УДК 004.457
DOI 10.21685/2587-7704-2019-4-2-6

Open Access | RESEARCH ARTICLE

Применение средств защиты информации от несанкционированного доступа для защиты ПЭВМ, функционирующих под управлением операционной системы Linux

К. А. Рузайкин
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 возможности применения средств защиты информации от несанкционированного доступа для защиты ПЭВМ, функционирующих под управлением операционной системы (ОС) Linux. Проведен обзор и анализ средств защиты информации (СЗИ) от несанкционированного доступа (НСД), имеющих действующий сертификат ФСТЭК. Анализ показал, что существующие СЗИ от НСД реализуют защиту информации на ПЭВМ, функционирующих под управлением ОС Linux, в соответствии требованиями, предъявляемыми специальными документами ФСТЭК. Также установлено, что количество СЗИ от НСД, имеющих сертификат ФСТЭК и работающих под управлением ОС Linux, незначительно.

Ключевые слова: сертифицированные средства защиты информации, операционная система, несанкционированный доступ, информационная безопасность, Linux.

The use of information security tools to prevent unauthorized access to personal computers operating under Linux

K. A. Ruzaykin
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 the possibility to use information security tools to protect computers, operating under Linux operating system (OS), against unauthorized access (UA) is carried out. A review and analysis of information security tools (IST) against unauthorized access having a valid certificate of Federal Service for Technical and Export Control (FSTEC) was conducted. The analysis showed that the existing information security tools against UA implement information protection on personal computers operating under Linux in accordance with the requirements of special FSTEC documents. It was also established that the number of IST against UA having FSTEC certificate and running under Linux OS is insignificant.

Keywords: certified information security tools, operating system, unauthorized access, information security, Linux.

Подавляющее большинство средств защиты информации разрабатывались для защиты персональных компьютеров на базе операционной системы (ОС) Microsoft Windows. Так как дистрибутивы ОС Linux ранее не имели широкого распространения, не было острой необходимости в средствах защиты информации (СЗИ) для этой ОС. Таким образом, СЗИ от несанкционированного доступа (НСД), применяемые для защиты ПЭВМ, работающих под управлением ОС на базе Linux, практически отсутствовали на рынке. В силу того что в федеральных и муниципальных органах власти Российской Федерации планируется произвести отказ от использования коммерческих ОС, в частности ОС Microsoft Windows, и перейти к бесплатной ОС Linux, возникла необходимость в разработке средств защиты информации от несанкционированного доступа на базе этой ОС. Компании-разработчики начали работу в этом направлении. Данные средства защиты информации присутствуют на рынке на сегодняшний день, но количество этих СЗИ крайне ограниченно. Операционная система Linux все больше применяется, и вместе с тем возрастает потребность в подготовке квалифицированных кадров (администраторов), обладающих навыками по развертыванию, настройке и эксплуатации средств защиты информации на базе ОС Linux.

Ключевой проблемой для осуществления планов по переходу на свободное программное обеспечение в первую очередь являются недостаток квалифицированных кадров для внедрения и обслуживания таких систем, а также опасения федеральных органов, связанные с использованием «сложного и незнакомого» программного обеспечения.

Также в соответствии с действующим законодательством при обработке персональных данных (ПДн), государственной тайны (ГТ) и другой конфиденциальной информации (КИ) должны использоваться сертифицированные средства защиты информации. Таким образом, возможный переход органов исполнительной власти на использование ОС Linux создаст дополнительный стимул в области развития рынка сертифицированных СЗИ от НСД.

Обзор и анализ СЗИ от НСД для ОС Linux проводился с использованием государственного реестра сертифицированных СЗИ [1]. Было установлено, что набор СЗИ от НСД, работающих под управлением ОС Linux, ограничен тремя продуктами: «СЗИ от НСД Dallas Lock Linux», «СЗИ от НСД Secret Net LSP» и «ПАК СЗИ от НСД Аккорд-X», а также включает два электронных замка, имеющих возможность работать на ПЭВМ с любой установленной ОС. Электронные замки рассматриваться не будут, поскольку их функционал ограничен.

