecretNet».

Таблица 41. Настройки параметров групповой политики, применяемой для файловых серверов и контроллеров платежного домена при использовании СЗИ от НСД «SecretNet»

| **Наименование раздела/параметра групповой политики** | **Значение параметра** |
| --- | --- |
| **Конфигурация программ** |  |
| **Конфигурация Windows — Сценарии (запуск/завершение)** |  |
| **Конфигурация Windows — Параметры безопасности — Политики учетных записей — Политика паролей [[75]](#footnote-76)** |  |
| Макс. срок действия пароля | 180 дней |
| Мин. длина пароля | 8 символов |
| Мин. срок действия пароля | 0 дней |
| Пароль должен отвечать требованиям сложности | Включен |
| Требовать неповторяемости паролей | 5 хранимых паролей |
| Хранить пароли всех пользователей в домене, используя обратимое шифрование | Отключен |
| **Конфигурация Windows — Параметры безопасности — Политики учетных записей — Политика блокировки учетной записи** |  |
| Блокировка учетной записи на | 0 |
| Пороговое значение блокировки | 3 ошибок входа в систему |
| Сброс счетчика блокировки через | 30 минут |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Политика аудита** |  |
| Аудит входа в систему | Успех, Отказ |
| Аудит доступа к объектам | Успех, Отказ |
| Аудит доступа к службе каталогов | Отказ (Нет аудита – для контроллеров домена) |
| Аудит изменения политики | Успех, Отказ |
| Аудит использования привилегий | Нет аудита |
| Аудит отслеживания процессов | Нет аудита |
| Аудит системных событий | Успех, Отказ |
| Аудит событий входа в систему | Успех, Отказ |
| Аудит управления учетными записями | Успех, Отказ |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Назначение прав пользователя** |  |
| Архивирование файлов и каталогов | Администраторы |
| Восстановление файлов и каталогов | Администраторы |
| Вход в качестве пакетного задания | Локальная система, Администраторы, musr\_mqadmin |
| Вход в качестве службы | <имя\_ домена>\mservice,  <имя\_домена>[[76]](#footnote-77) \HP ITO account,  Для серверов приложений АС ЭКР:  musr\_mqadmin, <имя\_домена> \HP ITO account |
| Добавление рабочих станций к домену | Администраторы |
| Доступ к компьютеру из сети | Прошедшие проверку |
| Завершение работы системы | Администраторы, Прошедшие проверку |
| Загрузка и выгрузка драйверов устройств | Администраторы |
| Закрепление страниц в памяти | [[77]](#footnote-78) |
| Замена маркера уровня процесса | Локальная система, Сетевая служба, musr\_mqadmin |
| Запретить вход в систему через службу терминалов |  |
| Запуск операций по обслуживанию тома | Администраторы |
| Извлечение компьютера из стыковочного узла | Администраторы |
| Изменение параметров среды оборудования | Администраторы |
| Изменение системного времени | Администраторы |
| Локальный вход в систему | Администраторы, Прошедшие проверку |
| Настройка квот памяти для процесса | Администраторы,  Локальная система, Сетевая служба, musr\_mqadmin |
| Обход перекрестной проверки | Прошедшие проверку,  musr\_mqadmin |
| Овладение файлами или иными объектами | Администраторы |
| Олицетворение клиента после проверки подлинности | СЛУЖБА, Администраторы |
| Отказ в доступе к компьютеру из сети | loser |
| Отказ во входе в качестве пакетного задания |  |
| Отказать во входе в качестве службы |  |
| Отклонить локальный вход |  |
| Отладка программ | Администраторы |
| Принудительное удаленное завершение | Администраторы |
| Профилирование загруженности системы | Администраторы |
| Профилирование одного процесса | Администраторы |
| Работа в режиме операционной системы | Локальная система,  musr\_mqadmin |
| Разрешать вход в систему через службу терминалов | Администраторы[[78]](#footnote-79) |
| Разрешение доверия к учетным записям при делегировании | Администраторы |
| Синхронизация данных службы каталогов | Администраторы |
| Создание глобальных объектов | Администраторы |
| Создание журналов безопасности | Локальная система, Сетевая служба |
| Создание маркерного объекта | Локальная система |
| Создание постоянных объектов совместного использования | Локальная система |
| Создание страничного файла | Администраторы |
| Увеличение приоритета диспетчирования | Администраторы |
| Управление аудитом и журналом безопасности[[79]](#footnote-80) | <имя\_домена>\Auditors, <имя\_домена>\HP ITO account[[80]](#footnote-81) |
| **Конфигурация Windows — Параметры безопасности — Локальные политики — Параметры безопасности** |  |
| DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language) | Не определено |
| DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language) | Не определено |
| Аудит: аудит доступа глобальных системных объектов | Отключен |
| Аудит: аудит прав на архивацию и восстановление | Отключен |
| Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности | Отключен |
| Доступ к сети: Разрешить трансляцию анонимного SID в имя | Отключен |
| Завершение работы: очистка страничного файла виртуальной памяти | Включен |
| Завершение работы: разрешить завершение работы системы без выполнения входа в систему | Включен |
| Интерактивный вход в систему: поведение при извлечении смарт-карты | Блокировка рабочей станции |
| Интерактивный вход в систему: требовать смарт-карту | Отключен |
| Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему | Не определено |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | 0 Входы в систему |
| Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее | 5 дн. |
| Интерактивный вход в систему: не отображать последнего имени пользователя | Включен |
| Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL | Включен |
| Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован | Не определено |
| Интерактивный вход в систему: текст сообщения для пользователей при входе в систему | Не определено |
| Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (всегда) | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) | Включен |
| Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам | Отключен |
| Консоль восстановления: разрешить автоматический вход администратора | Отключен |
| Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам | Отключен |
| Контроллер домена: запретить изменение пароля учетных записей компьютера | Отключен |
| Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию | Отключен |
| Контроллер домена: требования подписывания для LDAP сервера | Не определено |
| Сервер сети Microsoft: Длительность простоя перед отключением сеанса | 15 мин. |
| Сервер сети Microsoft: использовать цифровую подпись (всегда) | Отключен |
| Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента) | Включен |
| Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа | Отключен |
| Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC) | Не определено |
| Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC) | Не определено |
| Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля | Включен |
| Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы | Отключен |
| Сетевая безопасность: требования подписывания для LDAP клиента | Не определено |
| Сетевая безопасность: уровень проверки подлинности LAN Manager | Отправлять только NTLMv2 ответ |
| Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей | Не определено |
| Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями | Отключен |
| Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями | Включен |
| Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя | Отключен |
| Сетевой доступ: пути в реестре доступны через удаленное подключение | Не определено |
| Сетевой доступ: разрешать анонимный доступ к именованным каналам | Включен (SnHwSrv), SnicheckSrv)[[81]](#footnote-82) |
| Сетевой доступ: разрешать анонимный доступ к общим ресурсам | Не определено |
| Сетевой доступ: разрешать применение разрешений для всех к анонимным пользователям | Отключен |
| Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания | Не определено |
| Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов | Группа администраторов |
| Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок) | Включен |
| Системные объекты: учитывать регистр для подсистем, отличных от Windows | Включен |
| Устройства: запретить пользователям установку драйверов принтера | Включен |
| Устройства: поведение при установке неподписанного драйвера | Предупреждать, но разрешать установку |
| Устройства: разрешать отстыковку без входа в систему | Включен |
| Устройства: разрешено форматировать и извлекать съемные носители | Администраторы |
| Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям | Включен. |
| Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям | Включен |
| Учетные записи: ограничить использование пустых паролей только для консольного входа | Включен |
| Учетные записи: Переименование учетной записи администратора | adm |
| Учетные записи: Переименование учетной записи гостя | loser |
| Учетные записи: Состояние учетной записи 'Администратор' | Включен |
| Учетные записи: Состояние учетной записи 'Гость' | Отключен |
| Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала | Отключен |
| Член домена: максимальный срок действия пароля учетных записей компьютера | 180 дн. |
| Член домена: отключить изменение пароля учетных записей компьютера | Отключен |
| Член домена: требует стойкого ключа сеанса (Windows 2000 или выше) | Отключен |
| Член домена: цифровая подпись данных безопасного канала, когда это возможно | Включен |
| Член домена: шифрование данных безопасного канала, когда это возможно | Включен |
| **Конфигурация Windows — Параметры безопасности — Журнал событий** |  |
| Запретить доступ локальной группы гостей к журналу безопасности | Включен |
| Запретить доступ локальной группы гостей к журналу приложений | Включен |
| Запретить доступ локальной группы гостей к системному журналу | Включен |
| Максимальный размер журнала безопасности | 81920 КБ |
| Максимальный размер журнала приложений | 32768 КБ |
| Максимальный размер системного журнала | 32768 КБ |
|  |  |
| Сохранение событий в журнале безопасности | По мере надобности |
|  |  |
| Сохранение событий в журнале приложений | По мере надобности |
|  |  |
| Сохранение событий в системном журнале | По мере надобности |
| **Конфигурация Windows — Параметры безопасности — Группы с ограниченным доступом[[82]](#footnote-83)** |  |
| **Конфигурация Windows — Параметры безопасности — Системные службы[[83]](#footnote-84)** |  |
| BITS - фоновая интеллектуальная служба передачи | Отключено |
| Data Protector Inet | Авто |
| DHCP-клиент | Авто |
| DNS-клиент | Авто |
| DNS-сервер | Не определено [[84]](#footnote-85) |
| HP OpenView Ctrl Service | Автоматическое [[85]](#footnote-86) |
| HP ProLiant Remote Monitor Service |
| HP ProLiant System Shutdown Service |
| HP Smart Array SAS/SATA Event Notification Service |
| HP Software Shared Trace Service |
| HP System Management Homepage |
| HP Version Control Agent |
| HTTP SSL | Автоматическое |
| Microsoft Software Shadow Copy Provider | Авто |
| NetMeeting Remote Desktop Sharing | Отключено |
| Plug and Play | Авто |
| Portable Media Serial Number Service | Вручную |
| Secret Net 5 Hardware Support System | Авто |
| Secret Net Agent | Авто |
| Secret Net Core Service | Авто |
| Secret Net Integrity Check Service | Авто |
| SQL Server (MSSQLSERVER) | Авто |
| SQL Server, обозреватель | Авто |
| Telnet | Вручную |
| Windows Audio | Авто |
| Windows CardSpace | Отключено |
| Windows Installer | Вручную |
| Windows Presentation Foundation Font Cache 3.0.0.0 | Отключено |
| Автоматическое обновление | Отключено |
| Агент SQL Server (MSSQLSERVER) | Авто |
| Адаптер производительности WMI | Вручную |
| Беспроводная настройка | Отключено |
| Брандмауэр Windows/Общий доступ к Интернету (ICS) | Отключено |
| Веб-клиент | Отключено |
| Вторичный вход в систему | Вручную |
| Диспетчер автоматических подключений удаленного доступа | Вручную |
| Диспетчер логических дисков | Авто |
| Диспетчер очереди печати | Авто |
| Диспетчер подключений удаленного доступа | Вручную |
| Диспетчер сеанса справки для удаленного рабочего стола | Вручную |
| Диспетчер сетевого DDE | Вручную |
| Диспетчер учетных записей безопасности | Авто |
| Доступ к HID-устройствам | Вручную |
| Журнал событий | Авто |
| Журналы и оповещения производительности | Вручную |
| Запуск серверных процессов DCOM | Авто |
| Защищенное хранилище | Авто |
| Инструментарий управления Windows | Вручную  (Авто – для контроллеров домена) |
| Источник бесперебойного питания | Вручную |
| Каталог сеанса служб терминалов | Авто |
| Клиент отслеживания изменившихся связей | Авто |
| Клиент Паспорт АРМ УОС | Авто |
| Компонент драйверов пользовательского режима Windows | Авто |
| Координатор распределенных транзакций | Авто |
| Локатор удаленного вызова процедур (RPC) | Вручную |
| Маршрутизация и удаленный доступ | Отключено |
| Модуль поддержки NetBIOS через TCP/IP | Авто |
| Модуль поддержки специальной консоли администрирования | Вручную |
| Модуль сервера SQL Server для записи VSS | Авто |
| Обозреватель компьютеров | Авто |
| Оповещатель | Вручную |
| Определение оборудования оболочки | Вручную |
| Планировщик заданий | Авто |
| Поставщик поддержки безопасности NT LM | Авто |
| Поставщик результирующей политики (RSoP) | Авто |
| Рабочая станция | Авто |
| Распределенная файловая система DFS | Авто |
| Расширения драйверов WMI (Windows Management Instrumentation) | Авто |
| Сервер | Авто |
| Сервер генерации УИД | Авто |
| Сервер отслеживания изменившихся связей | Вручную |
| Сервер папки обмена | Вручную |
| Сервис аутентификации | Авто |
| Сервис имен CORBA | Авто |
| Сервис регистрационного журнала | Авто |
| Сетевой вход в систему | Авто |
| Сетевые подключения | Авто |
| Система событий COM+ | Вручную |
| Системное приложение COM+ | Вручную |
| Служба COM записи компакт-дисков IMAPI | Отключено |
| Служба Intersite Messaging | Отключено  (Авто – для контроллеров домена) |
| Служба авто-обнаружения веб-прокси WinHTTP | Отключено |
| Служба администрирования диспетчера логических дисков | Авто |
| Служба виртуальных дисков | Авто |
| Служба времени Windows | Авто |
| Служба загрузки изображений (WIA) | Вручную |
| Служба индексирования | Отключено |
| Служба обеспечения сети | Авто |
| Служба поддержки Active Directory сервера SQL Server | Вручную |
| Служба проверки совместимости приложений | Отключено |
| Служба регистрации ошибок | Авто |
| Служба репликации файлов | Авто |
| Служба сетевого DDE | Авто |
| Служба сетевого расположения (NLA) | Авто |
| Служба сообщений | Авто |
| Служба состояний ASP.NET | Отключено |
| Служба шлюза уровня приложения | Авто |
| Службы IPSEC | Авто |
| Службы SQL Server Integration Services 10.0 | Авто |
| Службы SQL Server Reporting Services (MSSQLSERVER) | Вручную |
| Службы криптографии | Вручную |
| Службы терминалов | Авто[[86]](#footnote-87) |
| Смарт-карты | Авто |
| Справка и поддержка | Отключено |
| Съемные ЗУ | Авто |
| Телефония | Вручную |
| Темы | Отключено |
| Теневое копирование тома | Вручную |
| Уведомление о системных событиях | Авто |
| Удаленный вызов процедур (RPC) | Авто |
| Удаленный реестр | Авто |
| Управление приложениями | Авто |
| Учет лицензий | Авто |
| Центр распространения ключей Kerberos | Вручную (Авто - для контроллеров домена). |
| **Конфигурация Windows — Параметры безопасности — Реестр** |  |
| **Конфигурация Windows — Параметры безопасности — Файловая система** |  |
| **Конфигурация Windows — Параметры безопасности — Политики открытого ключа** |  |
| Файловая система EFS |  |
| Параметры автоматического запроса сертификатов |  |
| Доверенные корневые центры сертификации |  |
| Доверительные отношения в предприятии |  |
| Параметры автоматической подачи заявок |  |
| **Конфигурация Windows — Параметры безопасности — Политики ограниченного использования программ** |  |
| **Конфигурация Windows — Параметры безопасности — Политики безопасности IP на "Служба каталогов Active Directory"** |  |
| Client (Respond Only) | Нет |
| Secure Server (Require Security) | Нет |
| Server (Request Security) | Нет |
| **Административные шаблоны — Компоненты Windows — NetMeeting** |  |
| Запретить удаленное управление рабочим столом | Включена |
| **Административные шаблоны — Компоненты Windows — Internet Explorer[[87]](#footnote-88)** |  |
| **Административные шаблоны — Компоненты Windows — Совместимость приложений** |  |
| Выключить обработчик совместимости приложений | Включена |
| Выключить мастер совместимости программ | Отключена |
| Удалить страницу свойств совместимости программ | Отключена |
| Выключить журнал событий справки приложения | Отключена |
| Предотвращение доступа к 16-разрядным приложениям | Отключена |
| **Административные шаблоны — Компоненты Windows — Просмотр событий** |  |
| URL-адрес EVENTS.ASP | Отключена |
| Программа EVENTS.ASP | Отключена |
| Параметры командной строки программы EVENTS.ASP | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы IIS (Internet Information Services)** |  |
| Запрет установки IIS | Отключена |
| **Административные шаблоны — Компоненты Windows — Центр обеспечения безопасности** |  |
| Включить "Центр обеспечения безопасности" (только для компьютеров в домене) | Отключена |
| **Административные шаблоны — Компоненты Windows — Планировщик заданий** |  |
| Скрывать страницы свойств | Отключена [[88]](#footnote-89) |
| Запретить запуск и завершение задач |
| Запретить перетаскивание с помощью мыши |
| Запретить создание новых заданий |
| Запретить удаление заданий |
| Скрыть флажок дополнительных свойств в мастере планирования заданий |
| Запретить обзор |
| **Административные шаблоны — Компоненты Windows — Службы терминалов[[89]](#footnote-90)** |  |
| Подключения, проверяемые на активность | Отключена |
| Автоматическое переподключение | Отключена |
| Ограничить пользователей службы терминалов одним удаленным сеансом | Отключена |
| Принудительная отмена фонового рисунка удаленного рабочего стола | Отключена |
| Запретить завершение консольного сеанса администратора | Отключена |
| Ограничить количество подключений | Отключена |
| Ограничить максимальную глубину цвета | Отключена |
| Разрешать удаленное подключение с использованием служб терминалов | Включено |
| Не разрешать локальным администраторам настраивать разрешения | Отключена |
| Удалить элемент "Безопасность Windows" из меню Пуск | Отключена |
| Удалить элемент 'Отключение сеанса' из диалога завершения работы | Отключена |
| Задать путь для перемещаемых профилей TS | Отключена |
| Домашняя папка пользователя сервера терминалов | Отключена |
| Устанавливает правила удаленного управления для сеансов пользователей служб терминалов | Отключена |
| Запускать программу при подключении | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Перенаправление данных клиент/сервер** |  |
| Разрешить перенаправление часового пояса | Отключена |
| Не разрешать перенаправление буфера обмена | Отключена |
| Не разрешать перенаправление устройства чтения смарт-карт | Отключена |
| Разрешить перенаправление звука | Отключена |
| Не разрешать перенаправление COM-портов | Отключена |
| Не разрешать перенаправление клиентских принтеров | Отключена |
| Не разрешать перенаправление LPT-портов | Отключена |
| Не разрешать перенаправление дисков | Отключена |
| Не устанавливать используемый по умолчанию принтер клиента в качестве принтера для сеанса | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Шифрование и безопасность — Политика RPC-безопасности** |  |
| Безопасный сервер (требовать безопасность) | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Шифрование и безопасность** |  |
| Всегда запрашивать у клиента пароль при подключении | Отключена |
| Установить уровень шифрования для клиентских подключений | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Лицензирование** |  |
| Группа безопасности сервера лицензий | Отключена |
| Запретить повышение лицензий | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Временные папки** |  |
| Не использовать временные папки для сеанса | Отключена |
| Не удалять временные папки при выходе | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Клиент** |  |
| Запретить сохранение паролей | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Каталог сеансов** |  |
| Перенаправление IP-адреса сервера терминалов | Отключена |
| Сводный каталог сеансов | Отключена |
| Сервер каталога сеансов | Отключена |
| Имя кластера каталога сеансов | Отключена |
| **Административные шаблоны — Компоненты Windows — Службы терминалов — Сеансы** |  |
| Задать ограничение по времени для отключенных сеансов | Отключена |
| Задать ограничение по времени для активных сеансов | Отключена |
| Задать ограничение по времени для бездействующих сеансов | Отключена |
| Разрешать переподключение только от исходного клиента | Отключена |
| Завершать сеанс при достижении ограничения по времени | Отключена |
| **Административные шаблоны — Компоненты Windows — Проводник** |  |
| Отключить защищенный режим протокола оболочки | Отключена |
| **Административные шаблоны — Компоненты Windows — Установщик Windows** |  |
| Запретить использование установщика Windows | Включена (никогда) |
| Всегда производить установку с повышенными привилегиями | Отключена |
| Запретить откат | Отключена |
| Удалить диалоговое окно обзора нового источника | Отключена |
| Запретить применение пакетов исправлений | Включена |
| Отключить запрос безопасности IE для сценариев Windows Installer | Отключена |
| Разрешить пользователям изменять параметры установки | Отключена |
| Разрешить обзор источника при повышенных привилегиях | Отключена |
| Разрешить использование носителей при повышенных привилегиях | Отключена |
| Разрешить применение пакетов исправлений во время привилегированных установок | Отключена |
| Разрешить администраторам выполнение установки в сеансе сервера терминалов | Включена |
| Кэшировать файлы трансформации в безопасном месте на рабочей станции | Отключена |
| Ведение журнала | Включена |
| Запретить установки для пользователей | Отключена |
| Отключить создание контрольных точек восстановления системы | Включена |
| Запретить удаление обновлений | Отключена |
| Задать обязательные правила обновления компонентов | Отключена |
| Запретить пользователям, не являющимися администраторами, устанавливать обновления, подписанные изготовителем программ | Отключена |
| Максимальный размер кэша базисных файлов | Отключена |
| **Административные шаблоны — Компоненты Windows — Windows Messenger** |  |
| Запретить выполнение Windows Messenger | Включена |
| Не запускать автоматически Windows Messenger при входе | Включена |
| **Административные шаблоны — Компоненты Windows — Управление цифровыми правами Windows Media (DRM)** |  |
| Запретить доступ к Интернету для Windows Media DRM | Отключена |
| **Административные шаблоны — Компоненты Windows — Windows Movie Maker** |  |
| Запретить выполнение программы Windows Movie Maker | Включена |
| **Административные шаблоны — Компоненты Windows — Windows Update** |  |
| Не отображать параметр "Установить обновления и завершить работу" в диалоговом окне завершения работы Windows | Включена |
| Не настраивать параметр "Установить обновления и завершить работу" в диалоговом окне завершения работы Windows в качестве параметра по умолчанию | Включена |
| Настройка автоматического обновления | Отключена |
| Указать размещение службы обновлений Microsoft в интрасети | Отключена |
| Разрешить клиенту присоединение к целевой группе | Отключена |
| Перенос запланированных автоматических установок обновлений | Отключена |
| Не выполнять автоматический повторный запуск для автоматических установок обновлений | Включена |
| Частота поиска автоматических обновлений | Отключена |
| Разрешить немедленную установку автоматических обновлений | Отключена |
| Задержка перезагрузки при запланированных установках | Отключена |
| Повторный запрос для перезагрузки при запланированных установках | Отключена |
| Разрешать пользователя, не являющимся администраторами, получать уведомления об обновлениях | Отключена |
| **Административные шаблоны — Компоненты Windows — Проигрыватель Windows Media** |  |
| Не отображать диалоговые окна первого использования | Включена |
| Не создавать ярлык на рабочем столе | Включена |
| Не создавать ярлык на панели быстрого запуска | Включена |
| Запретить автоматические обновления | Включена |
| Запретить сглаживание изображения | Включена |
| **Secret Net Integrity Check settings** |  |
| Extension Executive [[90]](#footnote-91) | Включена(.exe;.dll;.cpl;.drv;.sys;.ocx;.vbs;.scr;.rll;.ime;.bpl;.ax;.acm;.com;.ppl;.cmd;.bat;.ovl;.tbp;.lnk) [[91]](#footnote-92) |
| **Административные шаблоны — Система** |  |
| Предотвращение доступа к потенциально небезопасным функциям справки HTML для указанных папок | Включена (пустой список) |
| Не отображать страницу "Управление данным сервером" при входе | Включена |
| Отображать диалог слежения за завершением работы | Отключена |
| Включить свойство данных состояния системы слежения за завершением работы | Отключена |
| Включить постоянную временную метку | Включена (60 сек.) |
| Указать расположение установочных файлов Windows | Отключена |
| Указать размещение установочных файлов пакета обновления Windows | Отключена |
| Отключить сообщения о состоянии загрузки, завершения работы, входа и выхода из сети | Отключена |
| Подробные сообщения о состоянии | Отключена |
| Запретить запуск из Справки перечисленных программ | Включена (\*.\*) |
| Отключить автозапуск | Включена (все диски) |
| Не выполнять автоматическое шифрование файлов, перемещаемых в зашифрованные папки | Отключена |
| Загружать отсутствующие COM-компоненты | Включена |
| Разрешить клиентам отслеживания изменившихся связей использовать ресурсы домена | Отключена |
| Не выключайте питание компьютера после завершения работы Windows. | Отключена |
| Отключить запрос на использование Windows Update при поиске драйверов | Включена |
| **Административные шаблоны — Система — Профили пользователей** |  |
| Не проверять собственность пользователя перемещаемого профиля | Отключена |
| Удалять кэшированные копии перемещаемых профилей | Отключена |
| Не определять медленные подключения | Отключена |
| Таймаут для профилей пользователей для медленных сетевых подключений | Отключена |
| Дождаться загрузки перемещаемого пользовательского профиля | Отключена |
| Выдавать запрос пользователю при обнаружении медленного подключения | Отключена |
| Таймаут диалоговых окон | Отключена |
| Завершать сеанс пользователя в случае ошибки перемещаемого профиля | Отключена |
| Максимальное число повторов попыток выгрузки и обновления профиля пользователя | Отключена |
| Добавлять группу администраторов для перемещаемых профилей пользователя | Отключена |
| Запретить распространение изменений в перемещаемом профиле на сервер | Включена |
| Разрешать использование только локальных профилей | Отключена |
| Оставить установочные данные установщика Windows и групповой политики | Отключена |
| **Административные шаблоны — Система — Сценарии** |  |
| Синхронное выполнение сценариев входа в систему | Включена |
| Асинхронное выполнение сценариев загрузки | Отключена |
| Выполнять сценарии загрузки с отображением команд | Отключена |
| Выполнять сценарии завершения работы с отображением команд | Отключена |
| Максимальное время выполнения сценариев групповой политики | Отключена |
| **Административные шаблоны — Система — Вход в систему** |  |
| Не отображать окно "Первое знакомство" при входе в систему | Отключена |
| Всегда использовать классический вход в систему | Включена |
| Запускать указанные программы при входе в систему | Отключена |
| Не обрабатывать список автозапуска программ, выполняемых однажды | Отключена |
| Не обрабатывать список автозапуска для старых версий | Отключена |
| Всегда ожидать инициализации сети при загрузке и входе в систему | Включена |
| **Административные шаблоны — Система — Дисковые квоты** |  |
| Включить дисковые квоты | Отключена |
| Задать предел дисковой квоты | Отключена |
| Предел квоты по умолчанию и уровень предупреждения | Отключена |
| Вести журнал даже при превышении предела квоты | Отключена |
| Заносить событие превышение уровня предупреждения квоты | Отключена |
| Применять политику к съемным носителям | Отключена |
| **Административные шаблоны — Система — Сетевой вход в систему** |  |
| Ожидаемая задержка при удаленном входе | Отключена |
| Имя сайта | Не задана [[92]](#footnote-93) |
| Кэш-параметр негативного обнаружения контроллеров домена | Отключена |
| Начальный интервал попыток обнаружения контроллеров домена для фоновых клиентов | Отключена |
| Максимальный интервал повторных попыток обнаружения контроллера домена для фоновых клиентов | Отключена |
| Окончательный интервал попыток обнаружения контроллера домена для фоновых клиентов | Отключена |
| Положительное периодическое обновление кэша DC для фонового вызова | Отключена |
| Положительное периодическое обновление кэша DC для не фонового вызова | Отключена |
| Интервал очистки | Отключена |
| Обращение к PDC в случае неудачи входа в систему | Отключена |
| Уровень отладки файла журнала | Отключена |
| Максимальный размер файла журнала | Отключена |
| Совместимость общего ресурса Sysvol | Отключена |
| Совместимость общего сетевого доступа | Отключена |
| **Административные шаблоны — Система — Сетевой вход в систему — DNS-записи локатора контроллеров домена** [[93]](#footnote-94) |  |
| Динамическая регистрация DNS-записей локатора контроллеров домена | Не задана |
| DNS-записи локатора контроллеров домена, не регистрируемые контроллерами доменов | Не задана |
| Интервал обновления DNS-записей локатора контроллеров домена | Не задана |
| Набор весов DNS SRV-записей локатора контроллеров домена | Не задана |
| Приоритет, установленный в DNS SRV-записях локатора контроллеров домена | Не задана |
| Набор TTL DNS-записей локатора контроллеров домена | Не задана |
| Автоматическое обслуживание сайта DNS SRV-записями локатора контроллеров домена | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора контроллеров домена | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора глобального каталога | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора раздела каталога приложений | Не задана |
| Обнаружение DC, несущих домен с однокомпонентным DNS-именем | Не задана |
| **Административные шаблоны — Система — Групповая политика** |  |
| Отключить фоновое обновление групповой политики | Отключена |
| Интервал обновления групповой политики для компьютеров | Отключена |
| Интервал обновления групповой политики для контроллеров домена | Отключена |
| Режим обработки замыкания пользовательской групповой политики | Отключена |
| Включить политику пользователя перекрестного леса и перемещаемые профили пользователя | Отключена |
| Разрешить выполнение сценариев входа в систему при отключенной службе NetBIOS | Включена |
| Обнаружение медленных подключений для групповой политики | Отключена |
| Отключить протоколирование RSoP | Отключена |
| Запретить пользователям вызывать обновление политики компьютера | Отключена |
| Запретить интерактивным пользователям создавать данные результирующей политики (RSoP) | Включена |
| Обработка политики реестра | Отключена |
| Обработка политики настройки Internet Explorer | Отключена |
| Обработка политики установки программ | Отключена |
| Обработка политики перенаправления папки | Отключена |
| Обработка политики сценариев | Отключена |
| Обработка политики безопасности | Отключена |
| Обработка политики IP-безопасности | Отключена |
| Обработка беспроводной политики | Отключена |
| Обработка политики восстановления EFS | Отключена |
| Обработка политики дисковой квоты | Отключена |
| Всегда использовать локальные файлы ADM для редактора объектов групповой политики | Отключена |
| **Административные шаблоны — Система — Удаленный помощник** |  |
| Запрошенная удаленная помощь | Отключена |
| Разрешить предложение удаленной помощи | Отключена |
| **Административные шаблоны — Система — Восстановление системы** |  |
| Отключить восстановление системы | Включена |
| Отключить конфигурацию | Включена |
| **Административные шаблоны — Система — Отчет об ошибках** |  |
| Отображать уведомления об ошибках | Отключена |
| Настроить отчеты об ошибках | Отключена |
| **Административные шаблоны — Система — Отчет об ошибках — Параметры расширенного отчета об ошибках** |  |
| Параметры по умолчанию отчета об ошибках приложений | Отключена |
| Список приложений, для которых нужно отправлять отчет об ошибках | Отключена |
| Список приложений, для которых не нужно отправлять отчет об ошибках | Отключена |
| Сообщать о системных ошибках | Отключена |
| Отправлять отчет о незапланированном завершении работы | Отключена |
| **Административные шаблоны — Система — Защита файлов Windows** |  |
| Установить частоту сканирования защиты файлов Windows | Отключена |
| Скрывать окно индикации сканирования файлов | Включена |
| Ограничить размер кэша защиты файлов Windows | Отключена |
| Укажите размещение кэша для защиты файлов Windows | Отключена |
| **Административные шаблоны — Система — Удаленный вызов процедур (RPC)** |  |
| Диагностическая информация состояния RPC | Отключена |
| Передача расширенных сведений об ошибках | Отключена |
| Пропустить сбой делегирования | Отключена |
| Минимальный таймаут простаивающих подключений для RPC/HTTP-подключений | Отключена |
| Ограничения для не прошедших проверку подлинности RPC-клиентов | Включен (Отсутствует) |
| Проверка RPC-клиентов сопоставителя конечных точек | Отключена |
| **Административные шаблоны — Система — Служба времени Windows** |  |
| Глобальные параметры конфигурации | Отключена |
| **Административные шаблоны — Система — Служба времени Windows — Поставщики времени** |  |
| Включить Windows NTP-клиента | Включена |
| Настроить Windows NTP-клиента | Отключена |
| Включить Windows NTP-сервер | Включена |
| **Административные шаблоны — Система — Управление связью через Интернет** |  |
| Ограничить связь через Интернет | Включена |
| **Административные шаблоны — Система — Управление связью через Интернет — Параметры связи через Интернет** |  |
| Отключить веб-публикацию в списке задач для файлов и папок | Включена |
| Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков | Включена |
| Отключить заказ отпечатков через Интернет в списке задач для изображений | Включена |
| Отключить участие в программе улучшения поддержки пользователей Windows Messenger | Включена |
| Отключить отображение раздела "Знаете ли вы?" в окне "Центра справки и поддержки" | Включена |
| Отключить поиск в базе знаний Майкрософт в окне "Центра справки и поддержки" | Включена |
| Отключить отчеты об ошибках Windows | Включена |
| Отключить службу сопоставления файлов Интернета | Включена |
| Отключить мастер подключения к Интернету, если URL-адрес ссылается на MICROSOFT.COM | Включена |
| Отключить ссылки EVENTS.ASP в программе "Просмотр событий" | Включена |
| Отключить автоматическое обновление корневых сертификатов | Включена |
| Отключить регистрацию, если URL-адрес ссылается на MICROSOFT.COM | Включена |
| Отключить обновление информационных файлов "Помощника по поиску" | Включена |
| Отключить выполнение печати через HTTP-протокол | Включена |
| Отключить загрузку драйверов печати через HTTP-протокол | Включена |
| Отключить использование Windows Update при поиске драйверов | Включена |
| Отключить доступ ко всем возможностям Windows Update | Включена |
| Отключить автоматическую загрузку кодеков для Windows Movie Maker | Включена |
| Отключить веб-ссылки в Windows Movie Maker | Включена |
| Отключить сохранение видео на веб-узлах поставщиков видеохостинга в Windows Movie Maker | Включена |
| **Административные шаблоны — Система — DCOM — Параметры совместимости приложений** |  |
| Разрешать локальные исключения проверки безопасности при активации | Отключена |
| Задать исключения проверки безопасности при активации | Отключена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft — PNRP-протокол (Peer Name Resolution Protocol) — Глобальные облака** |  |
| Задать сервер инициализации | Отключена |
| Отключить многоадресную загрузку | Включена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft — PNRP-протокол (Peer Name Resolution Protocol) — Локальные облака сайта** |  |
| Задать сервер инициализации | Отключена |
| Отключить многоадресную загрузку | Включена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft — PNRP-протокол (Peer Name Resolution Protocol) — Локальные облака связи** |  |
| Задать сервер инициализации | Отключена |
| Отключить многоадресную загрузку | Включена |
| **Административные шаблоны — Сеть — Службы одноранговых сетей Microsoft** |  |
| Отключить службы одноранговых сетей Microsoft | Включена |
| **Административные шаблоны — Сеть — DNS-клиент** |  |
| Основной DNS суффикс | Отключена |
| Динамическое обновление | Включена |
| Порядок просмотра суффиксов DNS | Отключена |
| Регрессирование основного DNS-суффикса | Включена |
| Регистрация PTR-записей | Включена (регистрировать только если A-запись успешно зарегистрирована) |
| Интервал обновления регистрации | Включена (1800 сек.) |
| Замена адресов в случае конфликтов | Отключена |
| DNS-серверы | Отключена |
| DNS-суффикс этого подключения | Отключена |
| Регистрировать DNS-записи с DNS-суффиксом подключения | Включена |
| Установить TTL для A- и PTR-записей | Отключена |
| Уровень безопасности обновлений | Отключена |
| Обновлять зоны доменов верхнего уровня | Отключена |
| **Административные шаблоны — Сеть — Автономные файлы** |  |
| Разрешить или запретить использование автономных файлов | Отключена |
| Запретить пользовательскую настройку автономных файлов | Включена |
| Синхронизовать автономные файлы при входе в систему | Отключена |
| Синхронизация всех автономных файлов перед выходом из системы | Отключена |
| Синхронизовать автономные файлы перед приостановкой | Отключена |
| Размер кэша по умолчанию | Отключена |
| Действия при отключении от сервера | Отключена |
| Нестандартные действия при отключении от сервера | Отключена |
| Удалить "Сделать доступными автономно" | Включена |
| Запретить использование папки "Автономные файлы" | Включена |
| Некэшируемые файлы | Отключена |
| Административно назначенные автономные файлы | Отключена |
| Отключить всплывающие напоминания | Включена |
| Частота появления всплывающих напоминаний | Отключена |
| Длительность отображения первого всплывающего напоминания | Отключена |
| Длительность отображения всплывающих напоминаний | Отключена |
| При выходе из системы удалять локальную копию автономных файлов пользователя | Включена |
| Уровень регистрации событий | Отключена |
| Сделать подпапки всегда доступными в автономном режиме | Отключена |
| Шифровать кэш автономных файлов | Отключена |
| Запретить применение "Сделать доступными автономно" для этих файлов и папок | Отключена |
| Настроить скорость медленного подключения | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения — Брандмауэр Windows — Профиль домена** |  |
| Брандмауэр Windows: Защитить все сетевые подключения | Отключена |
| Брандмауэр Windows: Не разрешать исключения | Отключена |
| Брандмауэр Windows: Задать исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного управления | Отключена |
| Брандмауэр Windows: Разрешать исключения для общего доступа к файлам и принтерам | Отключена |
| Брандмауэр Windows: Разрешать исключения ICMP | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного рабочего стола | Отключена |
| Брандмауэр Windows: Разрешать исключения для UPnP-инфраструктуры | Отключена |
| Брандмауэр Windows: Запретить уведомления | Отключена |
| Брандмауэр Windows: Разрешать ведение журнала | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | Отключена |
| Брандмауэр Windows: Задать исключения для портов | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для портов | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения — Брандмауэр Windows — Стандартный профиль** |  |
| Брандмауэр Windows: Защитить все сетевые подключения | Отключена |
| Брандмауэр Windows: Не разрешать исключения | Отключена |
| Брандмауэр Windows: Задать исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для программ | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного управления | Отключена |
| Брандмауэр Windows: Разрешать исключения для общего доступа к файлам и принтерам | Отключена |
| Брандмауэр Windows: Разрешать исключения ICMP | Отключена |
| Брандмауэр Windows: Разрешать исключения для удаленного рабочего стола | Отключена |
| Брандмауэр Windows: Разрешать исключения для UPnP-инфраструктуры | Отключена |
| Брандмауэр Windows: Запретить уведомления | Отключена |
| Брандмауэр Windows: Разрешать ведение журнала | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | Отключена |
| Брандмауэр Windows: Задать исключения для портов | Отключена |
| Брандмауэр Windows: Разрешать локальные исключения для портов | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения — Брандмауэр Windows** |  |
| Брандмауэр Windows: Разрешать обход для прошедших проверку IPSec | Отключена |
| **Административные шаблоны — Сеть — Сетевые подключения** |  |
| Запретить использование общего доступа к подключению Интернета в сети DNS-домена | Включена |
| Запретить использование брандмауэра подключения к Интернету в сети DNS-домена | Отключена |
| Запретить установку и настройку сетевых мостов в вашей сети DNS-доменов | Отключена |
| IEEE 802.1x Центр Сертификации для проверки подлинности компьютеров | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS — Значение DSCP для соответствующих пакетов** |  |
| Тип службы "Best effort" | Отключена |
| Тип службы "Controlled load" | Отключена |
| Тип службы "Guaranteed" | Отключена |
| Тип службы "Network control" | Отключена |
| Тип службы "Qualitative" | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS — Значение DSCP для не соответствующих пакетов** |  |
| Тип службы "Best effort" | Отключена |
| Тип службы "Controlled load" | Отключена |
| Тип службы "Guaranteed" | Отключена |
| Тип службы "Network control" | Отключена |
| Тип службы "Qualitative" | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS — Значение приоритета второго уровня** |  |
| Не соответствующие пакеты | Отключена |
| Тип службы "Best effort" | Отключена |
| Тип службы "Controlled load" | Отключена |
| Тип службы "Guaranteed" | Отключена |
| Тип службы "Network control" | Отключена |
| Тип службы "Qualitative" | Отключена |
| **Административные шаблоны — Сеть — Диспетчер пакетов QoS** |  |
| Ограничить резервируемую пропускную способность | Отключена |
| Ограничение ожидающих обработки пакетов | Отключена |
| Задать разрешение таймера | Отключена |
| **Административные шаблоны — Сеть — SNMP** |  |
| Сообщества | Отключена |
| Разрешенные диспетчеры | Отключена |
| Ловушки только для публичного сообщества | Отключена |
| **Административные шаблоны — Сеть — Фоновая интеллектуальная служба передачи (BITS)** |  |
| Максимальная пропускная способность сети, используемая BITS | Отключена |
| Таймаут (в днях) для неактивных заданий | Отключена |
| **Административные шаблоны — Сеть** |  |
| Частота выполнения обнаружения контроллеров домена клиентом DFS | Отключена |
| **Административные шаблоны — Принтеры** |  |
| Разрешить публикацию принтеров | Включена |
| Разрешить очистку опубликованных принтеров | Включена |
| Автоматическая публикация новых принтеров в Active Directory | Отключена |
| Проверять состояние публикации | Отключена |
| Размещение компьютера | Отключена |
| Особый URL-адрес службы поддержки в левой панели папки принтеров | Отключена |
| Интервал очистки Active Directory | Отключена |
| Приоритет потока при очистке Active Directory | Отключена |
| Повторы при очистке Active Directory | Отключена |
| Запретить установку принтеров, использующих работающие в режиме ядра драйверы | Отключена |
| Записывать события контакта службы очистки каталогов | Отключена |
| Заполнение строки поиска принтеров | Отключена |
| Обзор принтеров | Включена |
| Удалять принтеры, которые не были автоматически повторно опубликованы | Отключена |
| Разрешить диспетчеру печати добавление новых клиентских подключений | Включена |
| Печать на основе использования веба | Отключена |

### Рекомендации по настройке политик безопасности для серверов и АРМ платежной системы при использовании СЗИ от НСД «Аккорд»

В Таблице (Таблица 42) приведены настройки параметров групповой политики, применяемой для серверов и АРМ платежной системы при использовании СЗИ от НСД «Аккорд».

