**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ**

**(БАНК РОССИИ)**

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  | |  | | |  |  |  | |  | |  | | |  | |  | | |  |  | | |  |  |  | |  | |  | | |  | |  | | |  |  | | |  |  |  | |  | |  | | \_\_\_\_\_\_\_\_\_\_М**.Р. Шагиахметов** | |  | |  | | «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г. | |  |  | | |  |
| Москва 2017 г. | |
|  | |

**технологические карты обновления (актуализации) унифицированных конфигураций СЗИ Территориальных учреждений Банка России**

**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. СПО «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) |
| 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. системного ПО контроллеров «Аккорд-5MX», «Аккорд-5.5», «Аккорд-5.5е» (версия 02.01.015); 3. СПО «Аккорд-Win32» (версия 4.0.9.50); 4. СПО «Аккорд-Win64» (версия 5.0.9.50); 5. СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 4 (версия 10.2.6.3733); 6. СЗ от ВВК Dr.Web Enterprise агент Agent for Windows (версия 11.0.1.05150), 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 |
| 4.2 | 17.10.2017 | Внесены замечания ГУБиЗИ Банка России | Учтены замечания в части порядка применения системы «Контроль-ПУ» на стендах тестирования ТУ |
| 4.3 | 28.11.2017 | Внесены замечания НБ по Республике Татарстан Волго-Вятского ГУ Банка России | Уточнена версия прошивки контроллеров Аккорд-5МХ/5.5/5.5e (02.01.015) |

Содержание

[1 Введение 6](#_Toc496013543)

[2 Технологические карты для обновления (актуализации) унифицированных конфигураций СЗИ от НСД Территориальных учреждений Банка России 7](#_Toc496013544)

[2.1 Технологическая карта обновления для сетевого режима функционирования на базе Secret Net 7.6 7](#_Toc496013545)

[2.2 Технологическая карта обновления СЗИ от НСД Аккорд 9](#_Toc496013546)

[2.2.1 Обновление ПО Аккорд-NT/2000 v2.0 и v3.0 на ПО Аккорд-Win32 в автономном режиме функционирования 9](#_Toc496013547)

[2.2.2 Обновление CПО «Аккорд-Win32» (до версии 4.0.9.50) и CПО «Аккорд-Win64» (до версии 5.0.9.50) в автономном режиме функционирования 10](#_Toc496013548)

[2.2.3 Обновление встроенного ПО контроллеров Аккорд 10](#_Toc496013549)

[2.2.4 Обновление СПО «Аккорд-Win32/64» 13](#_Toc496013550)

[3 Технологическая карта обновления (актуализации) унифицированных конфигураций СЗ от ВВК Территориальных учреждений Банка России на 14](#_Toc496013551)

[3.1 Технологическая карта создания сети СЗ от ВВК 14](#_Toc496013552)

[3.2 Технологическая карта путей обновления СЗ от ВВК на «Унифицированные конфигурации СЗИ» 15](#_Toc496013553)

[3.3 Технологическая карта обновления Агентов Централизованного управления СЗ от ВВК на АРМ и серверах 15](#_Toc496013554)

[3.4 Технологическая карта обновления СЗ от ВВК 16](#_Toc496013555)

[3.4.1 Технологическая карта обновления СЗ от ВВК на базе Антивируса Касперского 16](#_Toc496013556)

[3.4.1.1 Технологическая карта обновления сервера администрирования Kaspersky Administration Kit 8.0 до версии Kaspersky Security Center 10 16](#_Toc496013557)

[3.4.1.2 Технологическая карта обновления сервера администрирования Kaspersky Security Center 10 MAINTENANCE RELEASE 1 до версии Kaspersky Security Center 10 SERVICE PACK 2. 17](#_Toc496013558)

[3.4.1.3 Технологическая карта обновления сервера администрирования Kaspersky Security Center 10 SERVICE PACK 1 до версии Kaspersky Security Center 10 SERVICE PACK 2. 17](#_Toc496013559)

[3.4.1.4 Технологическая карта обновления сервера администрирования Kaspersky Security Center 10 SP2 до версии Kaspersky Security Center 10 SP2 MR1 17](#_Toc496013560)

[3.4.1.5 Технологическая карта обновления клиентов СЗ от ВВК антивируса Касперского в автоматическом режиме для АРМ 18](#_Toc496013561)

[3.4.1.6 Технологическая карта ручного обновления клиентов СЗ от ВВК антивируса Касперского для АРМ 19](#_Toc496013562)

[3.5 Технологическая карта обновления ПО СЗ от ВВК Dr.Web 19](#_Toc496013563)

[3.5.1 Технологическая карта обновления ПО СЗ от ВВК Dr.Web Enterprise Security Suite 6.0.4 на версию 10.0 19](#_Toc496013564)

[3.5.2 Технологическая карта обновления ПО СЗ от ВВК Dr.Web Enterprise Security Suite 10.0 на версию 10.01.0 20](#_Toc496013565)

[3.5.2.1 Обновление Сервера Dr.Web ESS 20](#_Toc496013566)

[3.5.2.2 Обновление расширения Центр управления безопасностью Dr.Web 22](#_Toc496013567)

[3.5.2.3 Обновление Агента Dr.Web 22](#_Toc496013568)

[4 Технологическая карта обновления (актуализации) унифицированных конфигураций системы «Контроль-ПУ» Территориальных учреждений Банка России 24](#_Toc496013569)

[4.1 Состав обновления системы «Контроль-ПУ» 24](#_Toc496013570)

[4.2 Технологическая карта обновления системы «Контроль-ПУ» 24](#_Toc496013571)

[4.2.1 Обновление DeviceLock Enterprise Server 25](#_Toc496013572)

[4.2.2 Обновление DeviceLock Service 27](#_Toc496013573)

[4.2.2.1 Обновление DeviceLock Service с помощью консоли DeviceLock Management Console 27](#_Toc496013574)

[4.2.2.1 Обновление DeviceLock Service с помощью консоли DeviceLock Enterprise Manager 28](#_Toc496013575)

[4.2.2.2 Локальное обновление DeviceLock Service 29](#_Toc496013576)

[4.3 Настройка системы «Контроль-ПУ» 29](#_Toc496013577)

[5 Технологическая карта обновления унифицированных конфигураций системы паспортизации ТУ Банка России 30](#_Toc496013578)

[5.1 Особенности перехода с предыдущих версий системы паспортизации 30](#_Toc496013579)

[5.2 Состав обновления системы паспортизации 31](#_Toc496013580)

[5.3 Технологическая карта обновления системы паспортизации 32](#_Toc496013581)

[5.3.1 Установка сервера данных ПК «Паспорт АРМ УОС» 32](#_Toc496013582)

[5.3.2 Установка клиентского ПО ПК «Паспорт АРМ УОС» 33](#_Toc496013583)

[5.3.3 Установка консоли централизованного управления ПК «Паспорт АРМ УОС» 34](#_Toc496013584)

[5.3.4 Установка консоли управления системой паспортизации автономных АРМ 35](#_Toc496013585)

[5.3.5 Заведение пользователей ПК «Паспорт АРМ УОС» 36](#_Toc496013586)

[5.4 Настройка системы паспортизации 36](#_Toc496013587)

[Список сокращений и терминов 37](#_Toc496013588)

# Введение

В настоящем документе приведены технологические карты обновления СЗ от ВВК, СЗИ от НСД, системы «Контроль-ПУ» и системы паспортизации на основе ПК «Паспорт АРМ УОС» до версий, указанных в методическом документе «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России».

# Технологические карты для обновления (актуализации) унифицированных конфигураций СЗИ от НСД Территориальных учреждений Банка России

## Технологическая карта обновления для сетевого режима функционирования на базе Secret Net 7.6

Совместно с данной документацией необходимо использовать следующую документацию разработчика ‑ «Средство защиты информации Secret Net 7. Установка, обновление и удаление. Руководство администратора», шифр документа ‑ RU.88338853.501410.015 91 2, разработчик – «КОД БЕЗОПАСНОСТИ».

