Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования

Национальный исследовательский университет “МИЭТ”

Кафедра информационной безопасности

Домашнее задание 1

**Дисциплина: Информационная безопасность**

Выполнили студенты П-42:

Селезнева Валерия  
  
Утева Александра

2021 год

**Задание.**

Необходимо провести настройку средств защиты информации (СДЗ, МЭ, СОВ…) в соответствии с функциональными требованиями безопасности с использованием возможностей ОС Windows и дополнительных программных средств по варианту 2 АС 2Б (СВТ КЗ 5).

Защиты от НСД осуществляется по 4 подсистемам:

управления доступом;

регистрации и учета;

криптографическая;

обеспечения целостности.

В зависимости от класса АС требования к перечисленным подсистемам различаются. Требования к подсистемам в зависимости от класса защищенности представлены в таблице.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Подсистемы и требования** | **Классы** | | | | | | | | |
| **3Б** | **3А** | **2Б** | **2А** | **1Д** | **1Г** | **1В** | **1Б** | **1А** |
| **1. Подсистема управления доступом** |  | | | | | | | | |
| 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: |  | | | | | | | | |
| в систему | + | + | + | + | + | + | + | + | + |
| к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ | - | - | - | + | - | + | + | + | + |
| к программам | - | - | - | + | - | + | + | + | + |
| к томам, каталогам, файлам, записям, полям записей | - | - | - | + | - | + | + | + | + |
| 1.2. Управление потоками информации | - | - | - | + | - | - | + | + | + |
| **2. Подсистема регистрации и учета** |  | | | | | | | | |
| 2.1. Регистрация и учет: |  | | | | | | | | |
| входа (выхода) субъектов доступа в (из) систему (узел сети) | + | + | + | + | + | + | + | + | + |
| выдачи печатных (графических) выходных документов | - | + | - | + | - | + | + | + | + |
| запуска (завершения) программ и процессов (заданий, задач) | - | - | - | + | - | + | + | + | + |
| доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи | - | - | - | + | - | + | + | + | + |
| доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей | - | - | - | + | - | + | + | + | + |
| изменения полномочий субъектов доступа | - | - | - | - | - | - | + | + | + |
| создаваемых защищаемых объектов доступа | - | - | - | + | - | - | + | + | + |
| 2.2. Учет носителей информации | + | + | + | + | + | + | + | + | + |
| 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей | - | + | - | + | - | + | + | + | + |
| 2.4. Сигнализация попыток нарушения защиты | - | - | - | - | - | - | + | + | + |
| **3. Криптографическая подсистема** |  | | | | | | | | |
| 3.1. Шифрование конфиденциальной информации | - | - | - | + | - | - | - | + | + |
| 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах | - | - | - | - | - | - | - | - | + |
| 3.3. Использование аттестованных (сертифицированных) криптографических средств | - | - | - | + | - | - | - | + | + |
| **4. Подсистема обеспечения целостности** |  | | | | | | | | |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | + | + | + | + | + | + | + | + | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации | + | + | + | + | + | + | + | + | + |
| 4.3. Наличие администратора (службы) защиты информации в АС | - | - | - | + | - | - | + | + | + |
| 4.4. Периодическое тестирование СЗИ НСД | + | + | - | + | + | + | + | + | + |
| 4.5. Наличие средств восстановления СЗИ НСД | + | + | + | + | + | + | + | + | + |
| 4.6. Использование сертифицированных средств защиты | - | + | - | + | - | - | + | + | + |

*Примечание: " - " - нет требований к данному классу;*

*" + " - есть требования к данному классу.*

Таким образом, в данной лабораторной работе мы проведем настройку средств защиты АС по классу защищенности 2Б с использованием возможностей ОС Windows и дополнительных программных средств.