Таблица 42. Настройки параметров групповой политики, применяемой для серверов и ПЭВМ платежной системы при использовании СЗИ от НСД «Аккорд»

| **Наименование раздела/параметра групповой политики** | | | **Значение параметра** | |
| --- | --- | --- | --- | --- |
| **Конфигурация компьютера** | | | |
| **Конфигурация Windows** | | | |
| **Параметры безопасности** | | | |
| **Политики учетных записей** | | | |
| **Политика паролей** | | | |
| Макс. срок действия пароля | | Не более 185 дней | |
| Мин. длина пароля | | 8 символов | |
| Требовать неповторяемости паролей | | не менее 5 хранимого пароля | |
| Хранить пароли всех пользователей в домене, используя обратимое шифрование | | отключен | |
| **Политика блокировки учетной записи** | | | |
| Блокировка учетной записи на | | 0 (бесконечно) или не менее 5 минут | |
| Пороговое значение блокировки | | не более 5 | |
| Время до сброса счетчика блокировки | | не менее 5 минут | |
| **Политика аудита** | | | |
| Аудит входа в систему | Успех, Отказ | | |
| Аудит изменения политики | Успех, Отказ | | |
| Аудит использования привилегий | Отказ | | |
| Аудит событий входа в систему | Успех, Отказ | | |
| Аудит управления учетными записями | Успех, Отказ | | |
| **Локальные политики** | | | |
| **Параметры безопасности** | | | |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | | 0 | |
| Интерактивный вход в систему: не отображать последнего имени пользователя | | Включен | |
| Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее | | 5 дней | |
| **Административные шаблоны** | | | |
| **Network** | | | |
| **Administrative Shares** | | | |
| De-Activate AdminShare on a Server | | Включен | |
| De-Activate AdminShare on a Workstation | | Включен | |

Для появления в редакторе политик настроек Administrative Shares необходимо загрузить файл шаблона следующего содержания

CLASS MACHINE

CATEGORY "Network"

POLICY "Administrative Shares"

KEYNAME "System\CurrentControlSet\Services\LanmanServer\Parameters"

PART "De-Activate AdminShare on a Server" CHECKBOX

VALUENAME "AutoShareServer"

VALUEON NUMERIC 0

VALUEOFF NUMERIC 1

END PART

PART "De-Activate AdminShare on a Workstation" CHECKBOX

VALUENAME "AutoShareWks"

VALUEON NUMERIC 0

VALUEOFF NUMERIC 1

END PART

END POLICY

END CATEGORY

### Настройки ОС на рабочих станциях и серверах (контроллерах домена) при использовании СЗИ от НСД «SecretNet» и «Аккорд» при функционировании рабочих станций c ОС Windows XP/7 под управлением контроллеров домена c ОС Windows Server 2008

Ниже приведены рекомендованные настройки ОС для рабочих станций и серверов.  Данные настройки при необходимости  могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

Значения настроек параметров групповых политик приведены для русскоязычной ОС Windows 2008 Server.

Внимание:

1. Политики для пользователей, АРМ, контроллеров домена и серверов, "Перенаправление папки" не применять к доменным группам Domain Admins, Enterprise Admins, SecretNetAdmins и локальной группе администраторов;

2. В соответствии с параметром настройки групповой политики для пользователей "Главное меню" (Таблица 43) рекомендуется меню запуска только необходимых пользователю приложений формировать с использованием механизма перенаправления папок:

|  |  |
| --- | --- |
| **Наименование раздела/параметра**  **групповой политики** | **Значение параметра** |
| Конфигурация Windows — Перенаправление папки |  |
| Главное меню | Устанавливается в отдельном объекте групповой политики. |

Для организации замкнутой программной среды и запрета возможности запуска "Проводника" необходимо дополнительно выполнить следующие требования:

1. В папке перенаправления:

* создать пустую подпапку "Программы", запретить доступ к ней всем пользователям и группам;
* не создавать другие подпапки (кроме пустой подпапки "Программы").

2. Необходимые ярлыки запуска приложений пользователя размещать в папке перенаправления.

3. Для обеспечения доступа к ресурсам файловой системы через графический интерфейс прикладного программного обеспечения, а также с целью выполнения регламентных операций для отдельных категорий пользователей подсистем РАБИС-НП, требуется разрешить отображение в диалоговых окнах "Открыть/сохранить файл" локальных ресурсов файловой системы и сетевого окружения.

Для отображения локальных (сетевых) ресурсов при функционировании рабочих станций c ОС Windows 2000/XP/7 (Rus) под управлением контроллеров домена c ОС Windows Server 2008 (Rus) в политике пользователей установить в значение "Отключена" следующие параметры групповой политики:

* "Конфигурация пользователя – Административные шаблоны – Рабочий стол –Удалить значок компьютер с рабочего стола";
* "Конфигурация пользователя – Административные шаблоны – Рабочий стол – Скрыть значок "Сеть" на рабочем столе".

4. Все изменения в профиль пользователя (в том числе настройку принтера) рекомендуется вносить до перемещения учетной записи пользователя под действие пользовательской политики.

5. Терминальный вход пользователя в соответствии с документацией к ПО СЗИ от НСД «Secret Net» обеспечивается "пробросом" TM-идентификатора на удаленный сервер за счет настройки соответствующих параметров в разделах:

1. Конфигурация компьютера – Административные шаблоны – Система – Удалённый вызов процедур (RPC) – Ограничения для не прошедших проверку RPC-клиентов.

2. Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Локальные политики – Параметры безопасности – Разрешать анонимный доступ к именованным каналам.

Для обеспечения штатного функционирования в ТУ Банка России на рабочих станциях терминала сбора данных Datalogic Falcon X3 при применении SecretNet версии 7.6 необходимо в ветке реестра:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\ActiveSyncWPDEnumerator\UMB\Device Parameters\WUDF

добавить параметр KernelModeClientPolicy типа REG\_DWORD со значением «1».



### Параметры групповой политики для пользователей СВТ при использовании СЗИ от НСД Secret Net

Параметры групповой политики и их значения, применяемые для пользователей на средствах вычислительной техники при использовании СЗИ от НСД «Secret Net», приведены в таблице (Таблица 43).

Таблица 43 Параметры групповой политики для пользователей СВТ при использовании СЗИ от НСД Secret Net

| **Наименование раздела/параметра политики** | **Значение** |
| --- | --- |
| **Конфигурация программ** |  |
| Установка программ | Не определено |
| **Конфигурация Windows** |  |
| **Сценарии (вход/выход из системы)** |  |
| Вход в систему | Не определено |
| Выход из системы | Не определено |
| **Параметры безопасности** |  |
| **Политики открытого ключа** |  |
| **Доверительные отношения в предприятии** | Не определено |
| **Доверенные лица** | Не определено |
| Клиент служб сертификатов - политика регистрации сертификатов | Не настроено |
| Клиент служб сертификации: перемещение учетных данных | Не настроено |
| Клиент служб сертификации: автоматическая регистрация | Не настроено |
| **Политики ограниченного использования программ** | Не определено |
| **Перенаправление папки** |  |
| AppData(перемещаемая) | Не задана |
| Рабочий стол | Не задана |
| Главное меню | Определяется отдельным объектом групповой политики |
| Документы | Не задана |
| Изображения | Не задана |
| Музыка | Не задана |
| Видео | Не задана |
| Избранное | Не задана |
| Контакты | Не задана |
| Загрузка | Не задана |
| Ссылки | Не задана |
| Поиски | Не задана |
| Сохраненные игры | Не задана |
| **QoS на основе политики** | Не определено |
| **Настройка Internet Explorer** |  |
| **Пользовательский интерфейс обозревателя** |  |
| Заголовок обозревателя | Не определено |
| Эмблема и анимированные рисунки | Не определено |
| Настройка панели инструментов обозревателя | Не определено |
| **Подключение** |  |
| Параметры подключения | Не определено |
| Автоматическая настройка обозревателя | Не определено |
| Параметры прокси-сервера | Не определено |
| Строка обозревателя | Не определено |
| **URL-адреса** |  |
| Избранное и ссылки | Не определено |
| Важные URL-адреса | Не определено |
| **Безопасность** |  |
| Зоны безопасности и оценка содержимого | Выставить признак «Импортировать текущие параметры безопасности и конфиденциальности». Добавить все сервера РАБИС-НП и АС ЭКР в форме \\<имя\_сервера> |
| Параметры Authenticode | Не определено |
| **Программы** |  |
| Программы |  |
| **Административные шаблоны** |  |
| **Компоненты Windows** |  |
| **Internet Explorer** | **Все параметры раздела и его подразделов перевести в состояние "Отключена", за исключением нижеприведенных** |
| Включить строку меню по умолчанию | Включена |
| Выключить автоматическое восстановление после сбоя | Не задана |
| Выключить повторное открытие последнего сеанса просмотра | Не задана |
| Разрешить режим завершения работы Internet Explorer 8 | Не задана |
| Выключить быстрые вкладки | Не задана |
| Выключить предложение для всех служб, установленных пользователем | Не задана |
| Выключить меню быстрого выбора | Не задана |
| **Панель управления браузером** |  |
| **Вкладка "Безопасность"** |  |
| Включить предупреждение о несоответствии адреса сертификата | Не задана |
| **Параметры браузера** |  |
| **Параметры экрана** |  |
| Запретить выбор размера текста по умолчанию | Не задана |
| **NetMeeting** |  |
| **Звук & Видео** |  |
| Отключить звук | Отключена |
| Запретить изменение параметра DirectSound | Отключена |
| Отключить полный дуплекс для звука | Отключена |
| Запретить получение видео | Отключена |
| Запретить отправку видео | Отключена |
| Ограничить использование пропускной способности для звука и видео | Отключена |
| **Общий доступ к приложениям** |  |
| Отключить общий доступ к приложениям | Отключена |
| Запретить управление | Отключена |
| Запретить предоставление общего доступа | Отключена |
| Запретить предоставление общего доступа к командной строке | Отключена |
| Запретить предоставление общего доступа к рабочему столу | Отключена |
| Запретить предоставление общего доступа к окнам Проводника | Отключена |
| Запретить общий доступ к приложениям в режиме True Color | Отключена |
| **Страница параметров** |  |
| Отключить кнопку «Расширенный вызов» | Отключена |
| Скрыть страницу «Звук» | Отключена |
| Скрыть страницу «Общие» | Отключена |
| Скрыть страницу «Безопасность» | Отключена |
| Скрыть страницу «Видео» | Отключена |
| Разрешить устойчивый автоматический прием вызовов | Отключена |
| Запретить разговор | Отключена |
| Запретить использование доски | Отключена |
| Запретить доску NetMeeting 2.x | Отключена |
| Разрешить автоматическую настройку | Отключена |
| Запретить добавление серверов каталога | Отключена |
| Запретить автоматический прием вызовов | Отключена |
| Запретить изменение метода выполнения вызова | Отключена |
| Отключение службы каталога NetMeeting | Отключена |
| Запретить получение файлов | Отключена |
| Запретить отправку файлов | Отключена |
| Запретить просматривать веб-каталоги | Отключена |
| Ограничить размер отправляемых файлов | Отключена |
| Указание веб-страницы, поддерживающей интрасеть | Отключена |
| Указание параметров безопасности вызовов | Отключена |
| **Windows Media Center** |  |
| Не запускать Windows Media Center | Включена |
| **Windows Messenger** |  |
| Не запускать Windows Messenger автоматически при входе. | Включена |
| Запретить запуск Windows Messenger | Включена |
| **Windows PowerShell** |  |
| Включить выполнение сценариев | Отключена |
| **Windows SideShow** |  |
| Удалять данные с устройств, использующих микропрограммы Майкрософт, при завершении сеанса пользователя. | Отключена |
| Отключить автоматическое пробуждение | Отключена |
| Отключить Windows SideShow | Отключена |
| Требовать ПИН-код для доступа к данным на устройствах с микропрограммами Майкрософт | Отключена |
| **Архивация данных** |  |
| **Клиент** |  |
| Запретить пользователям запускать программу "Состояние и настройка архивации" | Отключена |
| Запретить архивацию на локальные диски | Отключена |
| Запретить архивацию в сетевое расположение | Отключена |
| Запретить архивацию на оптические носители (CD/DVD) | Отключена |
| Отключить возможность архивации файлов данных | Отключена |
| Отключить функции восстановления | Отключена |
| Отключить возможность создания образа системы | Отключена |
| **Быстрый поиск** |  |
| Настраиваемое средство быстрого поиска в Интернете | Отключена |
| **Гаджеты рабочего стола** |  |
| Переопределить ссылку на дополнительные гаджеты | Отключена |
| Отключить гаджеты рабочего стола | Включена |
| Ограничить распаковку и установку гаджетов, не подписанных цифровой подписью. | Отключена |
| Отключить установленные пользователем гаджеты рабочего стола | Включена |
| **Диспетчер вложений** |  |
| Уведомлять антивирусную программу при открытии вложений | Отключена |
| Логика доверия для вложений | Отключена |
| Удаление сведений о зоне происхождения вложений | Отключена |
| Скрытие средств для удаления сведений о зонах | Отключена |
| Риск по умолчанию для вложений | Отключена |
| Список исключений для типов файлов с высоким риском | Отключена |
| Список исключений для типов файлов с низким риском | Отключена |
| Список исключений для типов файлов со средним риском | Отключена |
| **Диспетчер окон рабочего стола** |  |
| **Цвет рамки окна** |  |
| Укажите цвет по умолчанию | Отключена |
| Не разрешать смену цветов | Отключена |
| Не разрешать анимацию окон | Включена |
| Не разрешать композицию рабочего стола | Включена |
| Не разрешать вызов Flip3D | Включена |
| **Звукозапись** |  |
| Запретить выполнение программы "Звукозапись" | Включена |
| **Календарь Windows** |  |
| Выключить календарь Windows | Включена |
| **Каналы RSS** |  |
| Включить обычную проверку подлинности веб-каналов через HTTP | Отключена |
| Отключить синхронизацию веб-каналов и веб-фрагментов в фоновом режиме | Не задана |
| Отключить загрузку вложений | Отключена |
| Отключить добавление и удаление веб-каналов и веб-фрагментов | Отключена |
| Отключить обнаружение веб-каналов и веб-фрагментов | Отключена |
| Отключить список веб-каналов | Отключена |
| **Консоль управления (MMC)** |  |
| **Запрещенные и разрешенные оснастки** |  |
| **Групповая политика** |  |
| **Расширения вкладок предпочтений** |  |
| Разрешить использование расширения предпочтений "Приложения" | Отключена |
| Разрешить использование элемента "Параметры панели управления (компьютеры)" | Отключена |
| Разрешить использование расширения предпочтений "Источники данных" | Отключена |
| Разрешить использование расширения предпочтений "Устройства" | Отключена |
| Разрешить использование расширения предпочтений "Сопоставления дисков" | Отключена |
| Разрешить использование расширения предпочтений "Среда" | Отключена |
| Разрешить использование расширения предпочтений "Файлы" | Отключена |
| Разрешить использование расширения предпочтений "Параметры папок" | Отключена |
| Разрешить использование расширения предпочтений "Папки" | Отключена |
| Разрешить использование расширения предпочтений "INI-файлы | Отключена |
| Разрешить использование расширения предпочтений "Параметры браузера" | Отключена |
| Разрешить расширение предпочтений "Локальные пользователи и группы" | Отключена |
| Разрешить использование расширения предпочтений "Параметры сети" | Отключена |
| Разрешить использование расширения предпочтений "Общие сетевые ресурсы" | Отключена |
| Разрешить использование расширения предпочтений "Параметры электропитания" | Отключена |
| Разрешить использование расширения предпочтений "Принтеры" | Отключена |
| Разрешить использование расширения предпочтений "Региональные параметры" | Отключена |
| Разрешить использование расширения предпочтений "Реестр" | Отключена |
| Разрешить использование расширения предпочтений "Назначенные задания" | Отключена |
| Разрешить использование расширения предпочтений "Службы" | Отключена |
| Разрешить использование расширения предпочтений "Ярлыки" | Отключена |
| Разрешить использование расширения предпочтений "Главное меню" | Отключена |
| Разрешить использование элемента "Параметры панели управления (пользователи)" | Отключена |
| Разрешить использование вкладки "Предпочтения" | Отключена |
| Разрешить использование оснасток "Приложение" | Отключена |
| **Расширения оснастки «Групповая политика»** |  |
| Административные шаблоны (компьютеры) | Отключена |
| Административные шаблоны (пользователи) | Отключена |
| Перенаправление папок | Отключена |
| Настройка Internet Explorer | Отключена |
| Управление политикой IP-безопасности | Отключена |
| Настройка клиента NAP | Отключена |
| Службы удаленной установки | Отключена |
| Сценарии (запуск и завершение) | Отключена |
| Сценарии (вход и выход из системы) | Отключена |
| Параметры безопасности | Отключена |
| Установка программного обеспечения (Компьютеры) | Отключена |
| Установка программного обеспечения (Пользователи) | Отключена |
| Брандмауэр Windows в режиме повышенной безопасности | Отключена |
| Политики проводной сети (IEEE 802.3) | Отключена |
| Политики беспроводной сети (IEEE 802.11) | Отключена |
| **Расширения оснастки «Результирующая политика»** |  |
| Административные шаблоны (компьютеры) | Отключена |
| Административные шаблоны (пользователи) | Отключена |
| Перенаправление папок | Отключена |
| Настройка Internet Explorer | Отключена |
| Сценарии (запуск и завершение) | Отключена |
| Сценарии (вход и выход из системы) | Отключена |
| Параметры безопасности | Отключена |
| Установка программного обеспечения (Компьютеры) | Отключена |
| Установка программного обеспечения (Пользователи) | Отключена |
| Управление групповой политикой | Отключена |
| Редактор объектов групповой политики | Отключена |
| Вкладка «Групповая политика» для средств Active Directory | Отключена |
| Оснастка «Результирующая политика» | Отключена |
| Редактор управления групповыми политиками | Отключена |
| Редактор стартового GPO групповой политики | Отключена |
| **Оснастки расширения** |  |
| AppleTalk-маршрутизация | Отключена |
| Диспетчер авторизации | Отключена |
| Параметры политики центра авторизации | Отключена |
| Совместное использование подключения (NAT) | Отключена |
| Расширение конфигурации DCOM | Отключена |
| Управление ретрансляцией DHCP | Отключена |
| Диспетчер устройств | Отключена |
| Просмотр событий | Отключена |
| Ведение журнала IAS | Отключена |
| IGMP-маршрутизация | Отключена |
| IP-маршрутизация | Отключена |
| IPX-маршрутизация RIP | Отключена |
| IPX-маршрутизация | Отключена |
| IPX-маршрутизация SAP | Отключена |
| Логические и подключенные диски | Отключена |
| OSPF-маршрутизация | Отключена |
| Политики открытого ключа | Отключена |
| RAS-доступ — сайт пользователя | Отключена |
| RIP-маршрутизация | Отключена |
| Съемные ЗУ | Отключена |
| Удаленный доступ | Отключена |
| Маршрутизация | Отключена |
| Протокол SMTP | Отключена |
| SNMP | Отключена |
| Отправка сообщения консоли | Отключена |
| Зависимости между службами | Отключена |
| Расширения общих папок | Отключена |
| Свойства системы | Отключена |
| Расширение управления DFS | Отключена |
| Расширение управления дисками | Отключена |
| Расширение диспетчера ресурсов файлового сервера | Отключена |
| Расширение управления общими ресурсами и хранилищами | Отключена |
| Расширение диспетчера хранилища для сетей SAN | Отключена |
| Расширенное представление (веб-представление) | Отключена |
| Редактирование ADSI | Отключена |
| Active Directory — домены и доверие | Отключена |
| Active Directory — сайты и службы | Отключена |
| Active Directory — пользователи и компьютеры | Отключена |
| Центр сертификации | Отключена |
| Сертификаты | Отключена |
| Шаблоны сертификатов | Отключена |
| Службы компонентов | Отключена |
| Управление компьютером | Отключена |
| Распределенная файловая система | Отключена |
| Диспетчер устройств | Отключена |
| Дефрагментация диска | Отключена |
| Управление дисками | Отключена |
| PKI предприятия | Отключена |
| Просмотр событий | Отключена |
| Служба факсов | Отключена |
| Диспетчер отказоустойчивости кластеров | Отключена |
| Серверные расширения FrontPage | Отключена |
| Центр регистрации работоспособности (HRA) | Отключена |
| Служба IAS | Отключена |
| Службы IIS | Отключена |
| Служба индексирования | Отключена |
| Управление политикой IP-безопасности | Отключена |
| Монитор IP-безопасности | Отключена |
| Локальные пользователи и группы | Отключена |
| Сервер сетевых политик (NPS) | Отключена |
| Настройка клиента NAP | Отключена |
| Конфигурация .Net Framework | Отключена |
| Ответчик в сети | Отключена |
| Журналы и оповещения производительности | Отключена |
| Контроль допуска QoS | Отключена |
| Маршрутизация и удаленный доступ | Отключена |
| Управление съемными ЗУ | Отключена |
| Удаленные рабочие столы | Отключена |
| Анализ и настройка безопасности | Отключена |
| Шаблоны безопасности | Отключена |
| Диспетчер сервера | Отключена |
| Службы | Отключена |
| Общие папки | Отключена |
| Сведения о системе | Отключена |
| Управление TPM | Отключена |
| Телефония | Отключена |
| Настройка служб удаленных рабочих столов | Отключена |
| Управляющий элемент WMI | Отключена |
| Брандмауэр Windows в режиме повышенной безопасности | Отключена |
| Беспроводной монитор | Отключена |
| Управление DFS | Отключена |
| Диспетчер ресурсов файлового сервера | Отключена |
| Управление общими ресурсами и хранилищами | Отключена |
| Диспетчер хранилища для сетей SAN | Отключена |
| Элемент управления ActiveX | Отключена |
| Ссылка на веб-адрес | Отключена |
| Запретить пользователям использовать авторский режим | Включена |
| Ограничить пользователей списком явно разрешенных оснасток | Отключена |
| **Настройки презентации** |  |
| Выключить настройки презентации Windows | Отключена |
| **Общий сетевой доступ** |  |
| Запретить пользователям в их профиле предоставлять общий доступ к файлам. | Отключена |
| **Отчеты об ошибках Windows** |  |
| **Параметры расширенного отчета об ошибках** |  |
| Настроить архив отчетов | Отключена |
| Список исключаемых приложений | Отключена |
| Настроить очередь отчетов | Отключена |
| **Разрешение** |  |
| Настроить параметры разрешения | Отключена |
| Игнорировать настроенные параметры разрешения | Не задана |
| Настроить разрешение по умолчанию | Не задана |
| Отключить отчеты об ошибках Windows | Включена |
| Отключить запись в журнал | Отключена |
| Не отправлять дополнительные данные | Включена |
| **Параметры входа Windows** |  |
| Удалять предупреждения об окончании часов работы | Отключена |
| Задать действие, выполняемое при окончании времени входа | Отключена |
| Сообщать, когда сервер входа недоступен при входе пользователя | Отключена |
| **Планировщик заданий** |  |
| Запретить обзор | Включена |
| Скрыть флажок дополнительных свойств в мастере планирования заданий | Включена |
| Запретить перетаскивание с помощью мыши | Включена |
| Запретить запуск и завершение задач | Включена |
| Скрывать страницы свойств | Включена |
| Запретить создание новых заданий | Включена |
| Запретить удаление заданий | Включена |
| **Планшетный ПК** |  |
| **Аппаратные кнопки** |  |
| Запретить сопоставление кнопок «Назад» и ESC | Отключена |
| Запретить запуск приложения | Отключена |
| Запретить режим нажатия и удерживания | Отключена |
| Отключить аппаратные кнопки | Отключена |
| **Курсоры** |  |
| Отключит реакцию пера | Отключена |
| **Обучение пользованию пером на планшетном ПК** |  |
| Отключить обучение пользованию пером на планшетном ПК | Отключена |
| **панель ввода** |  |
| Отключение интеграции автозаполнения и панели ввода | Отключена |
| Запретить отображение значка панели ввода | Отключена |
| Для ввода планшетным пером не отображать значок панели ввода | Отключена |
| Для сенсорного ввода не отображать значок панели ввода | Отключена |
| Переключить на жесты стандарта упрощенного китайского письма (КНР) | Отключена |
| Отключить безопасность ввода паролей в панели ввода | Отключена |
| Отключить прогнозирование текста | Отключена |
| Включить редко используемые символы китайского языка, кандзи или ханджа. | Отключена |
| Отключить удобные и Z-образные жесты вычеркивания | Отключена |
| **Персонализация рукописного ввода** |  |
| Отключить автоматическое обучение | Отключена |
| **Поведение UX пера** |  |
| Задать режим многофункционального пера | Отключена |
| **Режим обучения пользованию многофункциональным пером** |  |
| Запретить режим обучения пользованию многофункциональными перьями | Отключена |
| **Сенсорный ввод** |  |
| Отключить сенсорное панорамирование | Отключена |
| Отключить сенсорный ввод планшетного ПК | Отключена |
| **Стандартные программы** |  |
| Запретить запуск игры «Инкбол» | Отключена |
| Запретить запуск журнала Windows | Отключена |
| Запретить печать в составитель заметок журнала | Отключена |
| Запретить запуск инструмента «Ножницы» | Отключена |
| **Политики автозапуска** |  |
| Отключить автозапуск | Включена (все устройства) |
| Не устанавливать флажок «Всегда выполнять выбранное действие» | Отключена |
| Отключить автозапуск устройств, не являющихся томами | Отключена |
| Вариант работы автозапуска по умолчанию | Отключена |
| **Почта Windows** |  |
| Выключить функции сообществ | Включена |
| Выключить приложение Почта Windows | Включена |
| **Проводник Windows.** |  |
| **Область кадра проводника** |  |
| Отключить область сведений | Отключена |
| Отключить область просмотра | Отключена |
| **Общее диалоговое окно открытия файлов** |  |
| Скрыть кнопку «Назад» в общих диалогах открытия файлов | Отключена |
| Скрыть раскрывающийся список недавно открывавшихся файлов | Отключена |
| Скрыть панель адресов из общих диалогов открытия файлов | Отключена |
| Элементы, отображаемые в панели мест | Отключена |
| **Предыдущие версии** |  |
| Запретить восстановление предыдущих версий из резервных копий | Включена |
| Скрыть список предыдущих версий для локальных файлов | Включена |
| Запретить восстановление локальных предыдущих версий | Включена |
| Скрыть список предыдущих версий для удаленных файлов | Включена |
| Запретить восстановление удаленных предыдущих версий | Включена |
| Скрыть предыдущие версии файлов в архиве | Включена |
| Отключить отображение эскизов и отображать только значки. | Отключена |
| Отключить отображение эскизов и отображать только значки в сетевых папках | Отключена |
| Отключить кэширование эскизов в скрытых файлах thumbs.db | Включена |
| Не показывать центр начальной настройки при входе пользователя в систему | Включена |
| Включить классическую оболочку | Включена |
| Запрашивать подтверждение при удалении файлов | Включена |
| Отключить прямую привязку к IPropertySetStorage без промежуточных уровней. | Отключена |
| Отключить возможности библиотеки Windows, использующие данные индексированных файлов | Отключена |
| Отключить известные папки | Отключена |
| Отключить отображение прошлых запросов поиска в поле поиска проводника Windows | Отключена |
| Разрешить использование только пользовательских или зарегистрированных расширений | Отключена |
| Отключить отображение фрагментов в режиме просмотра содержимого | Отключена |
| Не отслеживать ярлыки оболочки при перемещении | Включена |
| Максимальная длина списка «Недавние документы» | Включена (1) |
| Удалить возможности записи компакт-дисков | Включена |
| Отключить кэширование эскизов изображений | Включена |
| Запретить изменение видеоэффектов для меню | Включена |
| Запретить изменение указателя клавиатурного вызова | Отключена |
| Удалить вкладку DFS | Включена |
| Скрыть выбранные диски из окна «Мой компьютер» | Отключена |
| Скрыть значок «Вся сеть» в папке «Сеть» | Отключена |
| Удалить меню «Файл» из проводника Windows | Включена |
| Удалить команду «Свойства папки» из меню «Сервис» | Включена |
| Удалить вкладку «Оборудование» | Включена |
| Скрыть команду «Управление» из контекстного меню проводника Windows | Включена |
| Удалить «Общие документы» из окна «Мой компьютер» | Включена |
| Удалить команды «Подключить сетевой диск» и «Отключить сетевой диск» | Включена |
| Не перемещать удаляемые файлы в «Корзину» | Включена |
| Не запрашивать другие имя пользователя и пароль | Включена |
| Удалить ссылку "Повторить поиск" при поиске в Интернете | Включена |
| Удалить вкладку «Безопасность» | Включена |
| Удалить кнопку «Поиск» из проводника Windows | Включена |
| Отключить числовое упорядочивание проводника Windows | Отключена |
| Запретить вывод контекстного меню по умолчанию для проводника Windows | Включена |
| Запретить доступ к дискам через «Мой компьютер» | Отключена |
| Отключить сочетания клавиш Windows+X | Включена |
| Скрыть значок «Соседние компьютеры» в папке «Сеть» | Отключена |
| Запрашивать имя пользователя и пароль при установке по сети | Включена |
| Максимально допустимый размер «Корзины» | Отключена |
| Отключить защищенный режим протокола оболочки | Отключена |
| Прикрепить библиотеки или соединители поиска к ссылкам "Повторить поиск" и меню "Пуск" | Отключена |
| Прикрепить поисковые веб-сайты к ссылкам "Повторить поиск" и меню "Пуск" | Отключена |
| Отображать строку меню в проводнике Windows | Отключена |
| Запретить пользователям добавлять файлы в корневую папку с файлами пользователя. | Включена |
| Отключить анимацию общих элементов управления и окон | Включена |
| **Программа обновления Windows Anytime Upgrade** |  |
| Предотвращает запуск программы обновления Windows Anytime Upgrade. | Включена |
| **проигрыватель Windows Media** |  |
| **Воспроизведение** |  |
| Экранная заставка | Отключена |
| Запретить загрузку кодеков | Включена |
| **Пользовательский интерфейс** |  |
| Не отображать закрепленное окно | Включена |
| Скрыть вкладку «Конфиденциальность» | Включена |
| Скрыть вкладку «Безопасность» | Включена |
| Задать и закрепить обложку | Включена |
| **Сеть** |  |
| Настройка HTTP-прокси | Отключена |
| Настройка прокси-сервера MMS | Отключена |
| Настройка RTSP-прокси | Отключена |
| Скрыть вкладку «Сеть» | Отключена |
| Настройка сетевой буферизации | Отключена |
| Протоколы потоков мультимедиа | Отключена |
| Запретить получение сведений о компакт-диске и диске DVD | Отключена |
| Запретить получение сведений о музыкальных файлах | Отключена |
| Предотвращение получения настроек радиостанций | Отключена |
| **Расположение и датчики** |  |
| Отключить расположение со сценариями | Отключена |
| Отключить расположение | Отключена |
| Отключить датчики | Отключена |
| **Сетевой проектор** |  |
| Отсоединить сетевой проектор | Отключена |
| **Службы удаленных рабочих столов** |  |
| **Клиент подключения к удаленному рабочему столу** |  |
| Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию | Отключена |
| Разрешать RDP-файлы от неизвестных издателей | Отключена |
| Запретить сохранение паролей | Отключена |
| Указать отпечатки SHA1 сертификатов, представляющих доверенных издателей RDP | Отключена |
| **Перенаправление USB-устройств RemoteFx** |  |
| Разрешить перенаправление RDP для других поддерживаемых USB-устройств RemoteFx с этого компьютера | Отключена |
| **Узел сеансов удаленных рабочих столов** |  |
| **Ограничение сеансов по времени** |  |
| Задать ограничение по времени для отключенных сеансов | Отключена |
| Задать ограничение времени для активных, но бездействующих сеансов служб удаленных рабочих столов | Отключена |
| Задать ограничение по времени для активных сеансов служб удаленных рабочих столов | Отключена |
| Завершать сеанс при достижении ограничения по времени | Отключена |
| Задать предел времени для выхода из сеансов RemoteApp | Отключена |
| **Перенаправление принтеров** |  |
| Использовать в первую очередь драйвер принтера Easy Print удаленного рабочего стола | Отключена |
| Перенаправлять только используемый по умолчанию принтер клиента | Отключена |
| **Перенаправление устройств и ресурсов** |  |
| Не разрешать перенаправление буфера обмена | Отключена |
| Разрешить перенаправление часового пояса | Отключена |
| **Подключения** |  |
| Устанавливает правила удаленного управления для пользовательских сеансов служб удаленных рабочих столов | Отключена |
| **Среда удаленных сеансов** |  |
| Запускать программу при подключении | Отключена |
| Отменять фоновый рисунок удаленного рабочего стола | Отключена |
| Всегда отображать рабочий стол при подключении | Отключена |
| **Шлюз удаленных рабочих столов** |  |
| Установить метод проверки подлинности шлюза удаленных рабочих столов | Отключена |
| Разрешить подключение через шлюз удаленных рабочих столов | Не задана |
| Задать адрес сервера шлюза удаленных рабочих столов | Отключена |
| **Совместимость приложений** |  |
| Запрещение доступа к 16-разрядным приложениям. | Отключена |
| Отключение помощника по совместимости программ | Включена |
| **Установщик Windows** |  |
| Всегда устанавливать с повышенными правами | Отключена |
| Запрет установки со съемных носителей | Отключена |
| Запретить откат | Отключена |
| Порядок поиска | Отключена |
| **Цветовая система Windows Color System** |  |
| Запретить установку и удаление цветовых профилей | Отключена |
| **Центр мобильности Windows** |  |
| Отключить центр мобильности Windows | Включена |
| **Центр обновления Windows** |  |
| Не отображать параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows» | Включена |
| Не задавать по умолчанию параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows» | Включена |
| Запретить использование любых средств Центра обновления Windows | Включена |
| **Цифровой ящик** |  |
| Не разрешать работу цифрового ящика | Включена |
| **Меню «Пуск» и панель задач** |  |
| Добавить ссылку "Поиск в Интернете" в меню "Пуск" | Отключена |
| Очищать журнал недавно открывавшихся документов при выходе | Включена |
| Очистка списка недавно использовавшихся программ для новых пользователей | Включена |
| Добавить пункт выхода из системы в главное меню | Отключена |
| Затенить ярлыки меню «Пуск» на не полностью установленные программы | Отключена |
| Отключить сокращенные меню | Включена |
| Закрепить панель задач | Включена |
| Добавить флажок «Запустить в отдельной области памяти» в окно команды «Выполнить» | Отключена |
| Отключить очистку области уведомлений | Включена |
| Удалить всплывающие подсказки для элементов главного меню | Включена |
| Удалить контекстные меню и меню перетаскивания для элементов меню "Пуск" | Включена |
| Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands | Отключена |
| Скрыть общие группы программ в меню «Пуск» | Включена |
| Удалить меню «Избранное» из главного меню | Включена |
| Удалить ссылку «Поиск» из меню «Пуск» | Включена |
| Удалить список часто используемых программ в меню «Пуск» | Включена |
| Удалить ссылку «Игры» из меню «Пуск» | Включена |
| Удалить справку из главного меню | Включена |
| Отключить слежение за действиями пользователя | Включена |
| Удалить список всех программ в меню «Пуск» | Включена[[94]](#footnote-95) |
| Удалить «Сетевые подключения» из меню «Пуск» | Включена |
| Удалить список программ, закрепленных в меню «Пуск» | Включена |
| Не хранить сведения о недавно открывавшихся документах | Включена |
| Удалить меню «Недавние документы» из меню «Пуск» | Включена |
| Не использовать сопоставление ярлыков оболочки на основе поиска | Включена |
| Не использовать метод на основе отслеживания для сопоставления ярлыков | Включена |
| Удалить команду «Выполнить» из меню «Пуск» | Включена |
| Удалить ссылку «Программы по умолчанию» из меню «Пуск» | Включена |
| Удалить значок «Документы» из меню «Пуск» | Включена |
| Удалить значок «Музыка» из меню «Пуск» | Включена |
| Удалить значок «Сеть» из меню «Пуск» | Включена |
| Удалить значок «Изображения» из меню «Пуск» | Включена |
| Запретить поиск соединений | Включена |
| Удалить ссылку "Найти компьютер" | Включена |
| Удалить ссылку "Ознакомиться с другими результатами" или "Поиск везде" | Включена |
| Запретить поиск файлов | Включена |
| Запретить поиск в файлах Интернета | Включена |
| Запретить поиск программ и элементов панели управления | Включена |
| Отключить папки программ в меню «Настройка» | Включена |
| Запретить изменение параметров панели задач и меню «Пуск» | Включена |
| Удалить ссылку "Загрузки" из меню "Пуск" | Включена |
| Удалить ссылку "Домашняя группа" из меню "Пуск" | Включена |
| Удалить ссылку "ТВ-записи" из меню "Пуск" | Включена |
| Удалить папки пользователя из главного меню | Отключена |
| Удалить ссылку "Видео" из меню "Пуск" | Включена |
| Форсировать классическое меню «Пуск» | Включена |
| Удалить часы из системной области уведомлений | Отключена |
| Запретить группировку элементов панели задач | Включена |
| Не отображать панели инструментов в панели задач | Отключена |
| Запретить доступ к контекстному меню для панели задач | Включена |
| Скрыть область уведомлений | Отключена |
| Удалить ссылку на папку пользователя из меню «Пуск» | Включена |
| Удалить имя пользователя из меню «Пуск» | Включена |
| Удаляет ссылки на веб-сайт Центра обновления Windows и запрещает доступ к нему. | Включена |
| Изменить действие кнопки питания меню "Пуск" | Отключена |
| Отображение панели «Быстрый запуск» на панели задач | Включена |
| Удалить кнопку «Отстыковка ПК» из меню «Пуск» | Включена |
| Добавить команду «Выполнить» в меню «Пуск» | Отключена |
| Удалить «Завершение сеанса» из меню «Пуск» | Отключена |
| Удалить значок центра поддержки | Включена |
| Скрыть значок сети | Включена |
| Скрыть индикатор батареи | Включена |
| Скрыть значок регулятора громкости | Включена |
| Отключить всплывающие уведомления объявлений компонентов | Включена |
| Запретить закрепление элементов в списках переходов | Включена |
| Запретить закрепление программ в панели задач | Включена |
| Не отображать и не отслеживать элементы в списках переходов из удаленных расположений | Включена |
| Отключить автоматическое отображение значков уведомлений в панели задач | Включена |
| Блокировать все параметры панели задач | Включена |
| Запретить добавление и удаление панелей инструментов | Включена |
| Запретить перемещение панелей инструментов | Включена |
| Отключить всплывающие напоминания | Включена |
| Удалить закрепленные программы из панели задач | Отключена |
| Запретить перемещение панели задач в другое положение на экране | Включена |
| Запретить изменение размера панели задач | Включена |
| Отключить эскизы панели задач | Включена |
| **Общие папки** |  |
| Разрешить публикацию DFS-корней | Отключена |
| Разрешить публикацию общих папок | Отключена |
| **Панель управления** |  |
| **Окно свойств экрана** |  |
| Отключить окно свойств экрана в панели управления | Отключена |
| Скрыть вкладку «Настройка» | Отключена |
| **Персонализация** |  |
| Запретить изменение цветовой схемы | Отключена |
| Запретить изменение темы | Отключена |
| Запретить изменение стилей оформления окон и кнопок | Отключена |
| Включить заставку | Включена[[95]](#footnote-96) |
| Запретить выбор размера шрифта для стиля оформления | Отключена |
| Запретить изменение цвета и оформления окон | Отключена |
| Запретить изменение фона рабочего стола | Отключена |
| Запретить изменение значков рабочего стола | Отключена |
| Запретить изменение указателей мыши | Отключена |
| Запретить изменение заставки | Отключена |
| Запретить изменение звуков | Отключена |
| Парольная защита заставки | Включена |
| Таймаут заставки | Включена (900 сек.) [[96]](#footnote-97) |
| Применить указанную заставку | Отключена |
| Загрузить указанную тему | Отключена |
| Применить конкретный файл стиля оформления или классический стиль Windows | Отключена |
| **Принтеры** |  |
| Разрешить обзор сети для поиска принтеров | Отключена |
| Разрешить обзор общего веб-сайта с целью поиска принтеров | Отключена |
| Запретить добавление принтеров | Отключена |
| Запретить удаление принтеров | Отключена |
| Использовать только функцию указания и печати для пакета | Отключена |
| Функция указания и печати для пакетов - Разрешенные серверы | Отключена |
| Ограничения указания и печати | Отключена |
| Путь поиска принтеров Active Directory по умолчанию | Отключена |
| **Программы** |  |
| Скрытие страницы доступа к программам и параметров по умолчанию | Отключена |
| Скрыть страницу «Получение программ» | Отключена |
| Скрыть страницу «Установленные обновления» | Отключена |
| Скрыть страницу «Программы и компоненты» | Отключена |
| Скрыть панель управления «Программы» | Отключена |
| Скрыть «Компоненты Windows» | Отключена |
| Скрыть «Windows Marketplace» | Отключена |
| **Установка и удаление программ** |  |
| Категория программ, используемая по умолчанию для страницы «Установка программ» | Отключена |
| Скрытие параметра «Установка программ с компакт-диска или дискеты» | Отключена |
| Скрытие параметра «Установка программ от Майкрософт» | Отключена |
| Скрытие параметра «Установка программ из локальной сети» | Отключена |
| Скрытие страницы «Установка программ» | Отключена |
| Удаление окна «Установка и удаление программ» | Отключена |
| Скрытие страницы «Задание доступа к программам и параметров по умолчанию» | Отключена |
| Скрытие страницы «Изменение или удаление программ» | Отключена |
| Перейти на страницу мастера компонентов | Отключена |
| Удаление сведений о поддержке | Отключена |
| Скрытие страницы «Установка компонентов Windows» | Отключена |
| **Язык и региональные стандарты** |  |
| Скрыть параметры управления в панели «Язык и региональные стандарты» | Отключена |
| Скрыть параметр географического положения | Отключена |
| Скрыть параметры выбора языковой группы | Отключена |
| Скрыть параметры выбора и настройки языкового стандарта | Отключена |
| Ограничить язык интерфейса Windows для указанного пользователя | Отключена |
| Ограничить выбор языка меню и диалогов Windows | Отключена |
| Скрыть указанные элементы панели управления | Отключена |
| Всегда открывать все элементы панели управления при ее открытии | Отключена |
| Запретить доступ к панели управления | Включена |
| Показать только заданные элементы панели управления | Отключена |
| **Рабочий стол** |  |
| **Active Desktop** |  |
| Включить Active Desktop | Отключена |
| Отключить Active Desktop | Включена |
| Запретить изменения | Включена |
| Фоновые рисунки рабочего стола | Отключена |
| Запретить добавление элементов | Отключена |
| Запретить закрытие элементов | Отключена |
| Запретить удаление элементов | Отключена |
| Запретить изменение элементов | Отключена |
| Отключить все элементы | Отключена |
| Добавить или удалить элементы | Отключена |
| Разрешить только точечные рисунки для фонового рисунка. | Отключена |
| **Active Directory** |  |
| Включите фильтр в диалоговом окне «Найти» | Отключена |
| Скрыть папку Active Directory | Отключена |
| Максимальный объем результатов поиска в Active Directory | Отключена |
| Запретить пользователям вручную перенаправлять папки профилей. | Отключена |
| Скрыть и отключить все элементы рабочего стола | Включена |
| Удалить мастер очистки рабочего стола | Включена |
| Скрыть значок Internet Explorer на рабочем столе | Включена |
| Удалить значок «Компьютер» с рабочего стола | Включена |
| Удалить значок «Мои документы» с рабочего стола | Включена |
| Скрыть значок «Сеть» на рабочем столе | Включена |
| Удалить пункт «Свойства» из контекстного меню значка «Компьютер» | Включена |
| Удалить пункт «Свойства» из контекстного меню значка «Документы» | Включена |
| Не добавлять общие папки, из которых открыты документы в «Сеть» | Включена |
| Удалить значок «Корзина» с рабочего стола | Включена |
| Удалить пункт «Свойства» из контекстного меню компонента «Корзина» | Включена |
| Не сохранять параметры при выходе | Включена |
| Отключить сворачивание окна Aero Shake жестом мышью | Отключена |
| Запретить добавление, перетаскивание и закрытие панелей инструментов панели задач | Включена |
| Запретить настройку панелей инструментов рабочего стола | Включена |
| **Сеть** |  |
| **Windows Connect Now** |  |
| Запретить доступ к мастерам Windows Connect Now | Включена |
| **Автономные файлы** |  |
| Административно назначенные автономные файлы | Отключена |
| Нестандартные действия при отключении от сервера | Отключена |
| Уровень регистрации событий | Отключена |
| Действие при отключении от сервера | Отключена |
| Запретить использование папки «Автономные файлы» | Включена |
| Запретить пользовательскую настройку автономных файлов | Включена |
| Удалить «Сделать доступными автономно» | Включена |
| Запретить применение «Сделать доступными автономно» для этих файлов и папок | Отключена |
| Отключить всплывающие напоминания | Включена |
| Частота появления всплывающих напоминаний | Отключена |
| Исходное время отображения всплывающих напоминаний | Отключена |
| Время отображения всплывающих напоминаний | Отключена |
| Синхронизировать перед выходом из системы | Отключена |
| Синхронизировать автономные файлы при входе в систему | Отключена |
| Синхронизировать автономные файлы перед приостановкой | Отключена |
| **Сетевые подключения** |  |
| Запретить добавление и удаление компонентов для локальной сети (LAN) и подключений удаленного доступа | Включена |
| Запрет доступа к пункту «Дополнительные параметры» меню «Дополнительно» | Включена |
| Запретить дополнительные настройки TCP/IP | Включена |
| Запрет включения/отключения компонентов локальной сети | Включена |
| Запретить удаление подключений удаленного доступа | Включена |
| Запрет доступа к пункту «Настройки удаленного доступа» меню «Дополнительно» | Включена |
| Включение параметров сетевых подключений Windows 2000 для администраторов | Отключена |
| Выключение уведомлений при ограниченном или не установленном подключении | Отключена |
| Запрет доступа к свойствам компонентов подключений локальной сети | Включена |
| Возможность включения/разрыва подключения локальной сети | Отключена |
| Запрет доступа к свойствам подключений локальной сети | Включена |
| Запрет доступа к мастеру новых подключений | Включена |
| Возможность изменить свойства всех пользовательских подключений удаленного доступа | Отключена |
| Запрет доступа к свойствам компонентов подключений удаленного доступа | Включена |
| Запрет подключения и разрыва подключения удаленного доступа | Включена |
| Запрет изменения свойств частного подключения удаленного доступа | Включена |
| Возможность удалить все подключения удаленного доступа пользователей | Отключена |
| Возможность переименовать подключения локальной сети или подключения удаленного доступа, доступные всем пользователям. | Отключена |
| Возможность переименовать подключения локальной сети | Отключена |
| Запретить переименование частных подключений удаленного доступа | Включена |
| Запретить просмотр состояния активных подключений | Включена |
| **Система** |  |
| **Windows HotStart** |  |
| Отключить Windows HotStart | Отключена |
| **Варианты действий после нажатия CTRL+ALT+DEL** |  |
| Запретить изменение пароля | Отключена |
| Запретить блокировку компьютера | Отключена |
| Удалить диспетчер задач | Включена |
| Запретить завершение сеанса | Отключена |
| **Вход в систему** |  |
| Не обрабатывать список запуска старых программ | Отключена |
| Не обрабатывать список однократного запуска программ | Отключена |
| Выполнять эти программы при входе в систему | Отключена |
| **Групповая политика** |  |
| Запретить интерактивным пользователям создавать данные результирующей политики (Resultant Set of Policy — RSoP) | Отключена |
| Отключить автоматическое обновление ADM-файлов | Отключена |
| Вывод пункта «Показывать только политики» | Отключена |
| Выбор контроллера домена групповой политики | Отключена |
| Обнаружение медленных подключений для групповой политики | Включена |
| Интервал обновления групповой политики для пользователей | Отключена |
| Имя по умолчанию для новых объектов групповой политики | Отключена |
| Создание ссылок объектов групповой политики по умолчанию запрещено | Включена |
| **Доступ к съемным запоминающим устройствам** |  |
| Время (в секундах) до принудительной перезагрузки | Отключена |
| Компакт-диски и DVD-диски: Запретить чтение | Отключена |
| Компакт-диски и DVD-диски: Запретить запись | Отключена |
| Специальные классы: Запретить чтение | Отключена |
| Специальные классы: Запретить запись | Отключена |
| Накопители на гибких дисках: Запретить чтение | Отключена |
| Накопители на гибких дисках: Запретить запись | Отключена |
| Съемные диски: Запретить чтение | Отключена |
| Съемные диски: Запретить запись | Отключена |
| Съемные запоминающие устройства всех классов: Запретить любой доступ | Отключена |
| Ленточные накопители: Запретить чтение | Отключена |
| Ленточные накопители: Запретить запись | Отключена |
| WPD-устройства: Запретить чтение | Отключена |
| WPD-устройства: Запретить запись | Отключена |
| **Панель управления производительностью** |  |
| Отключение доступа к основному разделу панели управления производительностью | Отключена |
| Отключение доступа к разделу решения проблем производительности | Отключена |
| Отключение доступа к разделу изготовителя оборудования (OEM) и фирменной символики корпорации Майкрософт. | Отключена |
| **Перенаправление папки** |  |
| Не перенаправлять автоматически папки, доступные автономно | Отключена |
| Использовать локализованные имена при перенаправлении папок меню "Пуск" и "Мои документы" | Отключена |
| **Профили пользователей** |  |
| Подключить домашнюю папку к корню общего ресурса | Отключена |
| Синхронизировать сетевые папки только в момент входа или выхода из системы | Отключена |
| Исключить папки из перемещаемого профиля | Отключена |
| Ограничить размер профиля | Отключена |
| **Службы языковых стандартов** |  |
| Запретить выбор пользовательских языковых стандартов | Отключена |
| Ограничить пользовательские языковые стандарты | Отключена |
| Запретить изменение географического положения | Отключена |
| Не позволять пользователю переопределять параметры языкового стандарта | Отключена |
| **Сценарии** |  |
| Выполнять сценарии входа прежних версий в фоновом режиме | Отключена |
| Выполнять сценарии выхода с отображением команд | Отключена |
| Выполнять сценарии входа в систему синхронно | Отключена |
| Выполнять сценарии входа с отображением команд | Отключена |
| Выполнить сценарии Windows PowerShell при входе пользователя в систему, завершить сеанс | Отключена |
| **Управление связью через Интернет** |  |
| **Параметры связи через Интернет** |  |
| Отключение рейтинга справки | Включена |
| Отключение программы улучшения справки | Включена |
| Отключение «Windows в Интернете» | Включена |
| Отключить отчеты об ошибках распознавания рукописного текста | Включена |
| Отключить печать по протоколу HTTP | Включена |
| Отключение загрузки драйверов принтера по протоколу HTTP | Включена |
| Отключить службу сопоставления файлов Интернета | Включена |
| Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков | Включена |
| Отключить заказ отпечатков через Интернет в списке задач для изображений | Включена |
| Отключить веб-публикацию в списке задач для файлов и папок | Включена |
| Отключить участие в программе улучшения поддержки пользователей Windows Messenger | Включена |
| Ограничение соединения с Интернетом | Включена |
| **Управление электропитанием** |  |
| Запрашивать пароль при выходе из режима гибернации, спящего или ждущего режима | Включена |
| **Установка драйвера** |  |
| Настроить папки для поиска драйверов | Отключена |
| Отключить запрос на поиск драйверов устройств на веб-сайте Windows Update | Включена |
| Цифровая подпись драйверов устройств | Отключена |
| Загружать отсутствующие COM-компоненты | Отключена |
| Интерпретация столетия для 2000 года | Отключена |
| Запретить запуск из справки перечисленных программ | Включена (\*.\*) |
| Не показывать окно приветствия «Приступая к работе» при входе в систему | Включена |
| Настраиваемый интерфейс пользователя | Отключена |
| Запретить использование командной строки | Включена |
| Запретить доступ к средствам редактирования реестра | Отключена |
| Не запускать указанные приложения Windows[[97]](#footnote-98) | Включена (cmd.exe,explorer.exe,iexplore.exe[[98]](#footnote-99)) |
| Выполнять только указанные приложения Windows | Отключена |
| Автоматическое обновление Windows | Отключена |
| **Все параметры** | См. значение конкретного параметра выше в таблице |
| **Настройка** |  |
| **Конфигурация Windows** |  |
| **Приложения** | Не определено |
| **Сопоставления дисков** | Не определено |
| **Среда** | Не определено |
| **Файлы** | Не определено |
| **Папки** | Не определено |
| **INI-файлы** | Не определено |
| **Реестр** | Не определено |
| **Ярлыки** | Не определено |
| **Параметры панели управления** |  |
| Источники данных | Не определено |
| Устройства | Не определено |
| Параметры папок | Не определено |
| Параметры обозревателя | Не определено |
| Локальные пользователи и группы | Не определено |
| Сетевые параметры | Не определено |
| Электропитание | Не определено |
| Принтеры | Не определено |
| Региональные параметры | Не определено |
| Назначенные задания | Не определено |
| Главное меню | Не определено |
|  | |