СЗИ от НСД Dallas Lock Linux – сертифицированная система защиты от несанкционированного доступа к защищаемой информации, предназначенная для автономных персональных компьютеров и компьютеров в составе локальной сети [2]. Она представляет собой программный комплекс средств защиты информации от несанкционированного доступа в ОС семейства Linux с возможностью подключения аппаратных идентификаторов.

СЗИ от НСД Dallas Lock Linux предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), автоматизированных системах управления производственными и технологическими процессами (АСУ ТП), государственных информационных системах (ГИС) [2].

СЗИ от НСД Dallas Lock Linux соответствует требованиям руководящих документов (требования безопасности информации Федеральной службы по техническому и экспертному контролю (ФСТЭК) России):

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [3] по пятому классу защищенности;

– «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» [4] по четвертому уровню контроля.

Рассматриваемое СЗИ от НСД может быть использовано:

– при создании защищенных автоматизированных систем до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [5]);

– в государственных информационных системах первого класса защищенности (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [6]);

– для обеспечения первого уровня защищенности персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [7]).

Ключевые особенности:

– возможность работы на широком наборе наиболее популярных и распространенных дистрибутивов ОС Linux, включая российские ОС, например ОС «Лотос» и Alt Linux;

– консоль удаленного управления СЗИ из операционных систем Windows и Linux;

– современный графический интерфейс (GUI);

– сервис-ориентированная архитектура (позволяет использовать СЗИ от НСД Dallas Lock Linux для защиты сложных распределенных систем с учетом повышенных требований к масштабируемости и управляемости);

– собственные сертифицированные механизмы по управлению информационной безопасностью;

– «бесшовная» интеграция с другими решениями продуктовой линейки Dallas Lock;

– контроль целостности программного обеспечения, включая программное обеспечение СЗИ;

– выполнение требований законодательства РФ по защите информации ограниченного доступа.

Secret Net LSP является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы на платформе Linux в соответствие требованиям регулирующих документов [8]:

– Приказ ФСТЭК России от 11.02.2013 № 17 – требования по защите информации в ГИС [6];

– Приказ ФСТЭК России от 18.02.2013 № 21 – требования по защите персональных данных в ИСПДн [7].

В СЗИ от НСД Secret Net LSP реализован механизм парольной аутентификации пользователей [8].

В СЗИ от НСД Secret Net LSP реализован механизм дискреционного разграничения доступа, который дает возможность контроля и управления правами доступа пользователей и групп пользователей к объектам файловой системы (файлам и каталогам).

Функция обеспечивает возможность разграничения доступа к устройствам с целью предотвращения утечки защищаемой информации на защищаемом компьютере. Контролируется доступ пользователей и групп пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам. Контролируемые устройства идентифицируются по типу, производителю и серийному номеру, права доступа на эти устройства задаются не только для отдельных пользователей, но и для групп пользователей. Пользователи могут осуществлять подключение и выполнять рабочие обязанности только с теми устройствами, которые зарегистрированы в системе, и выполнять только те операции, которые заданы правами доступа к данному устройству.

СЗИ от НСД Secret Net LSP регистрирует все события, происходящие на компьютере: включение/выключение компьютера, вход/выход пользователей, события информационной безопасности, в том числе и события, связанные с доступом пользователей к защищаемым файлам, устройствам и узлам вычислительной сети. Существует возможность осуществления фильтрации событий безопасности, контекстный поиск в журнале безопасности, поиск по временному интервалу, сохранение отчетов в файл и интерактивный мониторинг событий. Также в журнале регистрируются события, связанные с выводом документов на печать.

Механизм позволяет контролировать целостность ключевых компонентов СЗИ от НСД Secret Net LSP и критических объектов файловой системы. Контроль ПО СЗИ осуществляется автоматически. Администратор вручную задает список контролируемых объектов файловой системы (файлов и каталогов) и реакцию СЗИ на факты нарушения целостности. Возможна настройка режимов реакции СЗИ для каждого объекта – от регистрации события в журнале безопасности до блокировки входа в систему.

