УДК 004.457
DOI 10.21685/2587-7704-2019-4-2-7

Open Access | RESEARCH ARTICLE

Применение системы защиты информации Secret Net Studio для реализации мер защиты информации

Д. А. Умаров
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. Г. Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Произведен анализ способов применения системы защиты информации (СЗИ) Secret Net Studio для реализации мер защиты информации. Проведен обзор и анализ основных функциональных возможностей СЗИ Secret Net Studio. Данный анализ показал, что СЗИ Secret Net Studio представляет собой комплексное средство защиты по сравнению с другими средствами защиты.

Ключевые слова: сертифицированные средства защиты информации, операционная система, несанкционированный доступ, информационная безопасность, СЗИ Secret Net Studio.

The use of Secret Net Studio information security system to implement information security measures

D. A. Umarov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. An analysis of methods for using Secret Net Studio information security system (ISS) to implement information security measures is performed. A review and analysis of basic functionalities of Secret Net Studio ISS are carried out. The analysis showed Secret Net Studio ISS is a comprehensive security tool compared to other information security tools.

Keywords: certified information security tools, operating system, unauthorized access, information security, Secret Net Studio ISS.

Подавляющее большинство средств защиты информации разрабатывались для защиты персональных компьютеров на базе операционной системы (ОС) Microsoft Windows. Данный факт свидетельствует о том, что системы защиты информации (СЗИ) на базе ОС Windows как никогда востребованы. Но в настоящее время большинство систем защиты не могут обеспечить комплексную защиту сети организации, за исключением СЗИ Secret Net Studio [1].

Ключевой особенностью, которая отличает СЗИ Secret Net Studio [1] от других систем защиты является ее обширный функционал. Secret Net Studio [1] включает в себя как межсетевой экран, так и антивирус, шифрование сетевого трафика и функцию обнаружения и предотвращения вторжений, что, в свою очередь, свидетельствует о том, что другие средства защиты ограничены в функционале

для защиты локальных сетей. И именно это отличает Secret Net Studio [1] от других систем защиты, в следствие того что в нее интегрировано множество других продуктов от компании «Код безопасности», которые сертифицированы ФСТЭК, а также поддержка большого спектра операционных систем.

Обзор и анализ СЗИ Secret Net Studio [1] проводился с использованием государственного реестра сертифицированных СЗИ [2].

Secret Net Studio [1] является сертифицированным средством защиты информации от несанкционированного доступа (НСД) и позволяет привести автоматизированные системы на платформе ОС Windows в соответствие требованиям регулирующих документов:

– приказ ФСТЭК России от 11.02.2013 № 17 – требования по защите информации в государственных информационных системах (ГИС) [3];

– приказ ФСТЭК России от 18.02.2013 № 21 – требования по защите персональных данных в информационных системах персональных данных (ИСПДн) [4].

СЗИ Secret Net Studio соответствует требованиям руководящих документов почетвертому уровню контроля отсутствия НДВ, 5 классу защищенности СВТ, 4 классу защиты СКН, 4 классу защиты САВЗ, 4 классу защиты МЭ тип "В", 4 классу защиты СОВ. Может применяться в АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до 1 класса включительно, АСУ ТП до 1 класса включительно [2].

Основными ключевыми возможностями Secret Net Studio [1] являются:

– независимое от ОС управление внутренними механизмами и драйверами;

– автоматическая настройка функций для соответствия требованиям регуляторов;

– интуитивно понятные графические инструменты для мониторинга состояния компьютеров в защищенной среде;

– комплексная пятиуровневая защита: защита данных, защита приложений, сетевое подключение, ОС и подключенные устройства;

– интеграция независимых от ОС механизмов безопасности для повышения общей безопасности рабочих станций и серверов;

– возможность создавать централизованные политики безопасности и их наследование в распределенных инфраструктурах;

– поддержка иерархии и резервирования серверов безопасности в распределенных инфраструктурах.

Основными вариантами развертывания Secret Net Studio является:

– автономный режим – предназначен для защиты небольшого количества (до 20–25) рабочих станций и серверов. Кроме того, каждая машина администрируется локально;

– сетевой режим (с централизованным управлением) – предназначен для развертывания в доменной сети с Active Directory. Эта опция имеет инструменты централизованного управления и позволяет применять политики безопасности во всей организации. Сетевая версия Secret Net может быть успешно развернута в сложной доменной сети (домен/лес).