### Параметры групповой политики для АРМ при использовании СЗИ от НСД Secret Net

Параметры групповой политики и их значения, применяемые для АРМ при использовании СЗИ от НСД «Secret Net», приведены в таблице (Таблица 44).

Таблица 44. Параметры групповой политики для АРМ при использовании СЗИ от НСД Secret Net

|  |  |  |
| --- | --- | --- |
| **Наименование раздела/параметра** | | **Значение** |
| **Политики** | |  |
| **Конфигурация программ** | |  |
| Установка программ | | Не определено |
| **Конфигурация Windows** | |  |
| **Политика разрешения имен** | | Не определено |
| **Сценарии (запуск/завершение)** | |  |
| Автозагрузка | | Не определено |
| Завершение работы | | Не определено |
| **Административные шаблоны** | |  |
| **Параметры безопасности** | |  |
| **Политики учетных записей** | |  |
| **Политика паролей** | |  |
| Вести журнал паролей | | 5 хранимых паролей |
| Максимальный срок действия пароля | | 180 дней |
| Минимальная длина пароля | | 8 символов |
| Минимальный срок действия пароля | | 0 дней |
| Пароль должен отвечать требованиям сложности | | Включен |
| Хранить пароли, используя обратимое шифрование | | Отключен |
| **Политика блокировки учетной записи** | |  |
| Время до сброса счетчика блокировки | | 30 мин. |
| Пороговое значение блокировки | | 5 ошибок входа в систему |
| Продолжительность блокировки учетной записи | | 0 |
| **Политика Kerberos [[99]](#footnote-100)** | |  |
| Максимальная погрешность синхронизации часов компьютера | | 5 |
| Максимальный срок жизни билета пользователя | | 10 |
| Максимальный срок жизни билета службы | | 600 |
| Максимальный срок жизни для возобновления билета пользователя | | 7 |
| Принудительные ограничения входа пользователей | | Включен |
| **Локальные политики** | |  |
| **Политика аудита** | |  |
| Аудит входа в систему | | успех, отказ |
| Аудит доступа к объектам | | нет аудита |
| Аудит доступа к службе каталогов | | отказ |
| Аудит изменения политики | | успех, отказ |
| Аудит использования привилегий | | нет аудита |
| Аудит отслеживания процессов | | нет аудита |
| Аудит системных событий | | успех, отказ |
| Аудит событий входа в систему | | успех, отказ |
| Аудит управления учетными записями | | успех, отказ |
| **Назначение прав пользователя** | |  |
| Архивация файлов и каталогов | | Администраторы |
| Блокировка страниц в памяти | | [[100]](#footnote-101) |
| Восстановление файлов и каталогов | | Администраторы |
| Вход в качестве пакетного задания | | Локальная служба |
| Вход в качестве службы | |  |
| Выполнение задач по обслуживанию томов | | Администраторы |
| Добавление рабочих станций к домену | | Администраторы |
| Доступ к диспетчеру учетных данных от имени доверенного вызывающего | |  |
| Доступ к компьютеру из сети | | Прошедшие проверку |
| Завершение работы системы | | Администраторы, Прошедшие проверку |
| Загрузка и выгрузка драйверов устройств | | Администраторы |
| Замена маркера уровня процесса | | Локальная служба, сетевая служба |
| Запретить вход в систему через службу удаленных рабочих столов | |  |
| Запретить локальный вход | |  |
| Изменение метки объекта | |  |
| Изменение параметров среды изготовителя | | Администраторы |
| Изменение системного времени | | Администраторы, локальная служба |
| Изменение часового пояса | | Администраторы, локальная служба |
| Имитация клиента после проверки подлинности | | Администраторы, локальная служба,  сетевая служба, служба |
| Локальный вход в систему | | Администраторы, Прошедшие проверку |
| Настройка квот памяти для процесса | | Администраторы |
| Обход перекрестной проверки | | Прошедшие проверку |
| Отказать в доступе к этому компьютеру из сети | | loser |
| Отказать во входе в качестве пакетного задания | |  |
| Отказать во входе в качестве службы | |  |
| Отключение компьютера от стыковочного узла | | Администраторы |
| Отладка программ | | Администраторы |
| Принудительное удаленное завершение работы | | Администраторы |
| Профилирование одного процесса | | Администраторы |
| Профилирование производительности системы | | Администраторы |
| Работа в режиме операционной системы | | Локальная служба |
| Разрешение доверия к учетным записям компьютеров и пользователей при делегировании | | Администраторы |
| Разрешить вход в систему через службу удаленных рабочих столов | | Администраторы |
| Синхронизация данных службы каталогов | | Администраторы |
| Смена владельцев файлов и других объектов | | Администраторы |
| Создание аудитов безопасности | | Локальная служба, сетевая служба |
| Создание глобальных объектов | | Администраторы |
| Создание маркерного объекта | | Локальная служба |
| Создание постоянных общих объектов | | Локальная служба |
| Создание символических ссылок | | Администраторы |
| Создание файла подкачки | | Администраторы |
| Увеличение приоритета выполнения | | Администраторы |
| Увеличение рабочего набора процесса | | Администраторы, Пользователи |
| Управление аудитом и журналом безопасности[[101]](#footnote-102) | | Auditors |
| **Параметры безопасности** | |  |
| DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language) | | Не определено |
| DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language) | | Не определено |
| Аудит: аудит доступа глобальных системных объектов | | Отключен |
| Аудит: аудит прав на архивацию и восстановление | | Отключен |
| Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности | | Отключен |
| Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows 7 или следующие версии) | | Включен |
| Доступ к сети: Разрешить трансляцию анонимного SID в имя | | Отключен |
| Завершение работы: очистка файла подкачки виртуальной памяти | | Включен |
| Завершение работы: разрешить завершение работы системы без выполнения входа в систему | | Отключен |
| Интерактивный вход в систему: поведение при извлечении смарт-карты | | Блокировка рабочей станции |
| Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему | | Не определено |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | | 0 |
| Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее | | 5 дн. |
| Интерактивный вход в систему: не отображать последнее имя пользователя | | Включен |
| Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL | | Отключен |
| Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован. | | Включен (Выводимое имя пользователя, имена домена и пользователя) |
| Интерактивный вход в систему: текст сообщения для пользователей при входе в систему | | Не определено |
| Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера | | Отключен |
| Интерактивный вход в систему: требовать смарт-карту | | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (всегда) | | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) | | Включен |
| Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам | | Отключен |
| Консоль восстановления: разрешить автоматический вход администратора | | Отключен |
| Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам | | Отключен |
| Контроллер домена: запретить изменение пароля учетных записей компьютера | | Отключен |
| Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию | | Отключен |
| Контроллер домена: требование цифровой подписи для LDAP-сервера | | Нет |
| Контроль учетных записей: все администраторы работают в режиме одобрения администратором | | Отключен |
| Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав | | Отключен |
| Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав | | Отключен |
| Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором | | Повышение без запроса |
| Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей | | Запрос учетных данных |
| Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах | | Отключен |
| Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов | | Отключен |
| Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя | | Отключен |
| Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол | | Отключен |
| Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора | | Отключен |
| Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ | | Отключен |
| Параметры системы: необязательные подсистемы | | Posix |
| Сервер сети Microsoft: время бездействия до приостановки сеанса | | 15 мин. |
| Сервер сети Microsoft: использовать цифровую подпись (всегда) | | Отключено |
| Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента) | | Отключено |
| Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа | | Отключен |
| Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC) | | Минимума нет |
| Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC) | | Минимума нет |
| Сетевая безопасность: настройка типов шифрования, разрешенных Kerberos | | Не определено |
| Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля | | Включен |
| Сетевая безопасность: ограничения NTLM: аудит входящего трафика NTLM | | Отключить |
| Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене | | Отключить |
| Сетевая безопасность: ограничения NTLM: входящий трафик NTLM | | Разрешить все |
| Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене | | Не определено |
| Сетевая безопасность: ограничения NTLM: добавить удаленные серверы в исключения проверки подлинности NTLM | | Не определено |
| Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удаленным серверам | | Разрешить все |
| Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене | | Отключить |
| Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы | | Отключен |
| Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы | | Включен |
| Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U к этому компьютеру | | Отключен |
| Сетевая безопасность: разрешить учетной записи локальной системы использовать удостоверение компьютера для NTLM | | Отключен |
| Сетевая безопасность: требование цифровой подписи для LDAP-клиента | | Согласование цифровой подписи |
| Сетевая безопасность: уровень проверки подлинности LAN Manager | | Отправлять только NTLMv2 ответ |
| Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам | | Включен |
| Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей | | Обычная (Обычная – локальные пользователи удостоверяются как они сами) |
| Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями | | Включен |
| Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями | | Отключен |
| Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности | | Включен |
| Сетевой доступ: разрешать анонимный доступ к именованным каналам | | Не определено |
| Сетевой доступ: разрешать анонимный доступ к общим ресурсам | | Не определено |
| Сетевой доступ: разрешать применение разрешений "Для всех" к анонимным пользователям | | Отключен |
| Сетевой доступ: удаленно доступные пути и вложенные пути реестра | System\CurrentControlSet\Control\Print\Printers,  System\CurrentControlSet\Services\Eventlog,  Software\Microsoft\OLAP Server,  Software\Microsoft\WindowsNT\CurrentVersion\Print,  Software\Microsoft\WindowsNT\CurrentVersion\Windows,  System\CurrentControlSet\Control\ContentIndex,  System\CurrentControlSet\Control\Terminal Server,  System\CurrentControlSet\Control\Terminal Server\UserConfig,  System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,  Software\Microsoft\Windows NT\CurrentVersion\Perflib,  System\CurrentControlSet\Services\SysmonLog,  System\CurrentControlSet\Services\CertSvc,  System\CurrentControlSet\Services\Wins | |
| Сетевой доступ: удаленно доступные пути реестра | System\CurrentControlSet\Control\ProductOptions,  System\CurrentControlSet\Control\Server Applications,  Software\Microsoft\Windows NT\CurrentVersion | |
| Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного объекта | | Откл. |
| Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания | | Отключен |
| Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере | | Не требуется ввод данных пользователем при сохранении и использовании новых ключей. |
| Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок) | | Включен |
| Системные объекты: учитывать регистр для подсистем, отличных от Windows | | Включен |
| Устройства: запретить пользователям установку драйверов принтера | | Отключен. |
| Устройства: разрешать отстыковку без входа в систему | | Включен |
| Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям | | Включен |
| Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям | | Включен |
| Устройства: разрешить форматирование и извлечение съемных носителей | | Администраторы |
| Учетные записи: Переименование учетной записи администратора | | adm |
| Учетные записи: Переименование учетной записи гостя | | loser |
| Учетные записи: разрешить использование пустых паролей только при консольном входе | | Отключен |
| Учетные записи: Состояние учетной записи 'Администратор' | | Отключен[[102]](#footnote-103) |
| Учетные записи: Состояние учетной записи 'Гость' | | Отключен |
| Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала | | Включен |
| Член домена: максимальный срок действия пароля учетных записей компьютера | | 180 дн. |
| Член домена: отключить изменение пароля учетных записей компьютера | | Отключен |
| Член домена: требовать стойкий ключ сеанса (Windows 2000 или выше) | | Включен |
| Член домена: цифровая подпись данных безопасного канала, когда это возможно | | Включен |
| Член домена: шифрование данных безопасного канала, когда это возможно | | Включен |
| **Журнал событий** | |  |
| Запретить доступ локальной группы гостей к журналу безопасности | | Включен |
| Запретить доступ локальной группы гостей к журналу приложений | | Включен |
| Запретить доступ локальной группы гостей к системному журналу | | Включен |
| Максимальный размер журнала безопасности | | 81920 КБ |
| Максимальный размер журнала приложений | | 32768 КБ |
| Максимальный размер системного журнала | | 32768 КБ |
| Метод сохранения событий в журнале безопасности | | Затирать старые события при необходимости |
| Метод сохранения событий в журнале приложений | | Затирать старые события при необходимости |
| Метод сохранения событий в системном журнале | | Затирать старые события при необходимости |
| Сохранять события в журнале безопасности | | Не определено |
| Сохранять события в журнале приложений | | Не определено |
| Сохранять события в системном журнале | | Не определено |
| **Группы с ограниченным доступом[[103]](#footnote-104)** | |  |
| **Системные службы[[104]](#footnote-105)** | |  |
| DHCP-клиент | | Авто |
| DNS-клиент | | Автоматическое |
| DNS-сервер | | Отключен |
| KtmRm для координатора распределенных транзакций | | Вручную |
| Microsoft .NET Framework NGEN v2.0.50727\_X64 | | Вручную |
| Microsoft .NET Framework NGEN v2.0.50727\_X86 | | Вручную |
| Plug-and-Play | | Автоматическое |
| Windows Audio | | Автоматическое |
| Windows CardSpace | | Отключен |
| Windows Driver Foundation - User-mode Driver Framework | | Вручную |
| WMI Performance Adapter | | Вручную |
| Агент защиты сетевого доступа | | Отключен |
| Агент политики IPsec | | Вручную |
| Брандмауэр Windows | | Отключен |
| Браузер компьютеров | | Отключен |
| Веб-службы Active Directory | | Автоматическое |
| Виртуальный диск | | Вручную |
| Вспомогательная служба IP | | Автоматическое |
| Вторичный вход в систему | | Вручную |
| Дефрагментация диска | | Вручную |
| Диспетчер автоматических подключений удаленного доступа | | Вручную |
| Диспетчер печати | | Автоматическое |
| Диспетчер подключений удаленного доступа | | Вручную |
| Диспетчер сеансов диспетчера окон рабочего стола | | Автоматическое |
| Диспетчер учетных данных | | Вручную |
| Диспетчер учетных записей безопасности | | Автоматическое |
| Доменные службы Active Directory | | Автоматическое |
| Доступ к HID-устройствам | | Вручную |
| Журнал событий Windows | | Автоматическое |
| Журналы и оповещения производительности | | Вручную |
| Защита программного обеспечения | | Автоматическое |
| Защищенное хранилище | | Вручную |
| Изоляция ключей CNG | | Вручную |
| Инструментарий управления Windows | | Автоматическое |
| Информация о совместимости приложений | | Вручную |
| Клиент групповой политики | | Автоматическое |
| Клиент отслеживания изменившихся связей | | Вручную |
| Координатор распределенных транзакций | | Автоматическое |
| Кэш шрифтов Windows Presentation Foundation 3.0.0.0 | | Вручную |
| Ловушка SNMP | | Вручную |
| Локатор удаленного вызова процедур (RPC) | | Вручную |
| Маршрутизация и удаленный доступ | | Отключен |
| Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности | | Вручную |
| Модуль запуска процессов DCOM-сервера | | Автоматическое |
| Модуль поддержки NetBIOS через TCP/IP | | Автоматическое |
| Модуль поддержки специальной консоли администрирования | | Вручную |
| Настройка сервера удаленных рабочих столов | | Вручную |
| Обнаружение SSDP | | Отключен |
| Обнаружение интерактивных служб | | Вручную |
| Общий доступ к подключению к Интернету (ICS) | | Отключен |
| Определение оборудования оболочки | | Вручную |
| Основные службы доверенного платформенного модуля | | Вручную |
| Перенаправитель портов пользовательского режима служб удаленных рабочих столов | | Вручную |
| Перечислитель IP-шин PnP-X | | Отключен |
| Питание | | Автоматическое |
| Планировщик заданий | | Автоматическое |
| Планировщик классов мультимедиа | | Вручную |
| Поддержка элемента панели управления "Отчеты о проблемах и их решениях" | | Вручную |
| Политика удаления смарт-карт | | Вручную |
| Поставщик результирующей политики (RSoP) | | Автоматическое |
| Проводная автонастройка | | Вручную |
| Программный поставщик теневого копирования (Microsoft) | | Вручную |
| Пространство имен DFS | | Автоматическое |
| Публикация ресурсов обнаружения функции | | Вручную |
| Рабочая станция | | Автоматическое |
| Распространение сертификата | | Вручную |
| Расширяемый протокол проверки подлинности (EAP) | | Вручную |
| Репликация DFS | | Автоматическое |
| Служба репликации файлов | | Отключен |
| Сборщик событий Windows | | Вручную |
| Сведения о приложении | | Вручную |
| Сервер | | Отключен[[105]](#footnote-106) |
| Сервер упорядочения потоков | | Вручную |
| Сетевой вход в систему | | Автоматическое |
| Сетевые подключения | | Автоматическое |
| Система событий COM+ | | Вручную |
| Системное приложение COM+ | | Вручную |
| Служба SSTP | | Вручную |
| Служба автоматического обнаружения веб-прокси WinHTTP | | Вручную |
| Служба базовой фильтрации | | Автоматическое |
| Служба времени Windows | | Автоматическое |
| Служба завершения работы в качестве гостя (Hyper-V) | | Автоматическое |
| Служба запросов на теневое копирование томов Hyper-V | | Автоматическое |
| Служба инициатора Майкрософт iSCSI | | Вручную |
| Служба интерфейса сохранения сети | | Автоматическое |
| Служба кэша шрифтов Windows | | Вручную |
| Служба межсайтовых сообщений | | Автоматическое |
| Служба обмена данными (Hyper-V) | | Автоматическое |
| Служба общего доступа к портам Net.Tcp | | Отключен |
| Служба перечислителя переносных устройств | | Вручную |
| Служба политики диагностики | | Автоматическое |
| Служба профилей пользователей | | Автоматическое |
| Служба пульса (Hyper-V) | | Автоматическое |
| Служба регистрации ошибок Windows | | Вручную |
| Служба регистрации платформы Fibre Channel Microsoft | | Вручную |
| Служба сведений о подключенных сетях | | Автоматическое |
| Служба синхронизации времени Hyper-V | | Автоматическое |
| Служба списка сетей | | Вручную |
| Служба уведомления SPP | | Вручную |
| Служба уведомления о системных событиях | | Автоматическое |
| Служба удаленного управления Windows (WS-Management) | | Отключен |
| Служба шлюза уровня приложения | | Отключен |
| Службы криптографии | | Автоматическое |
| Службы удаленных рабочих столов | | Отключен |
| Смарт-карта | | Автоматическое |
| Сопоставитель конечных точек RPC | | Автоматическое |
| Средство построения конечных точек Windows Audio | | Вручную |
| Телефония | | Вручную |
| Теневое копирование тома | | Отключен |
| Тополог канального уровня | | Вручную |
| Удаленный вызов процедур (RPC) | | Автоматическое |
| Удаленный реестр | | Отключен |
| Удостоверение приложения | | Вручную |
| Узел системы диагностики | | Вручную |
| Узел службы диагностики | | Вручную |
| Узел универсальных PNP-устройств | | Вручную |
| Управление приложениями | | Вручную |
| Управление сертификатами и ключом работоспособности | | Вручную |
| Установщик Windows | | Вручную |
| Установщик модулей Windows | | Вручную |
| Фоновая интеллектуальная служба передачи (BITS) | | Вручную |
| Хост библиотеки счетчика производительности | | Вручную |
| Хост поставщика функции обнаружения | | Вручную |
| Цветовая система Windows (WCS) | | Вручную |
| Центр обновления Windows | | Отключен |
| Центр распространения ключей Kerberos | | Вручную |
| Шифрованная файловая система (EFS) | | Вручную |
| **Реестр** | | Не определено |
| **Файловая система** | | Не определено |
| **Политики проводной сети (IEEE 802.3)** | | Не определено |
| **Брандмауэр Windows в режиме повышенной безопасности** | |  |
| Брандмауэр Windows в режиме повышенной безопасности | |  |
| Свойства брандмауэра Windows | | Все параметры: "не задано" или "по умолчанию" |
| Профиль домена | | Не настроено |
| Частный профиль | | Не настроено |
| Общий профиль | | Не настроено |
| Правила безопасности подключений | | Не определено |
| Правила для входящих подключений | | Не определено |
| Правила для исходящих подключений | | Не определено |
| **Политики диспетчера списка сетей** | |  |
| <DNS-имя домена> | | Указать полное имя домена |
| Неопознанные сети | | Не задано |
| Идентификация сетей | | Не задано |
| Все сети | | Не задано |
| **Политики беспроводной сети (IEEE 802.11)** | | Не определено |
| **Политики открытого ключа** | |  |
| **Шифрующая файловая система (EFS)** | | Не определено |
| **Шифрование диска BitLocker** | | Не определено |
| **Параметры автоматического запроса сертификатов** | | Не определено |
| **Доверенные корневые центры сертификации** | | Не определено |
| **Доверительные отношения в предприятии** | | Не определено |
| **Промежуточные центры сертификации** | | Не определено |
| **Доверенные издатели** | | Не определено |
| **Сертификаты, к которым нет доверия** | | Не определено |
| **Доверенные лица** | | Не определено |
| Клиент служб сертификатов - политика регистрации сертификатов | | Не настроено |
| Параметры подтверждения пути сертификата | | Не настроено |
| Клиент служб сертификации: автоматическая регистрация | | Не настроено |
| **Политики ограниченного использования программ** | | Не определено |
| **Защита доступа к сети** | |  |
| **Конфигурация клиента NAP** | |  |
| **Клиенты принудительной защиты** | |  |
| Клиента принудительного карантина для DHCP | | Отключено |
| Сторона, использующая IPSec | | Отключено |
| Клиент принудительного помещения на карантин шлюза удаленных рабочих столов | | Отключено |
| Клиент принудительного карантина EAP | | Отключено |
| Клиент принудительного удаленного доступа для Windows XP | | Отключено |
| Клиент принудительного использования EAOPL для Windows XP | | Отключено |
| **Параметры пользовательского интерфейса** | |  |
| Пользовательский интерфейс | | Не определено |
| **Параметры регистрации работоспособности** | |  |
| **Группы доверенных серверов** | |  |
| **Политика запроса** | |  |
| Алгоритм кэширования | | sha1RSA(1.3.14.3.2.29) |
| Поставщик службы криптографии | | Microsoft RSA SChannel Cryptographic Provider  2048 бит |
| **Политики управления приложениями** | |  |
| **AppLocker** | |  |
| Исполняемые правила | | Не определено |
| Правила установщика Windows | | Не определено |
| Правила сценариев | | Не определено |
| **Политики IP-безопасности на "Служба каталогов Active Directory (...)"** | |  |
| Client (Respond Only) | |  |
| Правила (*единственное, создано по умолчанию*) | |  |
| Список IP-фильтров | | Динамический |
| Действие фильтра | | Отклик по умолчанию |
| Методы проверки подлинности | | Kerberos |
| Конечная точка туннеля | | Нет |
| Тип подключения | | Все |
| Общие | |  |
| Проверять политику на наличие изменений каждые | | 180 мин. |
| Secure Server (Require Security) | |  |
| Правила (*три, созданы по умолчанию*) | |  |
| Список IP-фильтров | | 1.All IP traffic  2.All ICMP traffic  3. Динамический |
| Действие фильтра | | 1.Require Security  2.Permit  3.Отклик по умолчанию |
| Методы проверки подлинности | | 1.Kerberos  2.Отсутсвует  3.Kerberos |
| Конечная точка туннеля | | Для всех правил: Нет |
| Тип подключения | | Для всех правил: Все |
| Общие | |  |
| Проверять политику на наличие изменений каждые | | 180 мин. |
| Server (Request Security) | |  |
| Правила (*три, созданы по умолчанию*) | |  |
| Список IP-фильтров | | 1.All IP traffic  2.All ICMP traffic  3. Динамический |
| Действие фильтра | | 1.Request Security (Optional)  2.Permit  3.Отклик по умолчанию (только ранние версии Windows) |
| Методы проверки подлинности | | 1.Kerberos  2.Отсутсвует  3.Kerberos |
| Конечная точка туннеля | | Для всех правил: Нет |
| Тип подключения | | Для всех правил: Все |
| Общие | |  |
| Проверять политику на наличие изменений каждые | | 180 мин. |
| **Конфигурация расширенной политики аудита** | |  |
| **Политики аудита** | |  |
| **Вход учетной записи** | |  |
| Аудит проверки учетных данных | | Успех, отказ |
| Аудит службы проверки подлинности Kerberos | | Нет аудита |
| Аудит операций с билетами службы Kerberos | | Нет аудита |
| Аудит других событий входа учетных записей | | Успех, отказ |
| **Управление учетными записями** | |  |
| Аудит управления группами приложений | | Нет аудита |
| Аудит управления учетными записями компьютеров | | Успех, отказ |
| Аудит управления группами распространения | | Нет аудита |
| Аудит других событий управления учетными записями | | Успех, отказ |
| Аудит управления группами безопасности | | Успех, отказ |
| Аудит управления учетными записями пользователей | | Успех, отказ |
| **Подробное отслеживание** | |  |
| Аудит активности DPAPI | | Нет аудита |
| Аудит создания процессов | | Нет аудита |
| Аудит завершения процессов | | Нет аудита |
| Аудит событий RPC | | Нет аудита |
| **Доступ к службе каталогов (DS)** | |  |
| Аудит подробной репликации службы каталогов | | Нет аудита |
| Аудит доступа к службе каталогов | | Нет аудита |
| Аудит изменения службы каталогов | | Успех, отказ |
| Аудит репликации службы каталогов | | Нет аудита |
| **Вход/выход** | |  |
| Аудит блокировки учетных записей | | Успех, отказ |
| Аудит расширенного режима IPsec | | Нет аудита |
| Аудит основного режима IPsec | | Нет аудита |
| Аудит быстрого режима IPsec | | Нет аудита |
| Аудит выхода из системы | | Успех, отказ |
| Аудит входа в систему | | Успех, отказ |
| Аудит сервера политики сети | | Нет аудита |
| Аудит других событий входа и выхода | | Успех, отказ |
| Аудит специального входа | | Успех, отказ |
| **Доступ к объектам** | |  |
| Аудит событий, создаваемых приложениями | | Нет аудита |
| Аудит служб сертификации | | Нет аудита |
| Аудит сведений об общем файловом ресурсе | | Нет аудита |
| Аудит общих папок | | Нет аудита |
| Аудит файловой системы | | Нет аудита |
| Аудит подключения платформы фильтрации | | Нет аудита |
| Аудит отбрасывания пакетов платформой фильтрации | | Нет аудита |
| Аудит работы с дескрипторами | | Нет аудита |
| Аудит объектов ядра | | Нет аудита |
| Аудит других событий доступа к объектам | | Нет аудита |
| Аудит реестра | | Нет аудита |
| Аудит диспетчера учетных записей безопасности | | Нет аудита |
| **Изменение политики** | |  |
| Аудит изменения политики аудита | | Успех, отказ |
| Аудит изменения политики проверки подлинности | | Успех, отказ |
| Аудит изменения политики авторизации | | Нет аудита |
| Аудит изменения политики платформы фильтрации | | Нет аудита |
| Аудит изменения политики на уровне правил MPSSVC | | Нет аудита |
| Аудит других событий изменения политики | | Нет аудита |
| **Использование прав** | |  |
| Аудит использования прав, не затрагивающих конфиденциальные данные | | Нет аудита |
| Аудит других событий использования прав | | Нет аудита |
| Аудит использования прав, затрагивающих конфиденциальные данные | | Нет аудита |
| **Система** | |  |
| Аудит драйвера IPsec | | Нет аудита |
| Аудит других системных событий | | Нет аудита |
| Аудит изменения состояния безопасности | | Нет аудита |
| Аудит расширения системы безопасности | | Нет аудита |
| Аудит целостности системы | | Успех, отказ |
| **Аудит доступа к глобальным объектам** | |  |
| Файловая система | | Не настроено |
| Реестр | | Не настроено |
| **QoS на основе политики** | | Не определено |
| **Административные шаблоны** | |  |
| **Компоненты Windows** | |  |
| **Internet Explorer** | | **Все параметры раздела и его подразделов перевести в состояние "Отключена", за исключением нижеприведенных** |
| Включить строку меню по умолчанию | | Включена |
| Выключить автоматическое восстановление после сбоя | | Не задана |
| Выключить повторное открытие последнего сеанса просмотра | | Не задана |
| Разрешить режим завершения работы Internet Explorer 8 | | Не задана |
| Выключить быстрые вкладки | | Не задана |
| Выключить предложение для всех служб, установленных пользователем | | Не задана |
| Выключить меню быстрого выбора | | Не задана |
| **Панель управления браузером** | |  |
| **Вкладка "Безопасность"** | |  |
| Включить предупреждение о несоответствии адреса сертификата | | Не задана |
| **Параметры браузера** | |  |
| **Параметры экрана** | |  |
| Запретить выбор размера текста по умолчанию | | Не задана |
| **NetMeeting** | |  |
| Запретить удаленное управление рабочим столом | | Включен |
| **Parental Controls** | |  |
| Make Parental Controls control panel visible on a Domain | | Отключена |
| **Password Synchronization** | |  |
| Turn on extensive logging for Password Synchronization | | Отключена |
| Set the number of synchronization retries for servers running Password Synchronization | | Отключена |
| Turn on the Windows to NIS password synchronization for users that have been migrated to Active Directory | | Отключена |
| Set the interval between synchronization retries for Password Synchronization | | Отключена |
| **Server for NIS** | |  |
| Turn on extensive logging for Active Directory Domain Services domain controllers that are running Server for NIS | | Отключена |
| Set the map update interval for NIS subordinate servers | | Отключена |
| **Windows Media Center** | |  |
| Не запускать Windows Media Center | | Включена |
| **Windows Messenger** | |  |
| Не запускать Windows Messenger автоматически при входе. | | Включена |
| Запретить запуск Windows Messenger | | Включена |
| **Windows PowerShell** | |  |
| Включить выполнение сценариев | | Отключена |
| **Windows SideShow** | |  |
| Отключить автоматическое пробуждение | | Включена |
| Отключить Windows SideShow | | Включена |
| Требовать ПИН-код для доступа к данным на устройствах с микропрограммами Майкрософт | | Отключена |
| Удалять данные с устройств, использующих микропрограммы Майкрософт, при завершении сеанса пользователя. | | Отключена |
| **Анализ стабильности Windows** | |  |
| Настройка WMI-поставщиков стабильности системы | | Включен |
| **Архивация данных** | |  |
| **Клиент** | |  |
| Запретить пользователям запускать программу "Состояние и настройка архивации" | | Отключена |
| Запретить архивацию на локальные диски | | Отключена |
| Запретить архивацию в сетевое расположение | | Отключена |
| Запретить архивацию на оптические носители (CD/DVD) | | Отключена |
| Отключить возможность архивации файлов данных | | Отключена |
| Отключить функции восстановления | | Отключена |
| Отключить возможность создания образа системы | | Отключена |
| **Сервер** | |  |
| Разрешить только архивацию системы | | Отключена |
| Запретить архивацию данных в локальном хранилище | | Отключена |
| Запретить архивацию данных в общую сетевую папку | | Отключена |
| Запретить архивацию данных на оптические носители | | Отключена |
| Запретить архивацию данных однократного запуска | | Отключена |
| **Биометрия** | |  |
| Разрешить использование биометрии | | Отключена |
| Разрешить пользователям выполнять вход в систему с использованием биометрии | | Отключена |
| Разрешить пользователям домена выполнять вход в систему с использованием биометрии | | Отключена |
| Время ожидания для событий функции быстрого переключения пользователей | | Отключена |
| **Встроенная справка** | |  |
| Отключение активной справки | | Включена |
| **Гаджеты рабочего стола** | |  |
| Отключить гаджеты рабочего стола | | Включена |
| Переопределить ссылку на дополнительные гаджеты | | Отключена |
| Ограничить распаковку и установку гаджетов, не подписанных цифровой подписью. | | Включена |
| Отключить установленные пользователем гаджеты рабочего стола | | Включена |
| **Диспетчер окон рабочего стола** | |  |
| **Цвет рамки окна** | |  |
| Укажите цвет по умолчанию | | Отключена |
| Не разрешать смену цветов | | Включена |
| Не разрешать анимацию окон | | Включена |
| Не разрешать композицию рабочего стола | | Включена |
| Не разрешать вызов Flip3D | | Включена |
| **Диспетчер системных ресурсов** | |  |
| Включить функцию учета ДСР | | Отключена |
| Адреса электронной почты для рассылки уведомлений | | Отключена |
| Интервал времени (в минутах) для записи данных учета | | Отключена |
| Адрес SMTP-сервера для рассылки уведомлений | | Отключена |
| **Домашняя группа** | |  |
| Запретить присоединение компьютера к домашней группе | | Включена |
| **Защита доступа к сети** | |  |
| Разрешать поддержку компонента "Клиент системы ограничений 802.1x" клиентом защиты доступа к сети | | Отключена |
| **Защитник Windows** | |  |
| Включить обновление определений с помощью WSUS и Windows Update | | Отключена |
| Включить обновление определений через WSUS и Центр Майкрософт по защите от вредоносных программ | | Отключена |
| Проверять новые подписи перед запланированным сканированием | | Отключена |
| Отключить Защитника Windows | | Включена |
| Отключить наблюдение в реальном времени | | Включена |
| Отключить постоянные действия | | Включена |
| Настроить отчеты Microsoft SpyNet | | Отключена |
| **Звукозапись** | |  |
| Запретить выполнение программы «Звукозапись» | | Включена |
| **Календарь Windows** | |  |
| Выключить календарь Windows. | | Включена |
| **Каналы RSS** | |  |
| Включить обычную проверку подлинности веб-каналов через HTTP | | Включена |
| Отключить синхронизацию веб-каналов и веб-фрагментов в фоновом режиме | | Включена |
| Отключить загрузку вложений | | Включена |
| Отключить добавление и удаление веб-каналов и веб-фрагментов | | Включена |
| Отключить обнаружение веб-каналов и веб-фрагментов | | Включена |
| Отключить список веб-каналов | | Включена |
| **Настройки презентации** | |  |
| Выключить настройки презентации Windows | | Включена |
| **Обозреватель игр** | |  |
| Выключить загрузку сведений об игре | | Включена |
| Отключить обновления игр | | Включена |
| Не отслеживать время последнего сеанса игр в папке «Игры» | | Включена |
| **Отчеты об ошибках Windows** | |  |
| **Параметры расширенного отчета об ошибках** | |  |
| Отправлять отчет о незапланированном завершении работы | | Отключена |
| Параметры по умолчанию для отчетов приложений | | Отключена |