Осуществляется аудит действий пользователей с защищаемыми объектами, аудит сетевой активности пользователей, а также аудит отчуждения информации. Все события регистрируются в журнале аудита, существует возможность автоматического построения отчетов по результатам аудита.

Для предотвращения доступа к остаточной информации в СЗИ от НСД Secret Net LSP предусмотрено уничтожение (затирание) содержимого защищаемых файлов при их удалении пользователем. Очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств) происходит путем выполнения в них однократной (или многократной) произвольной записи.

Управление СЗИ от НСД Secret Net LSP возможно, как в режиме командной строки, так и с использованием приложения с графическим интерфейсом – панели безопасности. Программа обеспечи-

вает выполнение администратором всех необходимых операций в рамках контроля и управления работой защитных механизмов Secret Net для ОС Linux [8].

СЗИ от НСД Secret Net LSP способно функционировать совместно со средствами централизованного управления СЗИ от НСД Secret Net 7, которые обеспечивают:

– отображение информации о состоянии компьютеров, защищаемых с помощью СЗИ от НСД Secret Net LSP, и происходящих на них событиях;

– отображение журналов событий, полученных с компьютеров;

– управление механизмами защиты и выдачи команд для оперативного управления компьютерами;

– выполнение команд оперативного управления для блокировки или разблокирования, перезагрузки или выключения компьютеров.

В Secret Net LSP начиная с версии 1.4 есть возможность автоматизированного ввода компьютера под управлением ОС Linux в домен Windows [8].

Программно-аппаратный комплекс СЗИ от НСД «Аккорд-Х» – сертифицированная система защиты от несанкционированного доступа к защищаемой информации – предназначена для применения на средствах вычислительной техники (СВТ), функционирующих под управлением ОС Linux с целью обеспечения защиты от несанкционированного доступа к СВТ и АС на их основе при многопользовательском режиме эксплуатации [9]. Он представляет собой программно-аппаратный комплекс средств защиты информации от несанкционированного доступа в ОС семейства Linux с возможностью подключения аппаратных идентификаторов. ПАК СЗИ от НСД «Аккорд-Х» предназначен для разграничения доступа пользователей к рабочим станциям под управлением ОС семейства Linux [9].

СЗИ от НСД Dallas Lock Linux соответствует требованиям руководящих документов (требования безопасности информации ФСТЭК России):

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [3] по третьему классу защищенности;

– «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» [4] по второму уровню контроля.

Возможности ПАК СЗИ от НСД «Аккорд-Х»:

– защита от несанкционированного доступа к ПЭВМ (включая возможность ограничения разрешенных часов работы каждого пользователя);

– идентификация/аутентификация пользователей до загрузки операционной системы с возможностью последующей передачи результатов успешной идентификации/аутентификации в ОС;

– аппаратный контроль целостности системных файлов;

– доверенная загрузка ОС;

– статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;

– разграничение доступа пользователей, процессов к массивам данных (объектам) с помощью дискреционного контроля доступа;

– разграничение доступа пользователей, процессов к массивам данных (объектам) с помощью мандатного контроля доступа;

– разграничение доступа пользователей к определенным процессам;

– контроль доступа к периферийным устройствам;

– создание индивидуальной для каждого пользователя изолированной рабочей программной среды;

– автоматическое ведение протокола регистрируемых событий;

– контроль печати на локальных и сетевых принтерах, протоколирование вывода данных на печать, маркировка распечатанных данных (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация) [9].

Преимущество комплекса заключается в наличии модуля контроля печати, который предоставляет возможность маркировки данных, выводимых на печать на сетевых и локальных принтерах, с журналированием всех действий пользователя. Модуль контроля печати «Аккорд-Х» отрабатывает при печати документов из любого прикладного программного обеспечения, предусматривающего возможность вывода документа/файлов/данных на печать (не только OpenOffice и прочих текстовых редакторов). Контроль печати осуществляется на уровне подсистемы печати Linux, поэтому данные,

выводимые на печать из консоли, также маркируются в соответствии с настройками подсистемы контроля печати «Аккорд-Х».