Внимание: Обновление ПО сервера безопасности возможно только с версии 7.0 и выше. Выбор варианта установки сервера безопасности Secret Net версии 7.3 с размещением хранилища объектов централизованного управления Secret Net в базе данных доменных служб Active Directory или вне Active Directory ТУ осуществляют самостоятельно.

Обновление поддерживается для следующих версий и компонентов:

* 5.0.180.4 — клиент;
* 5.1.265.8 — клиент;
* 6.5.333.53 — клиент;
* 6.5.333.98 — клиент;
* 7.3.562.0 — клиент, сервер безопасности, программа оперативного управления;
* 7.4.577.0 — клиент, сервер безопасности, программа оперативного управления.

Для обновления СЗИ от НСД «Secret Net» версии 6.5 на версию 7.6 необходимо:

1. Включить все контроллеры домена.
2. При размещении хранилища объектов централизованного управления в БД доменных служб Active Directory - выполнить модификацию AD при помощи «Модификатора схемы AD» из состава дистрибутива Secret Net версии 7.6. Для модификации схемы AD:

* Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска и выберите команду "Модификатор схемы AD" (или запустите с установочного компакт-диска файл \Setup\AD\SnADMS.exe). На экране появится диалог "Модификатор схемы Active Directory". Программа автоматически определит контроллер домена, являющийся мастером схемы AD, и на фоне диалога появится сообщение: "Поиск мастера схемы Active Directory успешно завершен".
* Нажмите кнопку "ОК".
* В диалоге "Модификатор схемы Active Directory" заполните поля "Пользователь" и "Пароль" учетными данными пользователя, обладающего необходимыми правами. Совет. Если вход на компьютер выполнен с учетными данными пользователя, которому предоставлены права на изменение конфигурации каталога AD и права для модификации схемы AD, поля "Пользователь" и "Пароль" можно не заполнять.
* Для запуска процесса модификации AD нажмите кнопку "Применить". На экране появится запрос для подтверждения операции.
* Для начала процесса модификации нажмите кнопку "Да". Начнется процесс модификации AD, по окончании которого на экране появится сообщение: "Модификация схемы Active Directory успешно завершена". 6. Нажмите кнопку "ОК" и закройте диалог "Модификатор схемы Active Directory".

1. Дождитесь репликации схемы AD на все контроллеры домена.
2. Установить ПО сервера безопасности Secret Net версии 7.6 на дополнительный сервер. На время перехода на версию 7.6 в домене одновременно должны функционировать серверы безопасности версий 6.5 и 7.6.
3. Установить ПО клиента и ПО средств управления версии 7.6 на дополнительных рабочих местах администраторов СЗИ от НСД. На время перехода на версию 7.6, для сохранения управляемости клиентами версии 6.5, должны продолжать функционирование основные рабочие места администраторов СЗИ от НСД Secret Net 6.5.
4. Обновить ПО клиента в порядке:

* контроллеры домена;
* компьютеры работников.

1. После обновления последнего клиента защищаемого домена с привязкой его к серверу безопасности версии 7.6, вывести из эксплуатации сервер безопасности версии 6.5, обновить до версии 7.6 основные рабочие места администраторов СЗИ от НСД.

## Технологическая карта обновления СЗИ от НСД Аккорд

Совместно с данным документом необходимо использовать следующую документацию разработчика ОКБ САПР:

* «Комплекс СЗИ от НСД для ПЭВМ (PC) «Аккорд-АМДЗ». Руководство по установке».
* «Комплекс СЗИ от НСД для ПЭВМ (PC) «Аккорд-АМДЗ». Руководство администратора».
* «ПАК СЗИ от НСД Аккорд. Быстрый запуск».
* «ПАК СЗИ от НСД Аккорд-Win64 (версия 5.0). Руководство по установке».
* «ПАК СЗИ от НСД Аккорд-Win32 (версия 4.0). Руководство по установке».
* «ПАК СЗИ от НСД Аккорд-Win32 (версия 4.0). Руководство администратора».

#### Обновление ПО Аккорд-NT/2000 v2.0 и v3.0 на ПО Аккорд-Win32 в автономном режиме функционирования

Чтобы обновить Аккорд, необходимо:

1. Снять защиту комплекса Аккорд:

* Войти в систему с параметрами администратора ИБ;
* Запустить программу ACSETUP.EXE из каталога \ACCORD.NT. При этом повторно запрашивается идентификатор администратора ИБ;
* В пункте меню "Команды" следует выбрать подпункт "Снятие". Система разграничения доступа будет отключена, и при следующей загрузке не будет активизироваться. Каталог ACCORD.NT остается на жестком диске. Для полной деинсталляции системы «Аккорд» необходимо перезагрузить компьютер и запустить файл UnWise.EXE из каталога ACCORD.NT.

1. Произвести обновление встроенного ПО в соответствии с пунктом 2.2.1.1;
2. Произвести полную деинсталляцию системы «Аккорд» с помощью файла UnWise.exe из каталога ACCORD.NT.
3. Установить новую версию ПО с компакт-диска.
4. Произвести настройки системы «Аккорд» в соответствии с документом «Унифицированные настройки СЗИ».

#### Обновление CПО «Аккорд-Win32» (до версии 4.0.9.50) и CПО «Аккорд-Win64» (до версии 5.0.9.50) в автономном режиме функционирования

Перед обновлением CПО «Аккорд-Win32» и CПО «Аккорд-Win64» рекомендуется сохранить (выполнить резервное копирование) в какой-либо каталог файлы: accord.amz – база данных пользователей и политик безопасности СПО Аккорд, accord.ini – конфигурационные параметры СПО Аккорд, accord.key – лицензионный файл).

Для обновления CПО «Аккорд-Win32» до версии 4.0.9.50 с более ранних (начиная с 4.0.9.х) а также для обновления CПО «Аккорд-Win64» до версии 5.0.9.50 с более ранних (начиная с 5.0.7.34) необходимо:

1. В утилите "Настройка комплекса Аккорд" снять систему защиты (пункт меню "Команды" - "Снятие"). Выполнить перезагрузку компьютера.
2. Через оснастку «Панель управления/Программы и компоненты/ Установка/Удаление программ» удалить СПО "Аккорд".
3. Произвести установку СПО "Аккорд" актуальной версии (4.0.9.50 для «Аккорд-Win32», 5.0.9.50 для «Аккорд-Win64»):

* СПО для ПАК СЗИ НСД "Аккорд-Win32" устанавливается и работает только на ПК под управлением 32-х битных ОС Windows XP, Windows 7.
* СПО для ПАК СЗИ НСД "Аккорд-Win64" устанавливается и работает только на ПК под управлением 64-х битных ОС Windows XP, Windows 7.

1. Произвести необходимые настройки в утилите "Настройка комплекса Аккорд" в соответствии с документом «Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации ТУ для РАБИС-НП и АРМ АС ЭКР 2.0»;
2. Запустить редактор прав доступа Aced32: проверить наличие параметра "Блокировка клипборда" в опциях пользователей (флаг должен быть снят, если он установлен - снять его).
3. Изменить любой параметр, чтобы появился запрос о сохранении настроек.
4. Включить защиту комплекса Аккорд: в утилите "Настройка комплекса Аккорд" включить систему защиты (пункт меню "Команды" - "Активация").