| Список приложений, ошибки которых никогда не включать в отчет | | Отключена |
| Список приложений, ошибки которых всегда включать в отчет | | Отключена |
| Сообщать об ошибках операционной системы | | Отключена |
| Настроить архив отчетов | | Отключена |
| Настроить корпоративные отчеты об ошибках Windows | | Отключена |
| Список исключаемых приложений | | Отключена |
| Настроить очередь отчетов | | Отключена |
| **Разрешение** | |  |
| Настроить параметры разрешения | | Включена |
| Игнорировать настроенные параметры разрешения | | Отключена |
| Настроить разрешение по умолчанию | | Отключена |
| Настроить отчеты об ошибках | | Отключена |
| Отображать уведомления об ошибках | | Отключена |
| Отключить отчеты об ошибках Windows | | Включена |
| Запретить отображение интерфейса пользователя для критических ошибок | | Отключена |
| Отключить запись в журнал | | Отключена |
| Не отправлять дополнительные данные | | Отключена |
| **Параметры входа Windows** | |  |
| Отображать при входе пользователя сведения о предыдущих попытках входа | | Отключена |
| Сообщать, когда сервер входа недоступен при входе пользователя | | Отключена |
| Разрешить или запретить программам использование специального сочетания клавиш | | Отключена |
| **Параметры завершения работы** | |  |
| Отключить старый интерфейс удаленного завершения работы | | Отключена |
| Тайм-аут для зависших сеансов входа при завершении работы | | Отключена |
| **Пересылка событий** | |  |
| ForwarderResourceUsage | | Отключена |
| Настроить адрес сервера, интервал обновления и центр, выдающий сертификат для диспетчера подписки | | Отключена |
| **Планировщик заданий** | |  |
| Запретить обзор | | Включена |
| Скрыть флажок дополнительных свойств в мастере планирования заданий | | Включена |
| Запретить перетаскивание с помощью мыши | | Включена |
| Запретить запуск и завершение задач | | Включена |
| Скрывать страницы свойств | | Включена |
| Запретить создание новых заданий | | Включена |
| Запретить удаление заданий | | Включена |
| **Планшетный ПК** | |  |
| **Аппаратные кнопки** | |  |
| Запретить сопоставление кнопок «Назад» и ESC | | Отключена |
| Запретить запуск приложения | | Отключена |
| Запретить режим нажатия и удерживания | | Отключена |
| Отключить аппаратные кнопки | | Отключена |
| **Курсоры** | |  |
| Отключить реакцию пера | | Отключена |
| **Обучение пользованию пером на планшетном ПК** | |  |
| Отключить обучение пользованию пером на планшетном ПК | | Отключена |
| **Панель ввода** | |  |
| Отключение интеграции автозаполнения и панели ввода | | Отключена |
| Запретить отображение значка панели ввода | | Отключена |
| Для ввода планшетным пером не отображать значок панели ввода | | Отключена |
| Для сенсорного ввода не отображать значок панели ввода | | Отключена |
| Переключить на жесты стандарта упрощенного китайского письма (КНР) | | Отключена |
| Отключить безопасность ввода паролей в панели ввода | | Отключена |
| Отключить прогнозирование текста | | Отключена |
| Включить редко используемые символы китайского языка, кандзи или ханджа. | | Отключена |
| Отключить удобные и Z-образные жесты вычеркивания | | Отключена |
| **Персонализация рукописного ввода** | |  |
| Отключить автоматическое обучение | | Отключена |
| **Поведение UX пера** | |  |
| Запретить режим многофункционального пера | | Отключена |
| **Режим обучения пользованию многофункциональным пером** | |  |
| Запретить режим обучения пользованию многофункциональными перьями | | Отключена |
| **Сенсорный ввод** | |  |
| Отключить сенсорное панорамирование | | Отключена |
| Отключить сенсорный ввод планшетного ПК | | Отключена |
| **Стандартные программы** | |  |
| Запретить запуск игры «Инкбол» | | Включена |
| Запретить запуск журнала Windows | | Отключена |
| Запретить печать в составитель заметок журнала | | Включена |
| Запретить запуск инструмента «Ножницы» | | Включена |
| **Политики автозапуска** | |  |
| Отключить автозапуск | | Включена (Все устройства) |
| Не устанавливать флажок «Всегда выполнять выбранное действие» | | Отключена |
| Отключить автозапуск устройств, не являющихся томами | | Включена |
| Вариант работы автозапуска по умолчанию | | Включена (Не исполнять команды автозапуска) |
| **Пользовательский интерфейс учетных данных** | |  |
| Требовать достоверный путь для входа в учетную запись | | Включена |
| Отображать учетные записи администратора при повышении уровня прав | | Отключена |
| **Почта Windows** | |  |
| Выключить функции сообществ | | Включена |
| Выключить приложение Почта Windows | | Включена |
| **Проводник Windows** | |  |
| **Предыдущие версии** | |  |
| Запретить восстановление предыдущих версий из резервных копий | | Включена |
| Скрыть список предыдущих версий для локальных файлов | | Включена |
| Запретить восстановление локальных предыдущих версий | | Включена |
| Скрыть список предыдущих версий для удаленных файлов | | Включена |
| Запретить восстановление удаленных предыдущих версий | | Включена |
| Скрыть предыдущие версии файлов в архиве | | Включена |
| Проверить перед перенаправлением, указывают ли старый и новый конечный объект перенаправления папки на один общий ресурс | | Отключена |
| Отключить прямую привязку к IPropertySetStorage без промежуточных уровней. | | Отключена |
| Отключить числовое упорядочивание проводника Windows | | Отключена |
| Отключить защищенный режим протокола оболочки | | Отключена |
| Установить ссылку на веб-страницу поддержки | | Отключена |
| Отключить предотвращение выполнения данных для проводника | | Отключена |
| Отключить закрытие кучи по причине повреждения | | Отключена |
| **Программа обновления Windows Anytime Upgrade** | |  |
| Предотвращает запуск программы обновления Windows Anytime Upgrade. | | Включена |
| **Программа по улучшению качества программного обеспечения Windows** | |  |
| Разрешить перенаправление отчетов программы по улучшению качества программного обеспечения Windows | | Отключена |
| Помечать данные программы по улучшению качества программного обеспечения Windows идентификатором исследования | | Отключена |
| **проигрыватель Windows Media** | |  |
| Запретить автоматические обновления | | Включена |
| Не отображать диалоговые окна первого использования | | Включена |
| Запретить сглаживание изображения | | Включена |
| Запретить общий доступ к файлам мультимедиа | | Включена |
| Не создавать ярлык на панели быстрого запуска | | Включена |
| Не создавать ярлык на рабочем столе | | Включена |
| **Просмотр событий** | |  |
| Программа Events.asp | | Отключена |
| Параметры командной строки программы Events.asp | | Отключена |
| URL-адрес программы Events.asp | | Отключена |
| **Расположение и датчики** | |  |
| Отключить расположение со сценариями | | Отключена |
| Отключить расположение | | Отключена |
| Отключить датчики | | Отключена |
| **Сетевой проектор** | |  |
| Отсоединить сетевой проектор | | Отключена |
| Настройка порта сетевого проектора | | Отключена |
| **Служба журнала событий** | |  |
| **Безопасность** | |  |
| Путь файла журнала | | Отключена |
| Максимальный размер журнала (КБ) | | Отключена |
| При заполнении автоматически архивировать | | Отключена |
| Доступ к журналу | | Отключена |
| Сохранять старые события | | Отключена |
| **Настройка** | |  |
| Включить ведение журнала | | Включена |
| Путь файла журнала | | Отключена |
| Максимальный размер журнала (КБ) | | Отключена |
| При заполнении автоматически архивировать | | Отключена |
| Доступ к журналу | | Отключена |
| Сохранять старые события | | Отключена |
| **Приложение** | |  |
| Путь файла журнала | | Отключена |
| Максимальный размер журнала (КБ) | | Отключена |
| При заполнении автоматически архивировать | | Отключена |
| Доступ к журналу | | Отключена |
| Сохранять старые события | | Отключена |
| **Система** | |  |
| Путь файла журнала | | Отключена |
| Максимальный размер журнала (КБ) | | Отключена |
| При заполнении автоматически архивировать | | Отключена |
| Доступ к журналу | | Отключена |
| Сохранять старые события | | Отключена |
| **Служба установки ActiveX** | |  |
| Веб-сайты, разрешенные для установки элементов управления ActiveX | | Отключена |
| Политика установки ActiveX для сайтов в доверенных зонах | | Отключена |
| **Службы IIS** | |  |
| Предотвратить установку служб IIS | | Включена |
| **Службы удаленных рабочих столов** | |  |
| **Клиент подключения к удаленному рабочему столу** | |  |
| Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию | | Включена |
| Разрешать RDP-файлы от неизвестных издателей | | Отключена |
| Запретить сохранение паролей | | Включена |
| Указать отпечатки SHA1 сертификатов, представляющих доверенных издателей RDP | | Отключена |
| Запрашивать учетные данные на клиентском компьютере | | Отключена |
| Настройка проверки подлинности клиента на сервере | | Включена (Не подключаться, если проверка подлинности не прошла) |
| **Лицензирование удаленных рабочих столов** | |  |
| Группа безопасности сервера лицензирования | | Отключена |
| Запретить повышение лицензий | | Отключена |
| **Узел сеансов удаленных рабочих столов** | |  |
| **Profiles** | |  |
| Ограничить размер кэша всех перемещаемых профилей пользователей | | Отключена |
| Установить домашний каталог пользователя служб удаленных рабочих столов | | Отключена |
| Использовать обязательные профили на сервере узла сеансов удаленных рабочих столов | | Отключена |
| Задать путь для перемещаемого профиля пользователя служб удаленных рабочих столов | | Отключена |
| **Безопасность** | |  |
| Шаблон сертификата проверки подлинности сервера | | Отключена |
| Установить уровень шифрования для клиентских подключений | | Отключена |
| Всегда запрашивать пароль при подключении | | Включена |
| Требовать безопасное RPC-подключение | | Включена |
| Требовать использования специального уровня безопасности для удаленных подключений по методу RDP | | Отключена |
| Не разрешать локальным администраторам настраивать разрешения | | Отключена |
| Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети | | Включена |
| **Временные папки** | |  |
| Не удалять временные папки при выходе | | Отключена |
| Не использовать временные папки для сеанса | | Отключена |
| **Лицензирование** | |  |
| Использовать указанные серверы лицензирования удаленных рабочих столов | | Отключена |
| Скрывать уведомления о проблемах лицензирования удаленных рабочих столов, оказывающих влияние на сервер узла сеансов удаленных рабочих столов | | Отключена |
| Задать режим лицензирования узла сеансов удаленных рабочих столов | | Отключена |
| **Ограничение сеансов по времени** | |  |
| Задать ограничение по времени для отключенных сеансов | | Отключена |
| Задать ограничение времени для активных, но бездействующих сеансов служб удаленных рабочих столов | | Отключена |
| Задать ограничение по времени для активных сеансов служб удаленных рабочих столов | | Отключена |
| Завершать сеанс при достижении ограничения по времени | | Отключена |
| Задать предел времени для выхода из сеансов RemoteApp | | Отключена |
| **Перенаправление принтеров** | |  |
| Не устанавливать используемый по умолчанию принтер клиента в качестве принтера для сеанса | | Отключена |
| Не разрешать перенаправление клиентских принтеров | | Отключена |
| Использовать в первую очередь драйвер принтера Easy Print удаленного рабочего стола | | Отключена |
| Задать поведение сервера узла сеансов удаленных рабочих столов при выборе резервного драйвера принтера | | Отключена |
| Перенаправлять только используемый по умолчанию принтер клиента | | Отключена |
| **Перенаправление устройств и ресурсов** | |  |
| Разрешить перенаправление воспроизведения звука и видео | | Отключена |
| Разрешить перенаправление звукозаписи | | Отключена |
| Ограничить качество воспроизведения звука | | Отключена |
| Не разрешать перенаправление буфера обмена | | Отключена |
| Не разрешать перенаправление COM-портов | | Отключена |
| Не разрешать перенаправление дисков | | Отключена |
| Не разрешать перенаправление LPT-портов | | Отключена |
| Не разрешать перенаправление поддерживаемых устройств Plug and Play | | Отключена |
| Не разрешать перенаправление устройства чтения смарт-карт | | Отключена |
| Разрешить перенаправление часового пояса | | Отключена |
| **Подключения** | |  |
| Автоматическое переподключение | | Отключена |
| Разрешать удаленное подключение с использованием служб удаленных рабочих столов | | Отключена |
| Запретить завершение консольного сеанса администратора | | Отключена |
| Настроить интервал проверки активности подключения | | Отключена |
| Ограничить количество подключений | | Отключена |
| Устанавливает правила удаленного управления для пользовательских сеансов служб удаленных рабочих столов | | Отключена |
| Ограничить пользователей службы удаленных рабочих столов одним сеансом служб удаленных рабочих столов | | Отключена |
| Разрешать удаленный запуск любых программ | | Отключена |
| Отключить планирование ЦП со справедливым разделением | | Отключена |
| **Посредник подключений к удаленному рабочему столу** | |  |
| Присоединиться к посреднику подключений к удаленному рабочему столу | | Отключена |
| Настроить имя фермы посредника подключений к удаленному рабочему столу | | Отключена |
| Использовать перенаправление IP-адреса | | Отключена |
| Настроить имя сервера посредника подключений к удаленному рабочему столу | | Отключена |
| Использовать балансировку нагрузки посредника подключений к удаленному рабочему столу | | Отключена |
| **Совместимость приложений** | |  |
| Отключить совместимость служб удаленных рабочих столов с установщиком Windows | | Отключена |
| Включить IP-виртуализацию удаленных рабочих столов | | Отключена |
| Выбрать сетевой адаптер, используемый для IP-виртуализации удаленных рабочих столов | | Отключена |
| Не использовать IP-адрес сервера узла сеансов удаленных рабочих столов, если виртуальный IP-адрес недоступен | | Отключена |
| **Среда удаленных сеансов** | |  |
| Наибольшая глубина цвета | | Отключена |
| Принудительная отмена фонового рисунка удаленного рабочего стола | | Отключена |
| Ограничить максимальное разрешение экрана | | Отключена |
| Ограничить максимальное количество мониторов | | Отключена |
| Удалить элемент «Отключение сеанса» из диалога завершения работы | | Отключена |
| Удалить элемент «Безопасность Windows» из меню «Пуск» | | Отключена |
| Задание алгоритма сжатия для данных RDP | | Отключена |
| Оптимизировать визуальные эффекты для сеансов служб удаленных рабочих столов | | Отключена |
| Запускать программу при подключении | | Отключена |
| Всегда отображать рабочий стол при подключении | | Отключена |
| Разрешить композицию рабочего стола для сеансов удаленных рабочих столов | | Отключена |
| Не разрешать сглаживание шрифтов | | Отключена |
| **Службы федерации Active Directory** | |  |
| Отключить службу федерации | | Отключена |
| **Смарт-карта** | |  |
| Разрешить сертификаты без атрибута сертификата расширенного использования ключа | | Отключена |
| Показывать экран встроенной разблокировки при входе | | Отключена |
| Разрешить ключи подписей для входа | | Отключена |
| Разрешить сертификаты с истекшим сроком действия. | | Отключена |
| Включить распространение сертификатов со смарт-карты | | Отключена |
| Настроить очистку корневого сертификата | | Отключена |
| Включить распространение корневого сертификата со смарт-карты | | Отключена |
| Запретить возвращение текстовых PIN-кодов диспетчером учетных данных | | Отключена |
| Разрешить использование сертификатов ECC для входа и проверки подлинности | | Отключена |
| Отфильтровывать дубликаты сертификатов входа | | Отключена |
| Принудительно считывать со смарт-карты все сертификаты | | Отключена |
| Показывать строку при блокировке смарт-карты | | Отключена |
| Изменить хранящееся в сертификате имя субъекта | | Отключена |
| Включить службу самонастраивающихся устройств для смарт-карт | | Отключена |
| Уведомлять об успешной установке драйвера смарт-карт | | Отключена |
| Разрешить подсказку имени пользователя | | Отключена |
| **Совместимость приложений** | |  |
| Запрещение доступа к 16-разрядным приложениям. | | Отключена |
| Удаление страницы «Свойства совместимости программ» | | Отключена |
| Отключить дистанционное отслеживание приложений | | Отключена |
| Отключение обработчика совместимости приложений | | Отключена |
| Отключение помощника по совместимости программ | | Отключена |
| Отключить сборщик перечней программ | | Отключена |
| Отключить обработчик совместимости SwitchBack | | Отключена |
| Отключить средство записи действий по воспроизведению неполадок | | Отключена |
| **Удаленная оболочка Windows** | |  |
| Разрешить доступ к удаленной оболочке | | Отключена |
| Тайм-аут простоя | | Отключена |
| MaxConcurrentUsers | | Отключена |
| Максимальный объем памяти в мегабайтах для одной оболочки | | Отключена |
| Максимальное количество процессов для одной оболочки | | Отключена |
| Максимальное число удаленных оболочек для одного пользователя | | Отключена |
| Таймаут оболочки | |  |
| **Удаленное управление Windows** | |  |
| **Клиент службы удаленного управления Windows** | |  |
| Разрешить обычную проверку подлинности | | Отключена |
| Разрешить проверку подлинности CredSSP | | Отключена |
| Разрешить незашифрованный трафик | | Отключена |
| Запретить краткую проверку подлинности | | Отключена |
| Запретить проверку подлинности по протоколу Kerberos. | | Отключена |
| Запретить проверку подлинности согласованием | | Отключена |
| Надежные сайты | | Отключена |
| **Служба удаленного управления Windows** | |  |
| Разрешить автоматическую настройку прослушивателей | | Отключена |
| Разрешить обычную проверку подлинности | | Отключена |
| Разрешить проверку подлинности CredSSP | | Отключена |
| Разрешить незашифрованный трафик | | Отключена |
| Задайте уровень усиления защиты токена привязки канала | | Отключена |
| Запретить проверку подлинности по протоколу Kerberos | | Отключена |
| Запретить проверку подлинности согласованием | | Отключена |
| Включить HTTP-прослушиватель совместимости | | Отключена |
| Включить HTTPS-прослушиватель совместимости | | Отключена |
| **Управление цифровыми правами Windows Media** | |  |
| Запретить доступ к Интернету для Windows Media DRM | | Включена |
| **Установщик Windows** | |  |
| Разрешить обзор источника при повышенных правах | | Отключена |
| Разрешить использование носителей при повышенных правах | | Отключена |
| Разрешить применение пакетов исправлений при установке с повышенными правами | | Отключена |
| Всегда устанавливать с повышенными правами | | Отключена |
| Запретить диспетчер перезапуска | | Отключена |
| Удалить диалоговое окно обзора нового источника | | Отключена |
| Запретить оптимизацию применения пакетов исправлений | | Отключена |
| Отключить ведение журнала с помощью параметров пакета | | Отключена |
| Запретить установщик Windows | | Отключена |
| Запретить пакеты исправлений | | Отключена |
| Запретить откат | | Отключена |
| Разрешить администраторам установку в сеансе службы удаленных рабочих столов | | Отключена |
| Разрешить пользователям изменять параметры установки | | Отключена |
| Ведение журнала событий | | Включена |
| Запретить пользователям, не являющимися администраторами, устанавливать обновления, подписанные изготовителем программы | | Отключена |
| Запретить удаление обновлений | | Отключена |
| Отключить создание контрольных точек восстановления системы | | Отключена |
| Запретить установки пользователям | | Отключена |
| Задать обязательные правила обновления компонентов | | Отключена |
| Максимальный размер кэша базисных файлов | | Отключена |
| Отключить запрос безопасности IE для сценариев установщика Windows | | Отключена |
| Кэшировать файлы преобразования в безопасном месте на рабочей станции | | Отключена |
| **Цветовая система Windows Color System** | |  |
| Запретить установку и удаление цветовых профилей | | Отключена |
| **Центр мобильности Windows** | |  |
| Отключить центр мобильности Windows | | Включена |
| **Центр обеспечения безопасности** | |  |
| Включить центр обеспечения безопасности (только для компьютеров в домене) | | Отключена |
| **Центр обновления Windows** | |  |
| Не отображать параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows» | | Включена |
| Не задавать по умолчанию параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows» | | Включена |
| Разрешить управлению электропитанием центра обновления Windows выводить систему из спящего режима для установки запланированных обновлений | | Отключена |
| Настройка автоматического обновления | | Отключена |
| Указать размещение службы обновлений Майкрософт в интрасети | | Отключена |
| Частота поиска автоматических обновлений | | Отключена |
| Turn off the upgrade to the latest version of Windows through Windows Update | | Включена |
| Разрешать пользователям, не являющимся администраторами, получать уведомления об обновлениях | | Отключена |
| Включить уведомления о наличии программ | | Отключена |
| Разрешить немедленную установку автоматических обновлений | | Отключена |
| Включить рекомендуемые обновления через автоматическое обновление | | Отключена |
| Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи | | Включена |
| Повторный запрос для перезагрузки при запланированных установках | | Отключена |
| Задержка перезагрузки при запланированных установках | | Отключена |
| Перенос запланированных автоматических установок обновлений | | Отключена |
| Разрешить клиенту присоединение к целевой группе | | Отключена |
| Разрешить прием обновлений с подписью из службы обновления Майкрософт в интрасети | | Отключена |
| **Цифровой ящик** | |  |
| Не разрешать работу цифрового ящика | | Включена |
| **Шифрование диска BitLocker** | |  |
| **Диски операционной системы** | |  |
| Обязательная дополнительная проверка подлинности при запуске | | Отключена |
| Требовать дополнительную проверку подлинности при запуске (Windows Server 2008) | | Отключена |
| Разрешить использование улучшенных ПИН-кодов при запуске компьютера | | Отключена |
| Установить минимальную длину ПИН-кода для запуска | | Отключена |
| Выбор методов восстановления дисков операционной системы, защищенных с помощью BitLocker | | Отключена |
| Настройка профиля проверки платформы TPM | | Отключена |
| **Жесткие диски с данными** | |  |
| Настроить использование смарт-карт на фиксированных дисках с данными | | Отключена |
| Запретить запись на фиксированные диски, не защищенные BitLocker | | Отключена |
| Разрешить доступ к фиксированным дискам с данными, защищенным с помощью BitLocker, из более ранних версий Windows | | Отключена |
| Настроить использование паролей для фиксированных дисков с данными | | Отключена |
| Выбор методов восстановления жестких дисков, защищенных с помощью BitLocker | | Отключена |
| **Съемные диски с данными** | |  |
| Управление использованием BitLocker для съемных дисков | | Отключена |
| Настроить использование смарт-карт на съемных дисках с данными | | Отключена |
| Запретить запись на съемные диски, не защищенные BitLocker | | Отключена |
| Разрешить доступ к съемным дискам с данными, защищенным с помощью BitLocker, из более ранних версий Windows | | Отключена |
| Настроить использование паролей для съемных дисков с данными | | Отключена |
| Выбор методов восстановления съемных дисков, защищенных с помощью BitLocker | | Отключена |
| Хранить сведения о восстановлении BitLocker в доменных службах Active Directory (Windows Server 2008) | | Отключена |
| Выберите папку по умолчанию для пароля восстановления | | Отключена |
| Выберите способ восстановления пользователями дисков, защищенных с помощью BitLocker (Windows Server 2008) | | Отключена |
| Выберите метод шифрования диска и стойкость шифра | | Отключена |
| Укажите уникальные идентификаторы для организации | | Отключена |
| Запретить перезапись памяти при перезагрузке | | Отключена |
| Проверить согласованность правил использования сертификатов смарт-карт | | Отключена |
| **Панель управления** | |  |
| **Учетные записи пользователей** | |  |
| Применить изображение по умолчанию для учетной записи пользователя ко всем пользователям | | Отключена |
| **Язык и региональные стандарты** | |  |
| Ограничить язык интерфейса Windows для всех зарегистрированных пользователей | | Отключена |
| Подавление языка интерфейса на уровне пользователя языком системного интерфейса | | Отключена |
| **Принтеры** | |  |
| Печать на основе использования веб | | Отключена |
| Автоматическая публикация новых принтеров в Active Directory | | Отключена |
| Особый URL-адрес службы поддержки в левой панели папки принтеров | | Отключена |
| Расширить подключения указания и печати для поиска обновлений Windows | | Отключена |
| Мастер установки принтеров — страница сканирования сети (управляемая сеть) | | Отключена |
| Всегда обрабатывать задания печати на сервере | | Отключена |
| Разрешить очистку опубликованных принтеров | | Отключена |
| Запретить установку принтеров, использующих работающие в режиме ядра драйверы | | Отключена |
| Мастер установки принтеров — страница сканирования сети (неуправляемая сеть) | | Отключена |
| Использовать только функцию указания и печати для пакета | | Отключена |
| Функция указания и печати для пакетов - Разрешенные серверы | | Отключена |
| Размещение компьютера | | Отключена |
| Заполнение строки поиска принтеров | | Отключена |
| Ограничения указания и печати | | Отключена |
| Выполнить драйверы принтеров в изолированных процессах | | Отключена |
| Переопределить параметр совместимости выполнения драйвера печати, назначенный драйвером печати | | Отключена |
| Обзор принтеров | | Отключена |
| Удалять принтеры, которые не были автоматически повторно опубликованы | | Отключена |
| Интервал очистки Active Directory | | Отключена |
| Приоритет потока при очистке Active Directory | | Отключена |
| Повторы при очистке Active Directory | | Отключена |
| Записывать события контакта службы очистки каталогов | | Отключена |
| Разрешить публикацию принтеров | | Отключена |
| Разрешить диспетчеру печати добавление новых клиентских подключений | | Отключена |
| Проверять состояние публикации | | Отключена |
| **Сеть** | |  |
| **BranchCache** | |  |
| Включить BranchCache | | Отключена |
| Включить режим распределенного кэша BranchCache | | Отключена |
| Включить режим размещенного кэша BranchCache | | Отключена |
| Настройка BranchCache для сетевых файлов | | Отключена |
| Установить процент дискового пространства, используемого для кэша клиентского компьютера | | Отключена |
| **Cлужбы одноранговых сетей Майкрософт** | |  |
| **Протокол однорангового разрешения имен** | |  |
| **Глобальные облака** | |  |
| Отключение многоадресной загрузки | | Отключена |
| Отключить создание PNRP-облака | | Отключена |
| Настроить PNRP-облако только для разрешения | | Отключена |
| Задать сервер инициализации | | Отключена |
| **Локальные облака сайта** | |  |
| Отключение многоадресной загрузки | | Отключена |
| Отключить создание PNRP-облака | | Отключена |
| Настроить PNRP-облако только для разрешения | | Отключена |
| Задать сервер инициализации | | Отключена |
| **Локальные облака связи** | |  |
| Отключение многоадресной загрузки | | Отключена |
| Отключить создание PNRP-облака | | Отключена |
| Настроить PNRP-облако только для разрешения | | Отключена |
| Задать сервер инициализации | | Отключена |
| Отключить проверку надежности пароля для группирования одноранговой сети | | Отключена |
| Отключение служб одноранговых сетей Майкрософт | | Отключена |
| **DNS-клиент** | |  |
| Разрешить добавление DNS-суффиксов к запросам несоответствующих составных имен. | | Отключена |
| DNS-суффикс подключения | | Отключена |
| Уровень регрессии основного DNS-суффикса | | Отключена |
| DNS-серверы | | Отключена |
| Основной DNS-суффикс | | Отключена |
| Регистрировать DNS-записи с DNS-суффиксом подключения | | Отключена |
| Регистрировать PTR-записи | | Отключена |
| Динамическое обновление | | Отключена |
| Заменять адреса при конфликтах | | Отключена |
| Интервал обновления регистрации | | Отключена |
| Установить TTL для A- и PTR-записей | | Отключена |
| Порядок просмотра DNS-суффиксов | | Отключена |
| Уровень безопасности обновления | | Отключена |
| Обновлять зоны доменов верхнего уровня | | Отключена |
| Регрессирование основного DNS-суффикса | | Отключена |
| Отключить многоадресное разрешение имен | | Отключена |
| **SNMP** | |  |
| Сообщества | | Отключена |
| Разрешенные диспетчеры | | Отключена |
| Ловушки для публичного сообщества | | Отключена |
| **Windows Connect Now** | |  |
| Запретить доступ к мастерам Windows Connect Now | | Включена |
| Настройка параметров беспроводной сети с помощью Windows Connect Now | | Отключена |
| **Автономные файлы** | |  |
| Разрешить автономный доступ ко вложенным папкам | | Отключена |
| Административно назначенные автономные файлы | | Отключена |
| Настроить фоновую синхронизацию | | Отключена |
| Ограничить размер дискового пространства, используемого автономными файлами | | Отключена |
| Нестандартные действия при отключении от сервера | | Отключена |
| Размер кэша по умолчанию | | Отключена |
| Разрешить или запретить использование автономных файлов | | Отключена |
| Шифрование кэша автономных файлов | | Отключена |
| Уровень регистрации событий | | Отключена |
| Исключить файлы из числа кэшируемых | | Отключена |
| Некэшируемые файлы | | Отключена |
| Действие при отключении от сервера | | Отключена |
| Запретить использование папки «Автономные файлы» | | Включена |
| Запретить пользовательскую настройку автономных файлов | | Включена |
| Удалить «Сделать доступными автономно» | | Включена |
| Запретить применение «Сделать доступными автономно» для этих файлов и папок | | Отключена |
| Отключить всплывающие напоминания | | Включена |
| Включить прозрачное кэширование | | Отключена |
| При выходе из системы удалять локальную копию автономных файлов пользователя | | Включена |
| Включить экономичное использование административно назначенных автономных файлов | | Отключена |
| Частота появления всплывающих напоминаний | | Отключена |
| Исходное время отображения всплывающих напоминаний | | Отключена |
| Время отображения всплывающих напоминаний | | Отключена |
| Настроить режим медленного подключения | | Отключена |
| Настроить скорость медленного подключения | | Отключена |
| Синхронизировать перед выходом из системы | | Отключена |
| Синхронизировать автономные файлы при входе в систему | | Отключена |
| Синхронизировать автономные файлы перед приостановкой | | Отключена |
| **Индикатор состояния сетевого подключения** | |  |
| Адрес DNS-сервера организации, который используется для проверки | | Отключена |
| Имя сайта DNS-сервера организации, которое используется для проверки | | Отключена |
| Список префиксов сайтов организации | | Отключена |
| URL-адрес, используемый для проверки работы веб-сайта организации | | Отключена |
| URL-адрес определения расположения домена | | Отключена |
| **Обнаружение топологии связи (Link-Layer)** | |  |
| Включает драйвер отображения ввода/вывода (LLTDIO) | | Отключена |
| Включить драйвер «Ответчика» (RSPNDR) | | Отключена |
| **Параметры TCP/IP** | |  |
| **Параметры** | |  |
| Состояние масштабируемой эвристики Windows | | Отключена |
| **Технологии туннелирования IPv6** | |  |
| Имя ретранслятора 6to4 | | Отключена |
| Интервал разрешения имен ретранслятора 6to4 | | Отключена |
| Состояние 6to4 | | Отключена |
| Состояние IP-HTTPS | | Отключена |
| Имя маршрутизатора ISATAP | | Отключена |
| Состояние ISATAP | | Отключена |
| Порт клиента Teredo | | Отключена |
| Квалификация Teredo по умолчанию | | Отключена |
| Частота обновления Teredo | | Отключена |
| Имя сервера Teredo | | Отключена |
| Состояние Teredo | | Отключена |
| **Параметры настройки SSL** | |  |
| Порядок комплектов шифров SSL | | Отключена |
| **Планировщик пакетов QoS** | |  |
| **Значение DSCP для не соответствующих пакетов** | |  |
| Тип службы Best effort | | Отключена |
| Тип службы Controlled load | | Отключена |
| Тип службы Guaranteed | | Отключена |
| Тип службы Network control | | Отключена |
| Тип службы Qualitative | | Отключена |
| **Значение DSCP для соответствующих пакетов** | |  |
| Тип службы Best effort | | Отключена |
| Тип службы Controlled load | | Отключена |
| Тип службы Guaranteed | | Отключена |
| Тип службы Network control | | Отключена |
| Тип службы Qualitative | | Отключена |
| **Значение приоритета второго уровня** | |  |
| Тип службы Best effort | | Отключена |
| Тип службы Controlled load | | Отключена |
| Тип службы Guaranteed | | Отключена |
| Тип службы Network control | | Отключена |
| Не соответствующие пакеты | | Отключена |
| Тип службы Qualitative | | Отключена |
| Ограничение ожидающих обработки пакетов | | Отключена |
| Ограничить резервируемую пропускную способность | | Отключена |
| Задать разрешение таймера | | Отключена |
| **Сервер Lanman** | |  |
| Публикация хэша для службы BranchCache | | Отключена |
| **Сетевые подключения** | |  |
| **Брандмауэр Windows** | |  |
| **Профиль домена** | |  |
| Брандмауэр Windows: Разрешить локальные исключения программ | | Отключена |
| Брандмауэр Windows: Определение входящих исключений программ | | Отключена |
| Брандмауэр Windows: Защита всех сетевых подключений | | Отключена |
| Брандмауэр Windows: Не разрешать исключения | | Отключена |
| Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам | | Отключена |
| Брандмауэр Windows: Разрешить исключения ICMP | | Отключена |
| Брандмауэр Windows: Разрешить ведение журнала | | Отключена |
| Брандмауэр Windows: Запретить уведомления | | Отключена |
| Брандмауэр Windows: Разрешить локальные исключения портов | | Отключена |
| Брандмауэр Windows: «Брандмауэр Windows: Определение входящих исключений портов» | | Отключена |
| Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования | | Отключена |
| Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом | | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | | Отключена |
| Брандмауэр Windows: Разрешить исключения входящего трафика для UPnP | | Отключена |
| **Стандартный профиль** | |  |
| Брандмауэр Windows: Разрешить локальные исключения программ | | Отключена |
| Брандмауэр Windows: Определение входящих исключений программ | | Отключена |
| Брандмауэр Windows: Защита всех сетевых подключений | | Отключена |
| Брандмауэр Windows: Не разрешать исключения | | Отключена |
| Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам | | Отключена |
| Брандмауэр Windows: Разрешить исключения ICMP | | Отключена |
| Брандмауэр Windows: Разрешить ведение журнала | | Отключена |
| Брандмауэр Windows: Запретить уведомления | | Отключена |
| Брандмауэр Windows: Разрешить локальные исключения портов | | Отключена |
| Брандмауэр Windows: «Брандмауэр Windows: Определение входящих исключений портов» | | Отключена |
| Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования | | Отключена |
| Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом | | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | | Отключена |
| Брандмауэр Windows: Разрешить исключения входящего трафика для UPnP | | Отключена |