В качестве аппаратной базы комплекса может использоваться любой из контроллеров «Аккорд» в составе «Аккорд-АМДЗ», также поддерживаются аппаратные идентификаторы пользователей, перечень которых постоянно расширяется, поэтому его целесообразно уточнять при заказе.

В качестве маркера (штампа) может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация [9].

Рассмотренные выше средства защиты информации от несанкционированного доступа имеют действующий сертификат ФСТЭК, согласно реестру сертифицированных средств защиты информации, сертификаты для рассматриваемых СЗИ от НСД будут продлеваться.

СЗИ от НСД Secret Net LSP и Dallas Lock Linux отличаются тем, что имеют программную реализацию и могут быть использованы в среде виртуализации, в отличие от «Аккорд-Х», который не может быть установлен на виртуальные машины. Стоит принять во внимание тот факт, что «Аккорд-Х» реализует мандатное управление доступом, когда в двух других рассматриваемых СЗИ от НСД данный механизм отсутствует.

Стоит отметить, что СЗИ от НСД Dallas Lock Linux предоставляет больше функциональных возможностей для формирования информационной инфраструктуры организации и построения ее системы защиты. Также стоит учитывать то, что под определенный дистрибутив ОС есть своя версия СЗИ от НСД Dallas Lock Linux, учитывающая особенности выбранной ОС, чего нельзя сказать о СЗИ от НСД Secret Net LSP, в котором используется один дистрибутив системы под всевозможные ОС.

Продукт компании «Конфидент» Dallas Lock Linux поддерживает большее количество ОС, в том числе сертифицированные российские разработки Astra Linux Special Edition.

Кроме обзора СЗИ от НСД, были рассмотрены положения ФСТЭК [6, 7].

Анализ показал, что СЗИ от НСД Secret Net LSP и Dallas Lock Linux обеспечивает реализацию большинства мер защиты, кроме:

– ограничения программной среды (ОПС);
– антивирусной защиты (АВЗ);
– обнаружения вторжений (СОВ);
– обеспечения доступности (ОДТ);
– защиты технических средств (ЗТС);
– выявления инцидентов и реагирование на них (ИНЦ);
– управления конфигурацией информационной системы и системы защиты (УКФ).

Также существует ряд мер защиты из других наборов, которые не могут быть реализованы данными СЗИ от НСД, например идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2), идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6), контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны (ЗНИ.3) и другие. Оценка наглядно демонстрирует, что рассматриваемые СЗИ от НСД позволяют реализовать почти половину мер защиты, установленных положениями ФСТЭК [6, 7].

На основании сказанного выше целесообразно усовершенствовать СЗИ от НСД, работающих под управлением ОС Linux, в области реализации защитных мер, таких как:

– система обнаружения и предотвращение вторжений (СОВ), в частности реализация обнаружения атак сигнатурными и эвристическими методами и автоматической блокировкой атакующих хостов при наличии аномальных пакетов и DoS-атаках;

– выявление инцидентов и реагирование на них (ИНЦ), в частности получение информации об угрозе при нарушении контроля целостности информации, что дает возможность отреагировать на данный инцидент.