#### Обновление встроенного ПО контроллеров Аккорд

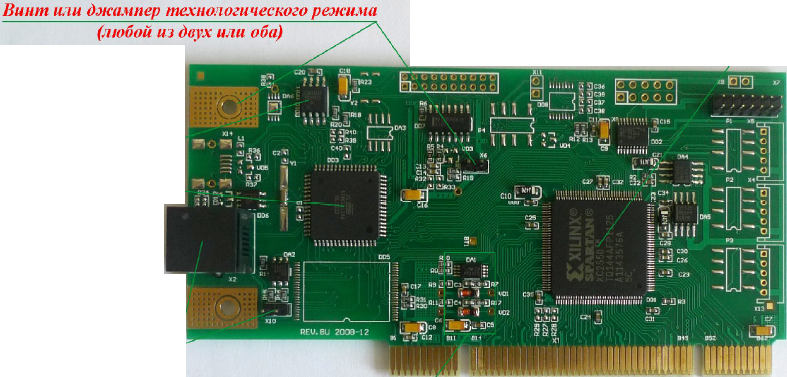
В случае необходимости рекомендуется обновить ПО контроллеров «Аккорд-5MX», «Аккорд-5.5» и «Аккорд-5.5е» до версии 02.01.015. Для этого необходимо:

1. Во избежание потери необходимых данных (процедура обновления встроенного ПО включает в себя процедуру очистки БД контроллера) рекомендуется сначала выполнить операции экспорта списка пользователей и списка контроля целостности (см. «Комплекс СЗИ от НСД для ПЭВМ (PC) «Аккорд-АМДЗ». Руководство администратора»);
2. Создать загрузочный USB-носитель[[1]](#footnote-2) либо использовать CD дистрибутив СЗИ НСД "Аккорд-АМДЗ", являющимся загрузочным.
3. Скопировать набор файлов обновления[[2]](#footnote-3) внутреннего ПО контроллера на USB-носитель.

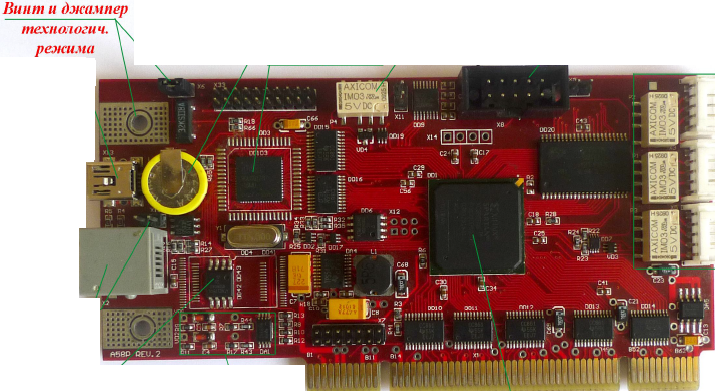
**Важно!!!** Набор файлов обновления должен точно соответствовать типу Вашего контроллера, а для Аккорд-5 и 5.5 еще и типу процессора Atmel, установленного на плате.

1. Выключить компьютер и вынуть плату контроллера Аккорд.
2. Перевести контроллер Аккорд в технологический режим:

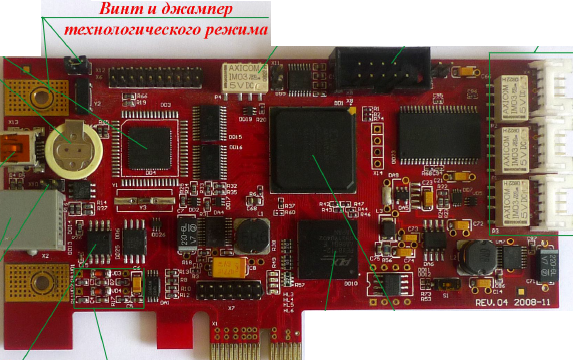
* снять установочную металлическую планку, которая крепится к плате контроллера двумя винтами;
* при наличии - снять джампер технологического режима;



*Рисунок 1 – Переключение контроллера Аккорд-5MX в технологический режим*



*Рисунок 2 – Переключение контроллера Аккорд-5.5 в технологический режим*



*Рисунок 3 – Переключение контроллера Аккорд-5.5e в технологический режим*

1. Вставить плату в компьютер и загрузить в OC MS-DOS с помощью загрузочного USB-устройства (дискеты, CD), созданного в рамках выполнения пункта 2) настоящей последовательности
2. В командной строке перейти в каталог, в который ранее был скопирован комплект файлов обновления согласно пункту 3), и выполнить команду: amdzeegn.exe ee.bin nnnnnnnn, где nnnnnnnn - восьмизначный серийный номер (он указан в формуляре на комплекс и присутствует на наклейке с обратной стороны платы). Эта команда записывает серийный номер в файл ee.bin, из которого в процессе прошивки данные заносятся в память микропроцессора. Для всех контроллеров rev.8 эту операцию выполнять не нужно, т.к. серийный номер в них записывается однократно при производстве.
3. В командной строке запустить командный файл all\_p.bat из каталога, в котором ранее был сгенерирован файл ee.bin из предыдущего пункта.

**Примечание**: Внимательно проследите, чтобы каждая операция завершалась сообщением "OK". В случае появления ошибки верификации при записи firmware микроконтроллера или EEPROM – выполнить командный файл обновления еще раз.

1. Выключить компьютер, вернуть контроллер Аккорд-5MX/5.5/5.5e в рабочий режим согласно пункту 5) и установить контроллер в компьютер.

#### Обновление СПО «Аккорд-Win32/64»

Обновление СПО «Аккорд-Win32/64» происходит путем полного удаления предыдущей версии продукта и дальнейшей установки и настройке комплекса Аккорд согласно Приложению 2 документа «Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации Территориальных учреждений для РАБИС-НП и АРМ АС ЭКР 2.0». Для полного удаления комплекса Аккорд необходимо:

1. Войти в ОС с параметрами администратора БИ.
2. Запустить программу ACSETUP.EXE из установочного каталога СПО «Аккорд-Win32/64». При этом повторно запрашивается идентификатор администратора БИ.
3. В пункте меню «Команды» следует выбрать подпункт «Снятие». Система разграничения доступа будет отключена, и при следующей загрузке не будет активизироваться. Установочный каталог СПО «Аккорд-Win32/64» остается на жестком диске. Для полной деинсталляции системы «Аккорд» необходимо перезагрузить компьютер и запустить процедуру удаления ПО Аккорд в панели управления компьютера.
4. После удаления ПО Аккорд удалить установочный каталог СПО «Аккорд-Win32/64»[[3]](#footnote-4). Отключить питание.
5. Включить компьютер и в стартовом меню АМДЗ «Аккорд-5MX/5.5/5.5e» выбрать пункт «Очистка БД контроллера».

# Технологическая карта обновления (актуализации) унифицированных конфигураций СЗ от ВВК Территориальных учреждений Банка России на

## Технологическая карта создания сети СЗ от ВВК

Чтобы создать сеть СЗ от ВВК, необходимо:

1. Определить перечень и версии СЗ от ВВК, которые будут устанавливаться на АРМ и серверы, согласно документу «Перечень унифицированных конфигураций средств защиты информации для использования в РАБИС-НП и АС ЭКР 2.0 Территориальных учреждений Банка России».
2. Составить план структуры сети СЗ от ВВК, включить в него все защищаемые компьютеры и определить, какие из них будут выполнять функцию «Сервера Управления».
3. Установить ПО «Сервера Управления» на выбранный сервер и подчиненные серверы.
4. Используя «Сервер Управления» произвести обновление репозитория (обновление антивирусных баз и ПО), при необходимости установить и настроить Прокси-сервер. Либо полностью заменить содержимое каталога репозитория основного «Сервера Управления» на актуальный.
5. Установить вручную или используя соответствующие задания на «Сервере Управления» ‑ ПО СЗ от ВВК на АРМ и сервера.
6. При использовании ручной установки ПО СЗ от ВВК необходимо установить ПО «Агента Сервера Управления» на АРМ и сервера.
7. Произвести настройку конфигураций и задач для АРМ и серверов на «Сервере Управления» согласно Приложению 1 документа «Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации Территориальных учреждений для РАБИС-НП и АРМ АС ЭКР 2.0» (Далее – «Порядок обновления»).
8. Используя Сервер Управления, настроить и запустить необходимые модули и настройки, согласно Приложению 1 документа «Порядок обновления».
9. В соответствии с пунктом 3.8 Положения Банка России от 25.11.2015 № 506-П «Об обеспечении информационной безопасности в структурных подразделениях Банка России при обработке, хранении и (или) передаче информации с использованием средств вычислительной техники» рекомендованы к использованию средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации:

Рекомендованными к применению в Банке России для контура безопасности УОС определены версии СЗ от ВВК:

* Dr.Web – версия 10.00.0-201502060;
* Kaspersky Security Center 10 Service Pack – версия 10.3.407;
* Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294) проходит сертификационные испытания.