СЗИ Secret Net Studio [1] спроектирована как целостная система, которая может использоваться для защиты локальных сетей, и может быть реализована с помощью дополнительных модулей, которые могут быть включены в систему защиты. Она также имеет такое преимущество перед другими системами защиты, как возможность установки на виртуальную машину. Поскольку локальная сеть, рассматриваемая в статье, будет развернута на виртуальных машинах, решение использовать СЗИ Secret Net Studio [1] является наиболее эффективным с точки зрения увеличения количества используемых защитных механизмов.

Сама система защиты делится на две основные части: это защита системы и защита данных. Далее будет рассмотрены более детально каждая из подсистемы Secret Net Studio [1].

Secret Net Studio [1] поддерживает широкий список управляемых внешних устройств (вебкамеры, сотовые телефоны, 3G-модемы, сетевые карты, USB-накопители, принтеры и т.д.) и различные сценарии ответа при подключении или отключении от компьютера. Одним из возможных сценариев является блокировка рабочей станции при изменении конфигурации оборудования.

Замкнутая программная среда включает в себя управление приложениями, запускаемыми в системе, а также создание белых списков.

Используя данный механизм, можно создать «статическую» систему, недоступную для внешних модификаций и в то же время постоянно отслеживающую активность программы на рабочей станции.

Поддерживается также блокировка исполнения скриптов и мобильного кода.

Администратор сервера безопасности может использовать автоматическую проверку и поиск различий между текущим и текущим паспортами защищаемой станции и текущими паспортами, что позволяет идентифицировать следы несанкционированной активности в системе и установить, что пользователь использует нерегулируемое программное обеспечение (включая переносимые версии программ).

Secret Net Studio [1] также включает дискреционный контроль доступа к информации, в том числе ограничение доступа пользователей к ресурсам на основе списков доступа пользователей (пользователей, групп) к определенным системным объектам.

Функция контроля доступа Secret Net Studio [1] реализована независимо от встроенных механизмов ОС Windows, что повышает уровень безопасности. Обязательный контроль доступа к информации включает в себя возможность определять различные уровни конфиденциальности и дифференцировать доступ к системным ресурсам на их основе.

Функции контроля доступа Secret Net Studio [1] делятся на виды:

– контроль доступа в систему (сессии различных уровней конфиденциальности);

– контроль доступа к файлам и директориям (как локально, так и в масштабе сети предприятия);

– контроль устройств (возможность подключения/работы с ними при наличии прав определенного уровня);

– контроль печати (возможность печати конфиденциальных документах исключительно на принтерах с соответствующей меткой);

– контроль потоков (контроль отсутствия попадания информации из доверенного поля в недоверенное при работе с приложениями/документами);

– метки конфиденциальности можно назначать на файлы и каталоги, а также устройства.

Функцию разделения уровней конфиденциальности сеансов можно сравнить с уровнем доступа сотрудников организации. Таким образом, информация не может быть прочитана, изменена или удалена из системы сотрудником, который не обладает правами соответствующего уровня.

Функция управления печатью означает, что при печати конфиденциальной информации документ автоматически помечается и печатается в журнале безопасности. Состав токена настраивается администратором. Можно определить несколько маркеров одновременно (для документов разных категорий безопасности). А также присутствует возможность ограничить уровень конфиденциальности документов, доступных для печати на конкретном принтере в системе.

Шифрование контейнера подразумевает, что данные на диске и других носителях могут храниться в защищенном контейнере. Фактически контейнер – это зашифрованная информационная область на диске. Для пользователя он отображается как подключенный локальный диск. Перезапись данных является гарантией уничтожения данных.

Применяется при необходимости удаления конфиденциальной информации без возможности последующего восстановления специализированными средствами. Есть возможность выбора количества циклов затирания данных.

Теневое копирование подразумевает под собой то, что при копировании информации на съемные носители, а также отправки документов на печать в защищенном хранилище автоматически создаются копии файлов.

В Secret Net Studio [1] обеспечивается защита информации на пяти уровнях, для каждого из которых представлены определенные защитные механизмы (продукт объединяет более 20 взаимно интегрированных защитных механизмов).

Лицензируются следующие компоненты системы:

– защита от НСД (включает в себя механизмы, обеспечивающие защиту входа в систему, доверенную информационную среду, контроль утечек и каналов распространения защищаемой информации);

– контроль устройств (входит в защиту от НСД, но может также приобретаться отдельно);

– защита диска и шифрование контейнеров;

– персональный межсетевой экран;

– средство обнаружения и предотвращения вторжений;

– антивирус;

– шифрование сетевого трафика.