| Брандмауэр Windows: Разрешить обход проверки подлинности IPsec | | Отключена |
| Запрет установки и настройки сетевого моста в сети DNS-домена | | Отключена |
| Не показывать значок сети "только локальный доступ" | | Отключена |
| Маршрутизировать весь трафик через внутреннюю сеть | | Отключена |
| Запрет использования брандмауэра подключения к Интернету в DNS-домене | | Отключена |
| Запрет использования общего интернет-подключения в DNS-домене | | Отключена |
| Требовать повышения прав пользователей домена при задании сетевого ресурса | | Отключена |
| **Фоновая интеллектуальная служба передачи (BITS)** | |  |
| Запретить клиенту BITS использование кэша филиалов Windows | | Отключена |
| Запретить компьютеру действовать как клиенту кэширования членов одноранговой группы BITS | | Отключена |
| Запретить компьютеру действовать как серверу кэширования членов одноранговой группы BITS | | Отключена |
| Разрешить кэширование членов одноранговой группы BITS | | Отключена |
| Время ожидания для неактивных заданий BITS | | Отключена |
| Ограничить максимальную пропускную способность сети для фоновой передачи BITS | | Отключена |
| Ограничить максимальную пропускную способность сети, используемую для кэширования членов одноранговой группы BITS | | Отключена |
| Ограничить максимальную пропускную способность сети, используемую службой BITS для фоновой передачи, с помощью расписания обслуживания | | Отключена |
| Ограничить максимальную пропускную способность сети, используемую службой BITS для фоновой передачи, с помощью расписания работы | | Отключена |
| Ограничить размер кэша членов одноранговой группы BITS | | Отключена |
| Ограничить срок хранения файлов в кэше членов одноранговой группы BITS | | Отключена |
| Ограничить максимальное время загрузки задания BITS | | Отключена |
| Ограничить максимальное количество файлов, допустимое для одного задания BITS | | Отключена |
| Ограничить максимальное количество заданий BITS для компьютера | | Отключена |
| Ограничить максимальное количество заданий BITS для каждого пользователя | | Отключена |
| Ограничить максимальное количество диапазонов, которые могут быть добавлены к файлу в задании BITS | | Отключена |
| Устанавливает частоту обнаружения контроллера домена (DC) клиентом распределенной файловой системы (DFS) | | Отключена |
| **Система** | |  |
| **iSCSI** | |  |
| **Безопасность iSCSI** | |  |
| Не разрешать изменение секрета CHAP инициатора | | Отключена |
| Не разрешать подключения без использования IPSec | | Отключена |
| Не разрешать сеансы без взаимной проверки подлинности CHAP | | Отключена |
| Не разрешать сеансы без односторонней проверки подлинности CHAP | | Отключена |
| **Обнаружение объектов iSCSI** | |  |
| Не разрешать ручную настройку конечных порталов | | Отключена |
| Не разрешать ручную настройку обнаруженных объектов | | Отключена |
| Не разрешать ручную настройку серверов iSNS | | Отключена |
| Не разрешать добавление новых объектов при ручной настройке | | Отключена |
| **Общие iSCSI** | |  |
| Не разрешать изменение iqn имени инициатора | | Отключена |
| Не разрешать дополнительные входы сеансов | | Отключена |
| **Kerberos** | |  |
| Использовать порядок поиска леса | | Отключена |
| Определить сопоставления «имя узла - сфера Kerberos» | | Отключена |
| Определить совместимые параметры сферы Kerberos V5 | | Отключена |
| Требовать строгого соответствия конечного SPN для удаленных вызовов процедур | | Отключена |
| Требовать обязательную проверку подлинности KDC | | Отключена |
| **Windows HotStart** | |  |
| Отключить Windows HotStart | | Включена |
| **Восстановление** | |  |
| Разрешить восстановление системы в состояние по умолчанию | | Отключена |
| **Восстановление системы** | |  |
| Отключить конфигурацию | | Включена |
| Отключить восстановление системы | | Включена |
| **Вход в систему** | |  |
| Установка домена по умолчанию для входа | | Отключена |
| Исключить поставщиков учетных данных | | Отключена |
| Не обрабатывать список запуска старых программ | | Отключена |
| Не обрабатывать список однократного запуска программ | | Отключена |
| Отключить звук запуска Windows | | Отключена |
| Скрыть точки входа для быстрого переключения пользователей | | Отключена |
| Всегда классический вход в систему | | Отключена |
| Не показывать окно приветствия «Приступая к работе» при входе в систему | | Отключена |
| Выполнять эти программы при входе в систему | | Отключена |
| Всегда ждать сеть при запуске и входе в систему | | Включена |
| Всегда использовать настраиваемый фон входа в систему | | Отключена |
| **Вызов удаленной процедуры** | |  |
| Проверка RPC-клиентов сопоставителя конечных точек | | Отключена |
| Передача расширенных сведений об ошибках | | Отключена |
| Пропустить сбой делегирования | | Отключена |
| Минимальное время ожидания простаивающих подключений для RPC/HTTP-подключений | | Отключена |
| Ограничения для не прошедших проверку подлинности RPC-клиентов | | Отключена |
| Диагностические сведения о состоянии RPC | | Отключена |
| **Групповая политика** | |  |
| **Ведение журнала и трассировка** | |  |
| Настроить ведение журнала и трассировку для предпочтений "Приложения" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Источники данных" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Устройства" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Сопоставления дисков" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Среда" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Файлы" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры папок" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Папки" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "INI-файлы" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры браузера" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Локальные пользователи и группы" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Общие сетевые ресурсы" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры сети" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры электропитания" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Реестр" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Принтеры" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Региональные параметры" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Назначенные задания" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Службы" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Ярлыки" | | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Главное меню" | | Отключена |
| Включить политику пользователей различных лесов и перемещаемые профили пользователей | | Отключена |
| Обработка политики установки программ | | Отключена |
| Обработка политики дисковых квот | | Отключена |
| Обработка политики восстановления EFS | | Отключена |
| Обработка политики перенаправления папки  Обработка политики настройки Internet Explorer | | Отключена |
|  | | Отключена |
| Обработка политики IP-безопасности | | Отключена |
| Обработка политики реестра. | | Отключена |
| Обработка политики сценариев | | Включена: разрешить обработку через медленное сетевое подключение |
| Обработка политики безопасности | | Отключена |
| Обработка политик проводных сетей | | Отключена |
| Обработка беспроводной политики | | Отключена |
| Запретить интерактивным пользователям создавать данные результирующей политики (Resultant Set of Policy — RSoP) | | Отключена |
| Отключить фоновое обновление групповой политики | | Отключена |
| Выключение обработки локальных объектов групповой политики | | Отключена |
| Запретить пользователям вызывать обновление политики компьютера | | Отключена |
| Обнаружение медленных подключений для групповой политики | | Включена |
| Интервал обновления групповой политики для компьютеров | | Отключена |
| Интервал обновления групповой политики для контроллеров домена | | Отключена |
| Всегда использовать локальные файлы ADM для редактора объектов групповой политики | | Отключена |
| Отключить протоколирование RSoP | | Отключена |
| Время ожидания при обработке политики загрузки | | Отключена |
| Режим обработки замыкания пользовательской групповой политики | | Отключена |
| Разрешить асинхронную обработку пользовательской групповой политики при входе в систему через службы удаленных рабочих столов | | Отключена |
| Обработка политики расширения предпочтений "Приложения" | | Не задана |
| Обработка политики расширения предпочтений "Источники данных" | | Не задана |
| Обработка политики расширения предпочтений "Устройства" | | Не задана |
| Обработка политики расширения предпочтений "Сопоставления дисков" | | Не задана |
| Обработка политики расширения предпочтений "Среда" | | Не задана |
| Обработка политики расширения предпочтений "Файлы" | | Не задана |
| Обработка политики расширения предпочтений "Свойства папки" | | Не задана |
| Обработка политики расширения предпочтений "Папки" | | Не задана |
| Обработка политики расширения предпочтений "INI-файлы" | | Не задана |
| Обработка политики расширения предпочтений "Параметры браузера" | | Не задана |
| Обработка политики расширения предпочтений "Локальные пользователи и группы" | | Не задана |
| Обработка политики расширения предпочтений "Общие сетевые ресурсы" | | Не задана |
| Обработка политики расширения предпочтений "Сетевые параметры" | | Не задана |
| Обработка политики расширения предпочтений "Параметры электропитания" | | Не задана |
| Обработка политики расширения предпочтений "Реестр" | | Не задана |
| Обработка политики расширения предпочтений "Принтеры" | | Не задана |
| Обработка политики расширения предпочтений "Региональные параметры" | | Не задана |
| Обработка политики расширения предпочтений "Назначенные задания" | | Не задана |
| Обработка политики расширения предпочтений "Службы" | | Не задана |
| Обработка политики расширения предпочтений "Ярлыки" | | Не задана |
| Обработка политики расширения предпочтений "Главное меню" | | Не задана |
| **Диагностика** | |  |
| **Быстродействие Windows PerfTrack** | |  |
| Включить или отключить PerfTrack | | Отключена |
| **Восстановление поврежденного файла** | |  |
| Настройка поведения восстановления поврежденного файла | | Включена (Только выявление неполадок) |
| **Восстановление поврежденного файла MSI** | |  |
| Настройка поведения восстановления поврежденного файла MSI | | Включена (Только выявление неполадок) |
| **Диагностика быстродействия завершения работы Windows** | |  |
| Настройки режима запуска сценария | | Отключена |
| **Диагностика быстродействия загрузки Windows** | |  |
| Настройки режима запуска сценария | | Отключена |
| **Диагностика диска** | |  |
| Диагностика диска. Настроить пользовательский текст предупреждения | | Отключена |
| Диагностика диска. Настроить уровень выполнения | | Отключена |
| **Диагностика производительности ждущего режима и возобновления работы Windows** | |  |
| Настройки режима запуска сценария | | Отключена |
| **Диагностика скорости отклика системы Windows** | |  |
| Настройки режима запуска сценария | | Отключена |
| **Диагностика со сценариями** | |  |
| Устранение неполадок: разрешить пользователям доступ к сведениям об устранении неполадок, расположенным на серверах корпорации Майкрософт, из компонента "Устранение неполадок" панели управления (через интернет-службу устранения неполадок Windows (WOTS)) | | Отключена |
| Устранение неполадок: разрешить пользователям запускать мастера устранения неполадок | | Отключена |
| Настройка политики безопасности для диагностики со сценариями | | Отключена |
| **Диагностика совместимости приложений** | |  |
| Уведомлять о блокированных драйверах | | Отключена |
| Обнаруживать сбои приложений, вызванные устаревшими COM-объектами | | Отключена |
| Обнаружение сбоев приложений, вызванных устаревшими библиотеками DLL Windows. | | Отключена |
| Обнаружение сбоев установки приложений | | Отключена |
| Обнаружение средств установки приложений, требующих прав администратора | | Отключена |
| Обнаружение приложений, неспособных запустить средства установки при включенном контроле учетных записей пользователей (UAC). | | Отключена |
| **Диагностика утечки памяти Windows** | |  |
| Настройка уровня выполнения сценария | | Отключена |
| **Обнаружение и устранение нехватки ресурсов Windows** | |  |
| Настройка уровня выполнения сценария | | Отключена |
| **Отказоустойчивая куча** | |  |
| Настройка уровня выполнения сценария | | Отключена |
| **Средство диагностики службы технической поддержки Майкрософт** | |  |
| Средство диагностики службы технической поддержки Майкрософт (MSDT): включите интерактивное взаимодействие с поставщиком поддержки | | Отключена |
| Средство диагностики службы технической поддержки Майкрософт: ограничить загрузку служебных средств | | Отключена |
| Средство диагностики службы технической поддержки Майкрософт: настройка режима работы | | Отключена |
| Диагностика: настройка сохранения сценария | | Отключена |
| Диагностика: настройка уровня выполнения сценария | | Отключена |
| **Дисковые квоты** | |  |
| Включить дисковые квоты | | Отключена |
| Задать предел дисковой квоты | | Отключена |
| Предел квоты по умолчанию и уровень предупреждения | | Отключена |
| Записывать в журнал события при превышении предела квоты | | Отключена |
| Записывать в журнал события, возникающие при превышении уровня предупреждения квоты | | Отключена |
| Применить политику к съемным носителям | | Отключена |
| **Диспетчер сервера** | |  |
| Не отображать окно "Задачи начальной настройки" автоматически при входе | | Отключена |
| Не отображать диспетчер сервера автоматически при входе | | Отключена |
| Настроить интервал обновления для диспетчера сервера | | Отключена |
| **Доступ к съемным запоминающим устройствам** | |  |
| Время (в секундах) до принудительной перезагрузки | | Отключена |
| Компакт-диски и DVD-диски: Запретить выполнение | | Отключена |
| Компакт-диски и DVD-диски: Запретить чтение | | Отключена |
| Компакт-диски и DVD-диски: Запретить запись | | Отключена |
| Специальные классы: Запретить чтение | | Отключена |
| Специальные классы: Запретить запись | | Отключена |
| Накопители на гибких дисках: Запретить выполнение | | Отключена |
| Накопители на гибких дисках: Запретить чтение | | Отключена |
| Накопители на гибких дисках: Запретить запись | | Отключена |
| Съемные диски: Запретить выполнение | | Отключена |
| Съемные диски: Запретить чтение | | Отключена |
| Съемные диски: Запретить запись | | Отключена |
| Съемные запоминающие устройства всех классов: Запретить любой доступ | | Отключена |
| Все съемные запоминающие устройства: разрешение прямого доступа в удаленных сеансах | | Отключена |
| Ленточные накопители: Запретить выполнение | | Отключена |
| Ленточные накопители: Запретить чтение | | Отключена |
| Ленточные накопители: Запретить запись | | Отключена |
| WPD-устройства: Запретить чтение | | Отключена |
| WPD-устройства: Запретить запись | | Отключена |
| **Доступ к устройствам Enhanced Storage** | |  |
| Разрешить предоставление сертификата на устройствах Enhanced Storage | | Отключена |
| Настройка списка устройств Enhanced Storage, которые могут использоваться на компьютере | | Отключена |
| Настройка списка приемников команд, совместимых с IEEE 1667, которые могут использоваться на компьютере | | Отключена |
| Запретить проверку подлинности устройств Enhanced Storage с помощью пароля | | Отключена |
| Запретить съемные устройства, которые не являются устройствами Enhanced Storage | | Отключена |
| Блокировать устройство Enhanced Storage при блокировании компьютера | | Отключена |
| Разрешить только корневой USB-концентратор, подключенный к устройствам Enhanced Storage | | Отключена |
| **Защита файлов Windows** | |  |
| Укажите размещение кэша для защиты файлов Windows | | Отключена |
| Ограничить размер кэша для защиты файлов Windows | | Отключена |
| Установить параметры сканирования защиты файлов Windows | | Отключена |
| Скрывать окно индикации выполнения сканирования файлов | | Отключена |
| **Панель управления производительностью** | |  |
| Отключение доступа к основному разделу панели управления производительностью | | Отключена |
| Отключение доступа к разделу решения проблем производительности | | Отключена |
| Отключение доступа к разделу изготовителя оборудования (OEM) и фирменной символики корпорации Майкрософт. | | Отключена |
| **Параметры завершения работы** | |  |
| Отключить автоматическое завершение работы приложений, которые блокируют или отменяют выключение компьютера. | | Отключена |
| **Передача учетных данных** | |  |
| Разрешить делегирование учетных данных, установленных по умолчанию, с проверкой подлинности сервера "только NTLM" | | Отключена |
| Разрешить передачу учетных данных, установленных по умолчанию | | Отключена |
| Разрешить передачу новых учетных данных | | Отключена |
| Разрешить делегирование новых учетных данных с проверкой подлинности сервера "только NTLM" | | Отключена |
| Разрешить передачу сохраненных учетных данных | | Отключена |
| Разрешить делегирование сохраненных учетных данных с проверкой подлинности сервера "только NTLM" | | Отключена |
| Запретить передачу учетных данных, установленных по умолчанию | | Отключена |
| Запретить передачу новых учетных данных | | Отключена |
| Запретить передачу сохраненных учетных данных | | Отключена |
| **Перенаправление папки** | |  |
| Использовать локализованные имена при перенаправлении папок меню "Пуск" и "Мои документы" | | Отключена |
| **Профили пользователей** | |  |
| Добавляет группу безопасности «Администраторы» к перемещаемым профилям пользователя. | | Отключена |
| Удалять при перезагрузке системы профили пользователей по истечении указанного числа дней | | Отключена |
| Не проверять собственность пользователя перемещаемых папок профиля | | Отключена |
| Удалять кэшированные копии перемещаемых профилей | | Отключена |
| Не выполнять принудительной выгрузки реестра пользователя при его выходе из системы | | Отключена |
| Не определять медленные сетевые подключения | | Отключена |
| Выдавать запрос пользователю при обнаружении медленного сетевого подключения | | Отключена |
| Оставить установочные данные установщика Windows и групповой политики | | Отключена |
| Разрешить использование только локальных профилей | | Отключена |
| Установить путь к перемещаемым профилям для всех пользователей, входящих в систему на данном компьютере | | Отключена |
| Таймаут диалоговых окон | | Отключена |
| Не регистрировать в системе пользователей с временными профилями | | Отключена |
| Максимальное число повторов попыток выгрузки и обновления профиля пользователя | | Отключена |
| Запретить передачу на сервер изменений в перемещаемом профиле | | Отключена |
| Дождаться загрузки перемещаемого пользовательского профиля | | Отключена |
| Таймаут медленных сетевых подключений для профилей пользователей | | Отключена |
| Фоновая передача файла cmdа перемещаемого профиля пользователя при входе пользователя в систему | | Отключена |
| Установить максимальное время ожидания для сети, если пользователь имеет перемещаемый профиль или удаленный основной каталог | | Отключена |
| **Распределенная модель СОМ** | |  |
| **Параметры совместимости приложений** | |  |
| Разрешать локальные исключения проверки безопасности при активации | | Отключена |
| Задать исключения проверки безопасности при активации | | Отключена |
| **Сетевой вход в систему** | |  |
| **DNS-записи локатора контроллеров домена [[106]](#footnote-107)** | |  |
| Тип возвращаемого адреса контроллера домена | | Не задана |
| Обнаружение контроллеров домена, несущих домен с однокомпонентным DNS-именем | | Не задана |
| Автоматическое обслуживание сайта DNS SRV-записями локатора контроллеров домена | | Не задана |
| DNS-записи локатора контроллеров домена, не регистрируемые контроллерами доменов | | Не задана |
| Интервал обновления DNS-записей локатора контроллеров домена | | Не задана |
| Набор TTL DNS-записей локатора контроллеров домена | | Не задана |
| Установить интервал повторного поиска контроллера домена | | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора глобального каталога | | Не задана |
| Не обрабатывать в слотах входящие сообщения, которые используются для поиска контроллеров доменов по NetBIOS-именам доменов | | Не задана |
| Установка приоритета в DNS SRV-записях локатора контроллеров домена | | Не задана |
| Установка веса в DNS SRV-записях локатора контроллеров домена | | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора раздела каталога приложений | | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора контроллеров домена | | Не задана |
| Попробовать следующий ближайший сайт. | | Не задана |
| Динамическая регистрация DNS-записей локатора контроллеров домена | | Не задана |
| Разрешать алгоритмы шифрования, совместимые с Windows NT 4.0 | | Отключена |
| Обращение к PDC при сбое входа в систему | | Включена |
| Начальный интервал попыток обнаружения контроллеров домена для фоновых клиентов | | Отключена |
| Максимальный интервал повторных попыток обнаружения контроллера домена для фоновых клиентов | | Отключена |
| Окончательный интервал попыток обнаружения контроллера домена для фоновых клиентов | | Отключена |
| Периодическое обновление кэша положительных ответов DC для фонового вызова | | Отключена |
| Уровень вывода данных отладки в файл журнала | | Отключена |
| Ожидаемая задержка при удаленном входе | | Отключена |
| Максимальный размер файла журнала | | Отключена |
| Настройка кэша отрицательных ответов обнаружения контроллеров домена | | Отключена |
| Совместимость общего сетевого доступа | | Отключена |
| Периодическое обновление кэша положительных ответов DC для нефонового вызова | | Отключена |
| Интервал очистки | | Отключена |
| Имя сайта | | Отключена |
| Совместимость общего ресурса Sysvol | | Отключена |
| **Служба времени Windows** | |  |
| **Поставщики времени** | |  |
| Настроить NTP-клиент Windows | | Отключена |
| Включить NTP-клиент Windows | | Включена |
| Включить NTP-сервер Windows | | Для контроллера домена: Включена. Для остальных: Отключена. |
| Глобальные параметры конфигурации | | Отключена |
| **Службы доверенного платформенного модуля** | |  |
| Включить резервное копирование TPM в доменные службы Active Directory | | Отключена |
| Настроить список заблокированных команд TPM | | Отключена |
| Игнорировать список заблокированных команд TPM по умолчанию | | Отключена |
| Игнорировать локальный список заблокированных команд TPM | | Отключена |
| **Службы языковых стандартов** | |  |
| Запретить выбор пользовательских языковых стандартов | | Отключена |
| Ограничить системные языковые стандарты | | Отключена |
| Ограничить пользовательские языковые стандарты | | Отключена |
| Запретить изменение географического положения | | Отключена |
| Не позволять пользователю переопределять параметры языкового стандарта | | Отключена |
| **Сценарии** | |  |
| Разрешение сценариев входа в систему при отключенных NetBIOS или WINS | | Отключена |
| Максимальное время выполнения сценариев групповой политики | | Отключена |
| Выполнить сценарии Windows PowerShell при запуске компьютера, завершить работу компьютера | | Отключена |
| Выполнять сценарии входа в систему синхронно | | Отключена |
| Выполнять сценарии завершения работы с отображением команд | | Отключена |
| Выполнять сценарии загрузки асинхронно | | Отключена |
| Выполнять сценарии загрузки с отображением команд | | Отключена |
| Выполнить сценарии Windows PowerShell при входе пользователя в систему, завершить сеанс | | Отключена |
| **Удаленный помощник** | |  |
| Разрешать подключения только с компьютеров под управлением Windows 7 или более новых систем | | Отключена |
| Включить ведение журнала сеансов | | Отключена |
| Включить оптимизацию пропускной способности | | Отключена |
| Настройка предупреждающих сообщений | | Отключена |
| Запрос удаленной помощи | | Отключена |
| Предлагать удаленную помощь | | Отключена |
| **Управление связью через Интернет** | |  |
| **Параметры связи через Интернет** | |  |
| Отключить отчеты об ошибках распознавания рукописного текста | | Включена |
| Отключить программу по улучшению качества программного обеспечения Windows | | Включена |
| Выключить автоматическое обновление корневых сертификатов | | Отключена |
| Отключить печать по протоколу HTTP | | Отключена |
| Отключение загрузки драйверов принтера по протоколу HTTP | | Отключена |
| Отключение поиска драйверов устройств в Центре обновления Windows | | Включена |
| Отключить ссылки просмотра событий «Events.asp» | | Включена |
| Отключение центра справки и поддержки «Знаете ли вы?» | | Включена |
| Отключить поиск в базе знаний Майкрософт в окне «Центр справки и поддержки» | | Включена |
| Отключить мастер подключения к Интернету, если URL-адрес ссылается на сайт Microsoft.com | | Включена |
| Отключить регистрацию, если адрес-URL указывает на сайт Microsoft.com | | Включена |
| Отключить активное зондирование для индикатора состояния сетевого подключения | | Включена |
| Отключить отчеты об ошибках Windows | | Включена |
| Отключить доступ ко всем возможностям Центра обновления Windows | | Включена |
| Отключить обновление информационных файлов «Помощника по поиску» | | Включена |
| Отключить службу сопоставления файлов Интернета | | Включена |
| Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков | | Включена |
| Отключить заказ отпечатков через Интернет в списке задач для изображений | | Включена |
| Отключить веб-публикацию в списке задач для файлов и папок | | Включена |
| Отключить участие в программе улучшения поддержки пользователей Windows Messenger | | Включена |
| Ограничение соединения с Интернетом | | Включена |
| **Управление электропитанием** | |  |
| **Параметры жесткого диска** | |  |
| Отключить жесткий диск (Питание от сети) | | Отключена |
| Отключить жесткий диск (Питание от батареи) | | Отключена |
| **Параметры кнопок** | |  |
| Выберите действие кнопки включения питания (Питание от сети) | | Отключена |
| Выберите действие кнопки перехода в режим сна (Питание от сети) | | Отключена |
| Выберите действие кнопки включения питания в меню «Пуск» (Питание от сети) | | Отключена |
| Выберите действие при закрытии крышки компьютера (Питание от сети) | | Отключена |
| Выберите действие кнопки включения питания (Питание от батареи) | | Отключена |
| Выберите действие кнопки перехода в режим сна (Питание от батареи) | | Отключена |
| Выберите действие кнопки включения питания меню «Пуск» (Питание от батареи) | | Отключена |
| Выберите действие при закрытии крышки компьютера (Питание от батареи) | | Отключена |
| **Параметры режимов сна** | |  |
| Разрешить приложениям препятствовать переходу системы в режим сна (Питание от сети) | | Отключена |
| Укажите время ожидания для перехода в режим гибернации (Питание от сети) | | Отключена |
| Требовать пароль при выходе из спящего режима (Питание от сети) | | Включена |
| Укажите время ожидания перехода в режим сна (Питание от сети) | | Отключена |
| Отключить гибридный спящий режим (Питание от сети) | | Отключена |
| Разрешить различные режимы сна (S1-S3) при простое компьютера (Питание от сети) | | Отключена |
| Разрешить различные режимы сна (S1-S3) при простое компьютера (Питание от батареи) | | Отключена |
| Разрешить приложениям предотвращать автоматический переход в спящий режим (питание от сети) | | Отключена |
| Разрешить приложениям предотвращать автоматический переход в спящий режим (питание от батареи) | | Отключена |
| Разрешить автоматический переход в спящий режим с открытыми сетевыми файлами (питание от сети) | | Отключена |
| Разрешить автоматический переход в спящий режим с открытыми сетевыми файлами (питание от батареи) | | Отключена |
| Разрешить приложениям препятствовать переходу системы в режим сна (Питание от батареи) | | Отключена |
| Укажите время ожидания для перехода в режим гибернации (Питание от батареи) | | Отключена |
| Требовать пароль при выходе из спящего режима (Питание от батареи) | | Включена |
| Укажите время ожидания перехода в режим сна (Питание от батареи) | | Отключена |
| Отключить гибридный спящий режим (Питание от батареи) | | Отключена |
| Укажите время ожидания автоматического перехода в режим сна (Питание от сети) | | Отключена |
| Укажите время ожидания автоматического перехода в режим сна (питание от батареи) | | Отключена |
| **Параметры уведомления** | |  |
| Действие при почти полной разрядке батареи | | Отключена |
| Действие при низком заряде батареи | | Отключена |
| Уровень сигнала почти полной разрядки батареи | | Отключена |
| Отключить уведомление при низком уровне заряда батареи | | Отключена |
| Уровень сигнала низкого заряда батареи | | Отключена |
| Уровень сигнала резервной батареи | | Отключена |
| **Параметры экрана и видео** | |  |
| Указать яркость монитора (питание от сети) | | Отключена |
| Указать яркость монитора (питание от батареи) | | Отключена |
| Уменьшить яркость монитора (питание от сети) | | Отключена |
| Уменьшить яркость монитора (питание от батареи) | | Отключена |
| Включить фоновый показ слайдов на рабочем столе (питание от сети) | | Отключена |
| Включить фоновый показ слайдов на рабочем столе (питание от батареи) | | Отключена |
| Выключить адаптивное время ожидания выключения дисплея (Питание от сети) | | Отключена |
| Выключить адаптивное время ожидания выключения дисплея (Питание от батареи) | | Отключена |
| Отключить дисплей (Питание от сети) | | Отключена |
| Отключить дисплей (Питание от батареи) | | Отключена |
| Укажите настраиваемую текущую схему управления питанием | | Отключена |
| Выберите текущую схему управления питанием | | Отключена |
| **Установка драйвера** | |  |
| Разрешить пользователям, не являющимся администраторами, устанавливать драйверы для этих классов установки устройств | | Отключена |
| Отключить запрос на поиск драйверов устройств на веб-сайте Windows Update | | Включена |
| **Установка устройства** | |  |
| **Ограничения на установку устройств** | |  |
| Разрешить администраторам заменять политики ограничения установки устройств | | Отключена |
| Разрешить установку устройств с использованием драйверов, соответствующих этим классам установки устройств | | Отключена |
| Запретить установку устройств с использованием драйверов, соответствующих этим классам установки устройств | | Отключена |
| Отображать специальное сообщение, когда установка запрещена параметром политики. | | Отключена |
| Отображать заголовок специального сообщения, когда установка устройства запрещена параметром политики. | | Отключена |
| Разрешить установку устройств, соответствующих какому-либо из этих кодов устройств | | Отключена |
| Запретить установку устройств с указанными кодами устройств | | Отключена |
| Время (сек.) до принудительной перезагрузки при необходимости введения параметров политики в действие | | Отключена |
| Запретить установку съемных устройств | | Отключена |
| Запретить установку устройств, не описанных другими параметрами политики | | Отключена |
| Устанавливать одинаковый приоритет для всех подписанных цифровой подписью драйверов при оценке и в процессе выбора | | Отключена |
| Отключить всплывающие напоминания «Найдено новое оборудование» во время установки драйвера | | Отключена |
| Не посылать отчет об ошибках Windows, если для устройства установлен общий драйвер. | | Отключена |
| Настроить время ожидания установки устройства | | Отключена |
| Запретить Windows отправлять отчет об ошибках, если драйвер устройства запрашивает дополнительное программное обеспечение в ходе установки | | Отключена |
| Не создавать контрольную точку восстановления системы во время работы устройства, при которой, как правило, требуется создание точки восстановления | | Отключена |
| Разрешить удаленный доступ к устройствам Plug and Play | | Отключена |
| Запретить получение метаданных устройств из Интернета | | Отключена |
| Задать порядок поиска в исходных расположениях драйверов устройств | | Отключена |
| **Файловая система** | |  |
| **NTFS** | |  |
| Запретить сжатие на всех томах NTFS | | Отключена |
| Запретить шифрование на всех томах NTFS | | Отключена |
| Включить шифрование файла подкачки NTFS | | Отключена |
| Параметры создания коротких имен | | Отключена |
| Отключить уведомления об удалении на всех томах | | Отключена |
| Оценка символьных ссылок на основе их источников и адресов | | Отключена |
| **Центр распространения ключей** | |  |
| Использовать порядок поиска леса | | Отключена |
| Предоставлять сведения о предыдущих попытках входа на клиентские компьютеры | | Отключена |
| **Энергонезависимый кэш диска** | |  |
| Отключить оптимизацию начальной загрузки и восстановления | | Отключена |
| Отключить режим питания кэша | | Отключена |
| Отключить функцию «Энергонезависимый кэш» | | Отключена |
| Отключить режим Solid State | | Отключена |
| Загружать отсутствующие COM-компоненты | | Отключена |
| Разрешить клиентам для отслеживания изменившихся связей использовать ресурсы домена | | Отключена |
| Не выполнять автоматическое шифрование файлов, перемещаемых в зашифрованные папки | | Отключена |
| Не отключайте питание компьютера после возникновения ошибки завершения работы системы Windows. | | Отключена |
| Включить постоянную временную метку | | Не задана |
| Включить свойство данных состояния системы слежения за завершением работы | | Не задана |
| Отображать диалог слежения за завершением работы | | Отключена |
| Не отображать страницу "Управление данным сервером" при входе | | Отключена |
| Отключить предотвращение выполнения данных для исполняемого файла справки в формате HTML | | Отключена |
| Ограничить применение потенциально небезопасных функций справки HTML указанными папками | | Включена (\*) |
| Запретить запуск из cправки перечисленных программ | | Включена (\*) |
| Удалить сообщения о состоянии загрузки / завершения работы системы / входа в систему / выхода из системы | | Отключена |
| Подробные или обычные сообщения состояния | | Отключена |
| Указать размещение установочных файлов пакета обновления Windows | | Отключена |
| Указать расположение установочных файлов Windows | | Отключена |
| **Классические административные шаблоны** | |  |
| **Secret Net Integrity Check settings** | |  |
| Extension Executive[[107]](#footnote-108) | | Включена (.exe;.dll;.cpl;.drv;.sys;.ocx;.vbs;.scr; .rll;.ime;.bpl;.ax;.acm;.com;.ppl;.cmd;.bat;.ovl;.tbp;.lnk) [[108]](#footnote-109) |
| **Все параметры** | | См. значение конкретного параметра выше в таблице |
| **Настройка** | |  |
| **Конфигурация Windows** | |  |
| Среда | | Не определено |
| Файлы | | Не определено |
| Папки | | Не определено |
| INI-файлы | | Не определено |
| Реестр | | Не определено |
| Сетевые общие ресурсы | | Не определено |
| Ярлыки | | Не определено |
| **Параметры панели управления** | |  |
| Источники данных | | Не определено |
| Устройства | | Не определено |
| Параметры папок | | Не определено |
| Локальные пользователи и группы | | Не определено |
| Сетевые параметры | | Не определено |
| Электропитание | | Не определено |
| Принтеры | | Не определено |
| Назначенные задания | | Не определено |
| Службы | | Не определено |