# Вторая Практическая часть

# Исходные данные

Домашнее задание выполняется согласно варианту: **2 АС 2Б (СВТ КЗ 5)**

# Определение требований классу защищенности систем обработки данных

Таблица 1 – Основные подсистемы и требования

|  |  |
| --- | --- |
| **Подсистемы и требования** | **Класс 2Б** |
| **1. Подсистема управления доступом** | |
| 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: | |
| в систему | + |
| *Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.* | |
| **2. Подсистема регистрации и учета** | |
| 2.1. Регистрация и учет: | |
| входа (выхода) субъектов доступа в (из) систему (узел сети) | + |
| 2.2. Учет носителей информации | + |
| должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.  В параметрах регистрации указываются:  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;  - должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку). | |
| **4. Подсистема обеспечения целостности** |  |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации | + |
| 4.5. Наличие средств восстановления СЗИ НСД | + |
| должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.  При этом:  - целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;  - целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;  - должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;  - должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности. | |

Таблица 2 – Варианты реализации настроек по классу защищенности АС

|  |  |
| --- | --- |
| **Подсистемы и требования** | **Вариант**  **реализации** |
| **1. Подсистема управления доступом** | |
| 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: | |
| в систему | Обеспечивается средствами SecretNet Studio |
| **2. Подсистема регистрации и учета** | |
| 2.1. Регистрация и учет: | |
| входа (выхода) субъектов доступа в (из) систему (узел сети) | Обеспечивается средствами SecretNet Studio |
| 2.2. Учет носителей информации | Учет носителей информации осуществляется путем занесения действий с носителями, подлежащим учету, в специальную таблицу-журнал |
| **4 Подсистема обеспечения целостности** | |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | Обеспечивается средствами SecretNet Studio |
| 4.2.Физическая охрана средств вычислительной техники и носителей информации | Обеспечивается посредством заключения контракта с ЧОП |
| 4.5. Наличие средств восстановления СЗИ НСД | Обеспечивается средствами операционной системы Windows 10 “Восстановление” |

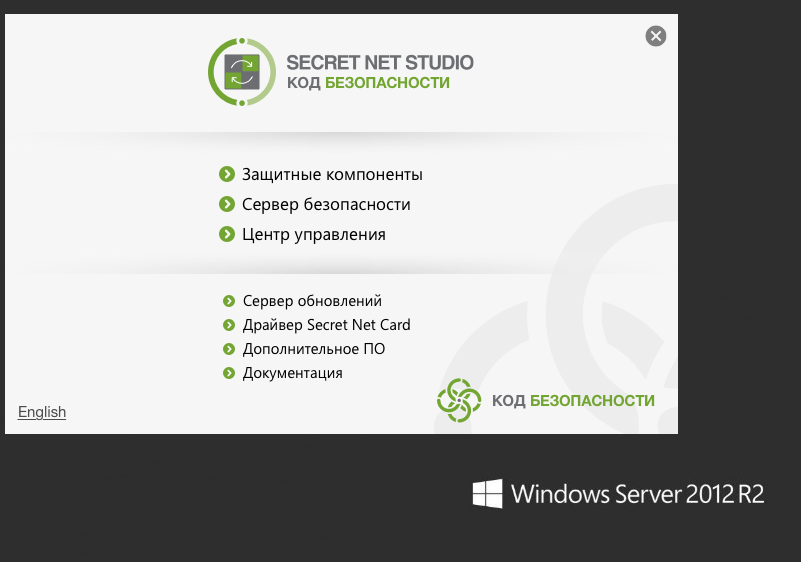
# Настройка средств защиты СВТ на ОС Windows по классу защищенности