Защита от НСД обеспечивается механизмами, применяемыми в СЗИ от НСД Secret Net. Их описание приведено ниже.

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к компьютеру. К механизму защиты входа относятся следующие средства:

– средства для идентификации и аутентификации пользователей; средства блокировки компьютера;

– аппаратные средства защиты от загрузки ОС со съемных носителей (интеграция с программно-аппаратным комплексом «Соболь»).

В Secret Net Studio поддерживается работа со следующими аппаратными средствами: средства идентификации и аутентификации на базе идентификаторов eToken, iKey, Rutoken, JaCarta и ESMART; устройство Secret Net Card; ПАК «Соболь».

Средства блокировки компьютера предназначены для предотвращения его несанкционированного использования. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора. Предусмотрены следующие варианты:

– блокировка при неудачных попытках входа в систему;

– временная блокировка компьютера;

– блокировка компьютера при срабатывании защитных подсистем (например, при нарушении функциональной целостности системы Secret Net Studio);

– блокировка компьютера администратором оперативного управления.

Кроме того, в СЗИ Secret Net Studio [1] есть функциональная проверка подсистем. Функциональная проверка заключается в том, чтобы при входе пользователя в ОС все ключевые подсистемы безопасности были загружены и работали. Если проверка работоспособности завершена успешно, этот факт записывается в журнал Secret Net Studio [1]. В случае сбоя регистрируется событие и причины его возникновения. Только пользователи в группе администраторов локального компьютера имеют доступ к системе.

Также необходимо упомянуть наличие функции контроля целостности. Механизм проверки целостности контролирует неизменность контролируемых объектов. Мониторинг осуществляется автоматически по заданному графику. Объектами управления могут быть файлы, каталоги, элементы системного реестра и сектора диска (последние только при использовании ПАК «Соболь»).

В случае обнаружения несоответствия возможны различные варианты реакций на ситуации нарушения целостности. Например, регистрация события в журнале Secret Net Studio [1] и блокировка компьютера. Все данные об объектах, параметрах и управляющих программах сосредоточены в модели данных. Он хранится в локальной базе данных системы Secret Net Studio [1] и представляет собой иерархический список объектов с описанием связей между ними.

В состав системы Secret Net Studio [1] также входит механизм дискреционного управления доступом к ресурсам файловой системы. Этот механизм обеспечивает:

– разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;

– контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;

– запрет доступа к объектам в обход установленных прав доступа;

– независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows. То есть установленные права доступа к файловым объектам в системе Secret Net Studio [1] не влияют на аналогичные права доступа в ОС Windows и наоборот.

Кроме того, пользователю предоставляется возможность определения учетных записей, которым даны привилегии по управлению правами доступа.

Основными механизмами сетевой защиты Secret Net Studio [1] являются:

– персональный межсетевой экран;

– антивирус;

– обнаружение и предотвращение вторжений;

– шифрование сетевого трафика.

Система Secret Net Studio [1] обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации. Подсистема межсетевого экранирования Secret Net Studio [1] реализует следующие основные функции:

– фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;

– фильтрация пакетов служебных протоколов (ICMP, IGMP и т.д.), необходимых для диагностики и управления работой сетевых устройств;

– фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;

– фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);

– фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);

– фильтрация с учетом полей сетевых пакетов;

– фильтрация по дате / времени суток.

Фильтрация сетевого трафика осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n).

Авторизация сетевых соединений в Secret Net Studio осуществляется с помощью механизма, основанного на протоколе Kerberos. С его помощью удостоверяются не только субъекты доступа, но и защищаемые объекты, что препятствует реализации угроз несанкционированной подмены (имитации) защищаемой информационной системы с целью осуществления некоторых видов атак. Механизмы аутентификации защищены от прослушивания, попыток подбора и перехвата паролей.

События, связанные с работой межсетевого экрана, регистрируются в журнале Secret Net Studio [1].

Также в Secret Net Studio реализована функция обнаружения и предотвращения вторжений. В Secret Net Studio [1] выполняется обнаружение и блокирование внешних и внутренних атак, направленных на защищаемый компьютер. Вся информация об активности механизма обнаружения и предотвращения вторжений регистрируется в журнале Secret Net Studio [1].

С помощью групповых и локальных политик администратор Secret Net Studio [1] настраивает параметры работы системы.

Защитный модуль «Антивирус» в Secret Net Studio [1] осуществляет обнаружение и блокировку вредоносного кода. В качестве модуля антивирусной защиты может использоваться модуль ESET NOD32, модуль антивируса Касперского или модуль, разработанный ООО «Код безопасности».