В соответствии с пунктом 3.9 Положения Банка России от 25.11.2015 № 506-П «Об обеспечении информационной безопасности в структурных подразделениях Банка России при обработке, хранении и (или) передаче информации с использованием средств вычислительной техники» использование других версий допустимо по согласованию с Главным управлением безопасности и защиты информации Банка России.

Применяемые версии СЗ от ВВК должны быть указаны в документе «Перечень разрешенных к применению средств защиты информационно-вычислительных ресурсов Банка России от воздействий вредоносного кода».

## Технологическая карта путей обновления СЗ от ВВК на «Унифицированные конфигурации СЗИ»

Пути обновления СЗ от ВВК:

1. Полное удаление СЗ от ВВК на АРМ и серверах, также удаление ПО Централизованного управления и установка новых версий унифицированной конфигурации;
2. Обновление версий СЗ от ВВК до версии унифицированной конфигурации.

## Технологическая карта обновления Агентов Централизованного управления СЗ от ВВК на АРМ и серверах

При обновлении Агентов Централизованного управления СЗ от ВВК, установленных на АРМ и серверах платежного сегмента, могут быть нежелательные перезагрузки станций или остановка сетевого ПО, работающего на таких станциях.

Во избежание функционального простоя предлагается следующий режим обновления Агентов и антивирусного ПО:

1. В расписании Сервера изменить стандартные задания для обновления всех компонентов на обновление только сигнатурных баз.
2. Создать новое задание на обновление всех компонентов в удобное время, когда это не скажется критически на работе АРМ и серверов.

## Технологическая карта обновления СЗ от ВВК

### Технологическая карта обновления СЗ от ВВК на базе Антивируса Касперского

#### Технологическая карта обновления сервера администрирования Kaspersky Administration Kit 8.0 до версии Kaspersky Security Center 10

Совместно с данной документацией необходимо использовать следующую документацию разработчика ‑ «Kaspersky Security Center 10. Руководство по внедрению. Версия программы: 10 Service pack ».

Переход на версию Kaspersky Security Center 10 возможен только с версии Kaspersky Administration Kit 8.0.2177 (Critical Fix3).

Чтобы обновить сервер администрирования Kaspersky Administration Kit 8.0.2177 (Critical Fix3) до версии Kaspersky Security Center 10, необходимо:

1. Для Kaspersky Administration Kit 8.0.2177 (Critical Fix3) создать резервную копию данных Сервера администрирования при помощи утилиты klbackup. Эта утилита входит в состав дистрибутива и располагается в корне папки установки Kaspersky Administration Kit.

Также из панели управления сохранить (экспортировать) созданные политики и задачи.

1. Установить Kaspersky Security Center 10 на компьютер, на котором установлена предыдущая версия Сервера администрирования. Обнаружив на компьютере версию Kaspersky Administration Kit 8.0.2177 (Critical Fix3), установщик Kaspersky Security Center 10 автоматически переходит в режим обновления. При этом никакие параметры обновления задать нельзя. Мастер автоматически обновляет установленные компоненты с сохранением настроек.

**Внимание!** Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности Kaspersky Administration Kit.

1. Для выбранных АРМ и серверов создайте и запустите задачу удаленной установки для новой версии Агента администрирования. После ее успешного завершения версия Агента администрирования будет обновлена.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера администрирования.

#### Технологическая карта обновления сервера администрирования Kaspersky Security Center 10 MAINTENANCE RELEASE 1 до версии Kaspersky Security Center 10 SERVICE PACK 2.

При обновлении следует руководствоваться документом разработчика ‑ «Kaspersky Security Center 10. Руководство по внедрению. Версия программы: 10 SERVICE PACK 1».

#### Технологическая карта обновления сервера администрирования Kaspersky Security Center 10 SERVICE PACK 1 до версии Kaspersky Security Center 10 SERVICE PACK 2.

При обновлении следует руководствоваться документом разработчика ‑ «Kaspersky Security Center 10. Руководство по внедрению. Версия программы: 10 SERVICE PACK 2».

#### Технологическая карта обновления сервера администрирования Kaspersky Security Center 10 SP2 до версии Kaspersky Security Center 10 SP2 MR1

Совместно с данной документацией необходимо использовать следующую документацию разработчика ‑ «Kaspersky Security Center. Руководство по внедрению. Версия программы: 10 Service Pack 2, Maintenance Releas 1».

Переход на версию Kaspersky Security Center 10 SP2 MR1 возможен с версии Kaspersky Security Center 10 SP2. При обновлении данные и параметры предыдущей версии Сервера администрирования сохраняются.

Чтобы обновить сервер администрирования KSC необходимо:

1. Запустить исполняемый файл setup.exe для новой версии.
2. В окне с выбором программ по ссылке Установить Сервер администрирования Kaspersky Security Center запустите мастер установки Сервера администрирования.
3. Принять условия Лицензионного соглашения. Мастер установки предложит создать резервную копию Сервера администрирования. Необходимо создать резервную копию: в открывшемся окне Создание резервной копии Сервера администрирования установить флажок Создать резервную копию Сервера администрирования.
4. Установите Сервер администрирования новой версии. Не рекомендуется прерывать работу Мастера установки. Прерывание процесса может привести к неработоспособности Сервера администрирования.
5. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создать и запустить задачу удаленной установки вручную или по расписанию новой версии Агента администрирования (10.4).
6. После успешного завершения этой задачи на клиентских устройствах будет обновлена версия Агента администрирования.

#### Технологическая карта обновления клиентов СЗ от ВВК антивируса Касперского в автоматическом режиме для АРМ

Чтобы обновить клиентов СЗ от ВВК антивируса Касперского, установленных на АРМ, необходимо:

1. Создать задачу в Центре Администрирования ‑ "удаленная установка программы" или выбрать нужный АРМ из списка "нераспределенные компьютеры" и нажать "установить программу":

* для АРМ под управлением ОС Windows XP SP3 RUS задача удаленной установки содержит пакет обновления СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 4 (версия 10.2.6.3733). Обновление возможно со следующих версий[[4]](#footnote-5):
  + Kaspersky Endpoint Security 10 MR 1 (версия 10.2.1.23);
  + Kaspersky Endpoint Security 10 SP 1 (версия 10.2.2.10535);
  + Kaspersky Endpoint Security 10 SP 1 MR 1 (версия 10.2.2.10535(MR1));
  + Kaspersky Endpoint Security 10 SP 1 MR 2 (версия 10.2.4.674);
  + Kaspersky Endpoint Security 10 SP 1 MR 3 (сборка 10.2.5.3201);
* для АРМ под управлением других версий ОС Windows задача удаленной установки содержит пакет обновления СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294). Обновление возможно со следующих версий4:
  + Kaspersky Endpoint Security 10 SP 1 (версия 10.2.2.10535);
  + Kaspersky Endpoint Security 10 SP 1 MR 1 (версия 10.2.2.10535(MR1));
  + Kaspersky Endpoint Security 10 SP 1 MR 2 (версия 10.2.4.674);
  + Kaspersky Endpoint Security 10 SP 1 MR 3 (версия 10.2.5.3201).

1. Добавить компьютеры в список при удаленной установке программ.
2. Запустить задачу установки[[5]](#footnote-6).
3. Дождаться завершения задачи и перезагрузить АРМ[[6]](#footnote-7).