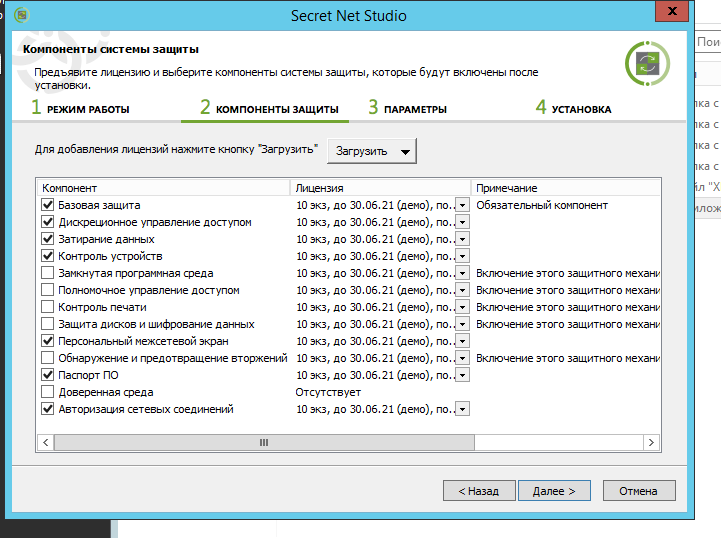
**Подсистема управления доступом**

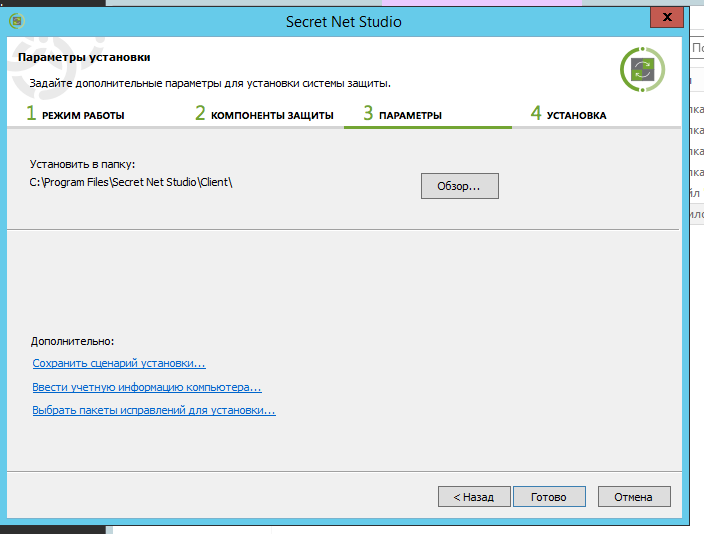
Идентификация, проверка подлинности и контроль доступа субъектов в систему.

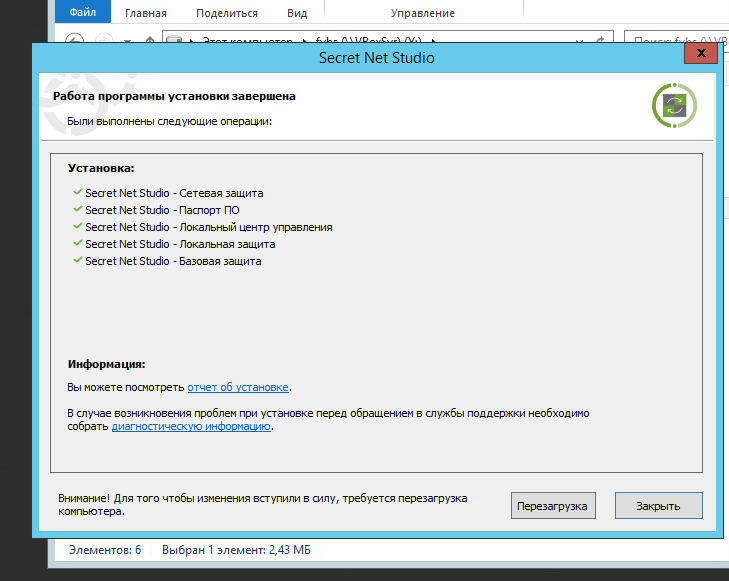
По требованию длина пароля должна быть не менее 6 символов. Настроили Secret Net согласно этому требованию.