### Параметры групповой политики для рядовых серверов и контролллеров домена при использовании СЗИ от НСД Secret Net

Параметры групповой политики и их значения, применяемые для рядовых серверов и контроллеров домена при использовании СЗИ от НСД SecretNet, приведены в таблице (Таблица 45).

Таблица 45. Параметры групповой политики для рядовых серверов и контроллеров домена при использовании СЗИ от НСД Secret Net

| **Наименование раздела/параметра** | **Значение** |
| --- | --- |
| **Политики** |  |
| **Конфигурация программ** |  |
| Установка программ | Не определено |
| **Конфигурация Windows** |  |
| **Политика разрешения имен** | Не определено |
| **Сценарии (запуск/завершение)** |  |
| Автозагрузка | Не определено |
| Завершение работы | Не определено |
| **Административные шаблоны** |  |
| **Параметры безопасности** |  |
| **Политики учетных записей** |  |
| **Политика паролей** |  |
| Вести журнал паролей | 5 хранимых паролей |
| Максимальный срок действия пароля | 180 дней |
| Минимальная длина пароля | 8 символов |
| Минимальный срок действия пароля | 0 дней |
| Пароль должен отвечать требованиям сложности | Включен |
| Хранить пароли, используя обратимое шифрование | Отключен |
| **Политика блокировки учетной записи** |  |
| Время до сброса счетчика блокировки | 30 мин. |
| Пороговое значение блокировки | 5 ошибок входа в систему |
| Продолжительность блокировки учетной записи | 0 |
| **Политика Kerberos [[109]](#footnote-110)** |  |
| Максимальная погрешность синхронизации часов компьютера | 5 |
| Максимальный срок жизни билета пользователя | 10 |
| Максимальный срок жизни билета службы | 600 |
| Максимальный срок жизни для возобновления билета пользователя | 7 |
| Принудительные ограничения входа пользователей | Включен |
| **Локальные политики** |  |
| **Политика аудита** |  |
| Аудит входа в систему | успех, отказ |
| Аудит доступа к объектам | нет аудита |
| Аудит доступа к службе каталогов | отказ (нет аудита – для контроллеров домена) |
| Аудит изменения политики | успех, отказ |
| Аудит использования привилегий | нет аудита |
| Аудит отслеживания процессов | нет аудита |
| Аудит системных событий | успех, отказ |
| Аудит событий входа в систему | успех, отказ |
| Аудит управления учетными записями | успех, отказ |
| **Назначение прав пользователя** |  |
| Архивация файлов и каталогов | Администраторы |
| Блокировка страниц в памяти | [[110]](#footnote-111) |
| Восстановление файлов и каталогов | Администраторы |
| Вход в качестве пакетного задания | Администраторы, локальная служба (Local Service), musr\_mqadmin |
| Вход в качестве службы | Имя домена\mservice, Имя домена\HP ITO account [[111]](#footnote-112) |
| Выполнение задач по обслуживанию томов | Администраторы |
| Добавление рабочих станций к домену | Администраторы |
| Доступ к диспетчеру учетных данных от имени доверенного вызывающего |  |
| Доступ к компьютеру из сети | Прошедшие проверку, Контроллеры домена предприятия |
| Завершение работы системы | Администраторы, Прошедшие проверку |
| Загрузка и выгрузка драйверов устройств | Администраторы |
| Замена маркера уровня процесса | Локальная служба, сетевая служба, musr\_mqadmin |
| Запретить вход в систему через службу удаленных рабочих столов |  |
| Запретить локальный вход |  |
| Изменение метки объекта |  |
| Изменение параметров среды изготовителя | Администраторы |
| Изменение системного времени | Администраторы, локальная служба |
| Изменение часового пояса | Администраторы, локальная служба |
| Имитация клиента после проверки подлинности | Администраторы, локальная служба, сетевая служба, служба |
| Локальный вход в систему | Администраторы, Прошедшие проверку |
| Настройка квот памяти для процесса | Администраторы, локальная служба, сетевая служба, musr\_mqadmin |
| Обход перекрестной проверки | Прошедшие проверку, musr\_mqadmin |
| Отказать в доступе к этому компьютеру из сети | loser |
| Отказать во входе в качестве пакетного задания |  |
| Отказать во входе в качестве службы |  |
| Отключение компьютера от стыковочного узла | Администраторы |
| Отладка программ | Администраторы |
| Принудительное удаленное завершение работы | Администраторы |
| Профилирование одного процесса | Администраторы |
| Профилирование производительности системы | Администраторы |
| Работа в режиме операционной системы | Локальная служба, musr\_mqadmin |
| Разрешение доверия к учетным записям компьютеров и пользователей при делегировании | Администраторы |
| Разрешить вход в систему через службу удаленных рабочих столов | Администраторы[[112]](#footnote-113) |
| Синхронизация данных службы каталогов | Администраторы |
| Смена владельцев файлов и других объектов | Администраторы |
| Создание аудитов безопасности | Локальная служба, сетевая служба |
| Создание глобальных объектов | Администраторы |
| Создание маркерного объекта | Локальная служба |
| Создание постоянных общих объектов | Локальная служба |
| Создание символических ссылок | Администраторы |
| Создание файла подкачки | Администраторы |
| Увеличение приоритета выполнения | Администраторы |
| Увеличение рабочего набора процесса | Администраторы, Пользователи |
| Управление аудитом и журналом безопасности[[113]](#footnote-114) | Auditors |
| **Параметры безопасности** |  |
| DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language) | Не определено |
| DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language) | Не определено |
| Аудит: аудит доступа глобальных системных объектов | Отключен |
| Аудит: аудит прав на архивацию и восстановление | Отключен |
| Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности | Отключен |
| Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows 7 или следующие версии) | Включен |
| Доступ к сети: Разрешить трансляцию анонимного SID в имя | Отключен |
| Завершение работы: очистка файла подкачки виртуальной памяти | Отключен |
| Завершение работы: разрешить завершение работы системы без выполнения входа в систему | Отключен |
| Интерактивный вход в систему: поведение при извлечении смарт-карты | Блокировка рабочей станции |
| Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему | Не определено |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | 0 |
| Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее | 5 дн. |
| Интерактивный вход в систему: не отображать последнее имя пользователя | Включен |
| Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL | Отключен |
| Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован. | Включен (Выводимое имя пользователя, имена домена и пользователя) |
| Интерактивный вход в систему: текст сообщения для пользователей при входе в систему | Не определено |
| Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера | Отключен |
| Интерактивный вход в систему: требовать смарт-карту | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (всегда) | Отключен |
| Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) | Включен |
| Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам | Отключен |
| Консоль восстановления: разрешить автоматический вход администратора | Отключен |
| Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам | Отключен |
| Контроллер домена: запретить изменение пароля учетных записей компьютера | Отключен |
| Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию | Отключен |
| Контроллер домена: требование цифровой подписи для LDAP-сервера | Нет |
| Контроль учетных записей: все администраторы работают в режиме одобрения администратором | Отключен |
| Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав | Отключен |
| Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав | Отключен |
| Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором | Повышение без запроса |
| Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей | Запрос учетных данных |
| Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах | Отключен |
| Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов | Отключен |
| Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя | Отключен |
| Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол | Отключен |
| Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора | Отключен |
| Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ | Отключен |
| Параметры системы: необязательные подсистемы | Posix |
| Сервер сети Microsoft: время бездействия до приостановки сеанса | 15 мин. |
| Сервер сети Microsoft: использовать цифровую подпись (всегда) | Отключено для рядового сервера.  Включено для контроллеров домена. |
| Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента) | Отключено для рядового сервера.  Включено для контроллеров домена. |
| Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа | Отключен |
| Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC) | Минимума нет |
| Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC) | Минимума нет |
| Сетевая безопасность: настройка типов шифрования, разрешенных Kerberos | Не определено |
| Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля | Включен |
| Сетевая безопасность: ограничения NTLM: аудит входящего трафика NTLM | Отключить |
| Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене | Отключить |
| Сетевая безопасность: ограничения NTLM: входящий трафик NTLM | Разрешить все |
| Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене | Не определено |
| Сетевая безопасность: ограничения NTLM: добавить удаленные серверы в исключения проверки подлинности NTLM | Не определено |
| Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удаленным серверам | Разрешить все |
| Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене | Отключить |
| Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы | Отключен |
| Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы | Включен |
| Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U к этому компьютеру | Отключен |
| Сетевая безопасность: разрешить учетной записи локальной системы использовать удостоверение компьютера для NTLM | Отключен |
| Сетевая безопасность: требование цифровой подписи для LDAP-клиента | Согласование цифровой подписи |
| Сетевая безопасность: уровень проверки подлинности LAN Manager | Отправлять только NTLMv2 ответ |
| Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам | Включен |
| Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей | (Обычная – локальные пользователи удостоверяются как они сами) |
| Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями | Отключен. |
| Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями | Отключен |
| Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности | Включен |
| Сетевой доступ: разрешать анонимный доступ к именованным каналам | Включен (SnHwSrv, SnIcheckSrv)[[114]](#footnote-115) |
| Сетевой доступ: разрешать анонимный доступ к общим ресурсам | Не определено |
| Сетевой доступ: разрешать применение разрешений "Для всех" к анонимным пользователям | Отключен |
| Сетевой доступ: удаленно доступные пути и вложенные пути реестра | System\CurrentControlSet\Control\Print\Printers,  System\CurrentControlSet\Services\Eventlog,  Software\Microsoft\OLAP Server,  Software\Microsoft\WindowsNT\CurrentVersion\Print,  Software\Microsoft\WindowsNT\CurrentVersion\Windows,  System\CurrentControlSet\Control\ContentIndex,  System\CurrentControlSet\Control\Terminal Server,  System\CurrentControlSet\Control\Terminal Server\UserConfig,  System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,  Software\Microsoft\Windows NT\CurrentVersion\Perflib,  System\CurrentControlSet\Services\SysmonLog,  System\CurrentControlSet\Services\CertSvc,  System\CurrentControlSet\Services\Wins |
| Сетевой доступ: удаленно доступные пути реестра | System\CurrentControlSet\Control\ProductOptions,  System\CurrentControlSet\Control\Server Applications,  Software\Microsoft\Windows NT\CurrentVersion |
| Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного объекта | Откл. |
| Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания | Отключен |
| Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере | Не требуется ввод данных пользователем при сохранении и использовании новых ключей. |
| Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок) | Включен |
| Системные объекты: учитывать регистр для подсистем, отличных от Windows | Включен |
| Устройства: запретить пользователям установку драйверов принтера | Включен. |
| Устройства: разрешать отстыковку без входа в систему | Включен |
| Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям | Включен |
| Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям | Включен |
| Устройства: разрешить форматирование и извлечение съемных носителей | Администраторы |
| Учетные записи: Переименование учетной записи администратора | adm |
| Учетные записи: Переименование учетной записи гостя | loser |
| Учетные записи: разрешить использование пустых паролей только при консольном входе | Отключен |
| Учетные записи: Состояние учетной записи 'Администратор' | Включен |
| Учетные записи: Состояние учетной записи 'Гость' | Отключен |
| Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала | Включен |
| Член домена: максимальный срок действия пароля учетных записей компьютера | 180 дн. |
| Член домена: отключить изменение пароля учетных записей компьютера | Отключен |
| Член домена: требовать стойкий ключ сеанса (Windows 2000 или выше) | Включен |
| Член домена: цифровая подпись данных безопасного канала, когда это возможно | Включен |
| Член домена: шифрование данных безопасного канала, когда это возможно | Включен |
| **Журнал событий** |  |
| Запретить доступ локальной группы гостей к журналу безопасности | Включен |
| Запретить доступ локальной группы гостей к журналу приложений | Включен |
| Запретить доступ локальной группы гостей к системному журналу | Включен |
| Максимальный размер журнала безопасности | 81920 КБ |
| Максимальный размер журнала приложений | 32768 КБ |
| Максимальный размер системного журнала | 32768 КБ |
| Метод сохранения событий в журнале безопасности | Затирать старые события при необходимости |
| Метод сохранения событий в журнале приложений | Затирать старые события при необходимости |
| Метод сохранения событий в системном журнале | Затирать старые события при необходимости |
| Сохранять события в журнале безопасности | Не определено |
| Сохранять события в журнале приложений | Не определено |
| Сохранять события в системном журнале | Не определено |
| **Группы с ограниченным доступом[[115]](#footnote-116)** |  |
| **Системные службы[[116]](#footnote-117)** |  |
| DHCP-клиент | Автоматическое |
| DNS-клиент | Автоматическое |
| DNS-сервер | Автоматическое для серверов DNS. Для остальных: Отключен. |
| KtmRm для координатора распределенных транзакций | Вручную |
| Microsoft .NET Framework NGEN v2.0.50727\_X64 | Вручную |
| Microsoft .NET Framework NGEN v2.0.50727\_X86 | Вручную |
| Plug-and-Play | Автоматическое |
| Windows Audio | Вручную |
| Windows CardSpace | Вручную |
| Windows Driver Foundation - User-mode Driver Framework | Вручную |
| WMI Performance Adapter | Вручную |
| Агент защиты сетевого доступа | Вручную |
| Агент политики IPsec | Вручную |
| Брандмауэр Windows | Отключен |
| Браузер компьютеров | Автоматическое |
| Веб-службы Active Directory | Автоматическое |
| Виртуальный диск | Вручную |
| Вспомогательная служба IP | Автоматическое |
| Вторичный вход в систему | Вручную |
| Дефрагментация диска | Вручную |
| Диспетчер автоматических подключений удаленного доступа | Вручную |
| Диспетчер печати | Автоматическое |
| Диспетчер подключений удаленного доступа | Вручную |
| Диспетчер сеансов диспетчера окон рабочего стола | Автоматическое |
| Диспетчер учетных данных | Вручную |
| Диспетчер учетных записей безопасности | Автоматическое |
| Доменные службы Active Directory | Автоматическое |
| Доступ к HID-устройствам | Вручную |
| Журнал событий Windows | Автоматическое |
| Журналы и оповещения производительности | Вручную |
| Защита программного обеспечения | Автоматическое |
| Защищенное хранилище | Вручную |
| Изоляция ключей CNG | Вручную |
| Инструментарий управления Windows | Вручную (Автоматическое – для контроллеров домена) |
| Информация о совместимости приложений | Вручную |
| Клиент групповой политики | Автоматическое |
| Клиент отслеживания изменившихся связей | Вручную |
| Координатор распределенных транзакций | Автоматическое |
| Кэш шрифтов Windows Presentation Foundation 3.0.0.0 | Вручную |
| Ловушка SNMP | Вручную |
| Локатор удаленного вызова процедур (RPC) | Вручную |
| Маршрутизация и удаленный доступ | Отключен |
| Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности | Вручную |
| Модуль запуска процессов DCOM-сервера | Автоматическое |
| Модуль поддержки NetBIOS через TCP/IP | Автоматическое |
| Модуль поддержки специальной консоли администрирования | Вручную |
| Настройка сервера удаленных рабочих столов | Вручную |
| Обнаружение SSDP | Отключен |
| Обнаружение интерактивных служб | Вручную |
| Общий доступ к подключению к Интернету (ICS) | Отключен |
| Определение оборудования оболочки | Автоматическое |
| Основные службы доверенного платформенного модуля | Вручную |
| Перенаправитель портов пользовательского режима служб удаленных рабочих столов | Вручную |
| Перечислитель IP-шин PnP-X | Отключен |
| Питание | Автоматическое |
| Планировщик заданий | Автоматическое |
| Планировщик классов мультимедиа | Вручную |
| Поддержка элемента панели управления "Отчеты о проблемах и их решениях" | Вручную |
| Политика удаления смарт-карт | Вручную |
| Поставщик результирующей политики (RSoP) | Автоматическое |
| Проводная автонастройка | Вручную |
| Программный поставщик теневого копирования (Microsoft) | Автоматическое |
| Пространство имен DFS | Автоматическое |
| Публикация ресурсов обнаружения функции | Вручную |
| Рабочая станция | Автоматическое |
| Распространение сертификата | Вручную |
| Расширяемый протокол проверки подлинности (EAP) | Вручную |
| Репликация DFS | Автоматическое |
| Служба репликации файлов | Автоматическое |
| Сборщик событий Windows | Вручную |
| Сведения о приложении | Вручную |
| Сервер | Автоматическое |
| Сервер упорядочения потоков | Вручную |
| Сетевой вход в систему | Автоматическое |
| Сетевые подключения | Автоматическое |
| Система событий COM+ | Автоматическое |
| Системное приложение COM+ | Вручную |
| Служба SSTP | Вручную |
| Служба автоматического обнаружения веб-прокси WinHTTP | Вручную |
| Служба базовой фильтрации | Автоматическое |
| Служба времени Windows | Автоматическое |
| Служба завершения работы в качестве гостя (Hyper-V) | Автоматическое |
| Служба запросов на теневое копирование томов Hyper-V | Автоматическое |
| Служба инициатора Майкрософт iSCSI | Вручную |
| Служба интерфейса сохранения сети | Автоматическое |
| Служба кэша шрифтов Windows | Вручную |
| Служба межсайтовых сообщений | Отключен (Автоматическое – для контроллеров домена) |
| Служба обмена данными (Hyper-V) | Автоматическое |
| Служба общего доступа к портам Net.Tcp | Отключен |
| Служба перечислителя переносных устройств | Вручную |
| Служба политики диагностики | Автоматическое |
| Служба профилей пользователей | Автоматическое |
| Служба пульса (Hyper-V) | Автоматическое |
| Служба регистрации ошибок Windows | Вручную |
| Служба регистрации платформы Fibre Channel Microsoft | Вручную |
| Служба сведений о подключенных сетях | Автоматическое |
| Служба синхронизации времени Hyper-V | Автоматическое |
| Служба списка сетей | Вручную |
| Служба уведомления SPP | Вручную |
| Служба уведомления о системных событиях | Автоматическое |
| Служба удаленного управления Windows (WS-Management) | Автоматическое |
| Служба шлюза уровня приложения | Вручную |
| Службы криптографии | Автоматическое |
| Службы удаленных рабочих столов | Автоматическое[[117]](#footnote-118) |
| Смарт-карта | Автоматическое |
| Сопоставитель конечных точек RPC | Автоматическое |
| Средство построения конечных точек Windows Audio | Вручную |
| Телефония | Вручную[[118]](#footnote-119) |
| Теневое копирование тома | Вручную |
| Тополог канального уровня | Вручную |
| Удаленный вызов процедур (RPC) | Автоматическое |
| Удаленный реестр | Отключен (Для контроллеров домена: Автоматическое) |
| Удостоверение приложения | Вручную |
| Узел системы диагностики | Вручную |
| Узел службы диагностики | Вручную |
| Узел универсальных PNP-устройств | Вручную |
| Управление приложениями | Вручную |
| Управление сертификатами и ключом работоспособности | Вручную |
| Установщик Windows | Вручную |
| Установщик модулей Windows | Вручную |
| Фоновая интеллектуальная служба передачи (BITS) | Вручную |
| Хост библиотеки счетчика производительности | Вручную |
| Хост поставщика функции обнаружения | Вручную |
| Цветовая система Windows (WCS) | Вручную |
| Центр обновления Windows | Отключен |
| Центр распространения ключей Kerberos | Вручную (Для контроллеров домена: Автоматическое) |
| Шифрованная файловая система (EFS) | Вручную |
| **Реестр** | Не определено |
| **Файловая система** | Не определено |
| **Политики проводной сети (IEEE 802.3)** | Не определено |
| **Брандмауэр Windows в режиме повышенной безопасности** |  |
| Брандмауэр Windows в режиме повышенной безопасности |  |
| Свойства брандмауэра Windows | Все параметры: "не задано" или "по умолчанию" |
| Профиль домена | Не настроено |
| Частный профиль | Не настроено |
| Общий профиль | Не настроено |
| Правила безопасности подключений | Не определено |
| Правила для входящих подключений | Не определено |
| Правила для исходящих подключений | Не определено |
| **Политики диспетчера списка сетей** |  |
| <DNS-имя домена> | Указать полное имя домена |
| Неопознанные сети | Не задано |
| Идентификация сетей | Не задано |
| Все сети | Не задано |
| **Политики беспроводной сети (IEEE 802.11)** | Не определено |
| **Политики открытого ключа** |  |
| **Шифрующая файловая система (EFS)** | Не определено |
| **Шифрование диска BitLocker** | Не определено |
| **Параметры автоматического запроса сертификатов** | Не определено |
| **Доверенные корневые центры сертификации** | Не определено |
| **Доверительные отношения в предприятии** | Не определено |
| **Промежуточные центры сертификации** | Не определено |
| **Доверенные издатели** | Не определено |
| **Сертификаты, к которым нет доверия** | Не определено |
| **Доверенные лица** | Не определено |
| Клиент служб сертификатов - политика регистрации сертификатов | Не настроено |
| Параметры подтверждения пути сертификата | Не настроено |
| Клиент служб сертификации: автоматическая регистрация | Не настроено |
| **Политики ограниченного использования программ** | Не определено |
| **Защита доступа к сети** |  |
| **Конфигурация клиента NAP** |  |
| **Клиенты принудительной защиты** |  |
| Клиента принудительного карантина для DHCP | Отключено |
| Сторона, использующая IPSec | Отключено |
| Клиент принудительного помещения на карантин шлюза удаленных рабочих столов | Отключено |
| Клиент принудительного карантина EAP | Отключено |
| Клиент принудительного удаленного доступа для Windows XP | Отключено |
| Клиент принудительного использования EAOPL для Windows XP | Отключено |
| **Параметры пользовательского интерфейса** |  |
| Пользовательский интерфейс | Не определено |
| **Параметры регистрации работоспособности** |  |
| **Группы доверенных серверов** |  |
| **Политика запроса** |  |
| Алгоритм кэширования | sha1RSA(1.3.14.3.2.29) |
| Поставщик службы криптографии | Microsoft RSA SChannel Cryptographic Provider  2048 бит |
| **Политики управления приложениями** |  |
| **AppLocker** |  |
| Исполняемые правила | Не определено |
| Правила установщика Windows | Не определено |
| Правила сценариев | Не определено |
| **Политики IP-безопасности на "Служба каталогов Active Directory (...)"** |  |
| Client (Respond Only) |  |
| Правила (*единственное, создано по умолчанию*) |  |
| Список IP-фильтров | Динамический |
| Действие фильтра | Отклик по умолчанию |
| Методы проверки подлинности | Kerberos |
| Конечная точка туннеля | Нет |
| Тип подключения | Все |
| Общие |  |
| Проверять политику на наличие изменений каждые | 180 мин. |
| Secure Server (Require Security) |  |
| Правила (*три, созданы по умолчанию*) |  |
| Список IP-фильтров | 1.All IP traffic  2.All ICMP traffic  3. Динамический |
| Действие фильтра | 1.Require Security  2.Permit  3.Отклик по умолчанию |
| Методы проверки подлинности | 1.Kerberos  2.Отсутсвует  3.Kerberos |
| Конечная точка туннеля | Для всех правил: Нет |
| Тип подключения | Для всех правил: Все |
| Общие |  |
| Проверять политику на наличие изменений каждые | 180 мин. |
| Server (Request Security) |  |
| Правила (*три, созданы по умолчанию*) |  |
| Список IP-фильтров | 1.All IP traffic  2.All ICMP traffic  3. Динамический |
| Действие фильтра | 1.Request Security (Optional)  2.Permit  3.Отклик по умолчанию (только ранние версии Windows) |
| Методы проверки подлинности | 1.Kerberos  2.Отсутсвует  3.Kerberos |
| Конечная точка туннеля | Для всех правил: Нет |
| Тип подключения | Для всех правил: Все |
| Общие |  |
| Проверять политику на наличие изменений каждые | 180 мин. |
| **Конфигурация расширенной политики аудита** |  |
| **Политики аудита** |  |
| **Вход учетной записи** |  |
| Аудит проверки учетных данных | Успех, отказ |
| Аудит службы проверки подлинности Kerberos | Нет аудита |
| Аудит операций с билетами службы Kerberos | Нет аудита |
| Аудит других событий входа учетных записей | Успех, отказ |
| **Управление учетными записями** |  |
| Аудит управления группами приложений | Нет аудита |
| Аудит управления учетными записями компьютеров | Успех, отказ |
| Аудит управления группами распространения | Нет аудита |
| Аудит других событий управления учетными записями | Успех, отказ |
| Аудит управления группами безопасности | Успех, отказ |
| Аудит управления учетными записями пользователей | Успех, отказ |
| **Подробное отслеживание** |  |
| Аудит активности DPAPI | Нет аудита |
| Аудит создания процессов | Нет аудита |
| Аудит завершения процессов | Нет аудита |
| Аудит событий RPC | Нет аудита |
| **Доступ к службе каталогов (DS)** |  |
| Аудит подробной репликации службы каталогов | Нет аудита |
| Аудит доступа к службе каталогов | Нет аудита |
| Аудит изменения службы каталогов | Успех, отказ |
| Аудит репликации службы каталогов | Нет аудита |
| **Вход/выход** |  |
| Аудит блокировки учетных записей | Успех, отказ |
| Аудит расширенного режима IPsec | Нет аудита |
| Аудит основного режима IPsec | Нет аудита |
| Аудит быстрого режима IPsec | Нет аудита |
| Аудит выхода из системы | Успех, отказ |
| Аудит входа в систему | Успех, отказ |
| Аудит сервера политики сети | Нет аудита |
| Аудит других событий входа и выхода | Успех, отказ |
| Аудит специального входа | Успех, отказ |
| **Доступ к объектам** |  |
| Аудит событий, создаваемых приложениями | Нет аудита |
| Аудит служб сертификации | Нет аудита |
| Аудит сведений об общем файловом ресурсе | Нет аудита |
| Аудит общих папок | Нет аудита |
| Аудит файловой системы | Нет аудита |
| Аудит подключения платформы фильтрации | Нет аудита |
| Аудит отбрасывания пакетов платформой фильтрации | Нет аудита |
| Аудит работы с дескрипторами | Нет аудита |
| Аудит объектов ядра | Нет аудита |
| Аудит других событий доступа к объектам | Нет аудита |
| Аудит реестра | Нет аудита |
| Аудит диспетчера учетных записей безопасности | Нет аудита |
| **Изменение политики** |  |
| Аудит изменения политики аудита | Успех, отказ |
| Аудит изменения политики проверки подлинности | Успех, отказ |
| Аудит изменения политики авторизации | Нет аудита |
| Аудит изменения политики платформы фильтрации | Нет аудита |
| Аудит изменения политики на уровне правил MPSSVC | Нет аудита |
| Аудит других событий изменения политики | Нет аудита |
| **Использование прав** |  |
| Аудит использования прав, не затрагивающих конфиденциальные данные | Нет аудита |
| Аудит других событий использования прав | Нет аудита |
| Аудит использования прав, затрагивающих конфиденциальные данные | Нет аудита |
| **Система** |  |
| Аудит драйвера IPsec | Нет аудита |
| Аудит других системных событий | Нет аудита |
| Аудит изменения состояния безопасности | Нет аудита |
| Аудит расширения системы безопасности | Нет аудита |
| Аудит целостности системы | Успех, отказ |
| **Аудит доступа к глобальным объектам** |  |
| Файловая система | Не настроено |
| Реестр | Не настроено |
| **QoS на основе политики** | Не определено |
| **Административные шаблоны** |  |
| **Компоненты Windows** |  |
| **Internet Explorer** | **Все параметры раздела и его подразделов перевести в состояние "Отключена", за исключением нижеприведенных** |
| Включить строку меню по умолчанию | Включена |
| Выключить автоматическое восстановление после сбоя | Не задана |
| Выключить повторное открытие последнего сеанса просмотра | Не задана |
| Разрешить режим завершения работы Internet Explorer 8 | Не задана |
| Выключить быстрые вкладки | Не задана |
| Выключить предложение для всех служб, установленных пользователем | Не задана |
| Выключить меню быстрого выбора | Не задана |
| **Панель управления браузером** |  |
| **Вкладка "Безопасность"** |  |
| Включить предупреждение о несоответствии адреса сертификата | Не задана |
| **Параметры браузера** |  |
| **Параметры экрана** |  |
| Запретить выбор размера текста по умолчанию | Не задана |
| **NetMeeting** |  |
| Запретить удаленное управление рабочим столом | Включен |
| **Parental Controls** |  |
| Make Parental Controls control panel visible on a Domain | Отключена |
| **Password Synchronization** |  |
| Turn on extensive logging for Password Synchronization | Отключена |
| Set the number of synchronization retries for servers running Password Synchronization | Отключена |
| Turn on the Windows to NIS password synchronization for users that have been migrated to Active Directory | Отключена |
| Set the interval between synchronization retries for Password Synchronization | Отключена |
| **Server for NIS** |  |
| Turn on extensive logging for Active Directory Domain Services domain controllers that are running Server for NIS | Отключена |
| Set the map update interval for NIS subordinate servers | Отключена |
| **Windows Media Center** |  |
| Не запускать Windows Media Center | Включена |
| **Windows Messenger** |  |
| Не запускать Windows Messenger автоматически при входе. | Включена |
| Запретить запуск Windows Messenger | Включена |
| **Windows PowerShell** |  |
| Включить выполнение сценариев | Отключена |
| **Windows SideShow** |  |
| Отключить автоматическое пробуждение | Включена |
| Отключить Windows SideShow | Включена |
| Требовать ПИН-код для доступа к данным на устройствах с микропрограммами Майкрософт | Отключена |
| Удалять данные с устройств, использующих микропрограммы Майкрософт, при завершении сеанса пользователя. | Отключена |
| **Анализ стабильности Windows** |  |
| Настройка WMI-поставщиков стабильности системы | Включен |
| **Архивация данных** |  |
| **Клиент** |  |
| Запретить пользователям запускать программу "Состояние и настройка архивации" | Отключена |
| Запретить архивацию на локальные диски | Отключена |
| Запретить архивацию в сетевое расположение | Отключена |
| Запретить архивацию на оптические носители (CD/DVD) | Отключена |
| Отключить возможность архивации файлов данных | Отключена |
| Отключить функции восстановления | Отключена |
| Отключить возможность создания образа системы | Отключена |
| **Сервер** |  |
| Разрешить только архивацию системы | Отключена |
| Запретить архивацию данных в локальном хранилище | Отключена |
| Запретить архивацию данных в общую сетевую папку | Отключена |
| Запретить архивацию данных на оптические носители | Отключена |
| Запретить архивацию данных однократного запуска | Отключена |
| **Биометрия** |  |
| Разрешить использование биометрии | Отключена |
| Разрешить пользователям выполнять вход в систему с использованием биометрии | Отключена |
| Разрешить пользователям домена выполнять вход в систему с использованием биометрии | Отключена |
| Время ожидания для событий функции быстрого переключения пользователей | Отключена |
| **Встроенная справка** |  |
| Отключение активной справки | Включена |
| **Гаджеты рабочего стола** |  |
| Отключить гаджеты рабочего стола | Включена |
| Переопределить ссылку на дополнительные гаджеты | Отключена |
| Ограничить распаковку и установку гаджетов, не подписанных цифровой подписью. | Включена |
| Отключить установленные пользователем гаджеты рабочего стола | Включена |
| **Диспетчер окон рабочего стола** |  |
| **Цвет рамки окна** |  |
| Укажите цвет по умолчанию | Отключена |
| Не разрешать смену цветов | Включена |
| Не разрешать анимацию окон | Включена |
| Не разрешать композицию рабочего стола | Включена |
| Не разрешать вызов Flip3D | Включена |
| **Диспетчер системных ресурсов** |  |
| Включить функцию учета ДСР | Отключена |
| Адреса электронной почты для рассылки уведомлений | Отключена |
| Интервал времени (в минутах) для записи данных учета | Отключена |
| Адрес SMTP-сервера для рассылки уведомлений | Отключена |
| **Домашняя группа** |  |
| Запретить присоединение компьютера к домашней группе | Включена |
| **Защита доступа к сети** |  |
| Разрешать поддержку компонента "Клиент системы ограничений 802.1x" клиентом защиты доступа к сети | Отключена |
| **Защитник Windows** |  |
| Включить обновление определений с помощью WSUS и Windows Update | Отключена |
| Включить обновление определений через WSUS и Центр Майкрософт по защите от вредоносных программ | Отключена |
| Проверять новые подписи перед запланированным сканированием | Отключена |
| Отключить Защитника Windows | Включена |
| Отключить наблюдение в реальном времени | Включена |
| Отключить постоянные действия | Включена |
| Настроить отчеты Microsoft SpyNet | Отключена |
| **Звукозапись** |  |
| Запретить выполнение программы «Звукозапись» | Включена |
| **Календарь Windows** |  |
| Выключить календарь Windows. | Включена |
| **Каналы RSS** |  |
| Включить обычную проверку подлинности веб-каналов через HTTP | Включена |
| Отключить синхронизацию веб-каналов и веб-фрагментов в фоновом режиме | Включена |
| Отключить загрузку вложений | Включена |
| Отключить добавление и удаление веб-каналов и веб-фрагментов | Включена |
| Отключить обнаружение веб-каналов и веб-фрагментов | Включена |
| Отключить список веб-каналов | Включена |
| **Настройки презентации** |  |
| Выключить настройки презентации Windows | Включена |
| **Обозреватель игр** |  |
| Выключить загрузку сведений об игре | Включена |
| Отключить обновления игр | Включена |
| Не отслеживать время последнего сеанса игр в папке «Игры» | Включена |
| **Отчеты об ошибках Windows** |  |
| **Параметры расширенного отчета об ошибках** |  |
| Отправлять отчет о незапланированном завершении работы | Отключена |
| Параметры по умолчанию для отчетов приложений | Отключена |
| Список приложений, ошибки которых никогда не включать в отчет | Отключена |
| Список приложений, ошибки которых всегда включать в отчет | Отключена |
| Сообщать об ошибках операционной системы | Отключена |
| Настроить архив отчетов | Отключена |
| Настроить корпоративные отчеты об ошибках Windows | Отключена |
| Список исключаемых приложений | Отключена |
| Настроить очередь отчетов | Отключена |
| **Разрешение** |  |
| Настроить параметры разрешения | Включена |
| Игнорировать настроенные параметры разрешения | Отключена |
| Настроить разрешение по умолчанию | Отключена |
| Настроить отчеты об ошибках | Отключена |
| Отображать уведомления об ошибках | Отключена |
| Отключить отчеты об ошибках Windows | Включена |
| Запретить отображение интерфейса пользователя для критических ошибок | Отключена |
| Отключить запись в журнал | Отключена |
| Не отправлять дополнительные данные | Отключена |
| **Параметры входа Windows** |  |
| Отображать при входе пользователя сведения о предыдущих попытках входа | Отключена |
| Сообщать, когда сервер входа недоступен при входе пользователя | Отключена |
| Разрешить или запретить программам использование специального сочетания клавиш | Отключена |
| **Параметры завершения работы** |  |
| Отключить старый интерфейс удаленного завершения работы | Отключена |
| Тайм-аут для зависших сеансов входа при завершении работы | Отключена |
| **Пересылка событий** |  |
| ForwarderResourceUsage | Отключена |
| Настроить адрес сервера, интервал обновления и центр, выдающий сертификат для диспетчера подписки | Отключена |
| **Планировщик заданий** |  |
| Запретить обзор | Включена |
| Скрыть флажок дополнительных свойств в мастере планирования заданий | Включена |
| Запретить перетаскивание с помощью мыши | Включена |
| Запретить запуск и завершение задач | Включена |
| Скрывать страницы свойств | Включена |
| Запретить создание новых заданий | Включена |
| Запретить удаление заданий | Включена |
| **Планшетный ПК** |  |
| **Аппаратные кнопки** |  |
| Запретить сопоставление кнопок «Назад» и ESC | Отключена |
| Запретить запуск приложения | Отключена |
| Запретить режим нажатия и удерживания | Отключена |
| Отключить аппаратные кнопки | Отключена |
| **Курсоры** |  |
| Отключить реакцию пера | Отключена |
| **Обучение пользованию пером на планшетном ПК** |  |
| Отключить обучение пользованию пером на планшетном ПК | Отключена |
| **Панель ввода** |  |
| Отключение интеграции автозаполнения и панели ввода | Отключена |
| Запретить отображение значка панели ввода | Отключена |
| Для ввода планшетным пером не отображать значок панели ввода | Отключена |
| Для сенсорного ввода не отображать значок панели ввода | Отключена |
| Переключить на жесты стандарта упрощенного китайского письма (КНР) | Отключена |
| Отключить безопасность ввода паролей в панели ввода | Отключена |
| Отключить прогнозирование текста | Отключена |
| Включить редко используемые символы китайского языка, кандзи или ханджа. | Отключена |
| Отключить удобные и Z-образные жесты вычеркивания | Отключена |
| **Персонализация рукописного ввода** |  |
| Отключить автоматическое обучение | Отключена |
| **Поведение UX пера** |  |
| Запретить режим многофункционального пера | Отключена |
| **Режим обучения пользованию многофункциональным пером** |  |
| Запретить режим обучения пользованию многофункциональными перьями | Отключена |
| **Сенсорный ввод** |  |
| Отключить сенсорное панорамирование | Отключена |
| Отключить сенсорный ввод планшетного ПК | Отключена |
| **Стандартные программы** |  |
| Запретить запуск игры «Инкбол» | Включена |
| Запретить запуск журнала Windows | Отключена |
| Запретить печать в составитель заметок журнала | Включена |
| Запретить запуск инструмента «Ножницы» | Включена |
| **Политики автозапуска** |  |
| Отключить автозапуск | Включена (Все устройства) |
| Не устанавливать флажок «Всегда выполнять выбранное действие» | Отключена |
| Отключить автозапуск устройств, не являющихся томами | Включена |
| Вариант работы автозапуска по умолчанию | Включена (Не исполнять команды автозапуска) |
| **Пользовательский интерфейс учетных данных** |  |
| Требовать достоверный путь для входа в учетную запись | Включена |
| Отображать учетные записи администратора при повышении уровня прав | Отключена |
| **Почта Windows** |  |
| Выключить функции сообществ | Включена |
| Выключить приложение Почта Windows | Включена |
| **Проводник Windows** |  |
| **Предыдущие версии** |  |
| Запретить восстановление предыдущих версий из резервных копий | Включена |
| Скрыть список предыдущих версий для локальных файлов | Включена |
| Запретить восстановление локальных предыдущих версий | Включена |
| Скрыть список предыдущих версий для удаленных файлов | Включена |
| Запретить восстановление удаленных предыдущих версий | Включена |
| Скрыть предыдущие версии файлов в архиве | Включена |
| Проверить перед перенаправлением, указывают ли старый и новый конечный объект перенаправления папки на один общий ресурс | Отключена |
| Отключить прямую привязку к IPropertySetStorage без промежуточных уровней. | Отключена |
| Отключить числовое упорядочивание проводника Windows | Отключена |
| Отключить защищенный режим протокола оболочки | Отключена |
| Установить ссылку на веб-страницу поддержки | Отключена |
| Отключить предотвращение выполнения данных для проводника | Отключена |
| Отключить закрытие кучи по причине повреждения | Отключена |
| **Программа обновления Windows Anytime Upgrade** |  |
| Предотвращает запуск программы обновления Windows Anytime Upgrade. | Включена |
| **Программа по улучшению качества программного обеспечения Windows** |  |
| Разрешить перенаправление отчетов программы по улучшению качества программного обеспечения Windows | Отключена |
| Помечать данные программы по улучшению качества программного обеспечения Windows идентификатором исследования | Отключена |
| **проигрыватель Windows Media** |  |
| Запретить автоматические обновления | Включена |
| Не отображать диалоговые окна первого использования | Включена |
| Запретить сглаживание изображения | Включена |
| Запретить общий доступ к файлам мультимедиа | Включена |
| Не создавать ярлык на панели быстрого запуска | Включена |
| Не создавать ярлык на рабочем столе | Включена |
| **Просмотр событий** |  |
| Программа Events.asp | Отключена |
| Параметры командной строки программы Events.asp | Отключена |
| URL-адрес программы Events.asp | Отключена |
| **Расположение и датчики** |  |
| Отключить расположение со сценариями | Отключена |
| Отключить расположение | Отключена |
| Отключить датчики | Отключена |
| **Сетевой проектор** |  |
| Отсоединить сетевой проектор | Отключена |
| Настройка порта сетевого проектора | Отключена |
| **Служба журнала событий** |  |
| **Безопасность** |  |
| Путь файла журнала | Отключена |
| Максимальный размер журнала (КБ) | Отключена |
| При заполнении автоматически архивировать | Отключена |
| Доступ к журналу | Отключена |
| Сохранять старые события | Отключена |
| **Настройка** |  |
| Включить ведение журнала | Включена |
| Путь файла журнала | Отключена |
| Максимальный размер журнала (КБ) | Отключена |
| При заполнении автоматически архивировать | Отключена |
| Доступ к журналу | Отключена |
| Сохранять старые события | Отключена |
| **Приложение** |  |
| Путь файла журнала | Отключена |
| Максимальный размер журнала (КБ) | Отключена |
| При заполнении автоматически архивировать | Отключена |
| Доступ к журналу | Отключена |
| Сохранять старые события | Отключена |
| **Система** |  |
| Путь файла журнала | Отключена |
| Максимальный размер журнала (КБ) | Отключена |
| При заполнении автоматически архивировать | Отключена |
| Доступ к журналу | Отключена |
| Сохранять старые события | Отключена |
| **Служба установки ActiveX** |  |
| Веб-сайты, разрешенные для установки элементов управления ActiveX | Отключена |
| Политика установки ActiveX для сайтов в доверенных зонах | Отключена |
| **Службы IIS** |  |
| Предотвратить установку служб IIS | Включена |
| **Службы удаленных рабочих столов** |  |
| **Клиент подключения к удаленному рабочему столу** |  |
| Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию | Включена |
| Разрешать RDP-файлы от неизвестных издателей | Отключена |
| Запретить сохранение паролей | Включена |
| Указать отпечатки SHA1 сертификатов, представляющих доверенных издателей RDP | Отключена |
| Запрашивать учетные данные на клиентском компьютере | Отключена |
| Настройка проверки подлинности клиента на сервере | Включена (Не подключаться, если проверка подлинности не прошла) |
| **Перенаправление USB-устройств RemoteFx** |  |
| Разрешить перенаправление RDP для других поддерживаемых USB-устройств RemoteFx с этого компьютера | Отключена |
| **Лицензирование удаленных рабочих столов** |  |
| Группа безопасности сервера лицензирования | Отключена |
| Запретить повышение лицензий | Отключена |
| **Узел сеансов удаленных рабочих столов[[119]](#footnote-120)** |  |
| **Profiles** |  |
| Ограничить размер кэша всех перемещаемых профилей пользователей | Отключена |
| Установить домашний каталог пользователя служб удаленных рабочих столов | Отключена |
| Использовать обязательные профили на сервере узла сеансов удаленных рабочих столов | Отключена |
| Задать путь для перемещаемого профиля пользователя служб удаленных рабочих столов | Отключена |
| **Безопасность** |  |
| Шаблон сертификата проверки подлинности сервера | Отключена |
| Установить уровень шифрования для клиентских подключений | Отключена |
| Всегда запрашивать пароль при подключении | Включена |
| Требовать безопасное RPC-подключение | Включена |
| Требовать использования специального уровня безопасности для удаленных подключений по методу RDP | Отключена |
| Не разрешать локальным администраторам настраивать разрешения | Отключена |
| Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети | Включена |
| **Временные папки** |  |
| Не удалять временные папки при выходе | Отключена |
| Не использовать временные папки для сеанса | Отключена |
| **Лицензирование** |  |
| Использовать указанные серверы лицензирования удаленных рабочих столов | Отключена |
| Скрывать уведомления о проблемах лицензирования удаленных рабочих столов, оказывающих влияние на сервер узла сеансов удаленных рабочих столов | Отключена |
| Задать режим лицензирования узла сеансов удаленных рабочих столов | Отключена |
| **Ограничение сеансов по времени** |  |
| Задать ограничение по времени для отключенных сеансов | Отключена |
| Задать ограничение времени для активных, но бездействующих сеансов служб удаленных рабочих столов | Отключена |
| Задать ограничение по времени для активных сеансов служб удаленных рабочих столов | Отключена |
| Завершать сеанс при достижении ограничения по времени | Отключена |
| Задать предел времени для выхода из сеансов RemoteApp | Отключена |
| **Перенаправление принтеров** |  |
| Не устанавливать используемый по умолчанию принтер клиента в качестве принтера для сеанса | Отключена |
| Не разрешать перенаправление клиентских принтеров | Отключена |
| Использовать в первую очередь драйвер принтера Easy Print удаленного рабочего стола | Отключена |
| Задать поведение сервера узла сеансов удаленных рабочих столов при выборе резервного драйвера принтера | Отключена |
| Перенаправлять только используемый по умолчанию принтер клиента | Отключена |
| **Перенаправление устройств и ресурсов** |  |
| Разрешить перенаправление воспроизведения звука и видео | Отключена |
| Разрешить перенаправление звукозаписи | Отключена |
| Ограничить качество воспроизведения звука | Отключена |
| Не разрешать перенаправление буфера обмена | Отключена |
| Не разрешать перенаправление COM-портов | Отключена |
| Не разрешать перенаправление дисков | Отключена |
| Не разрешать перенаправление LPT-портов | Отключена |
| Не разрешать перенаправление поддерживаемых устройств Plug and Play | Отключена |
| Не разрешать перенаправление устройства чтения смарт-карт | Отключена |
| Разрешить перенаправление часового пояса | Отключена |
| **Подключения[[120]](#footnote-121)** |  |
| Автоматическое переподключение | Отключена |
| Разрешать удаленное подключение с использованием служб удаленных рабочих столов | Включено |
| Запретить завершение консольного сеанса администратора | Отключена |
| Настроить интервал проверки активности подключения | Включена (5) |
| Ограничить количество подключений | Включена (3) |
| Устанавливает правила удаленного управления для пользовательских сеансов служб удаленных рабочих столов | Отключена |
| Ограничить пользователей службы удаленных рабочих столов одним сеансом служб удаленных рабочих столов | Отключена |
| Разрешать удаленный запуск любых программ | Отключена |
| Отключить планирование ЦП со справедливым разделением | Отключена |
| **Посредник подключений к удаленному рабочему столу** |  |
| Присоединиться к посреднику подключений к удаленному рабочему столу | Отключена |
| Настроить имя фермы посредника подключений к удаленному рабочему столу | Отключена |
| Использовать перенаправление IP-адреса | Отключена |
| Настроить имя сервера посредника подключений к удаленному рабочему столу | Отключена |
| Использовать балансировку нагрузки посредника подключений к удаленному рабочему столу | Отключена |
| **Совместимость приложений** |  |
| Отключить совместимость служб удаленных рабочих столов с установщиком Windows | Отключена |
| Включить IP-виртуализацию удаленных рабочих столов | Отключена |
| Выбрать сетевой адаптер, используемый для IP-виртуализации удаленных рабочих столов | Отключена |
| Не использовать IP-адрес сервера узла сеансов удаленных рабочих столов, если виртуальный IP-адрес недоступен | Отключена |
| **Среда удаленных сеансов** |  |
| Наибольшая глубина цвета | Отключена |
| Принудительная отмена фонового рисунка удаленного рабочего стола | Отключена |
| Ограничить максимальное разрешение экрана | Отключена |
| Ограничить максимальное количество мониторов | Отключена |
| Удалить элемент «Отключение сеанса» из диалога завершения работы | Отключена |
| Удалить элемент «Безопасность Windows» из меню «Пуск» | Отключена |
| Задание алгоритма сжатия для данных RDP | Отключена |
| Оптимизировать визуальные эффекты для сеансов служб удаленных рабочих столов | Отключена |
| Запускать программу при подключении | Отключена |
| Всегда отображать рабочий стол при подключении | Отключена |
| Разрешить композицию рабочего стола для сеансов удаленных рабочих столов | Отключена |
| Не разрешать сглаживание шрифтов | Отключена |
| **Службы федерации Active Directory** |  |
| Отключить службу федерации | Отключена |
| **Смарт-карта** |  |
| Разрешить сертификаты без атрибута сертификата расширенного использования ключа | Отключена |
| Показывать экран встроенной разблокировки при входе | Отключена |
| Разрешить ключи подписей для входа | Отключена |
| Разрешить сертификаты с истекшим сроком действия. | Отключена |
| Включить распространение сертификатов со смарт-карты | Отключена |
| Настроить очистку корневого сертификата | Отключена |
| Включить распространение корневого сертификата со смарт-карты | Отключена |
| Запретить возвращение текстовых PIN-кодов диспетчером учетных данных | Отключена |
| Разрешить использование сертификатов ECC для входа и проверки подлинности | Отключена |
| Отфильтровывать дубликаты сертификатов входа | Отключена |
| Принудительно считывать со смарт-карты все сертификаты | Отключена |
| Показывать строку при блокировке смарт-карты | Отключена |
| Изменить хранящееся в сертификате имя субъекта | Отключена |
| Включить службу самонастраивающихся устройств для смарт-карт | Отключена |
| Уведомлять об успешной установке драйвера смарт-карт | Отключена |
| Разрешить подсказку имени пользователя | Отключена |
| **Совместимость приложений** |  |
| Запрещение доступа к 16-разрядным приложениям. | Отключена |
| Удаление страницы «Свойства совместимости программ» | Отключена |
| Отключить дистанционное отслеживание приложений | Отключена |
| Отключение обработчика совместимости приложений | Отключена |
| Отключение помощника по совместимости программ | Отключена |
| Отключить сборщик перечней программ | Отключена |
| Отключить обработчик совместимости SwitchBack | Отключена |
| Отключить средство записи действий по воспроизведению неполадок | Отключена |
| **Удаленная оболочка Windows** |  |
| Разрешить доступ к удаленной оболочке | Отключена |
| Тайм-аут простоя | Отключена |
| MaxConcurrentUsers | Отключена |
| Максимальный объем памяти в мегабайтах для одной оболочки | Отключена |
| Максимальное количество процессов для одной оболочки | Отключена |
| Максимальное число удаленных оболочек для одного пользователя | Отключена |
| Таймаут оболочки |  |
| **Удаленное управление Windows** |  |
| **Клиент службы удаленного управления Windows** |  |
| Разрешить обычную проверку подлинности | Отключена |