#### Технологическая карта ручного обновления клиентов СЗ от ВВК антивируса Касперского для АРМ

Рекомендуется выполнить следующие действия:

1. Удалить установленное ПО СЗ от ВВК.
2. Установить версию Антивирус Касперского, согласно рекомендованной в документе «Унифицированные конфигурации СЗИ»:

* для АРМ под управлением ОС Windows XP SP3 RUS использовать пакет обновления СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 1 Maintenance Release 4 (версия 10.2.6.3733);
* для АРМ под управлением других версий ОС Windows использовать пакет обновления СЗ от ВВК Kaspersky Endpoint Security 10 для Windows Service Pack 2 (версия 10.3.0.6294).

1. При установке используйте установку с параметрами по умолчанию.
2. Установить «Агент администрирования», введя IP-адрес Центра администрирования.
3. Зайти в Центр управления и добавить компьютер в группу, для которой применяются настройки согласно приложению 1 документа «Порядок обновления».

### Технологическая карта обновления ПО СЗ от ВВК Dr.Web

### Технологическая карта обновления ПО СЗ от ВВК Dr.Web Enterprise Security Suite 6.0.4 на версию 10.0

При обновлении следует руководствоваться документом "Dr.Web Enterprise Security Suite. Версия 10.0. Руководство по установке".

Перед началом проведения работ обязательно сделать резервное копирование базы данных сервера СЗ от ВВК Dr.Web.

Для успешного выполнения обновления ПО СЗ от ВВК Dr.Web Enterprise Security Suite с версии 6.0.4 до версии 10.0, функционирующем на платформе ОС Windows 2003 Server, необходимо предварительно для ОС установить программное исправление kb925336 (размещено на КПИ - карточка КС РПС номер 26425).

Внимание: После выполнения обновления сервера до версии Dr.Web Enterprise Security Suite 10.0 ранее подключенные к серверу агенты и пакеты Dr.Web версии 6 автоматически (без запроса) обновляются до версии 10.

### Технологическая карта обновления ПО СЗ от ВВК Dr.Web Enterprise Security Suite 10.0 на версию 10.01.0

При обновлении следует руководствоваться следующими документами:

* Dr.Web Enterprise Security Suite. Версия 10.01.0 Руководство по установке;
* Dr.Web Enterprise Security Suite. Версия 10.01.0 Руководство администратора.

Перед началом обновления Сервера Dr.Web Enterprise Security Suite (далее – Dr.Web ESS) рекомендуется проверить корректность настроек протокола TCP/IP для возможности доступа в Интернет. В частности, должна быть включена и содержать корректные настройки служба DNS.

#### Обновление Сервера Dr.Web ESS

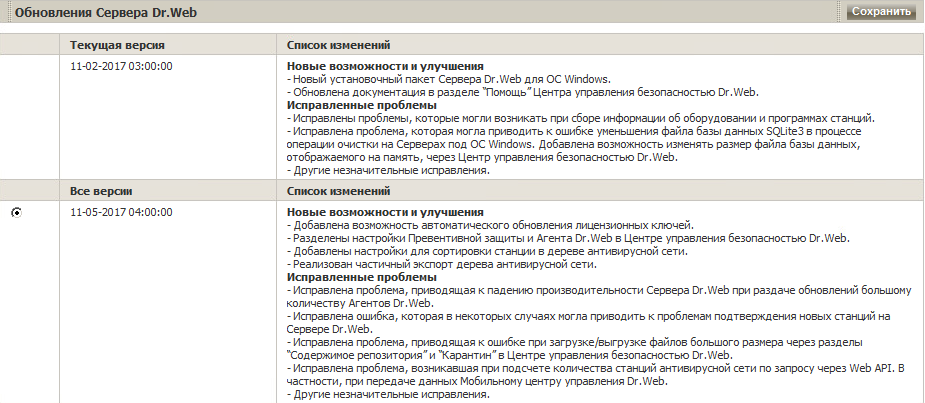
Обновление Сервера Dr.Web ESS в пределах версии 10 осуществлять при помощи Центра управления. Выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**.

В открывшемся окне отображается информация обо всех компонентах, а также дата их последней ревизии и ее текущее состояние. Для проверки наличия обновлений на сервере ВСО нажмите кнопку **Проверить обновления.**

Центр управления предоставляет обновление ПО Сервера Dr.Web ESS на доступную версию 10.01.0, скачанную из ВСО, и хранящуюся в репозитории Сервера Dr.Web ESS.

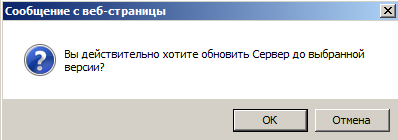
Для обновления ПО Сервера Dr.Web:

1. Выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Сервер Dr.Web**.
2. Перейдите к списку версий Сервера: нажмите на текущую версию Сервера в главном окне. Нажмите кнопку **Список версий**. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера Dr.Web ESS.

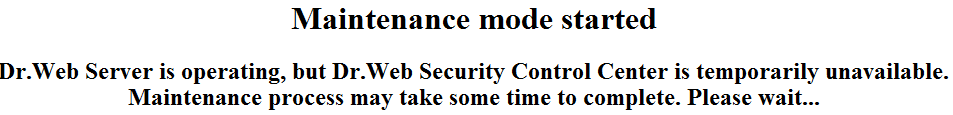


*Рисунок 4 – Раздел Обновления Сервера Dr.Web*

1. Установите опцию напротив версии Сервера 10.01.0 (11-05-2017) в списке **Все версии** и нажмите кнопку **Сохранить** и подтвердите процесс обновления Сервера Dr.Web.



Дождитесь окончания процесса обновления, в течение которого будет информационное окно:



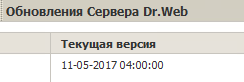
В процессе обновления Сервера Dr.Web ESS текущая версия сохраняется как резервная копия (помещается в раздел Резервные копии), а версия, на которую осуществляется обновление, перемещается из раздела **Все версии** в раздел **Текущая версия**.

Резервные копии сохраняются в каталоге:

var\update\_backup\_<старая\_версия>\_<новая\_версия>.

В процессе обновления создается или дополняется файл журнала var\dwupdater.log.

По окончании процесса обновления можно проверить текущую версию Сервера Dr.Web ESS.



#### Обновление расширения Центр управления безопасностью Dr.Web

Для обновления расширения Центра управления безопасностью Dr.Web (используется **Центром управления**) необходимо вручную удалить предыдущую версию расширения и установить новое расширение Центра управления безопасностью Dr.Web. Процесс установки описан в документе «Dr.Web Enterprise Security Suite. Версия 10.01.0 Руководство по установке» раздел 4.1.4. (Установка расширения Центра управления безопасностью Dr.Web).

#### Обновление Агента Dr.Web

В процессе автоматического обновления Агентов осуществляется удаление старой версии Агента (11.0.x) и установка новой версии (11.0.1.05150). Установка новой версии Агента осуществляется согласно заданию в расписании Сервера Dr.Web ESS, которое будет выполняться после перезагрузки серверов РАБИС-НП и АС ЭКР 2.0. Перезагрузку необходимо запускать вручную[[7]](#footnote-8) после удаления старой версии Агента.

При обновлении Агентов, установленных на серверах, могут быть нежелательны перезагрузки или остановы сетевого ПО, работающего на серверах. Во избежание функционального простоя сервера, предлагается для автоматического режима обновления Агентов и антивирусного ПО в расписании Сервера Dr.Web ESS создать новое задание на обновление нужных компонентов в удобное время, когда это не скажется критически на работе серверов.

Создание и редактирование заданий в расписании Сервера Dr.Web приведено в документе «Dr.Web Enterprise Security Suite. Версия 10.01.0 Руководство администратора» раздел 8.4 (Настройка расписания Сервера Dr.Web).

На серверы не нужно устанавливать компоненты SpIDer Gate, Антиспам Dr.Web, SpIDer Mail, Брандмауэр Dr.Web, Dr.Web для Microsoft Outlook, Офисный контроль Dr.Web.