Таким образом, Secret Net Studio [1] позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. При проверке компьютера осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др. Это позволяет обнаружить и заблокировать внешние и внутренние сетевые атаки, направленные на защищаемый компьютер.

Благодаря использованию в рамках одного продукта СЗИ от НСД и антивируса время на проверку и открытие файлов составляет на 30 % меньше, чем при независимой реализации защитных механизмов [1].

Обновление антивируса можно осуществлять как в режиме онлайн с серверов «Кода безопасности» при подключении защищаемого компьютера к Интернету, так и с сервера обновлений компании (в случае, когда компьютер не имеет прямого выхода в Интернет).

Администратору доступна настройка параметров антивируса с помощью групповых и локальных политик в программе управления Secret Net Studio [1]. Вся информация об активности механизма регистрируется в журнале Secret Net Studio [1].

В состав клиентского ПО системы Secret Net Studio [1] включен VPN-клиент, предназначенный для организации доступа удаленных пользователей к ресурсам, защищаемым средствами АПКШ «Континент». VPN-клиент «Континент-АП» обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи, по алгоритму ГОСТ 28147–89.

При подключении абонентского пункта к серверу доступа выполняется процедура установки соединения, в ходе которой осуществляется взаимная аутентификация абонентского пункта и сервера доступа. Процедура установки соединения завершается генерацией сеансового ключа, который используется для шифрования трафика между удаленным компьютером и сетью предприятия.

При аутентификации используются сертификаты x.509v3. Расчет хеш-функции выполняется по алгоритму ГОСТ Р 34.11–1994 или ГОСТ Р 34.11–2012, формирование и проверка электронной подписи – по алгоритму ГОСТ Р 34.10–2001 или ГОСТ Р 34.10–2012.

Также Secret Net Studio [1] обладает гибким лицензированием, а именно возможность приобретения и установки как отдельных функциональных модулей, так и их пакетов. Лицензирование не зависит от режима развертывания – автономного или централизованного. Система централизованного управления предоставляется бесплатно. Лицензии могут быть срочными (один или три года) или бессрочными (на весь срок поддержки продукта).

Если обобщить все сказанное выше, можно сделать вывод, что Secret Net Studio [1] представляет собой комплексное средство защиты по сравнению с такими средствами защиты, как «Страж NT» или Dallas Lock. Secret Net Studio [1] включает в себя как межсетевой экран, так и антивирус, шифрование сетевого трафика и функцию обнаружения и предотвращения вторжений. Это, в свою очередь, свидетельствует о том, что другие средства защиты ограничены в функционале для защиты локальных сетей. И именно это отличает Secret Net Studio [1] от других систем защиты, вследствие того что

в нее интегрировано множество других продуктов от компании «Код безопасности», которые сертифицированы ФСТЭК, а также поддержка большого спектра операционных систем.

На основании рассмотрения функциональных возможностей можно сделать вывод о том, что приобретение и применение СЗИ Secret Net Studio [1] является наиболее эффективным решением. СЗИ Secret Net Studio [1] является именно решением, поскольку позволяет решать задачи обеспечения соответствия требованиям по защите информации, предъявляемым к ИСПДн и ГИС. Большой набор функциональных возможностей позволяет реализовать большинство мер защиты информации, установленных документами ФСТЭК [3, 4]. Применение СЗИ Secret Net Studio [1] позволит отказаться от приобретения нескольких различных средств защиты информации, таких как межсетевые экраны, антивирусы и др. Это исключит проблемы обеспечения совместимости нескольких средств защиты. Также использование одной СЗИ вместо нескольких уменьшит затраты на внедрение и администрирование. Анализ рынка СЗИ от НСД позволяет сделать вывод о том, что СЗИ Secret Net Studio [1] единственным решением.

Библиографический список

1. Система защиты информации Secret Net Studio. – URL: https://www.securitycode.ru/products/secret-net-studio/.
2. Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения: 21.10.2019).
3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11.02.2013 № 17 (зарег. в Минюсте России 31.05.2013 № 28608).
4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18.02.2013 № 21 (зарег. в Минюсте России 14.05.2013 № 28375).

Образец цитирования:

Умаров, Д. А. Применение системы защиты информации Secret Net Studio для реализации мер защиты информации / Д. А. Умаров, А. Г. Фатеев // Инжиниринг и технологии. – 2019. – Vol. 4(2). – С. 1–6. – DOI 10.21685/2587-7704-2019-4-2-7.