| Разрешить проверку подлинности CredSSP | Отключена |
| Разрешить незашифрованный трафик | Отключена |
| Запретить краткую проверку подлинности | Отключена |
| Запретить проверку подлинности по протоколу Kerberos. | Отключена |
| Запретить проверку подлинности согласованием | Отключена |
| Надежные сайты | Отключена |
| **Служба удаленного управления Windows** |  |
| Разрешить автоматическую настройку прослушивателей | Отключена |
| Разрешить обычную проверку подлинности | Отключена |
| Разрешить проверку подлинности CredSSP | Отключена |
| Разрешить незашифрованный трафик | Отключена |
| Задайте уровень усиления защиты токена привязки канала | Отключена |
| Запретить проверку подлинности по протоколу Kerberos | Отключена |
| Запретить проверку подлинности согласованием | Отключена |
| Включить HTTP-прослушиватель совместимости | Отключена |
| Включить HTTPS-прослушиватель совместимости | Отключена |
| **Управление цифровыми правами Windows Media** |  |
| Запретить доступ к Интернету для Windows Media DRM | Включена |
| **Установщик Windows** |  |
| Разрешить обзор источника при повышенных правах | Отключена |
| Разрешить использование носителей при повышенных правах | Отключена |
| Разрешить применение пакетов исправлений при установке с повышенными правами | Отключена |
| Всегда устанавливать с повышенными правами | Отключена |
| Запретить диспетчер перезапуска | Отключена |
| Удалить диалоговое окно обзора нового источника | Отключена |
| Запретить оптимизацию применения пакетов исправлений | Отключена |
| Отключить ведение журнала с помощью параметров пакета | Отключена |
| Запретить установщик Windows | Отключена |
| Запретить пакеты исправлений | Отключена |
| Запретить откат | Отключена |
| Разрешить администраторам установку в сеансе службы удаленных рабочих столов | Включена |
| Разрешить пользователям изменять параметры установки | Отключена |
| Ведение журнала событий | Включена |
| Запретить пользователям, не являющимися администраторами, устанавливать обновления, подписанные изготовителем программы | Отключена |
| Запретить удаление обновлений | Отключена |
| Отключить создание контрольных точек восстановления системы | Отключена |
| Запретить установки пользователям | Отключена |
| Задать обязательные правила обновления компонентов | Отключена |
| Максимальный размер кэша базисных файлов | Отключена |
| Отключить запрос безопасности IE для сценариев установщика Windows | Отключена |
| Кэшировать файлы преобразования в безопасном месте на рабочей станции | Отключена |
| **Цветовая система Windows Color System** |  |
| Запретить установку и удаление цветовых профилей | Отключена |
| **Центр мобильности Windows** |  |
| Отключить центр мобильности Windows | Включена[[121]](#footnote-122) |
| **Центр обеспечения безопасности** |  |
| Включить центр обеспечения безопасности (только для компьютеров в домене) | Отключена |
| **Центр обновления Windows** |  |
| Не отображать параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows» | Включена |
| Не задавать по умолчанию параметр «Установить обновления и завершить работу» в диалоговом окне «Завершение работы Windows» | Включена |
| Разрешить управлению электропитанием центра обновления Windows выводить систему из спящего режима для установки запланированных обновлений | Отключена |
| Настройка автоматического обновления | Отключена |
| Указать размещение службы обновлений Майкрософт в интрасети | Отключена |
| Частота поиска автоматических обновлений | Отключена |
| Turn off the upgrade to the latest version of Windows through Windows Update | Включена |
| Разрешать пользователям, не являющимся администраторами, получать уведомления об обновлениях | Отключена |
| Включить уведомления о наличии программ | Отключена |
| Разрешить немедленную установку автоматических обновлений | Отключена |
| Включить рекомендуемые обновления через автоматическое обновление | Отключена |
| Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи | Включена |
| Повторный запрос для перезагрузки при запланированных установках | Отключена |
| Задержка перезагрузки при запланированных установках | Отключена |
| Перенос запланированных автоматических установок обновлений | Отключена |
| Разрешить клиенту присоединение к целевой группе | Отключена |
| Разрешить прием обновлений с подписью из службы обновления Майкрософт в интрасети | Отключена |
| **Цифровой ящик** |  |
| Не разрешать работу цифрового ящика | Включена |
| **Шифрование диска BitLocker** |  |
| **Диски операционной системы** |  |
| Обязательная дополнительная проверка подлинности при запуске | Отключена |
| Требовать дополнительную проверку подлинности при запуске (Windows Server 2008) | Отключена |
| Разрешить использование улучшенных ПИН-кодов при запуске компьютера | Отключена |
| Установить минимальную длину ПИН-кода для запуска | Отключена |
| Выбор методов восстановления дисков операционной системы, защищенных с помощью BitLocker | Отключена |
| Настройка профиля проверки платформы TPM | Отключена |
| **Жесткие диски с данными** |  |
| Настроить использование смарт-карт на фиксированных дисках с данными | Отключена |
| Запретить запись на фиксированные диски, не защищенные BitLocker | Отключена |
| Разрешить доступ к фиксированным дискам с данными, защищенным с помощью BitLocker, из более ранних версий Windows | Отключена |
| Настроить использование паролей для фиксированных дисков с данными | Отключена |
| Выбор методов восстановления жестких дисков, защищенных с помощью BitLocker | Отключена |
| **Съемные диски с данными** |  |
| Управление использованием BitLocker для съемных дисков | Отключена |
| Настроить использование смарт-карт на съемных дисках с данными | Отключена |
| Запретить запись на съемные диски, не защищенные BitLocker | Отключена |
| Разрешить доступ к съемным дискам с данными, защищенным с помощью BitLocker, из более ранних версий Windows | Отключена |
| Настроить использование паролей для съемных дисков с данными | Отключена |
| Выбор методов восстановления съемных дисков, защищенных с помощью BitLocker | Отключена |
| Хранить сведения о восстановлении BitLocker в доменных службах Active Directory (Windows Server 2008) | Отключена |
| Выберите папку по умолчанию для пароля восстановления | Отключена |
| Выберите способ восстановления пользователями дисков, защищенных с помощью BitLocker (Windows Server 2008) | Отключена |
| Выберите метод шифрования диска и стойкость шифра | Отключена |
| Укажите уникальные идентификаторы для организации | Отключена |
| Запретить перезапись памяти при перезагрузке | Отключена |
| Проверить согласованность правил использования сертификатов смарт-карт | Отключена |
| **Панель управления** |  |
| **Учетные записи пользователей** |  |
| Применить изображение по умолчанию для учетной записи пользователя ко всем пользователям | Отключена |
| **Язык и региональные стандарты** |  |
| Ограничить язык интерфейса Windows для всех зарегистрированных пользователей | Отключена |
| Подавление языка интерфейса на уровне пользователя языком системного интерфейса | Отключена |
| **Принтеры** |  |
| Печать на основе использования веб | Отключена |
| Автоматическая публикация новых принтеров в Active Directory | Отключена |
| Особый URL-адрес службы поддержки в левой панели папки принтеров | Отключена |
| Расширить подключения указания и печати для поиска обновлений Windows | Отключена |
| Мастер установки принтеров — страница сканирования сети (управляемая сеть) | Отключена |
| Всегда обрабатывать задания печати на сервере | Отключена |
| Разрешить очистку опубликованных принтеров | Отключена |
| Запретить установку принтеров, использующих работающие в режиме ядра драйверы | Отключена |
| Мастер установки принтеров — страница сканирования сети (неуправляемая сеть) | Отключена |
| Использовать только функцию указания и печати для пакета | Отключена |
| Функция указания и печати для пакетов - Разрешенные серверы | Отключена |
| Размещение компьютера | Отключена |
| Заполнение строки поиска принтеров | Отключена |
| Ограничения указания и печати | Отключена |
| Выполнить драйверы принтеров в изолированных процессах | Отключена |
| Переопределить параметр совместимости выполнения драйвера печати, назначенный драйвером печати | Отключена |
| Обзор принтеров | Отключена |
| Удалять принтеры, которые не были автоматически повторно опубликованы | Отключена |
| Интервал очистки Active Directory | Отключена |
| Приоритет потока при очистке Active Directory | Отключена |
| Повторы при очистке Active Directory | Отключена |
| Записывать события контакта службы очистки каталогов | Отключена |
| Разрешить публикацию принтеров | Отключена |
| Разрешить диспетчеру печати добавление новых клиентских подключений | Отключена |
| Проверять состояние публикации | Отключена |
| **Сеть** |  |
| **BranchCache** |  |
| Включить BranchCache | Отключена |
| Включить режим распределенного кэша BranchCache | Отключена |
| Включить режим размещенного кэша BranchCache | Отключена |
| Настройка BranchCache для сетевых файлов | Отключена |
| Установить процент дискового пространства, используемого для кэша клиентского компьютера | Отключена |
| **Службы одноранговых сетей Майкрософт** |  |
| **Протокол однорангового разрешения имен** |  |
| **Глобальные облака** |  |
| Отключение многоадресной загрузки | Отключена |
| Отключить создание PNRP-облака | Отключена |
| Настроить PNRP-облако только для разрешения | Отключена |
| Задать сервер инициализации | Отключена |
| **Локальные облака сайта** |  |
| Отключение многоадресной загрузки | Отключена |
| Отключить создание PNRP-облака | Отключена |
| Настроить PNRP-облако только для разрешения | Отключена |
| Задать сервер инициализации | Отключена |
| **Локальные облака связи** |  |
| Отключение многоадресной загрузки | Отключена |
| Отключить создание PNRP-облака | Отключена |
| Настроить PNRP-облако только для разрешения | Отключена |
| Задать сервер инициализации | Отключена |
| Отключить проверку надежности пароля для группирования одноранговой сети | Отключена |
| Отключение служб одноранговых сетей Майкрософт | Отключена |
| **DNS-клиент** |  |
| Разрешить добавление DNS-суффиксов к запросам несоответствующих составных имен. | Отключена |
| DNS-суффикс подключения | Отключена |
| Уровень регрессии основного DNS-суффикса | Отключена |
| DNS-серверы | Отключена |
| Основной DNS-суффикс | Отключена |
| Регистрировать DNS-записи с DNS-суффиксом подключения | Отключена |
| Регистрировать PTR-записи | Отключена |
| Динамическое обновление | Отключена |
| Заменять адреса при конфликтах | Отключена |
| Интервал обновления регистрации | Отключена |
| Установить TTL для A- и PTR-записей | Отключена |
| Порядок просмотра DNS-суффиксов | Отключена |
| Уровень безопасности обновления | Отключена |
| Обновлять зоны доменов верхнего уровня | Отключена |
| Регрессирование основного DNS-суффикса | Отключена |
| Отключить многоадресное разрешение имен | Отключена |
| **SNMP** |  |
| Сообщества | Отключена |
| Разрешенные диспетчеры | Отключена |
| Ловушки для публичного сообщества | Отключена |
| **Windows Connect Now** |  |
| Запретить доступ к мастерам Windows Connect Now | Включена |
| Настройка параметров беспроводной сети с помощью Windows Connect Now | Отключена |
| **Автономные файлы** |  |
| Разрешить автономный доступ ко вложенным папкам | Отключена |
| Административно назначенные автономные файлы | Отключена |
| Настроить фоновую синхронизацию | Отключена |
| Ограничить размер дискового пространства, используемого автономными файлами | Отключена |
| Нестандартные действия при отключении от сервера | Отключена |
| Размер кэша по умолчанию | Отключена |
| Разрешить или запретить использование автономных файлов | Отключена |
| Шифрование кэша автономных файлов | Отключена |
| Уровень регистрации событий | Отключена |
| Исключить файлы из числа кэшируемых | Отключена |
| Некэшируемые файлы | Отключена |
| Действие при отключении от сервера | Отключена |
| Запретить использование папки «Автономные файлы» | Включена |
| Запретить пользовательскую настройку автономных файлов | Включена |
| Удалить «Сделать доступными автономно» | Включена |
| Запретить применение «Сделать доступными автономно» для этих файлов и папок | Отключена |
| Отключить всплывающие напоминания | Включена |
| Включить прозрачное кэширование | Отключена |
| При выходе из системы удалять локальную копию автономных файлов пользователя | Включена |
| Включить экономичное использование административно назначенных автономных файлов | Отключена |
| Частота появления всплывающих напоминаний | Отключена |
| Исходное время отображения всплывающих напоминаний | Отключена |
| Время отображения всплывающих напоминаний | Отключена |
| Настроить режим медленного подключения | Отключена |
| Настроить скорость медленного подключения | Отключена |
| Синхронизировать перед выходом из системы | Отключена |
| Синхронизировать автономные файлы при входе в систему | Отключена |
| Синхронизировать автономные файлы перед приостановкой | Отключена |
| **Индикатор состояния сетевого подключения** |  |
| Адрес DNS-сервера организации, который используется для проверки | Отключена |
| Имя сайта DNS-сервера организации, которое используется для проверки | Отключена |
| Список префиксов сайтов организации | Отключена |
| URL-адрес, используемый для проверки работы веб-сайта организации | Отключена |
| URL-адрес определения расположения домена | Отключена |
| **Обнаружение топологии связи (Link-Layer)** |  |
| Включает драйвер отображения ввода/вывода (LLTDIO) | Отключена |
| Включить драйвер «Ответчика» (RSPNDR) | Отключена |
| **Параметры TCP/IP** |  |
| **Параметры** |  |
| Состояние масштабируемой эвристики Windows | Отключена |
| **Технологии туннелирования IPv6** |  |
| Имя ретранслятора 6to4 | Отключена |
| Интервал разрешения имен ретранслятора 6to4 | Отключена |
| Состояние 6to4 | Отключена |
| Состояние IP-HTTPS | Отключена |
| Имя маршрутизатора ISATAP | Отключена |
| Состояние ISATAP | Отключена |
| Порт клиента Teredo | Отключена |
| Квалификация Teredo по умолчанию | Отключена |
| Частота обновления Teredo | Отключена |
| Имя сервера Teredo | Отключена |
| Состояние Teredo | Отключена |
| **Параметры настройки SSL** |  |
| Порядок комплектов шифров SSL | Отключена |
| **Планировщик пакетов QoS** |  |
| **Значение DSCP для не соответствующих пакетов** |  |
| Тип службы Best effort | Отключена |
| Тип службы Controlled load | Отключена |
| Тип службы Guaranteed | Отключена |
| Тип службы Network control | Отключена |
| Тип службы Qualitative | Отключена |
| **Значение DSCP для соответствующих пакетов** |  |
| Тип службы Best effort | Отключена |
| Тип службы Controlled load | Отключена |
| Тип службы Guaranteed | Отключена |
| Тип службы Network control | Отключена |
| Тип службы Qualitative | Отключена |
| **Значение приоритета второго уровня** |  |
| Тип службы Best effort | Отключена |
| Тип службы Controlled load | Отключена |
| Тип службы Guaranteed | Отключена |
| Тип службы Network control | Отключена |
| Не соответствующие пакеты | Отключена |
| Тип службы Qualitative | Отключена |
| Ограничение ожидающих обработки пакетов | Отключена |
| Ограничить резервируемую пропускную способность | Отключена |
| Задать разрешение таймера | Отключена |
| **Сервер Lanman** |  |
| Публикация хэша для службы BranchCache | Отключена |
| **Сетевые подключения** |  |
| **Брандмауэр Windows** |  |
| **Профиль домена** |  |
| Брандмауэр Windows: Разрешить локальные исключения программ | Отключена |
| Брандмауэр Windows: Определение входящих исключений программ | Отключена |
| Брандмауэр Windows: Защита всех сетевых подключений | Отключена |
| Брандмауэр Windows: Не разрешать исключения | Отключена |
| Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам | Отключена |
| Брандмауэр Windows: Разрешить исключения ICMP | Отключена |
| Брандмауэр Windows: Разрешить ведение журнала | Отключена |
| Брандмауэр Windows: Запретить уведомления | Отключена |
| Брандмауэр Windows: Разрешить локальные исключения портов | Отключена |
| Брандмауэр Windows: «Брандмауэр Windows: Определение входящих исключений портов» | Отключена |
| Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования | Отключена |
| Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | Отключена |
| Брандмауэр Windows: Разрешить исключения входящего трафика для UPnP | Отключена |
| **Стандартный профиль** |  |
| Брандмауэр Windows: Разрешить локальные исключения программ | Отключена |
| Брандмауэр Windows: Определение входящих исключений программ | Отключена |
| Брандмауэр Windows: Защита всех сетевых подключений | Отключена |
| Брандмауэр Windows: Не разрешать исключения | Отключена |
| Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам | Отключена |
| Брандмауэр Windows: Разрешить исключения ICMP | Отключена |
| Брандмауэр Windows: Разрешить ведение журнала | Отключена |
| Брандмауэр Windows: Запретить уведомления | Отключена |
| Брандмауэр Windows: Разрешить локальные исключения портов | Отключена |
| Брандмауэр Windows: «Брандмауэр Windows: Определение входящих исключений портов» | Отключена |
| Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования | Отключена |
| Брандмауэр Windows: Разрешить исключения для входящих сообщений удаленного управления рабочим столом | Отключена |
| Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы | Отключена |
| Брандмауэр Windows: Разрешить исключения входящего трафика для UPnP | Отключена |
| Брандмауэр Windows: Разрешить обход проверки подлинности IPsec | Отключена |
| Запрет установки и настройки сетевого моста в сети DNS-домена | Отключена |
| Не показывать значок сети "только локальный доступ" | Отключена |
| Маршрутизировать весь трафик через внутреннюю сеть | Отключена |
| Запрет использования брандмауэра подключения к Интернету в DNS-домене | Отключена |
| Запрет использования общего интернет-подключения в DNS-домене | Отключена |
| Требовать повышения прав пользователей домена при задании сетевого ресурса | Отключена |
| **Фоновая интеллектуальная служба передачи (BITS)** |  |
| Запретить клиенту BITS использование кэша филиалов Windows | Отключена |
| Запретить компьютеру действовать как клиенту кэширования членов одноранговой группы BITS | Отключена |
| Запретить компьютеру действовать как серверу кэширования членов одноранговой группы BITS | Отключена |
| Разрешить кэширование членов одноранговой группы BITS | Отключена |
| Время ожидания для неактивных заданий BITS | Отключена |
| Ограничить максимальную пропускную способность сети для фоновой передачи BITS | Отключена |
| Ограничить максимальную пропускную способность сети, используемую для кэширования членов одноранговой группы BITS | Отключена |
| Ограничить максимальную пропускную способность сети, используемую службой BITS для фоновой передачи, с помощью расписания обслуживания | Отключена |
| Ограничить максимальную пропускную способность сети, используемую службой BITS для фоновой передачи, с помощью расписания работы | Отключена |
| Ограничить размер кэша членов одноранговой группы BITS | Отключена |
| Ограничить срок хранения файлов в кэше членов одноранговой группы BITS | Отключена |
| Ограничить максимальное время загрузки задания BITS | Отключена |
| Ограничить максимальное количество файлов, допустимое для одного задания BITS | Отключена |
| Ограничить максимальное количество заданий BITS для компьютера | Отключена |
| Ограничить максимальное количество заданий BITS для каждого пользователя | Отключена |
| Ограничить максимальное количество диапазонов, которые могут быть добавлены к файлу в задании BITS | Отключена |
| Устанавливает частоту обнаружения контроллера домена (DC) клиентом распределенной файловой системы (DFS) | Отключена |
| **Система** |  |
| **iSCSI** |  |
| **Безопасность iSCSI** |  |
| Не разрешать изменение секрета CHAP инициатора | Отключена |
| Не разрешать подключения без использования IPSec | Отключена |
| Не разрешать сеансы без взаимной проверки подлинности CHAP | Отключена |
| Не разрешать сеансы без односторонней проверки подлинности CHAP | Отключена |
| **Обнаружение объектов iSCSI** |  |
| Не разрешать ручную настройку конечных порталов | Отключена |
| Не разрешать ручную настройку обнаруженных объектов | Отключена |
| Не разрешать ручную настройку серверов iSNS | Отключена |
| Не разрешать добавление новых объектов при ручной настройке | Отключена |
| **Общие iSCSI** |  |
| Не разрешать изменение iqn имени инициатора | Отключена |
| Не разрешать дополнительные входы сеансов | Отключена |
| **Kerberos** |  |
| Использовать порядок поиска леса | Отключена |
| Определить сопоставления «имя узла - сфера Kerberos» | Отключена |
| Определить совместимые параметры сферы Kerberos V5 | Отключена |
| Требовать строгого соответствия конечного SPN для удаленных вызовов процедур | Отключена |
| Требовать обязательную проверку подлинности KDC | Отключена |
| **Windows HotStart** |  |
| Отключить Windows HotStart | Включена |
| **Восстановление** |  |
| Разрешить восстановление системы в состояние по умолчанию | Отключена |
| **Восстановление системы** |  |
| Отключить конфигурацию | Включена |
| Отключить восстановление системы | Включена |
| **Вход в систему** |  |
| Установка домена по умолчанию для входа | Отключена |
| Исключить поставщиков учетных данных | Отключена |
| Не обрабатывать список запуска старых программ | Отключена |
| Не обрабатывать список однократного запуска программ | Отключена |
| Отключить звук запуска Windows | Отключена |
| Скрыть точки входа для быстрого переключения пользователей | Отключена |
| Всегда классический вход в систему | Отключена |
| Не показывать окно приветствия «Приступая к работе» при входе в систему | Отключена |
| Выполнять эти программы при входе в систему | Отключена |
| Всегда ждать сеть при запуске и входе в систему | Включена |
| Всегда использовать настраиваемый фон входа в систему | Отключена |
| **Вызов удаленной процедуры** |  |
| Проверка RPC-клиентов сопоставителя конечных точек | Отключена |
| Передача расширенных сведений об ошибках | Отключена |
| Пропустить сбой делегирования | Отключена |
| Минимальное время ожидания простаивающих подключений для RPC/HTTP-подключений | Отключена |
| Ограничения для не прошедших проверку подлинности RPC-клиентов | Включен (Отсутствует) |
| Диагностические сведения о состоянии RPC | Отключена |
| **Групповая политика** |  |
| **Ведение журнала и трассировка** |  |
| Настроить ведение журнала и трассировку для предпочтений "Приложения" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Источники данных" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Устройства" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Сопоставления дисков" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Среда" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Файлы" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры папок" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Папки" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "INI-файлы" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры браузера" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Локальные пользователи и группы" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Общие сетевые ресурсы" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры сети" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Параметры электропитания" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Реестр" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Принтеры" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Региональные параметры" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Назначенные задания" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Службы" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Ярлыки" | Отключена |
| Настроить ведение журнала и трассировку для предпочтений "Главное меню" | Отключена |
| Включить политику пользователей различных лесов и перемещаемые профили пользователей | Отключена |
| Обработка политики установки программ | Отключена |
| Обработка политики дисковых квот | Отключена |
| Обработка политики восстановления EFS | Отключена |
| Обработка политики перенаправления папки  Обработка политики настройки Internet Explorer | Отключена |
|  | Отключена |
| Обработка политики IP-безопасности | Отключена |
| Обработка политики реестра. | Отключена |
| Обработка политики сценариев | Отключена |
| Обработка политики безопасности | Отключена |
| Обработка политик проводных сетей | Отключена |
| Обработка беспроводной политики | Отключена |
| Запретить интерактивным пользователям создавать данные результирующей политики (Resultant Set of Policy — RSoP) | Отключена |
| Отключить фоновое обновление групповой политики | Отключена |
| Выключение обработки локальных объектов групповой политики | Отключена |
| Запретить пользователям вызывать обновление политики компьютера | Отключена |
| Обнаружение медленных подключений для групповой политики | Включена |
| Интервал обновления групповой политики для компьютеров | Отключена |
| Интервал обновления групповой политики для контроллеров домена | Отключена |
| Всегда использовать локальные файлы ADM для редактора объектов групповой политики | Отключена |
| Отключить протоколирование RSoP | Отключена |
| Время ожидания при обработке политики загрузки | Отключена |
| Режим обработки замыкания пользовательской групповой политики | Отключена |
| Разрешить асинхронную обработку пользовательской групповой политики при входе в систему через службы удаленных рабочих столов | Отключена |
| Обработка политики расширения предпочтений "Приложения" | Не задана |
| Обработка политики расширения предпочтений "Источники данных" | Не задана |
| Обработка политики расширения предпочтений "Устройства" | Не задана |
| Обработка политики расширения предпочтений "Сопоставления дисков" | Не задана |
| Обработка политики расширения предпочтений "Среда" | Не задана |
| Обработка политики расширения предпочтений "Файлы" | Не задана |
| Обработка политики расширения предпочтений "Свойства папки" | Не задана |
| Обработка политики расширения предпочтений "Папки" | Не задана |
| Обработка политики расширения предпочтений "INI-файлы" | Не задана |
| Обработка политики расширения предпочтений "Параметры браузера" | Не задана |
| Обработка политики расширения предпочтений "Локальные пользователи и группы" | Не задана |
| Обработка политики расширения предпочтений "Общие сетевые ресурсы" | Не задана |
| Обработка политики расширения предпочтений "Сетевые параметры" | Не задана |
| Обработка политики расширения предпочтений "Параметры электропитания" | Не задана |
| Обработка политики расширения предпочтений "Реестр" | Не задана |
| Обработка политики расширения предпочтений "Принтеры" | Не задана |
| Обработка политики расширения предпочтений "Региональные параметры" | Не задана |
| Обработка политики расширения предпочтений "Назначенные задания" | Не задана |
| Обработка политики расширения предпочтений "Службы" | Не задана |
| Обработка политики расширения предпочтений "Ярлыки" | Не задана |
| Обработка политики расширения предпочтений "Главное меню" | Не задана |
| **Диагностика** |  |
| **Быстродействие Windows PerfTrack** |  |
| Включить или отключить PerfTrack | Отключена |
| **Восстановление поврежденного файла** |  |
| Настройка поведения восстановления поврежденного файла | Включена (Только выявление неполадок) |
| **Восстановление поврежденного файла MSI** |  |
| Настройка поведения восстановления поврежденного файла MSI | Включена (Только выявление неполадок) |
| **Диагностика быстродействия завершения работы Windows** |  |
| Настройки режима запуска сценария | Отключена |
| **Диагностика быстродействия загрузки Windows** |  |
| Настройки режима запуска сценария | Отключена |
| **Диагностика диска** |  |
| Диагностика диска. Настроить пользовательский текст предупреждения | Отключена |
| Диагностика диска. Настроить уровень выполнения | Отключена |
| **Диагностика производительности ждущего режима и возобновления работы Windows** |  |
| Настройки режима запуска сценария | Отключена |
| **Диагностика скорости отклика системы Windows** |  |
| Настройки режима запуска сценария | Отключена |
| **Диагностика со сценариями** |  |
| Устранение неполадок: разрешить пользователям доступ к сведениям об устранении неполадок, расположенным на серверах корпорации Майкрософт, из компонента "Устранение неполадок" панели управления (через интернет-службу устранения неполадок Windows (WOTS)) | Отключена |
| Устранение неполадок: разрешить пользователям запускать мастера устранения неполадок | Отключена |
| Настройка политики безопасности для диагностики со сценариями | Отключена |
| **Диагностика совместимости приложений** |  |
| Уведомлять о блокированных драйверах | Отключена |
| Обнаруживать сбои приложений, вызванные устаревшими COM-объектами | Отключена |
| Обнаружение сбоев приложений, вызванных устаревшими библиотеками DLL Windows. | Отключена |
| Обнаружение сбоев установки приложений | Отключена |
| Обнаружение средств установки приложений, требующих прав администратора | Отключена |
| Обнаружение приложений, неспособных запустить средства установки при включенном контроле учетных записей пользователей (UAC) | Отключена |
| **Диагностика утечки памяти Windows** |  |
| Настройка уровня выполнения сценария | Отключена |
| **Обнаружение и устранение нехватки ресурсов Windows** |  |
| Настройка уровня выполнения сценария | Отключена |
| **Отказоустойчивая куча** |  |
| Настройка уровня выполнения сценария | Отключена |
| **Средство диагностики службы технической поддержки Майкрософт** |  |
| Средство диагностики службы технической поддержки Майкрософт (MSDT): включите интерактивное взаимодействие с поставщиком поддержки | Отключена |
| Средство диагностики службы технической поддержки Майкрософт: ограничить загрузку служебных средств | Отключена |
| Средство диагностики службы технической поддержки Майкрософт: настройка режима работы | Отключена |
| Диагностика: настройка сохранения сценария | Отключена |
| Диагностика: настройка уровня выполнения сценария | Отключена |
| **Дисковые квоты** |  |
| Включить дисковые квоты | Отключена |
| Задать предел дисковой квоты | Отключена |
| Предел квоты по умолчанию и уровень предупреждения | Отключена |
| Записывать в журнал события при превышении предела квоты | Отключена |
| Записывать в журнал события, возникающие при превышении уровня предупреждения квоты | Отключена |
| Применить политику к съемным носителям | Отключена |
| **Диспетчер сервера** |  |
| Не отображать окно "Задачи начальной настройки" автоматически при входе | Включена |
| Не отображать диспетчер сервера автоматически при входе | Включена |
| Настроить интервал обновления для диспетчера сервера | Отключена |
| **Доступ к съемным запоминающим устройствам** |  |
| Время (в секундах) до принудительной перезагрузки | Отключена |
| Компакт-диски и DVD-диски: Запретить выполнение | Отключена |
| Компакт-диски и DVD-диски: Запретить чтение | Отключена |
| Компакт-диски и DVD-диски: Запретить запись | Отключена |
| Специальные классы: Запретить чтение | Отключена |
| Специальные классы: Запретить запись | Отключена |
| Накопители на гибких дисках: Запретить выполнение | Отключена |
| Накопители на гибких дисках: Запретить чтение | Отключена |
| Накопители на гибких дисках: Запретить запись | Отключена |
| Съемные диски: Запретить выполнение | Отключена |
| Съемные диски: Запретить чтение | Отключена |
| Съемные диски: Запретить запись | Отключена |
| Съемные запоминающие устройства всех классов: Запретить любой доступ | Отключена |
| Все съемные запоминающие устройства: разрешение прямого доступа в удаленных сеансах | Отключена |
| Ленточные накопители: Запретить выполнение | Отключена |
| Ленточные накопители: Запретить чтение | Отключена |
| Ленточные накопители: Запретить запись | Отключена |
| WPD-устройства: Запретить чтение | Отключена |
| WPD-устройства: Запретить запись | Отключена |
| **Доступ к устройствам Enhanced Storage** |  |
| Разрешить предоставление сертификата на устройствах Enhanced Storage | Отключена |
| Настройка списка устройств Enhanced Storage, которые могут использоваться на компьютере | Отключена |
| Настройка списка приемников команд, совместимых с IEEE 1667, которые могут использоваться на компьютере | Отключена |
| Запретить проверку подлинности устройств Enhanced Storage с помощью пароля | Отключена |
| Запретить съемные устройства, которые не являются устройствами Enhanced Storage | Отключена |
| Блокировать устройство Enhanced Storage при блокировании компьютера | Отключена |
| Разрешить только корневой USB-концентратор, подключенный к устройствам Enhanced Storage | Отключена |
| **Защита файлов Windows** |  |
| Укажите размещение кэша для защиты файлов Windows | Отключена |
| Ограничить размер кэша для защиты файлов Windows | Отключена |
| Установить параметры сканирования защиты файлов Windows | Отключена |
| Скрывать окно индикации выполнения сканирования файлов | Отключена |
| **Панель управления производительностью** |  |
| Отключение доступа к основному разделу панели управления производительностью | Отключена |
| Отключение доступа к разделу решения проблем производительности | Отключена |
| Отключение доступа к разделу изготовителя оборудования (OEM) и фирменной символики корпорации Майкрософт. | Отключена |
| **Параметры завершения работы** |  |
| Отключить автоматическое завершение работы приложений, которые блокируют или отменяют выключение компьютера. | Отключена |
| **Передача учетных данных** |  |
| Разрешить делегирование учетных данных, установленных по умолчанию, с проверкой подлинности сервера "только NTLM" | Отключена |
| Разрешить передачу учетных данных, установленных по умолчанию | Отключена |
| Разрешить передачу новых учетных данных | Отключена |
| Разрешить делегирование новых учетных данных с проверкой подлинности сервера "только NTLM" | Отключена |
| Разрешить передачу сохраненных учетных данных | Отключена |
| Разрешить делегирование сохраненных учетных данных с проверкой подлинности сервера "только NTLM" | Отключена |
| Запретить передачу учетных данных, установленных по умолчанию | Отключена |
| Запретить передачу новых учетных данных | Отключена |
| Запретить передачу сохраненных учетных данных | Отключена |
| **Перенаправление папки** |  |
| Использовать локализованные имена при перенаправлении папок меню "Пуск" и "Мои документы" | Отключена |
| **Профили пользователей** |  |
| Добавляет группу безопасности «Администраторы» к перемещаемым профилям пользователя. | Отключена |
| Удалять при перезагрузке системы профили пользователей по истечении указанного числа дней | Отключена |
| Не проверять собственность пользователя перемещаемых папок профиля | Отключена |
| Удалять кэшированные копии перемещаемых профилей | Отключена |
| Не выполнять принудительной выгрузки реестра пользователя при его выходе из системы | Отключена |
| Не определять медленные сетевые подключения | Отключена |
| Выдавать запрос пользователю при обнаружении медленного сетевого подключения | Отключена |
| Оставить установочные данные установщика Windows и групповой политики | Отключена |
| Разрешить использование только локальных профилей | Отключена |
| Установить путь к перемещаемым профилям для всех пользователей, входящих в систему на данном компьютере | Отключена |
| Таймаут диалоговых окон | Отключена |
| Не регистрировать в системе пользователей с временными профилями | Отключена |
| Максимальное число повторов попыток выгрузки и обновления профиля пользователя | Отключена |
| Запретить передачу на сервер изменений в перемещаемом профиле | Отключена |
| Дождаться загрузки перемещаемого пользовательского профиля | Отключена |
| Таймаут медленных сетевых подключений для профилей пользователей | Отключена |
| Фоновая передача файла реестра перемещаемого профиля пользователя при входе пользователя в систему | Отключена |
| Установить максимальное время ожидания для сети, если пользователь имеет перемещаемый профиль или удаленный основной каталог | Отключена |
| **Распределенная модель СОМ** |  |
| **Параметры совместимости приложений** |  |
| Разрешать локальные исключения проверки безопасности при активации | Отключена |
| Задать исключения проверки безопасности при активации | Отключена |
| **Сетевой вход в систему** |  |
| **DNS-записи локатора контроллеров домена [[122]](#footnote-123)** |  |
| Тип возвращаемого адреса контроллера домена | Не задана |
| Обнаружение контроллеров домена, несущих домен с однокомпонентным DNS-именем | Не задана |
| Автоматическое обслуживание сайта DNS SRV-записями локатора контроллеров домена | Не задана |
| DNS-записи локатора контроллеров домена, не регистрируемые контроллерами доменов | Не задана |
| Интервал обновления DNS-записей локатора контроллеров домена | Не задана |
| Набор TTL DNS-записей локатора контроллеров домена | Не задана |
| Установить интервал повторного поиска контроллера домена | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора глобального каталога | Не задана |
| Не обрабатывать в слотах входящие сообщения, которые используются для поиска контроллеров доменов по NetBIOS-именам доменов | Не задана |
| Установка приоритета в DNS SRV-записях локатора контроллеров домена | Не задана |
| Установка веса в DNS SRV-записях локатора контроллеров домена | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора раздела каталога приложений | Не задана |
| Сайты, обслуживаемые DNS SRV-записями локатора контроллеров домена | Не задана |
| Попробовать следующий ближайший сайт. | Не задана |
| Динамическая регистрация DNS-записей локатора контроллеров домена | Не задана |
| Разрешать алгоритмы шифрования, совместимые с Windows NT 4.0 | Отключена |
| Обращение к PDC при сбое входа в систему | Включена |
| Начальный интервал попыток обнаружения контроллеров домена для фоновых клиентов | Отключена |
| Максимальный интервал повторных попыток обнаружения контроллера домена для фоновых клиентов | Отключена |
| Окончательный интервал попыток обнаружения контроллера домена для фоновых клиентов | Отключена |
| Периодическое обновление кэша положительных ответов DC для фонового вызова | Отключена |
| Уровень вывода данных отладки в файл журнала | Отключена |
| Ожидаемая задержка при удаленном входе | Отключена |
| Максимальный размер файла журнала | Отключена |
| Настройка кэша отрицательных ответов обнаружения контроллеров домена | Отключена |
| Совместимость общего сетевого доступа | Отключена |
| Периодическое обновление кэша положительных ответов DC для нефонового вызова | Отключена |
| Интервал очистки | Отключена |
| Имя сайта | Отключена |
| Совместимость общего ресурса Sysvol | Отключена |
| **Служба времени Windows** |  |
| **Поставщики времени** |  |
| Настроить NTP-клиент Windows | Отключена |
| Включить NTP-клиент Windows | Включена |
| Включить NTP-сервер Windows | Для контроллера домена: Включена. Для остальных: Отключена. |
| Глобальные параметры конфигурации | Отключена |
| **Службы доверенного платформенного модуля** |  |
| Включить резервное копирование TPM в доменные службы Active Directory | Отключена |
| Настроить список заблокированных команд TPM | Отключена |
| Игнорировать список заблокированных команд TPM по умолчанию | Отключена |
| Игнорировать локальный список заблокированных команд TPM | Отключена |
| **Службы языковых стандартов** |  |
| Запретить выбор пользовательских языковых стандартов | Отключена |
| Ограничить системные языковые стандарты | Отключена |
| Ограничить пользовательские языковые стандарты | Отключена |
| Запретить изменение географического положения | Отключена |
| Не позволять пользователю переопределять параметры языкового стандарта | Отключена |
| **Сценарии** |  |
| Разрешение сценариев входа в систему при отключенных NetBIOS или WINS | Отключена |
| Максимальное время выполнения сценариев групповой политики | Отключена |
| Выполнить сценарии Windows PowerShell при запуске компьютера, завершить работу компьютера | Отключена |
| Выполнять сценарии входа в систему синхронно | Отключена |
| Выполнять сценарии завершения работы с отображением команд | Отключена |
| Выполнять сценарии загрузки асинхронно | Отключена |
| Выполнять сценарии загрузки с отображением команд | Отключена |
| Выполнить сценарии Windows PowerShell при входе пользователя в систему, завершить сеанс | Отключена |
| **Удаленный помощник** |  |
| Разрешать подключения только с компьютеров под управлением Windows 7 или более новых систем | Отключена |
| Включить ведение журнала сеансов | Отключена |
| Включить оптимизацию пропускной способности | Отключена |
| Настройка предупреждающих сообщений | Отключена |
| Запрос удаленной помощи | Отключена |
| Предлагать удаленную помощь | Отключена |
| **Управление связью через Интернет** |  |
| **Параметры связи через Интернет** |  |
| Отключить отчеты об ошибках распознавания рукописного текста | Включена |
| Отключить программу по улучшению качества программного обеспечения Windows | Включена |
| Выключить автоматическое обновление корневых сертификатов | Отключена |
| Отключить печать по протоколу HTTP | Отключена |
| Отключение загрузки драйверов принтера по протоколу HTTP | Отключена |
| Отключение поиска драйверов устройств в Центре обновления Windows | Включена |
| Отключить ссылки просмотра событий «Events.asp» | Включена |
| Отключение центра справки и поддержки «Знаете ли вы?» | Включена |
| Отключить поиск в базе знаний Майкрософт в окне «Центр справки и поддержки» | Включена |
| Отключить мастер подключения к Интернету, если URL-адрес ссылается на сайт Microsoft.com | Включена |
| Отключить регистрацию, если адрес-URL указывает на сайт Microsoft.com | Включена |
| Отключить активное зондирование для индикатора состояния сетевого подключения | Включена |
| Отключить отчеты об ошибках Windows | Включена |
| Отключить доступ ко всем возможностям Центра обновления Windows | Включена |
| Отключить обновление информационных файлов «Помощника по поиску» | Включена |
| Отключить службу сопоставления файлов Интернета | Включена |
| Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков | Включена |
| Отключить заказ отпечатков через Интернет в списке задач для изображений | Включена |
| Отключить веб-публикацию в списке задач для файлов и папок | Включена |
| Отключить участие в программе улучшения поддержки пользователей Windows Messenger | Включена |
| Ограничение соединения с Интернетом | Включена |
| **Управление электропитанием** |  |
| **Параметры жесткого диска** |  |
| Отключить жесткий диск (Питание от сети) | Отключена |
| Отключить жесткий диск (Питание от батареи) | Отключена |
| **Параметры кнопок** |  |
| Выберите действие кнопки включения питания (Питание от сети) | Отключена |
| Выберите действие кнопки перехода в режим сна (Питание от сети) | Отключена |
| Выберите действие кнопки включения питания в меню «Пуск» (Питание от сети) | Отключена |
| Выберите действие при закрытии крышки компьютера (Питание от сети) | Отключена |
| Выберите действие кнопки включения питания (Питание от батареи) | Отключена |
| Выберите действие кнопки перехода в режим сна (Питание от батареи) | Отключена |
| Выберите действие кнопки включения питания меню «Пуск» (Питание от батареи) | Отключена |
| Выберите действие при закрытии крышки компьютера (Питание от батареи) | Отключена |
| **Параметры режимов сна** |  |
| Разрешить приложениям препятствовать переходу системы в режим сна (Питание от сети) | Отключена |
| Укажите время ожидания для перехода в режим гибернации (Питание от сети) | Отключена |
| Требовать пароль при выходе из спящего режима (Питание от сети) | Включена |
| Укажите время ожидания перехода в режим сна (Питание от сети) | Отключена |
| Отключить гибридный спящий режим (Питание от сети) | Отключена |
| Разрешить различные режимы сна (S1-S3) при простое компьютера (Питание от сети) | Отключена |
| Разрешить различные режимы сна (S1-S3) при простое компьютера (Питание от батареи) | Отключена |
| Разрешить приложениям предотвращать автоматический переход в спящий режим (питание от сети) | Отключена |
| Разрешить приложениям предотвращать автоматический переход в спящий режим (питание от батареи) | Отключена |
| Разрешить автоматический переход в спящий режим с открытыми сетевыми файлами (питание от сети) | Отключена |
| Разрешить автоматический переход в спящий режим с открытыми сетевыми файлами (питание от батареи) | Отключена |
| Разрешить приложениям препятствовать переходу системы в режим сна (Питание от батареи) | Отключена |
| Укажите время ожидания для перехода в режим гибернации (Питание от батареи) | Отключена |
| Требовать пароль при выходе из спящего режима (Питание от батареи) | Включена |
| Укажите время ожидания перехода в режим сна (Питание от батареи) | Отключена |
| Отключить гибридный спящий режим (Питание от батареи) | Отключена |
| Укажите время ожидания автоматического перехода в режим сна (Питание от сети) | Отключена |
| Укажите время ожидания автоматического перехода в режим сна (питание от батареи) | Отключена |
| **Параметры уведомления** |  |
| Действие при почти полной разрядке батареи | Отключена |
| Действие при низком заряде батареи | Отключена |
| Уровень сигнала почти полной разрядки батареи | Отключена |
| Отключить уведомление при низком уровне заряда батареи | Отключена |
| Уровень сигнала низкого заряда батареи | Отключена |
| Уровень сигнала резервной батареи | Отключена |
| **Параметры экрана и видео** |  |
| Указать яркость монитора (питание от сети) | Отключена |
| Указать яркость монитора (питание от батареи) | Отключена |
| Уменьшить яркость монитора (питание от сети) | Отключена |
| Уменьшить яркость монитора (питание от батареи) | Отключена |
| Включить фоновый показ слайдов на рабочем столе (питание от сети) | Отключена |
| Включить фоновый показ слайдов на рабочем столе (питание от батареи) | Отключена |
| Выключить адаптивное время ожидания выключения дисплея (Питание от сети) | Отключена |
| Выключить адаптивное время ожидания выключения дисплея (Питание от батареи) | Отключена |
| Отключить дисплей (Питание от сети) | Отключена |
| Отключить дисплей (Питание от батареи) | Отключена |
| Укажите настраиваемую текущую схему управления питанием | Отключена |
| Выберите текущую схему управления питанием | Отключена |
| **Установка драйвера** |  |
| Разрешить пользователям, не являющимся администраторами, устанавливать драйверы для этих классов установки устройств | Отключена |
| Отключить запрос на поиск драйверов устройств на веб-сайте Windows Update | Включена |
| **Установка устройства** |  |
| **Ограничения на установку устройств** |  |
| Разрешить администраторам заменять политики ограничения установки устройств | Отключена |
| Разрешить установку устройств с использованием драйверов, соответствующих этим классам установки устройств | Отключена |
| Запретить установку устройств с использованием драйверов, соответствующих этим классам установки устройств | Отключена |
| Отображать специальное сообщение, когда установка запрещена параметром политики. | Отключена |
| Отображать заголовок специального сообщения, когда установка устройства запрещена параметром политики. | Отключена |
| Разрешить установку устройств, соответствующих какому-либо из этих кодов устройств | Отключена |
| Запретить установку устройств с указанными кодами устройств | Отключена |
| Время (сек.) до принудительной перезагрузки при необходимости введения параметров политики в действие | Отключена |
| Запретить установку съемных устройств | Отключена |
| Запретить установку устройств, не описанных другими параметрами политики | Отключена |
| Устанавливать одинаковый приоритет для всех подписанных цифровой подписью драйверов при оценке и в процессе выбора | Отключена |
| Отключить всплывающие напоминания «Найдено новое оборудование» во время установки драйвера | Отключена |
| Не посылать отчет об ошибках Windows, если для устройства установлен общий драйвер. | Отключена |
| Настроить время ожидания установки устройства | Отключена |
| Запретить Windows отправлять отчет об ошибках, если драйвер устройства запрашивает дополнительное программное обеспечение в ходе установки | Отключена |
| Не создавать контрольную точку восстановления системы во время работы устройства, при которой, как правило, требуется создание точки восстановления | Отключена |
| Разрешить удаленный доступ к устройствам Plug and Play | Отключена |
| Запретить получение метаданных устройств из Интернета | Отключена |
| Задать порядок поиска в исходных расположениях драйверов устройств | Отключена |
| **Файловая система** |  |
| **NTFS** |  |
| Запретить сжатие на всех томах NTFS | Отключена |
| Запретить шифрование на всех томах NTFS | Отключена |
| Включить шифрование файла подкачки NTFS | Отключена |
| Параметры создания коротких имен | Отключена |
| Отключить уведомления об удалении на всех томах | Отключена |
| Оценка символьных ссылок на основе их источников и адресов | Отключена |
| **Центр распространения ключей** |  |
| Использовать порядок поиска леса | Отключена |
| Предоставлять сведения о предыдущих попытках входа на клиентские компьютеры | Отключена |
| **Энергонезависимый кэш диска** |  |
| Отключить оптимизацию начальной загрузки и восстановления | Отключена |
| Отключить режим питания кэша | Отключена |
| Отключить функцию «Энергонезависимый кэш» | Отключена |
| Отключить режим Solid State | Отключена |
| Загружать отсутствующие COM-компоненты | Отключена |
| Разрешить клиентам для отслеживания изменившихся связей использовать ресурсы домена | Отключена |
| Не выполнять автоматическое шифрование файлов, перемещаемых в зашифрованные папки | Отключена |
| Не отключайте питание компьютера после возникновения ошибки завершения работы системы Windows. | Отключена |
| Включить постоянную временную метку | Не задана |
| Включить свойство данных состояния системы слежения за завершением работы | Не задана |
| Отображать диалог слежения за завершением работы | Отключена |
| Не отображать страницу "Управление данным сервером" при входе | Отключена |
| Отключить предотвращение выполнения данных для исполняемого файла справки в формате HTML | Отключена |
| Ограничить применение потенциально небезопасных функций справки HTML указанными папками | Включена (\*) |
| Запретить запуск из cправки перечисленных программ | Включена (\*) |
| Удалить сообщения о состоянии загрузки / завершения работы системы / входа в систему / выхода из системы | Отключена |
| Подробные или обычные сообщения состояния | Отключена |
| Указать размещение установочных файлов пакета обновления Windows | Отключена |
| Указать расположение установочных файлов Windows | Отключена |
| **Классические административные шаблоны** |  |
| **Secret Net Integrity Check settings** |  |
| Extension Executive [[123]](#footnote-124) | Включена (.exe; .dll; .cpl; .drv; .sys; .ocx; .vbs; .scr; .rll; .ime; .bpl; .ax; .acm; .com; .ppl; .cmd; .bat; .ovl; .tbp; .lnk) [[124]](#footnote-125) |
| **Все параметры** | См. значение конкретного параметра выше в таблице |
| **Настройка** |  |
| **Конфигурация Windows** |  |
| Среда | Не определено |
| Файлы | Не определено |
| Папки | Не определено |
| INI-файлы | Не определено |
| Реестр | Не определено |
| Сетевые общие ресурсы | Не определено |
| Ярлыки | Не определено |
| **Параметры панели управления** |  |
| Источники данных | Не определено |
| Устройства | Не определено |
| Параметры папок | Не определено |
| Локальные пользователи и группы | Не определено |
| Сетевые параметры | Не определено |
| Электропитание | Не определено |
| Принтеры | Не определено |
| Назначенные задания | Не определено |
| Службы | Не определено |