Обновление Агентов Dr.Web (в автоматическом режиме) происходит в следующем порядке:

1. При запуске обновления удаляется старая версия Агента.
2. Осуществляется перезагрузка компьютера вручную.
3. Осуществляется установка новой версии Агента путем автоматического создания задания в расписании Сервера Dr.Web ESS.
4. После завершения обновления Агента, компьютер автоматически подключается к Серверу Dr.Web ESS. В разделе Состояние Центра управления для обновленного компьютера будет отображаться уведомление о необходимости перезагрузки. Необходимо выполнить перезагрузку компьютера.

Обновление Агентов Dr.Web в ручном режиме происходит если по какой-либо причине автоматическое обновление не было успешно и происходит в соответствии с документом «Dr.Web Enterprise Security Suite. Версия 10.01.0 Руководство по установке» разделы 4.2.3.1 – 4.2.3.2. При этом после установки нового Агента потребуется объединить новую и старую станции в Центре управления, в иерархическом списке антивирусной сети.

# Технологическая карта обновления (актуализации) унифицированных конфигураций системы «Контроль-ПУ» Территориальных учреждений Банка России

## Состав обновления системы «Контроль-ПУ»

В качестве унифицированной системы «Контроль-ПУ» для стендов тестирования ТУ необходимо применять программный комплекс (ПК) DeviceLock (версия 8.2.69641) в составе:

* агентов DeviceLock Service, устанавливаемых на АРМ пользователей и администраторов РАБИС-НП и АС ЭКР 2.0;
* серверов указанной системы – сервер DeviceLock Enterprise Server и сервер DeviceLock Content Security Server (опционально);
* консоли управления, устанавливаемой на АРМ администратора системы: DeviceLock Management Console / DeviceLock Group Policy Manager / DeviceLock Enterprise Manager / DeviceLock WebConsole.

По умолчанию DeviceLock Service, DeviceLock Enterprise Server и DeviceLock Content Security Server используют порты 9132, 9133 и 9134 соответственно. Если эти порты заняты, то динамически выделяются другие порты.

При управлении через групповые политики Active Directory, DeviceLock не использует собственные RPC-подключения. В этом случае все управляется с помощью Active Directory.

Для просмотра отчетов - графов связей (Relations Charts) на АРМ администратора системы «Контроль-ПУ» должен быть установлен обозреватель Microsoft Internet Explorer 9 или более поздней версии.

## Технологическая карта обновления системы «Контроль-ПУ»

При обновлении системы следует руководствоваться документом «DeviceLock DLP Suite 8.2. Руководство пользователя».

Для обновления компонент DeviceLock необходимо иметь права администратора (локального администратора в случае использовать DeviceLock только на локальном компьютере, администратора домена в случае использования DeviceLock в сети).

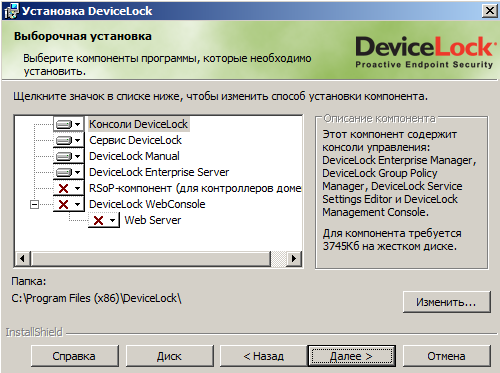
Следующие TCP/UDP-порты необходимо открыть для передачи данных между службами DeviceLock Service и DeviceLock Enterprise Server:

* 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).

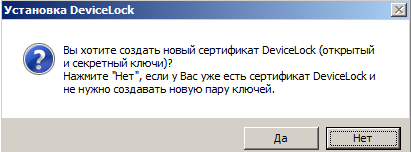
### Обновление DeviceLock Enterprise Server

1. Для обновления сервера DeviceLock Enterprise Server запустить установщик новой версии DeviceLock (файл setup.exe из состава дистрибутива).
2. Следовать указаниям мастера установки DeviceLock и принять условия Лицензионного соглашения.
3. Указать вид установки Выборочная и выбрать необходимые обновляемые компоненты, установленные ранее на сервере:

* Консоли DeviceLock;
* DeviceLock Manual;
* DeviceLock Enterprise Server;
* RSoP-компонент.



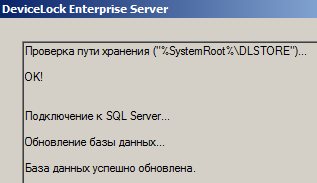
1. На вопрос о создании нового сертификата для Консолей DeviceLock ответьте Нет и используйте действующие сертификаты пары ключей (открытый и секретный). По использованию сертификатов руководствуйтесь документом "DeviceLock DLP Suite. Руководство пользователя. Версия продукта 8.2".



1. В процессе установки вам необходимо сконфигурировать DeviceLock Enterprise Server и задать его основные параметры, используя специальный мастер настроек. Если вы устанавливаете обновление DeviceLock Enterprise Server’а и при этом не хотите ничего менять в текущих настройках, вы можете нажать кнопку Отмена, чтобы закрыть мастер настроек и сохранить текущую конфигурацию, либо нажать кнопку Далее и проверить действующие настройки:

* запуска DeviceLock Enterprise Server;
* настроек подключения;
* настроек безопасности;
* данные сертификата секретного ключа;
* параметры подключения к СУБД;
* параметры настроек теневого копирования в SQL Server.

По окончании проверки действующих настроек будет выдано сообщение об успешности обновления базы данных.



1. В случае если вам все же надо изменить какой-либо параметр, но сохранить все остальные настройки – отредактируйте только этот нужный параметр и пройдите через все страницы мастера настроек и нажмите кнопку Завершить на последней странице.
2. При обновлении на сервере службы DeviceLock в окне настроек «Заблокировать каналы» нажать клавишу Пропустить.

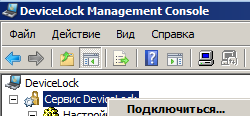
### Обновление DeviceLock Service

Обновление сервиса DeviceLock возможно следующими способами:

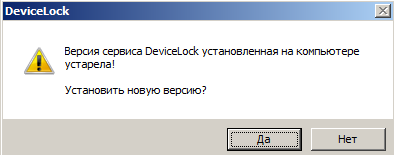
* с помощью консоли DeviceLock Management Console;
* с помощью консоли DeviceLock Enterprise Manager;
* локально.

### Обновление DeviceLock Service с помощью консоли DeviceLock Management Console

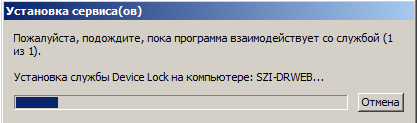
Для обновления данным способом необходимо запустить консоль DeviceLock Management Console и подключиться к обновляемому сервису DeviceLock компьютера.



При попытке подключения к компьютеру будет предложено установить новую версию. На предложение установки новой версии выбрать Да.



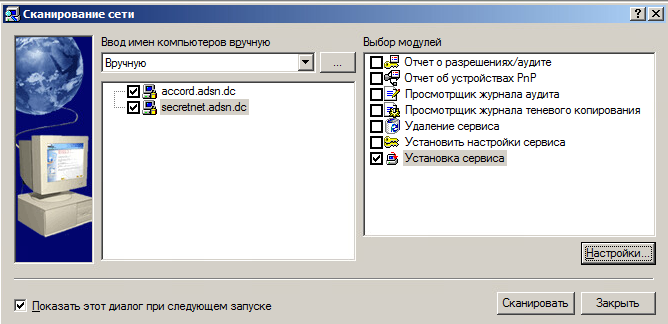
Необходимо дождаться окончания установки новой версии сервиса DeviceLock.