1. **Установка Secret Net**

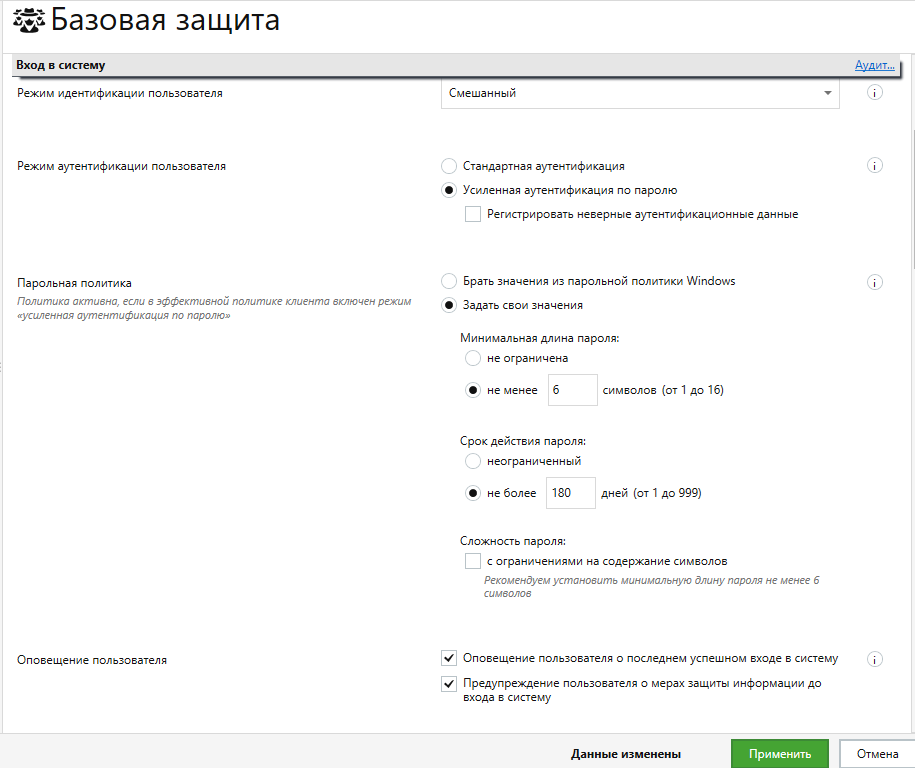




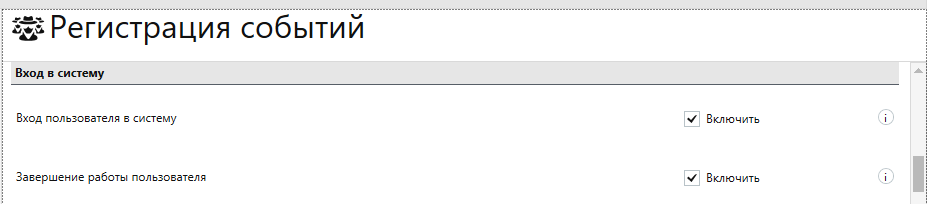




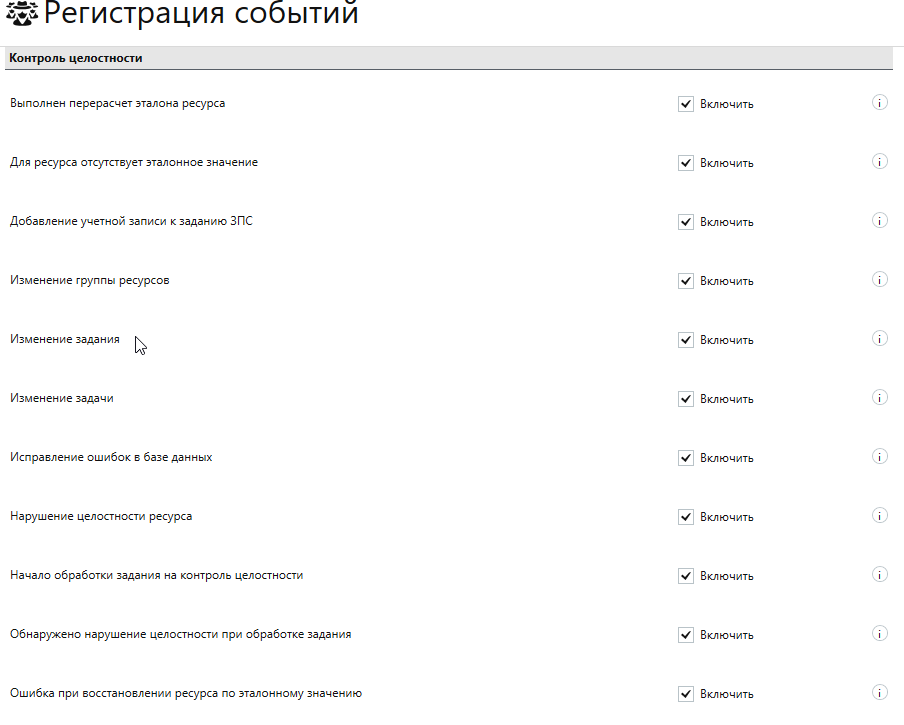
1. **Настройка средств защиты СВТ на ОС Windows по классу защищенности**