### Настройки СЗИ от НСД «Аккорд» на рабочих станциях и серверах (контроллерах домена) (при функционировании рабочих станций c ОС Windows 2000/XP/7 под управлением контроллеров домена c ОС Windows Server 2008.

Настройки параметров групповой политики, применяемой для серверов и АРМ платежной системы при использовании СЗИ от НСД «Аккорд» приведены в таблице (Таблица 46):

Таблица 46. Настройки параметров групповой политики для серверов и АРМ при использовании СЗИ от НСД Аккорд

|  |  |
| --- | --- |
| **Наименование раздела/параметра групповой политики** | **Значение параметра** |
| **Конфигурация компьютера** | |
| **Конфигурация Windows** | |
| **Параметры безопасности** | |
| **Политики учетных записей** | |
| **Политика паролей** | |
| Макс. срок действия пароля | Не более 185 дней |
| Мин. длина пароля | 8 символов |
| Вести журнал паролей | не менее 5 хранимых паролей |
| Хранить пароли, используя обратимое шифрование | отключен |
| **Политика блокировки учетной записи** | |
| Продолжительность блокировки учетной записи | 0 (бесконечно) или не менее 5 минут |
| Пороговое значение блокировки | не более 5 |
| Время до сброса счетчика блокировки | не менее 5 минут |
| **Политика аудита** | |
| Аудит входа в систему | Успех, Отказ |
| Аудит изменения политики | Успех, Отказ |
| Аудит использования привилегий | Отказ |
| Аудит событий входа в систему | Успех, Отказ |
| Аудит управления учетными записями | Успех, Отказ |
| **Локальные политики** | |
| **Параметры безопасности** | |
| Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) | 0 |
| Интерактивный вход в систему: не отображать последнего имени пользователя | Включен |
| Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее | 5 дней |
| **Административные шаблоны** | |
| **Классические административные шаблоны** | |
| **Network** | |
| **Administrative Shares** | |
| De-Activate AdminShare on a Server | Включен |
| De-Activate AdminShare on a Workstation | Включен |

Для появления в редакторе политик настроек Administrative Shares необходимо загрузить файл шаблона следующего содержания

CLASS MACHINE

CATEGORY "Network"

POLICY "Administrative Shares"

KEYNAME "System\CurrentControlSet\Services\LanmanServer\Parameters"

PART "De-Activate AdminShare on a Server" CHECKBOX

VALUENAME "AutoShareServer"

VALUEON NUMERIC 0

VALUEOFF NUMERIC 1

END PART

PART "De-Activate AdminShare on a Workstation" CHECKBOX

VALUENAME "AutoShareWks"

VALUEON NUMERIC 0

VALUEOFF NUMERIC 1

END PART

END POLICY

END CATEGORY

### Настройка системы «Контроль-ПУ»

Ниже приведены рекомендованные настройки для системы «Контроль-ПУ», используемой для организации блокировки и контроля доступа к коммуникационным портам и устройствам ввода-вывода на средствах вычислительной техники стендов сопровождения и тестирования РАБИС-НП и АС ЭКР 2.0 ТУ Банка России. Данные настройки, при необходимости, могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

Система «Контроль-ПУ» включает в себя три основные части:

* агент (DeviceLock Service),
* сервер (DeviceLock Enterprise Server и DeviceLock Content Security Server),
* консоль управления (DeviceLock Management Console / DeviceLock Group Policy Manager / DeviceLock Enterprise Manager / DeviceLock WebConsole).

Для просмотра отчетов - графов связей (Relations Charts) на компьютере с консолью управления должен быть установлен обозреватель Microsoft Internet Explorer 9 или более поздней версии.

Для установки и использования DeviceLock на локальном компьютере, необходимо иметь права локального администратора. Для установки и использовать DeviceLock в доменной сети, необходимо иметь права администратора домена.

Для передачи данных между службами DeviceLock Service, DeviceLock Enterprise Server и DeviceLock Content Security Server необходимо открыть следующие порты:

* 135 (TCP) - для службы "Локатор удалённого вызова процедур (RPC)";
* 137 (UDP) - для службы "NetBIOS Name Service";
* 138 (UDP) - для "NetBIOS Netlogon and Browsing";
* 139 (TCP) - для сессии NetBIOS (NET USE).

По умолчанию DeviceLock Service, DeviceLock Enterprise Server и DeviceLock Content Security Server используют порты 9132, 9133 и 9134 соответственно.

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ», применяемые для АРМ РАБИС-НП и АС ЭКР 2.0 приведены в таблице (Таблица 47).

Таблица 47. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ», применяемые для АРМ РАБИС-НП и АС ЭКР 2.0

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Администраторы DeviceLock | | |
| 1 | Включить безопасность по умолчанию | Отключено |
| 2 | Включить защиту от отключения | Включено |
| 3 | Только протоколировать | Включено |
| 4 | Предотвращать изменения в системных файлах настройки | Включено |
| 5 | Использовать усиленную проверку целостности | Отключено |
| 6 | Пользователи | Добавить привилегированных пользователей системы Контроль-ПУ (Администраторов (полный доступ), Операторов (изменение), Аудиторов (Только чтение) |
| Сервис DeviceLock → Настройки сервиса | | |
| 7 | Сообщение о блокировании USB/FireWire-устройств | Включено |
| 8 | Сообщение об истечении срока доступа | Включено |
| 9 | Контентно-зависимое сообщение о блокировании чтения | Включено |
| 10 | Контентно-зависимое сообщение о блокировании записи | Включено |
| 11 | Сообщение о блокировании протокола | Включено |
| 12 | Сообщение о блокировании от IP-файрвола | Включено |
| 13 | Сообщение о блокировании чтения с устройства | Включено |
| 14 | Сообщение о блокировании записи на устройство | Включено |
| 15 | Сообщение о проверке содержимого | Отключено |
| 16 | Сообщение о завершении проверки содержимого | Отключено |
| 17 | Настройки Oracle IRM Server | Не задано |
| 18 | DeviceLock Enterprise Server (ы) | IP-адрес сервера |
| 19 | Записывать события об изменении политики и старте/остановке сервиса | Включено |
| 20 | Сертификат DeviceLock | Сертификат открытого ключа DeviceLock Enterprise Server |
| 21 | Источник политики | Локальная и Enterprise Server |
| 22 | Использовать групповые/серверные политики | Включено |
| 23 | Подавлять локальную политику | Включено |
| 24 | Быстрые серверы в начале | Не задано |
| 25 | Приоритет трафика | Средний |
| 26 | Всегда отображать значек в системной области | Отключено |
| 27 | Проверка содержимого архивов при чтении | Выключено |
| 28 | Проверка содержимого архивов при записи | Выключено |
| 29 | Способ определения режима офлайн | Режим: Подключение кабеля |
| 30 | OWA-серверы | Не задано |
| 31 | Применять контентно-зависимые правила для имен файлов/папок | Отключено |

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части аудита и теневого копирования приведены в таблице (Таблица 48).

Таблица 48. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части аудита и теневого копирования

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Аудит и теневое копирование | | |
| 1 | Локальная директория | \%SystemRoot%\SHADOW |
| 2 | Включить локальную квоту | Включено |
| 3 | Затирать файлы старше чем (дней) | 90 |
| 4 | Локальная квота (%) | 5 |
| 5 | Сохранять файлы нулевой длины | Отключено |
| 6 | Аудит операций с папками | Отключено |
| 7 | Безопасная перезапись файла | Отключено |
| 8 | Запретить передачу данных при ошибках | Отключено |
| 9 | Тип журнала аудита | Журнал событий |
| 10 | Настройки журнала аудита | 5000Kb, Перезаписывать события по необходимости (сначала старые события) |
| 11 | Настройки Syslog | Не задано |
| 12 | Порог лога аудита для файловых операций (секунд) | 1200 |
| 13 | Отправлять данные теневого копирования на сервер | Включено |
| 14 | Сервис DeviceLock → Настройки сервиса → Шифрование | Не задано |

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части алертинга приведены в таблице (Таблица 49).

Таблица 49. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части алертинга

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Алерты | | |
| 1 | SNMP | Не задано |
| 2 | SMTP | Не задано |
| 3 | Syslog | Не задано |
| 4 | Параметры повторной доставки | Задано (количество попыток повторной доставки – 3; интервал повторной попытки – 600 сек.; сохранить в очереди – 1 час) |
| Сервис DeviceLock → Настройки сервиса → Алерты →Административные алерты | | |
| 5 | Оповещать при изменении настроек администраторов DeviceLock | Включено |
| 6 | Оповещать при отказе доступа при попытке изменить настройки агента | Включено |
| 7 | Оповещать при отказе доступа при попытке изменить настройки агента и включённой настройке ‘Подавлять локальную политику’ | Включено |
| 8 | Оповещать при изменении политик агента | Отключено |
| 9 | Оповещать при повреждении политик агента | Включено |
| 10 | Оповещать при восстановлении агента | Включено |
| 11 | Оповещать при превышении локальной квоты | Включено |
| 12 | Оповещать при остановке агента | Отключено |
| 13 | Оповещать при деинсталляции агента | Включено |
| 14 | Оповещать при неожиданном завершении процесса агента | Включено |
| 15 | Оповещать при изменении настроек алертов | Отключено |
| 16 | Оповещать при обнаружении кейлогера | Включено |

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования Анти-кейлогера на АРМ РАБИС-НП и АС ЭКР 2.0 приведены в таблице (Таблица 50).

Таблица 50. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования Анти-кейлогера

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Алерты →Анти-кейлогер | | |
| 1 | Блокировать клавиатуру | Включено |
| 2 | Протоколировать событие | Включено |
| 3 | Считать USB-хаб кейлогером | Отключено |
| 4 | Оповестить пользователя | Отключено |
| 5 | Скремблирование PS/2-клавиатуры | Отключено |

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования устройств на АРМ РАБИС-НП и АС ЭКР 2.0 приведены в таблице (Таблица 51).

Таблица 51. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования устройств

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Устройства → Разрешения | | |
| 1 | BlackBerry-устройства | Нет доступа |
| 2 | Bluetooth | Полный доступ |
| 3 | FireWire-порт | Полный доступ |
| 4 | iPhone-устройства | Нет доступа |
| 5 | MTP | Нет доступа |
| 6 | Palm | Нет доступа |
| 7 | USB-порт | Полный доступ |
| 8 | WiFi | Нет доступа |
| 9 | Windows Mobile | Нет доступа |
| 10 | Буфер обмена | Полный доступ |
| 11 | Гибкий диск | Полный доступ |
| 12 | Жесткий диск | Полный доступ |
| 13 | ИК-порт | Полный доступ |
| 14 | Ленточные накопители | Полный доступ |
| 15 | Оптический привод | Полный доступ |
| 16 | Параллельный порт | Полный доступ |
| 17 | Последовательный порт | Полный доступ |
| 18 | Принтер | Полный доступ |
| 19 | Съемные устройства | Полный доступ |
| 20 | ТС-устройства | Полный доступ |
| Сервис DeviceLock → Настройки сервиса → Устройства → Аудит, Теневое копирование и Алерты | | |
| 21 | Задано для всех типов устройств | √Аудит запретов  √Алерт запретов |

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части безопасности устройств приведены в таблице (Таблица 52).

Таблица 52. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части безопасности устройств

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Устройства → Настройки безопасности | | |
| 1 | Управлять доступом к USB HID (мышь, клавиатура и т.д.) | Отключено |
| 2 | Управлять доступом к USB-принтерам | Отключено |
| 3 | Управлять доступом к USB Bluetooth-адаптерам | Включено |
| 4 | Управлять доступом к сетевым картам USB и FireWire | Включено |
| 5 | Управлять доступом к USB-сканерам и устройствам обработки изображения | Отключено |
| 6 | Управлять доступом к последовательным модемам (внутренним и внешним) | Включено |
| 7 | Управлять доступом к устройствам хранения USB | Включено |
| 8 | Управлять доступом к виртуальным оптическим приводам (для Windows 2000 и выше) | Включено |
| 9 | Управлять доступом к устройствам хранения FireWire | Включено |
| 10 | Управлять доступом к виртуальным принтерам (для Windows 2000 и выше) | Отключено |
| 11 | Управлять доступом для операций копирования/вставки буфера обмена в пределах одного приложения | Отключено |
| 12 | Блокировать FireWire контроллер при запрете доступа | Отключено |
| 13 | Трактовать ТС перенаправляемые USB-устройства как обычные | Включено |
| 14 | Переключать PostScript-принтер в не PostScript-режим | Включено |
| 15 | Управлять доступом к Bluetooth HID (мышь, клавиатура и т.д.) | Включено |

Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования протоколов приведены в таблице (Таблица 53).

Таблица 53. Параметры настроек сервиса DeviceLock системы «Контроль-ПУ» в части использования протоколов

| **№** | **Название параметра** | **Значение параметра** |
| --- | --- | --- |
| Сервис DeviceLock → Настройки сервиса → Протоколы | | |
| 1 | Разрешения | Полный доступ |
| 2 | Аудит, Теневое копирование и Алерты | Не определено |

### Настройка системы паспортизации

Ниже приведены рекомендованные настройки для системы паспортизации на основе ПК «Паспорт АРМ УОС». Данные настройки, при необходимости, могут быть изменены с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ Банка России.

ПК «Паспорт АРМ УОС» обеспечивает возможность контроля целостности программного обеспечения на персональных компьютерах и серверах под управлением операционных систем семейства Windows не ниже Windows XP Service Pack 3.

Сервер должен функционировать под управлением операционной системы не ниже ОС Windows Server 2003.

В состав ПК «Паспорт АРМ УОС» входят следующие компоненты:

* Внутренний архив ПС – приложение Сервер данных;
* Анализатор изменений ПО – клиентское ПО АРМ пользователей и администраторов РАБИС-НП и АС ЭКР 2.0;
* консоли управления АРМ администратора ИБ:
  + Управление ПС – приложение Консоль пользователя (централизованное управление системой паспортизации);
  + Получение изменений (данных) с автономных АРМ – приложение Перенос данных (управление системой паспортизации автономных АРМ).

Для настройки системы паспортизации необходимо пользователю ПК «Паспорт АРМ УОС» назначить роль Администратор комплекса (см. документ «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД Территориальных учреждений Банка России»).

Для передачи данных между компонентами ПК «Паспорт АРМ УОС» необходимо использовать следующие параметры соединения по протоколу HTTP:

* Порт сервера: 5050 (по умолчанию);
* Порт анализатора: 5051 (по умолчанию).
* Имя сервера: NetBIOS-имя сервера.

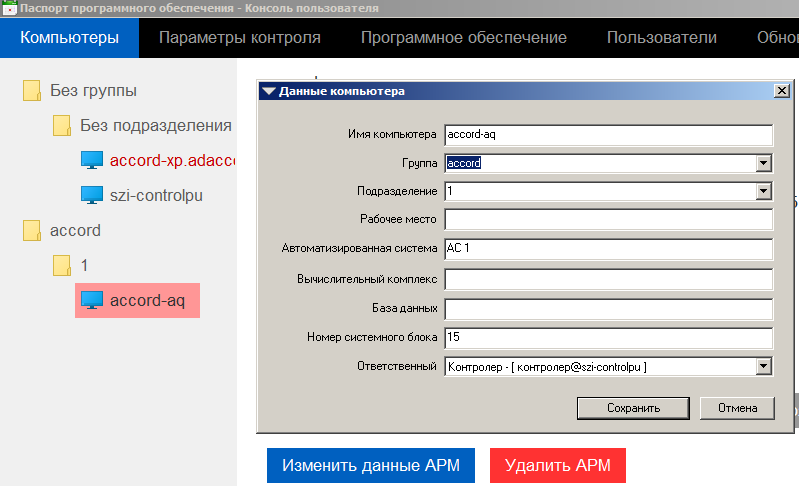
Так же необходимо открыть следующие порты:

* 135 (TCP) - для службы "Локатор удалённого вызова процедур (RPC)";
* 137 (UDP) - для службы "NetBIOS Name Service";
* 138 (UDP) - для "NetBIOS Netlogon and Browsing";
* 139 (TCP) - для сессии NetBIOS (NET USE).

### Настройка зарегистрированных компьютеров

После установки ПО анализатора изменений на АРМ пользователей и cерверов РАБИС-НП и АС ЭКР 2.0 необходимо войти в систему паспортизации через Консоль пользователя и, после появления компьютера в списке подключенных, настроить необходимые данные:

* Имя компьютера: наименование имени компьютера;
* Группа: наименование группы, в которую входит компьютер пользователя РАБИС-НП и АС ЭКР 2.0. Группа создается автоматически при первоначальном вводе и сохранении её данных, в дальнейшем её нужно выбирать из выпадающего списка;
* Подразделение: наименование подразделения, в которое входит компьютер пользователя РАБИС-НП и АС ЭКР 2.0. Подразделение создается автоматически при первоначальном вводе и сохранении её данных, в дальнейшем его нужно выбирать из выпадающего списка;
* Рабочее место;
* Автоматизированная система: наименование автоматизированных систем (РАБИС-НП, АС ЭКР 2.0 и т.п.), с которыми взаимодействуют пользователи данного компьютера;
* Вычислительный комплекс;
* База данных: указать СУБД при её наличии на компьютере пользователя РАБИС-НП и АС ЭКР 2.0;
* Номер системного блока (инвентарный);
* Ответственный: назначить ответственного Контролера с целью контроля состава ПО компьютера в системе паспортизации.[[125]](#footnote-126)

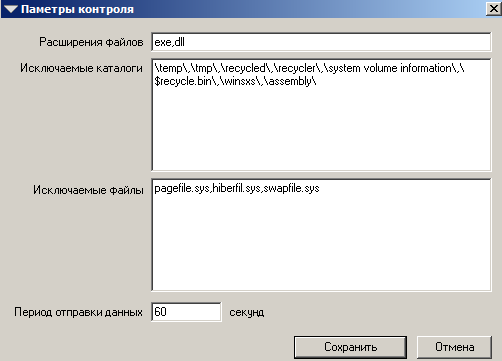


*Рисунок 22 – Описание данных АРМ пользователя РАБИС и АС ЭКР 2.0*

### Настройка параметров контроля состава ПО

Для настроек параметров контроля состава ПО компьютеров пользователей РАБИС и АС ЭКР 2.0 в меню приложения необходимо выбрать команду «*Параметры контроля*» и настроить следующие параметры:

* Расширения файлов: exe,dll (помимо расширений по умолчанию рекомендуется добавить следующие типы файлов: com,bat,sys,cmd,ini,inf,cpl,ocx); для контроля целостности ярлыков приложений РАБИС и АС ЭКР 2.0, расположенных на рабочем столе, рекомендуется добавить тип lnk.
* Исключаемые каталоги: \temp\,\tmp\,\recycled\,\recycler\,\system volume information\,\$recycle.bin\,\winsxs\,\assembly\.[[126]](#footnote-127)
* Исключаемые файлы: pagefile.sys,hiberfil.sys,swapfile.sys;
* Период отправки данных: 60 секунд.

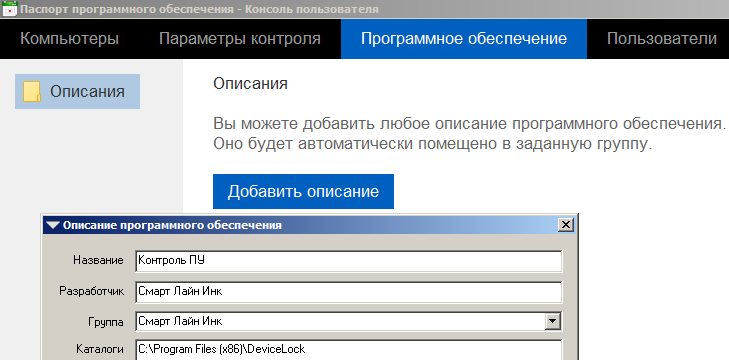


*Рисунок 23 – Настройка параметров контроля целостности ПО*

### Настройка списка программного обеспечения

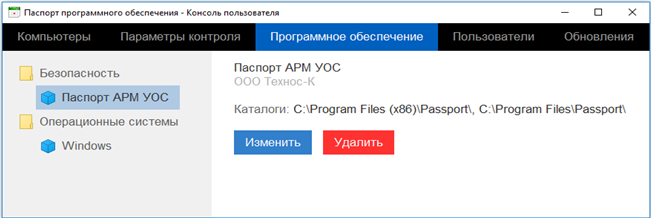
Список программного обеспечения предназначен для удобства формирования отчетности в его разрезе (т.е. делать выборки (использовать как фильтр) из полного сформированного отчета контроля целостности.

Для настройки списка программного обеспечения, используемого на компьютере пользователя РАБИС и АС ЭКР 2.0, Администратор через Консоль пользователя в разделе «Программное обеспечение» нажимает клавишу «Добавить описание» и настраивает соответствующие параметры:



*Рисунок 24 – Настройка описания программного обеспечения*

* Название: наименование ПО (с указанием версии);
* Разработчик: наименование разработчика ПО;
* Группа: наименование группы ПО (группировать можно по назначению ПО). Группа создается автоматически после сохранения введенных параметров.
* Каталоги: указать каталоги, в которых размещаются модули соответствующего ПО (каталоги должны быть разделены ***запятой***, ***точка с запятой*** автоматически заменяется на ***запятую***).



*Рисунок 25 – Настройка перечня программного обеспечения*

В перечень программного ПО возможно добавить следующие:

* СЗИ от НСД Аккорд: программные файлы из каталога C:\Accord.NT\х64\RAU;
* СЗИ от НСД Secret Net: программные файлы из каталога C:\Program Files\Secret Net;
* СКАД Сигнатура: C:\Program Files\Validata;
* ПО ЕСМИБ: C:\Program Files\Crystall\ZObserver;
* JRE: C:\Program Files\Java, C:\Program Files(x86)\Java.

1. Могут применяться более свежие версии клиентской части (агента) Agent for Windows с учетом внутренних особенностей организации обеспечения информационной безопасности в ТУ Банка России по согласованию с подразделением информационной безопасности ТУ и Главным управлением безопасности и защиты информации Банка России. Согласование должно быть оформлено документально и утверждено руководством ТУ. [↑](#footnote-ref-2)
2. Внимание: Указанный раздел настраивается, в том числе, в соответствии с техническими решениями автоматизированных систем (например, ЕСМИБ), функционирующих в платежной системе ТУ. [↑](#footnote-ref-3)
3. При отключении параметра файл с вредоносным кодом не блокируется и остается доступным пользователю и системе. [↑](#footnote-ref-4)
4. Отключен – при возниковении сбоев на ПЭВМ, на которых выполняется выгрузка информации на сетевые ресурсы (в том числе АРМ оператора криптоцентра). [↑](#footnote-ref-5)
5. Мониторинг и аудит состояния ПО СЗ от ВВК KES 10 рекомендуется осуществлять удаленно с помощью консоли KSC 10 в режиме "только чтение" (для этого соответствующие учетные записи включить в локальную группу "KLOperators" сервера администрирования СЗ от ВВК KSC 10). В целях мониторинга пользователем состояния ПО СЗ от ВВК KES10 необходимо дополнительно настроить группу параметров "Уведомлять на экране" в разделе "Дополнительные параметры - Интерфейс –Уведомления". [↑](#footnote-ref-6)
6. Пароль устанавливается и используется сотрудниками, ответственными за установку, настройку и администрирование СЗ от ВВК. [↑](#footnote-ref-7)
7. Расписание устанавливается в соответствии с принятыми в ТУ требованиями и может отличаться от указанных значений. [↑](#footnote-ref-8)
8. При отключении параметра файл с вредоносным кодом не блокируется и остается доступным пользователю и системе. [↑](#footnote-ref-9)
9. Для загрузки обновления модулей программы с установкой критических и одобренных обновлений рекомендуется использовать отдельную задачу обновления в определённое время, согласованное с подразделением безопасности ТУ. [↑](#footnote-ref-10)
10. Значения параметров могут быть изменены по согласованию с территориальным подразделением безопасности и защиты информации при иной организации обновления сигнатурных баз в ТУ. [↑](#footnote-ref-11)
11. Значения параметров могут отличаться от указанных в таблице. При изменении параметра "Номер UDP-порта" необходимо обеспечить сетевое взаимодействие между Сервером администрирования и Агентом администрирования по заданному значению порта. [↑](#footnote-ref-12)
12. Пароль устанавливается и используется сотрудниками ответственными за установку, настройку и администрирование ПО СЗ от ВВК. [↑](#footnote-ref-13)
13. Внимание: Указанный раздел настраивается, в том числе, в соответствии с техническими решениями автоматизированных систем (например, ЕСМИБ), функционирующих в платежной системе ТУ. [↑](#footnote-ref-14)
14. При отключении параметра файл с вредоносным кодом не блокируется и остается доступным пользователю и системе. [↑](#footnote-ref-15)
15. Отключен – при возниковении сбоев на ПЭВМ, на которых выполняется выгрузка информации на сетевые ресурсы (в том числе АРМ оператора криптоцентра). [↑](#footnote-ref-16)
16. Мониторинг и аудит состояния ПО СЗ от ВВК KES 10 рекомендуется осуществлять удаленно с помощью консоли KSC 10 в режиме "только чтение" (для этого соответствующие учетные записи включить в локальную группу "KLOperators" сервера администрирования СЗ от ВВК KSC 10). В целях мониторинга пользователем состояния ПО СЗ от ВВК KES10 необходимо дополнительно настроить группу параметров "Уведомлять на экране" в разделе "Дополнительные параметры - Интерфейс –Уведомления". [↑](#footnote-ref-17)
17. Пароль устанавливается и используется сотрудниками, ответственными за установку, настройку и администрирование СЗ от ВВК. [↑](#footnote-ref-18)
18. Внимание: Указанный раздел настраивается, в том числе, в соответствии с техническими решениями автоматизированных систем (например, ЕСМИБ), функционирующих в платежной системе ТУ. [↑](#footnote-ref-19)
19. При отключении параметра файл с вредоносным кодом не блокируется и остается доступным пользователю и системе. [↑](#footnote-ref-20)
20. Отключен – при возниковении сбоев на ПЭВМ, на которых выполняется выгрузка информации на сетевые ресурсы (в том числе АРМ оператора криптоцентра). [↑](#footnote-ref-21)
21. Пароль устанавливается и используется сотрудниками, ответственными за установку, настройку и администрирование СЗ от ВВК. [↑](#footnote-ref-22)
22. Мониторинг и аудит состояния ПО СЗ от ВВК KES 10 рекомендуется осуществлять удаленно с помощью консоли KSC 10 в режиме "только чтение" (для этого соответствующие учетные записи включить в локальную группу "KLOperators" сервера администрирования СЗ от ВВК KSC 10). В целях мониторинга пользователем состояния ПО СЗ от ВВК KES10 необходимо дополнительно настроить группу параметров "Уведомлять на экране" в разделе "Дополнительные параметры - Интерфейс –Уведомления". [↑](#footnote-ref-23)
23. Расписание устанавливается в соответствии с принятыми в ТУ требованиями и может отличаться от указанных значений. [↑](#footnote-ref-24)
24. При отключении параметра файл с вредоносным кодом не блокируется и остается доступным пользователю и системе. [↑](#footnote-ref-25)
25. Для загрузки обновления модулей программы с установкой критических и одобренных обновлений рекомендуется использовать отдельную задачу обновления в определённое время, согласованное с подразделением безопасности ТУ. [↑](#footnote-ref-26)
26. Значения параметров могут быть изменены по согласованию с территориальным подразделением безопасности и защиты информации при иной организации обновления сигнатурных баз в ТУ. [↑](#footnote-ref-27)
27. Значения параметров могут отличаться от указанных в таблице. При изменении параметра "Номер UDP-порта" необходимо обеспечить сетевое взаимодействие между Сервером администрирования и Агентом администрирования по заданному значению порта. [↑](#footnote-ref-28)
28. Пароль устанавливается и используется сотрудниками ответственными за установку, настройку и администрирование ПО СЗ от ВВК. [↑](#footnote-ref-29)
29. Внимание: параметры данного раздела настраивать не требуется – сервер Dr.Web формирует их автоматически при установке. Приведен пример значений параметров при использовании внешней базы данных MS SQL сервера/ Данный раздел настраивается в соответствии с документацией разработчика СЗ от ВВК и зависит от параметров установки. [↑](#footnote-ref-30)
30. Установите флаг, чтобы разрешить взаимодействие между Серверами Dr.Web при многосерверной конфигурации (т.е. при наличии нескольких серверов DrWeb ESS). При наличии одного сервера Dr.Web флаг не используется. [↑](#footnote-ref-31)
31. Внимание: Указанный раздел настраивается, в том числе, в соответствии с техническими решениями автоматизированных систем (например, ЕСМИБ), функционирующих в платежной системе ТУ. [↑](#footnote-ref-32)
32. Для сервера приложений АС ЭКР настроить в соответствии с рекомендациями, приведенными в таблице (Таблица 20) «Рекомендуемые к применению на сервере приложений АС ЭКР 2.0 настройки исключений компонеты SplDer Guard G3 for Windows Server ПО СЗ от ВВК "Dr.Web 10». [↑](#footnote-ref-33)
33. Разрешать – при функционировании ПО СЗ от ВВК Dr.Web под управлением ОС Windows Server 2003, при этом значение параметра "Уровень блокировки подозрительных действий" изменится на "Пользовательский". [↑](#footnote-ref-34)
34. Если идентификатор регистрируется администратором ИБ впервые, то следует сгенерировать новый секретный ключ, если идентификатор у администратора ИБ уже существует (зарегистрирован на другом комплексе Аккорд, то следует выбрать опцию «Использовать существующий» с вводом действующего пароля. [↑](#footnote-ref-35)
35. Основные утилиты комплекса Аккорд запускаются из меню Пуск → Все программы → Аккорд/Аккорд-Win64 [↑](#footnote-ref-36)
36. База данных пользователей в контроллере АМДЗ Аккорд-5MX/5.5/5.5e синхронизируется с базой программной части комплекса Аккорд (СПО Аккорд-Win32/64). [↑](#footnote-ref-37)
37. После идентификатора администратора ИБ утилита запросит идентификатор с ключевым лицензионным файлом. Прикоснитесь идентификатором с красным стикером к контактному устройству и удерживайте его. Программа настройки комплекса считает данные из идентификатора и запишет их в файл Accord.key на жестком диске в папке, где установлено ПО "Аккорд". [↑](#footnote-ref-38)
38. Для уменьшения количества записей в журнале регистрации событий с результатом НСД при операциях Traverse и Search, возникающих при попытке доступа к файлам комплекса антивирусных средств и системных процессов, таких как System, Services, WinLogon, SvcHost и т. д. [↑](#footnote-ref-39)
39. Для непрерывного мониторинга АРМ РАБИС-НП, АС ЭКР, СЗИ от НСД. Окончательный перечень СВТ ТУ определяют самостоятельно по согласованию с территориальным подразделением безопасности. [↑](#footnote-ref-40)
40. < имя домена>- NetBIOS-имя домена защищаемого домена. Например, PAYMENT. [↑](#footnote-ref-41)
41. В доменную группу SecretNetAdmins включены учетные записи сотрудников подразделения информатизации, осуществляющих установку, настройку и администрирование средств защиты. [↑](#footnote-ref-42)
42. В доменную группу Auditors включены учетные записи сотрудников подразделения безопасности и защиты информации, осуществляющие аудит средств защиты. [↑](#footnote-ref-43)
43. В доменную группу SPOAdmins включены учетные записи сотрудников подразделения информатизации, осуществляющих установку, настройку и администрирование системного программного обеспечения. [↑](#footnote-ref-44)
44. В доменную группу ModifyAdmins включены учетные записи пользователей АРМ Администратор модификаций АС ЭКР 2.0. [↑](#footnote-ref-45)
45. Для непрерывного мониторинга серверов РАБИС-НП. [↑](#footnote-ref-46)
46. < имя домена>- NetBIOS-имя домена защищаемого домена. Например, PAYMENT. [↑](#footnote-ref-47)
47. В доменную группу SecretNetAdmin\_Forest включены пользователи – администраторы леса доменов безопасности. В доменную группу SecretNetAdmin\_Domain включены пользователи – администраторы доменов безопасности. В указанные группы рекомендуется включить учетные записи сотрудников подразделения информатизации, осуществляющих установку, настройку и администрирование средств защиты. [↑](#footnote-ref-48)
48. В доменную группу Auditors включены учетные записи сотрудников подразделения безопасности и защиты информации, осуществляющие аудит средств защиты. [↑](#footnote-ref-49)
49. В доменную группу SPOAdmins включены учетные записи сотрудников подразделения информатизации, осуществляющих установку, настройку и администрирование системного программного обеспечения. [↑](#footnote-ref-50)
50. В доменную группу ModifyAdmins включены учетные записи пользователей АРМ Администратор модификаций АС ЭКР 2.0. [↑](#footnote-ref-51)
51. Для отдельных пользователей и эксплуатационного персонала при необходимости может быть установлено значение «Подключение устройства разрешено». [↑](#footnote-ref-52)
52. При использовании внешних, подключаемых по USB дисководов гибких дисков пользователю могут быть даны разрешения на использование устройства хранения, с заявленными полномочиями. Фактически, таким образом, создаётся «белый список» разрешённых к использованию отдельных устройств, хотя доступ к классу устройств в целом запрещён. [↑](#footnote-ref-53)
53. Для обеспечения возможности использования ключевых носителей vdToken без необходимости поэкземплярной регистрации на каждом рабочем месте УОС [↑](#footnote-ref-54)
54. Внимание: При запрете cmd.exe средствами СЗИ от НСД Secret Net ПО РАБИС-НП функционирует корректно, однако невозможен запуск командных файлов, исполняемых указанным командным интерпретатором. [↑](#footnote-ref-55)
55. Исключение из задания контроля целостности параметров определенной ветви реестра. Исключение возможно по согласованию с территориальным подразделением безопасности. [↑](#footnote-ref-56)
56. Внимание: При запрете cmd.exe средствами СЗИ от НСД Secret Net ПО РАБИС-НП функционирует корректно, однако невозможен запуск командных файлов, исполняемых указанным командным интерпретатором. [↑](#footnote-ref-57)
57. Все параметры раздела и его подразделов перевести в состояние "Отключена". [↑](#footnote-ref-58)
58. Отключена - при формировании ярлыков необходимых для запуска пользователю приложений на рабочем столе. [↑](#footnote-ref-59)
59. Данный перечень может быть расширен и не является окончательным. [↑](#footnote-ref-60)
60. Для ПЭВМ персонала ЕСМИБ ТУ запуск iexplore.exe разрешен [↑](#footnote-ref-61)
61. Параметры данного раздела настраиваются для Default Domain Policy. [↑](#footnote-ref-62)
62. Пустое значение означает, что данная привилегия не предоставляется никому. [↑](#footnote-ref-63)
63. Членами локальной группы Пользователи является доменная группа Доменные пользователи. [↑](#footnote-ref-64)
64. Для установки программных исправлений операционной системы АРМ необходимо на время установки предоставить указанное право учетным записям администраторов, выполняющих установку исправлений. [↑](#footnote-ref-65)
65. Включен - по согласованию с территориальным подразделением безопасности ТУ. [↑](#footnote-ref-66)
66. Настройка групп и их состава выполняется по согласованию с территориальным подразделением безопасности ТУ. [↑](#footnote-ref-67)
67. Допускаются отклонения в количестве и наименовании служб. [↑](#footnote-ref-68)
68. Включена – по согласованию с территориальным подразделением безопасности. [↑](#footnote-ref-69)
69. Тип запуска службы ТУ определяют самостоятельно по согласованию с территориальным подразделением безопасности. [↑](#footnote-ref-70)
70. Все параметры раздела и его подразделов перевести в состояние "Отключена". [↑](#footnote-ref-71)
71. Используется для централизованного управления списком расширений исполняемых файлов Secret Net. Параметр появляется при использовании версии Secret Net 6.5 с помощью специального административного шаблона (присутствует всоставе дистрибутива Secret Net 6.5). [↑](#footnote-ref-72)
72. Данный перечень не является исчерпывающим и может дополняться в процессе построения ЗПС. [↑](#footnote-ref-73)
73. Данный параметр конфигурируется другими средствами управления Active Directory. [↑](#footnote-ref-74)
74. Значение параметров «Не задана» позволит ОС Windows самостоятельно управлять работой DNS. [↑](#footnote-ref-75)
75. Параметры данного раздела настраиваются для Default Domain Policy. [↑](#footnote-ref-76)
76. <имя\_домена> - наименование домена. [↑](#footnote-ref-77)
77. Пустое значение означает, что данная привилегия не предоставляется никому. [↑](#footnote-ref-78)
78. Или иная группа, в зависимости от способа организации удаленного доступа в ТУ, [↑](#footnote-ref-79)
79. Для установки программных исправлений операционной системы сервера необходимо на время установки предоставить указанное право учетным записям администраторов, выполняющих установку исправлений. [↑](#footnote-ref-80)
80. Требуется документацией на ПО HP OpenView и РЗ ИСУ ТИР. [↑](#footnote-ref-81)
81. Указанные значения параметра определить при использовании ПО СЗИ от НСД Secret Net версии 6.5 При использовании ПО СЗИ от НСД Secret Net версии 7.x значение параметра перевести в "Не определено". [↑](#footnote-ref-82)
82. Настройка групп и их состава выполняется по согласованию с территориальным подразделением безопасности ТУ. [↑](#footnote-ref-83)
83. Допускаются отклонения в количестве и наименовании служб. [↑](#footnote-ref-84)
84. Значение данного параметра определяется локальными настройками на контроллерах домена. [↑](#footnote-ref-85)
85. Перечень и наличие данных сервисов зависит от аппаратной платформы. [↑](#footnote-ref-86)
86. Отключено - при использовании ПО удаленного управления сторонних производителей (например, PCAnywhere). [↑](#footnote-ref-87)
87. Все параметры раздела и его подразделов перевести в состояние "Отключена". [↑](#footnote-ref-88)
88. Для обеспечения функций резервного копирования по расписанию. [↑](#footnote-ref-89)
89. При использовании "Службы терминалов" параметры настраиваются в соответсвии с требования ТУ. В случае использования иного средства удаленного управления значение всех параметров устанавливается в режим "Отключено". [↑](#footnote-ref-90)
90. Используется для централизованного управления списком расширений исполняемых файлов Secret Net. Параметр появляется при использовании версии Secret Net 6.5 с помощью специального административного шаблона (присутствует всоставе дистрибутива Secret Net 6.5). [↑](#footnote-ref-91)
91. Данный перечень не является исчерпывающим и может дополняться при построении ЗПС. [↑](#footnote-ref-92)
92. Данный параметр конфигурируется другими средствами управления Active Directory. [↑](#footnote-ref-93)
93. Значение параметров «Не задана» позволит ОС Windows самостоятельно управлять работой DNS. [↑](#footnote-ref-94)
94. Установить в значение «Отключена» – для корректного формирования меню запуска только необходимых пользователю приложений в ОС Windows 7 при использовании механизма пользовательской политики "Перенаправление папок" (Folder redirection). [↑](#footnote-ref-95)
95. Отключена – для отключения механизма блокировки экрана на ПЭВМ АРМ МИБ АС ЭКР. [↑](#footnote-ref-96)
96. Отключена – для отключения механизма блокировки экрана на ПЭВМ АРМ МИБ АС ЭКР. [↑](#footnote-ref-97)
97. Данный перечень может быть расширен и не является окончательным. [↑](#footnote-ref-98)
98. Для ПЭВМ персонала ЕСМИБ ТУ запуск iexplore.exe разрешен [↑](#footnote-ref-99)
99. Параметры данного раздела настраивается для политики домена по умолчанию. [↑](#footnote-ref-100)
100. Пустое значение означает, что данная привилегия не предоставляется никому. [↑](#footnote-ref-101)
101. Для установки программных исправлений операционной системы АРМ необходимо на время установки предоставить указанное право учетным записям администраторов, выполняющих установку исправлений. [↑](#footnote-ref-102)
102. Включен - по согласованию с территориальным подразделением безопасности ТУ. [↑](#footnote-ref-103)
103. Настройка групп и их состава выполняется по согласованию с подразделением безопасности ТУ. [↑](#footnote-ref-104)
104. Допускаются отклонения в количестве и наименовании служб. [↑](#footnote-ref-105)
105. Включена – по согласованию с территориальным подразделением безопасности. [↑](#footnote-ref-106)
106. Значения "Не задана" для параметров данного раздела позволяет ОС Windows самостоятельно управлять работой DNS. [↑](#footnote-ref-107)
107. Используется для централизованного управления списком расширений исполняемых файлов Secret Net 6.5. Параметр появляется при использовании версии Secret Net 6.5 с помощью специального административного шаблона (присутствует в составе дистрибутива Secret Net 6.5). [↑](#footnote-ref-108)
108. Данный перечень не является исчерпывающим и может дополняться в процессе построения ЗПС. [↑](#footnote-ref-109)
109. Параметры данного раздела настраивается для политики домена по умолчанию. [↑](#footnote-ref-110)
110. Пустое значение означает, что данная привилегия не предоставляется никому. [↑](#footnote-ref-111)
111. Для серверов приложений АС ЭКР: musr\_mqadmin, Имя домена\HP ITO account. [↑](#footnote-ref-112)
112. Или иная группа, в зависимости от способа организации удаленного доступа в ТУ, [↑](#footnote-ref-113)
113. Для установки программных исправлений операционной системы сервера необходимо на время установки предоставить указанное право учетным записям администраторов, выполняющих установку исправлений. [↑](#footnote-ref-114)
114. Указанные значения параметра определить при использовании ПО СЗИ от НСД Secret Net версии 6.5 При использовании ПО СЗИ от НСД Secret Net версии 7.x значение параметра перевести в "Не определено". [↑](#footnote-ref-115)
115. Настройка групп и их состава выполняется по согласованию с подразделением безопасности ТУ. [↑](#footnote-ref-116)
116. Допускаются отклонения в количестве и наименовании служб. [↑](#footnote-ref-117)
117. Отключен – при использовании ПО удаленного управления сторонних производителей (например, PCAnywhere). [↑](#footnote-ref-118)
118. По согласованию с территориальным подразделением безопасности и защиты информации значение параметра можно перевести в "Автоматическое". [↑](#footnote-ref-119)
119. При использовании "Службы удаленных рабочих столов" на серверах параметры настраиваются в соответсвии с требованиями ТУ. [↑](#footnote-ref-120)
120. В случае не использования "Службы удаленных рабочих столов", значение всех параметров устанавливается в режим "Отключено". [↑](#footnote-ref-121)
121. Отключен – для АРМ заведующего кладовой АС ЭКР (при использовании терминала сбора данных (ТСД) Falcon Datalogic  X3, функционирующим под управлением ОС Windows CE 6.x). Для обеспечения обмена информации с АС ЭКР. [↑](#footnote-ref-122)
122. Значения "Не задана" для параметров данного раздела позволяет ОС Windows самостоятельно управлять работой DNS. [↑](#footnote-ref-123)
123. Используется для централизованного управления списком расширений исполняемых файлов Secret Net 6.5. Параметр появляется при использовании версии Secret Net 6.5 с помощью специального административного шаблона (присутствует в составе дистрибутива Secret Net 6.5). [↑](#footnote-ref-124)
124. Данный перечень не является исчерпывающим и может дополняться в процессе построения ЗПС. [↑](#footnote-ref-125)
125. Заведение ответственных описано в разделе 5.3.5 документа «Технологические карты обновления (актуализации) унифицированных конфигураций СЗИ от НСД ТУ Банка России» [↑](#footnote-ref-126)
126. Предупреждение! Если папка, расположенная на компьютере, содержит в своем имени любую из указанных в настройках «Исключаемые каталоги» комбинацию символов, то она автоматически исключается из контроля системы паспортизации. [↑](#footnote-ref-127)