### Обновление DeviceLock Service с помощью консоли DeviceLock Enterprise Manager

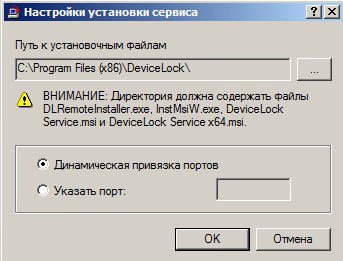
Консоль DeviceLock Enterprise Manager содержит специальный модуль «Установка сервиса», который позволяет автоматически установить обновленные версии DeviceLock Service на все компьютеры системы «Контроль-ПУ». Для обновления:

1. Выбрать компьютеры, на которых DeviceLock Service должен быть обновлен (можно выбрать по типам и именам, загрузить список из внешнего файла или выбрать из LDAP-дерева (Active Directory и т.п.)).
2. Выберите модуль Установка сервиса и нажмите Настройки, чтобы указать местонахождение исполняемого файла обновленной версии Device Lock Service.



*Рисунок 5 – Окно выбора модуля Установки сервиса Device Lock*

1. Если не используется Динамическая привязка портов (по умолчанию 9132), укажите используемый порт.



*Рисунок 6 – Окно настройки установки сервиса Device Lock*

1. Нажмите кнопку Сканировать.

### Локальное обновление DeviceLock Service

Для локального обновления необходимо запустить файл установщика setup.exe из каталога установки дистрибутива и следовать указаниям мастера установки DeviceLock.

Выбрать компоненту Сервис DeviceLock и нажать «Установить» в завершающем окне мастера установки. Дождаться окончания обновления сервиса: сервис DeviceLock будет обновлен автоматически, настройки предыдущей версии будут сохранены.

## Настройка системы «Контроль-ПУ»

После обновления агента DeviceLock Service произойдет унаследование настроек от предыдущей версии агента DeviceLock. Если необходимо включить или настроить дополнительные механизмы системы «Контроль ПУ», то необходимо руководствоваться документами "DeviceLock DLP Suite. Руководство пользователя. Версия продукта 8.2" и ''Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации Территориальных учреждений для РАБИС-НП и АРМ АС ЭКР 2.0''.

# Технологическая карта обновления унифицированных конфигураций системы паспортизации ТУ Банка России

Совместно с данной документацией необходимо использовать следующую документацию разработчика ООО «Технос-К»:

* «ПК «Паспорт АРМ УОС». Руководство Администратора информационной безопасности», шифр документа ‑ ТК.4257101-29 91 01;
* «ПК «Паспорт АРМ УОС». Руководство пользователя», шифр документа - ТК.4257101-29 34 01.

## Особенности перехода с предыдущих версий системы паспортизации

Внимание. Версия 5.17.8.4 системы паспортизации ПК «Паспорт АРМ УОС» несовместима с предыдущими версиями: 4.Х.Х.Х и 5.13.Х.Х - 5.15.Х.Х. Переход на новую версию возможен только путем удаления предыдущих версий и установкой новой версии с применением собственных установочных модулей.

Для формирования дальнейшей структуры сети ПК «Паспорт АРМ УОС», создания необходимых сетевых информационных ресурсов и организации контроля целостности прикладного ПО ПЭВМ и серверов РАБИС и АС ЭКР 2.0 возможен экспорт и использование следующих данных из предыдущих версий ПК «Паспорт АРМ УОС»:

1. Список и информация о зарегистрированных компьютерах, содержащий всю необходимую информацию. Для этого необходимо выполнить «Экспорт данных» из меню «Сервис» под ролью Администратора системы паспортизации.



*Рисунок 7 – Окно экспорта списков компьютеров*

Необходимо убедиться в формировании всех текущих паспортов на основании ответов от клиентских компонент. После окончания экспорта будет сформирован файл *COMPUTERS.XML* содержащий всю необходимую информацию. Структура данного файла описана в «Руководстве программиста» соответствующей версии системы паспортизации.

1. Базу программных модулей, содержащую параметры контроля целостности прикладного ПО АРМ пользователей и серверов РАБИС-НП и АС ЭКР 2.0. Для этого необходимо выполнить «Экспорт справочников программных модулей» из меню «Сервис» под ролью Администратора системы паспортизации. После окончания экспорта будет сформирован файл *MODULES.XML* содержащий необходимую информацию для настройки параметров контроля в новой версии ПК «Паспорт АРМ УОС» (см. раздел 5.4). Структура данного файла описана в «Руководстве программиста» соответствующей версии системы паспортизации.

Для установки и первоначальной настройки системы паспортизации на локальном компьютере необходимо иметь права локального администратора. Для установки и первоначальной настройки системы паспортизации в доменной сети необходимо иметь права администратора домена.

## Состав обновления системы паспортизации

В состав ПК «Паспорт АРМ УОС» (версия 5.17.8.4) входят следующие компоненты:

* Внутренний архив ПС – сервер данных ПК «Паспорт АРМ УОС»;
* Анализатор изменений ПО – клиентское ПО АРМ пользователей и серверов РАБИС-НП и АС ЭКР 2.0;
* в качестве консоли управления АРМ администратора ИБ:
  + Управление ПС (консоль пользователя) - централизованное управление системой паспортизации;
  + Получение изменений (данных) с автономных АРМ – управление системой паспортизации автономными АРМ.
* Автоматическое проведение модификаций (обновлений) входит в состав устанавливаемой компоненты Управление ПС (*spupdate.exe*).

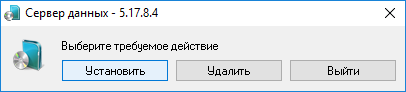
По умолчанию в ПК «Паспорт АРМ УОС» используется протокол HTTP и порты:

* входящий порт компоненты «Внутренний архив ПС»: 5050;
* входящий порт клиентской части: 5051.

## Технологическая карта обновления системы паспортизации

#### Установка сервера данных ПК «Паспорт АРМ УОС»

Для установки компоненты «Внутренний архив ПС» необходимо запустить на выполнение инсталляционный исполняемый модуль **ds05170804.exe** из состава инсталляционного пакета.

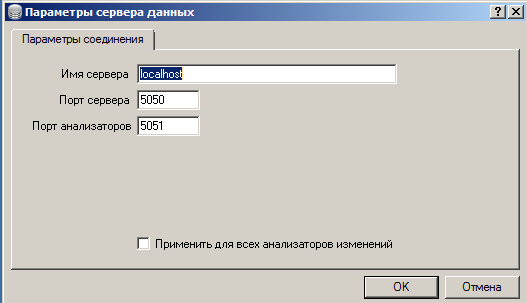


*Рисунок 8 – Установка сервера данных ПК «Паспорт АРМ УОС»*

Установка компоненты производится автоматически, без каких-либо дополнительных действий пользователя.

В случае инсталляции на ОС Windows 7 и/или Windows Server 2008 и более поздних запуск на выполнение сопровождается предупреждением системы безопасности о повышении прав доступа.

После установки необходимо запустить конфигуратор компоненты путем выбора пункта меню **«Паспорт программного обеспечения – Параметры сервера данных»** в основном меню Windows и настроить параметры сервера данных ПК «Паспорт АРМ УОС».

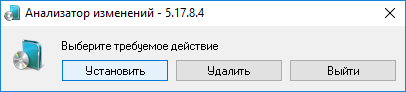


*Рисунок 9 –Настройка параметров соединения Внутреннего архива ПС (сервера данных)*

После выполнения операций по установке и настройке необходимо открыть соответствующие порты соединения на средствах межсетевого экранирования АРМ пользователей и серверов РАБИС-НП и АС ЭКР 2.0 и сетевой инфраструктуры ТУ.

#### Установка клиентского ПО ПК «Паспорт АРМ УОС»

Для установки компоненты «Анализатор изменений ПО» необходимо запустить на выполнение инсталляционный исполняемый модуль **ca05170804.exe** из состава инсталляционного пакета.