В настоящее время на российском рынке уже существуют локализированные дистрибутивы Linux со встроенными программными СЗИ, сертифицированными ФСТЭК России. Это системы ALT Linux СПТ, Astra Linux SE, ROSA, Mandriva Linux, GosLinux и др. Однако наличие встроенных механизмов защиты в дистрибутиве не означает, что нужно отказаться от применения дополнительных СЗИ, даже если они дублируют какие-либо возможности защитных подсистем. Для этого есть ряд объективных причин, связанных не только с возможными архитектурными недостатками и ошибками программирования, но и с наличием определенных ограничений, которые появляются при использовании специализированных дистрибутивов. Среди таких ограничений стоит выделить потерю гибкости системы ввиду невозможности изменения конфигурации и состава файлов из комплекта поставки после фиксации набора файлов при сертификации дистрибутива. Таким образом, пока издатель не сертифицирует обновления, их нельзя применять, что влияет и на степень надежности ОС. Также к

невозможности аттестации объекта информации приводит установка приложения, вносящего изменения в общесистемное программное обеспечение. С другой стороны, наложенное СЗИ дает не только свободу при выборе дистрибутива и возможность расширения функционала ОС, но и наиболее полное выполнение мер, определяемых, в частности, приказами № 21 и 17 ФСТЭК России [1].

СЗИ от НСД реализует следующие защитные механизмы:

– мандатный контроль доступа пользователей и процессов;
– контроль доступа к периферийным устройствам и портам ввода-вывода;
– идентификация и аутентификация пользователей;
– контроль целостности критичных файлов и данных;
– дискреционный контроль доступа пользователей;
– маркировка документов и контроль их вывода на печать;
– регистрация событий безопасности в журнале событий;
– защита ввода и вывода информации на отчуждаемый физический носитель;
– гарантированное удаление данных на дисках и выборочное затирание файлов и др.

Наличие дополнительных защитных механизмов и функционала для управления системой защиты значительно повышает уровень защищенности информационной системы.

На данный момент очевидно, что средств защиты, имеющих сертификат ФСТЭК, предназначенных для ОС Linux, крайне мало по сравнению с ОС Windows. Как уже было сказано, связано это с малым распространением системного программного обеспечения (СПО) и недостатком квалифицированных кадров, а также со сложностью технологической реализации защитного функционала. Компании-разработчики, реализующие СЗИ от НСД, формируют свой список поддерживаемых ОС Linux. Решением проблемы будет являться увеличение количества квалифицированных специалистов путем разработки технической документации и лабораторных стендов, направленных на повышение квалификации кадров, расширение рынка СПО на фоне увеличения спроса на него российскими государственными структурами. Также необходимо произвести выборку среди уже существующих ОС Linux и создать единый реестр операционных систем на базе ОС Linux для разработки СЗИ от НСД, это позволит создать эшелонированную комплексную систему защиты.

Библиографический список

1. Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 // Официальный сайт ФСТЭК России. – URL: https://fstec.ru/tekhnicheskaya- zaschita-informatsii/dokumenty-po-sertifickatsii/153-sistema–sertifikatsii/591 (дата обращения: 23.10.2019).
2. СЗИ от НСД Dallas Lock Linux. – URL: https://www.dallaslock.ru/products/szi-nsd-dallas-lock-linux/ (дата обращения: 23.10.2019).
3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации // Официальный сайт ФСТЭК России. – URL: https://fstec.ru/component/attachments/download/297 (дата обращения: 23.10.2019).
4. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей // Официальный сайт ФСТЭК России. – URL: https://fstec.ru/component/attachments/download/294 (дата обращения: 23.10.2019).
5. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации // Официальный сайт ФСТЭК России. – URL: https://fstec.ru/component/attachments/download/296 (дата обращения: 23.10.2019).
6. 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).
7. 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).
8. СЗИ от НСД Secret Net LSP. – URL: https://www.securitycode.ru/products/szi_secret_net/ (дата обращения: 23.10.2019).
9. ПАК СЗИ от НСД Аккорд-X. – URL: http://www.accord.ru/acx.html (дата обращения: 23.10.2019).

Образец цитирования:

Рузайкин, К. А. Применение средств защиты информации от несанкционированного доступа для защиты ПЭВМ, функционирующих под управлением операционной системы Linux / К. А. Рузайкин, А. Г. Фатеев // Инжиниринг и технологии. – 2019. – Vol. 4(2). – С. 1–6. – DOI 10.21685/2587-7704-2019-4-2-6.