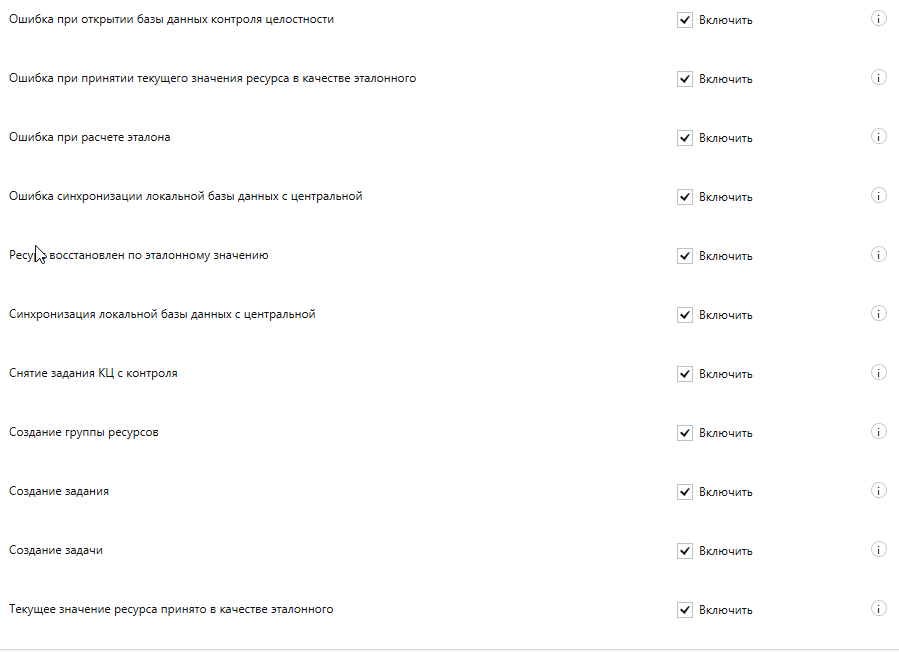
****

1. **Регистрация и учет входа**

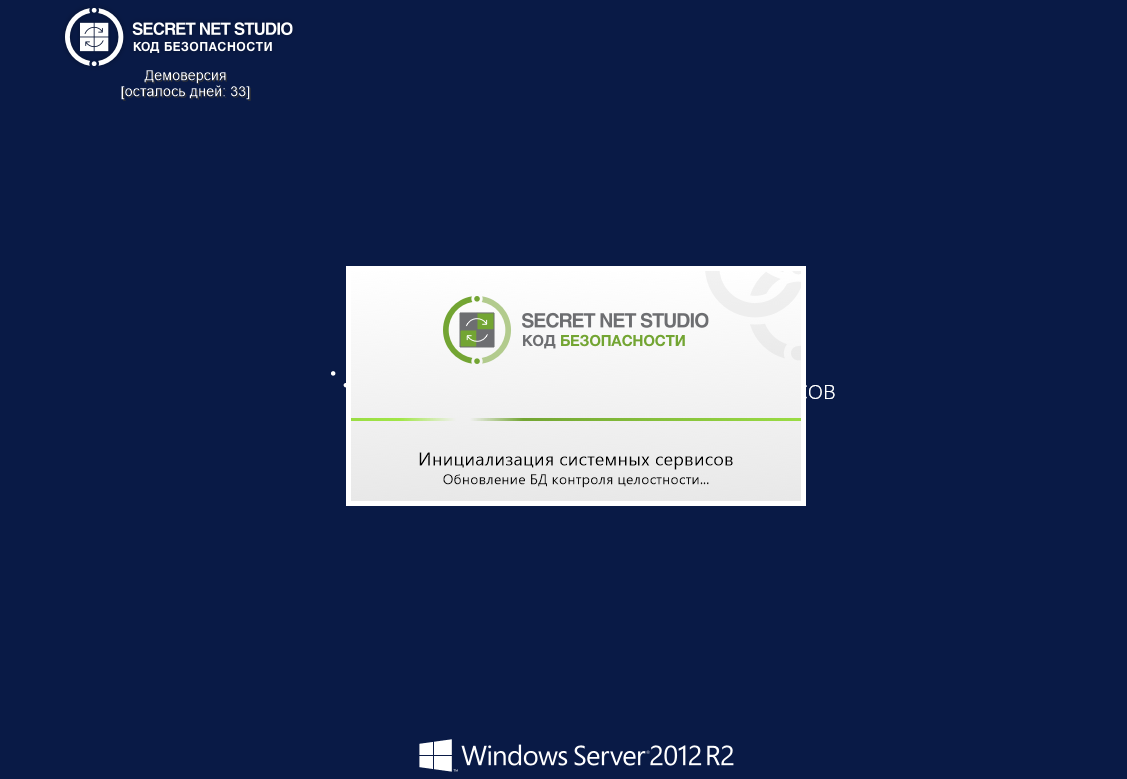
****

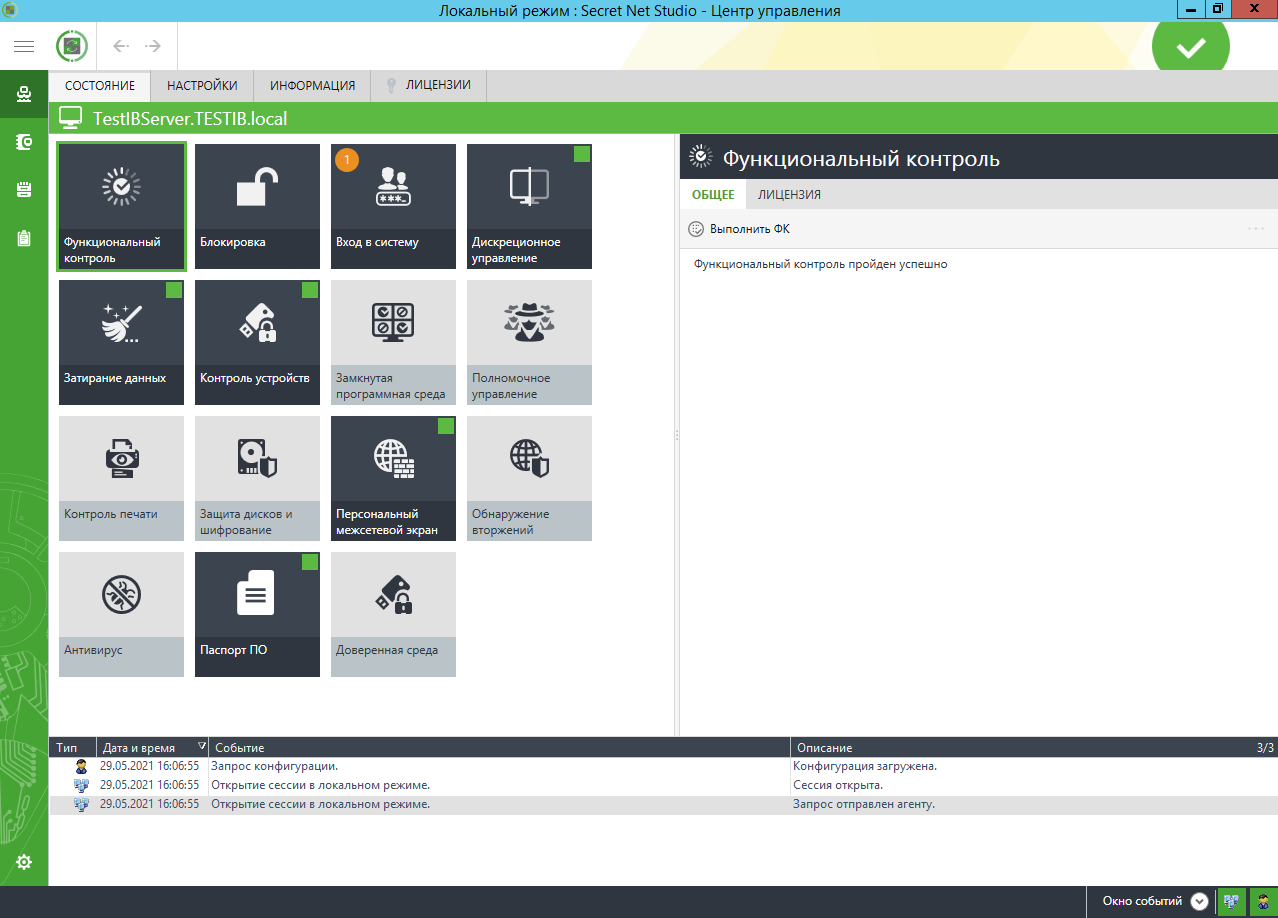