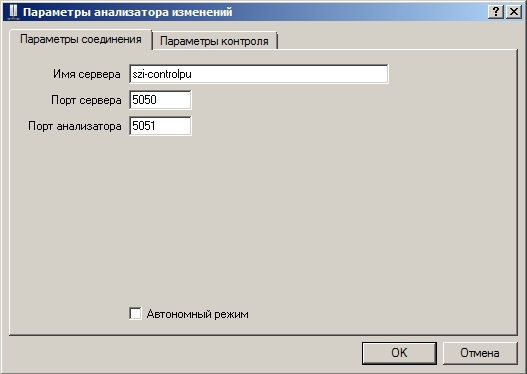


**Установка клиентского ПО ПК «Паспорт АРМ УОС»**

Установка компоненты производится автоматически, без каких-либо дополнительных действий пользователя. Данная компонента устанавливается на все контролируемые компьютеры пользователей и серверов РАБИС-НП и АС ЭКР 2.0.

В случае инсталляции на ОС Windows 7 и/или Windows Server 2008 и более поздних запуск на выполнение сопровождается предупреждением системы безопасности о повышении прав доступа.

После установки необходимо запустить конфигуратор компоненты путем выбора пункта меню **«Паспорт программного обеспечения – Параметры анализатора изменений»** в основном меню Windows.



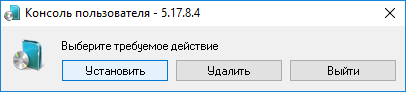
*Рисунок 10 –Настройка параметров соединения Анализатора изменений (клиентское ПО) с архивом ПС (сервером данных)*

Параметры соединения необходимо установить в соответствии с параметрами соединения внутреннего архива (сервера данных).

В случае если анализатор изменений устанавливается на автономном АРМ пользователя РАБИС-НП и АС ЭКР 2.0, необходимо установить метку **«Автономный режим»** для обеспечения выполнения синхронизации с внутренним архивом посредством компоненты «Получение изменений с автономных АРМ».

#### Установка консоли централизованного управления ПК «Паспорт АРМ УОС»

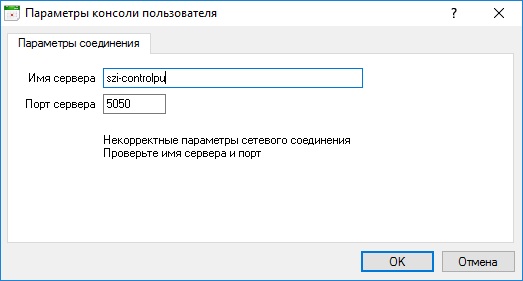
Для установки консоли управления АРМ Администратора ИБ (компоненты «Управление ПС») необходимо запустить на выполнение инсталляционный исполняемый модуль **uc05170804.exe** из состава инсталляционного пакета.



Установка компоненты производится автоматически, без каких-либо дополнительных действий пользователя. Компонента устанавливается на АРМ администраторов, контролеров и операторов системы паспортизации.

В случае инсталляции на ОС Windows 7 и/или Windows Server 2008 и более поздних запуск на выполнение сопровождается предупреждением системы безопасности о повышении прав доступа.

После установки запуск производится путем выбора пункта меню **«Паспорт программного обеспечения – Консоль пользователя»** в основном меню Windows.

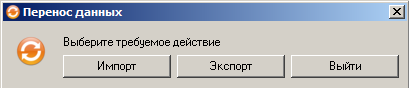


*Рисунок 11 – Настройка параметров соединения консоли управления ПК «Паспорт АРМ УОС»*

Параметры соединения консоли управления ПК «Паспорт АРМ УОС» необходимо установить в соответствии с параметрами соединения внутреннего архива (сервера данных).

#### Установка консоли управления системой паспортизации автономных АРМ

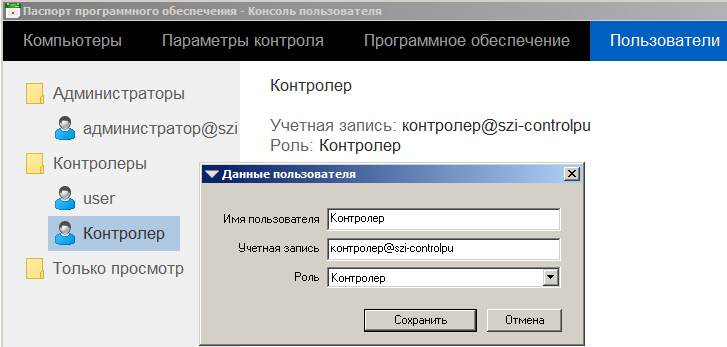
Исполняемый модуль и модуль автозапуска компоненты «Получение изменений с автономных АРМ» (SPOFFLINE.EXE) должны располагаться на съемном USB носителе информации в корневом каталоге. Для этого необходимо скопировать данные файлы из состава инсталляционного пакета на съемный носитель.



Настройка компоненты не требуется, так как все необходимые данные получает из настроек анализаторов изменений установленных на СВТ.

#### Заведение пользователей ПК «Паспорт АРМ УОС»

После установки системы паспортизации Администратору ИБ с помощью консоли пользователя необходимо выбрать роль пользователя системы паспортизации (Администратор; Контролер; только просмотр) и добавить нового пользователя нажав клавишу **Добавить пользователя**.



*Рисунок 12 – Добавление пользователя ПК «Паспорт АРМ УОС»*

## Настройка системы паспортизации

После установки компонент ПК «Паспорт АРМ УОС» необходимо настроить параметры контроля целостности прикладного ПО ПЭВМ и серверов РАБИС и АС ЭКР 2.0. Для выполнения настройки комплекса необходимо руководствоваться документами «ПК «Паспорт АРМ УОС». Руководство пользователя» (шифр документа ТК.4257101-29 34 01) и «Порядок обновления (актуализации) унифицированных конфигураций средств защиты информации Территориальных учреждений для РАБИС-НП и АРМ АС ЭКР 2.0».

### Список сокращений и терминов

|  |  |
| --- | --- |
| АС ЭКР | автоматизированная система эмиссионно- кассовых работ |
| СЗ от ВВК | средство защиты от воздействия вредоносного кода |
| СЗИ | средство защиты информации |
| РАБИС-НП | типовой программный комплекс Региональная автоматизированная банковская информационная система |
| ТУ | Территориальное учреждение Банка России |
| НСД | Несанкционированный доступ |

1. Процедура создания загрузочного носителя описана в разделе 3 документа «Комплекс СЗИ от НСД для ПЭВМ (PC) «Аккорд–АМДЗ» (Аппаратный модуль доверенной загрузки) Руководство по установке» [↑](#footnote-ref-2)
2. Набор файлов обновления можно получить службе технической поддержки разработчика продукта ОКБ САПР ([help@okbsapr.ru](mailto:help@okbsapr.ru)). Версия встроенного ПО контроллера Аккорд-5MX/5.5/5.5e должна быть 02.01.015. [↑](#footnote-ref-3)
3. Перед удалением каталога возможно сохранить ключ лицензии – файл accord.key [↑](#footnote-ref-4)
4. Обновление с бета-версий до версии Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 для Windows не поддерживается. [↑](#footnote-ref-5)
5. Перед установкой обновления вам необходимо ознакомиться с текстом Лицензионного соглашения с конечным пользователем и подтвердить, что вы согласны с его условиями. Если вы не подтвердите свое согласие, то обновление не будет установлено: подтверждение выполняется с помощью консоли Kaspersky Security Center в узле **Управление программами** в разделе **Обновление программного обеспечения.**  [↑](#footnote-ref-6)
6. После установки обновления настройка установки обновлений программы будет изменена на **Устанавливать только подтвержденные обновления.**  [↑](#footnote-ref-7)
7. После удаления Агента, оповещение о необходимости перезагрузки на станции не отображается. Администратор ИБ СЗ от ВВК должен сам инициировать перезагрузку станции. После обновления Агента без перезагрузки станции функционирование антивирусного ПО будет ограничено (при этом не обеспечивается полная антивирусная защита станции). Необходимо выполнить перезагрузку компьютера по требованию Агента. [↑](#footnote-ref-8)