

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ПРАКТИЧЕСКОГО ЗАДАНИЯ №10**

**В РАМКАХ ДИСЦИПЛИНЫ «**[**ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ**](https://online-edu.mirea.ru/course/view.php?id=10256)**»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Secret-Net studio выпускается компанией «Код Безопасности». Офис компании расположен в Москве. Первая версия secret net была запущена в продажу в 1992 году. На данный момент компания обладает рядом лицензий.

1. (ФСБ РОСИИ) На осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
2. (ФСБ РОСИИ) На осуществление разработки и (или) производства средств защиты конфиденциальной информации.
3. (ФСБ РЩССИИ) На осуществление мероприятий и (или) оказания услуг в области защиты государственной тайны.
4. (ФСБ РОСИИ) На осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну.
5. (УФСБ России по г.Москве и Московской обл.) На осуществление работ, связанных с использованием сведений, составляющих государственную тайну.
6. (МО РФ) На деятельность в области создания средств защиты информации.
7. (ФСТЭК России №2457) На проведение работ, связанных с созданием средств защиты информации.
8. (ФСТЭК России №0499) На осуществление разработки и производства средств защиты конфиденциальной информации.
9. (ФСТЭК России №0829) На деятельность по технической защите конфиденциальной информации.

Программный продукт Secret net был разработан для защиты конечных точек (ПК) от угроз ИБ.

1. Угрозы данным
   1. Кража данных внешним злоумышленником
   2. Потеря данных в результате атаки вирусашифровальщика
   3. Утечка данных в результате действий внутреннего нарушителя
2. Угрозы системе
   1. Заражение вредоносным ПО
   2. Закрепление злоумышленника в системе
   3. Несанкционированный доступ к конфиденциальным данным
   4. Несанкционированное изменение прикладного ПО
3. Угрозы LAN
   1. Горизонтальное распространение злоумышленника (один из этапов атаки на организацию, во время которого злоумышленник, уже сумевший проникнуть внутрь корпоративной инфраструктуры и закрепиться в ней, начинает продвигаться по сети от точки входа (например, скомпрометированного устройства или аккаунта) к другим объектам.)
   2. Перехват трафика
   3. Распространение червей

В данное работе изучается программный продукт Secret Net Studio. Данный продукт имеет следующие сертификаты

**Минобороны России:317/6/1610**

**Secret Net Studio, Secret Net Studio – C**

Подтверждает, что для продуктов Secret Net Studio и Secret Net Studio - C, имеющих сертификат соответствия ФСТЭК России, при использовании на объектах информатизации Министерства Обороны России, дополнительная сертификация в системе сертификации СЗИ (Средства Защиты Информации)ч Минобороны России не требуется

**Действителен:**12.12.2024

**ФСТЭК России****[3675](https://www.securitycode.ru/upload/iblock/75e/wz9ch028ew48vur4iwm4tfcxj6mabj0g/3675%20%D0%A4%D0%A1%D0%A2%D0%AD%D0%9A%20%D0%A1%D0%97%D0%98%20SNS-C%20%D0%B4%D0%BE%202024%20%D0%BF%D0%B5%D1%80%D0%B5%D0%BE%D1%84%D0%BE%D1%80%D0%BC%D0%BB%D0%B5%D0%BD%202022.pdf" \t "_blank)**

**Secret Net Studio - C**

Подтверждает соответствие требованиям руководящих документов (**Требования по безопасности информации. Утверждены приказом ФСТЭК России от 2 июня 2020 г. N 76)** по 2 уровню доверия (из 6, соответствует 5 уровню), по 3 классу защищенности(из 6) СВТ(Средства Вычислительной Техники, **Руководящий документ от 30 марта 1992 г.**), 2 классу защиты МЭ(Межсетевой Экран) тип "В" (ИТ.МЭ.В2.ПЗ, **Информационное сообщение ФСТЭК России от 12 сентября 2016 г. N 240/24/4278**). Может применяться в АС(Автоматизированных Системах) до классов 1Б, 2А, 3А включительно (**Руководящий документ от 30 марта 1992 г**), АС до классов(всего 9) 3А, 3Б, 2А, 2Б включительно (**приказ ФСТЭК России №025 от 20.10.2016**), ИСПДн (Информационная Система Персональных Данных) до УЗ1(Уровни Защищенности) включительно (**Приказ ФСТЭК России от 18 февраля 2013 г. N 21)**, ГИС(государственные Информационные Системы) до 1 класса включительно, АСУ ТП до 1 класса включительно, объектах КИИ(критической Информационная Инфраструктуры) до 1 категории значимости включительно

**Действителен:**12.12.2024

**ФСБ России****:**[**СФ/СЗИ-0718**](https://www.securitycode.ru/upload/iblock/275/8nkyjuj9lnuf6scrpt45fr31j7ki11am/%D0%A1%D0%A4%20%D0%A1%D0%97%D0%98-0718%20%D0%A1%D0%97%D0%98%20SNS.pdf)

**Secret Net Studio**

Подтверждает соответствие "Требованиям к средствам защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа"( **Приказ Федеральной службы по техническому и экспортному контролю  
от 11 февраля 2013 г. N 17)** для класса АК3 (всего 6)при совместном использовании с АПМДЗ(**Аппаратно-Программный Модуль Доверенной Загрузки)** соответствующего класса

**Действителен:**30.05.2029

**ФСТЭК России****:**[**3745**](https://www.securitycode.ru/upload/iblock/e59/3745.pdf)

**Secret Net Studio**

Подтверждает соответствие требованиям руководящих документов по 4 уровню доверия, 5 классу защищенности СВТ, 4 классу защиты СКН (средство контроля съемных машинных носителей информации) (ИТ.СКН.П4.ПЗ), 4 классу защиты САВЗ(Средства Анти Вирусной Защиты) (**Методический документ от 14 июня 2012 г.**), 4 классу защиты МЭ тип "В" (**Информационное сообщение ФСТЭК России от 12 сентября 2016 г. N 240/24/4278**), 4 классу защиты СОВ (Система Обнаружения Вторжений) (**Информационное письмо ФСТЭК России**). Может применяться в АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно

**Действителен:**16.05.2025

**Тех. Поддержка:**16.05.2025

Сертификаты были выданы на два продукта Secret Net Studio и Secret Net Studio-C. Приписка C обозначает возможность работы данного программного продукта с сведениями содержащими информацию уровня допуска «Совершенно секретно»

Каждый программный продукт содержит три компонента

1. Клиент
2. Сервер безопасности
3. Центр управления

Реализация защиты базируется на строгом контроле доступа, контроле устройств, контроле печати, а права доступа выдаются после многофакторной аутентификации (пароли, карты, биометрия, Программно-Аппаратный комплекс Соболь, производство код безопасности).

Предусмотрены средства защиты данных такие как

1. Контроль целостности данных (хэш сумма)
2. Шифрование контейнеров (шифрование данных на диске)
3. Теневые копии
4. Гарантированное удаление данных

Программный продукт предоставляет IPS/IDS систему, ведет аудит устройств и поддерживает возможность подписи последних.

На этапе распространения в LAN Secret net производит обнаружение на основе ip адресов, портов, активности пользователя. Поддерживает разграничение LAN на VLAN.

В случае проникновения злоумышленника на конечное устройство Secret Net гарантирует запуск только разрешенных приложений\процессов, гарантирует не низменность файловой системы, имеет антивирусный модуль.

Основным механизмом защиты при проникновении на конечное устройство злоумышленника с в высокими правами является доверенная среда. Это выделенная область в комплектующих компьютера, которая выполняет функции гипервизора ОС, при этом не завися от состояния ОС