1. **Обеспечение целостности программных средств и обрабатываемой информации**



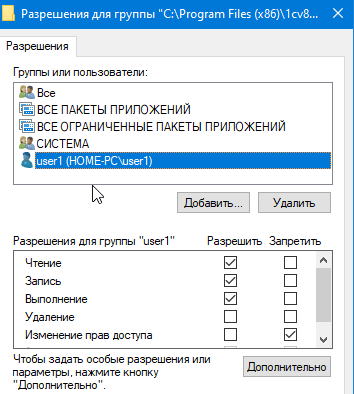


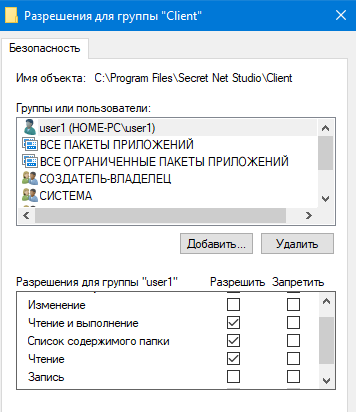
1. **Результат**





1. **Настройка прав доступа к папке с программой “1С: Предприятие 8. Аптека”**



1. **Изменение прав доступа к папке с СЗИ “Secret Net”**
2. **Настройка прав доступа пользователя к папке с СЗАИ “ESET.NOD 32”**

