СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Dallas Lock 8.0-C

Описание применения

RU.48957919.501410-02 31

Листов 24

2018

Аннотация

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие «Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C» RU.48957919.501410-02 31 (далее по тексту – «изделие»).

В настоящем документе содержатся общие сведения о назначении изделия и программного обеспечения изделия (далее по тексту – «ПО изделия» или «СЗИ НСД»), условиях применения, описание задачи, перечень входных и выходных данных.

Содержание

1. НАЗНАЧЕНИЕ

1.1. Изделие предназначено для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему и выходящими за её пределы, обеспечения защиты информации в АС посредством её фильтрации. Может использоваться в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС) и автоматизированных системах управления производственными и технологическими процессами (АСУ ТП).

1.2. Изделие предназначено для использования на технических средствах (ТС), таких как: персональные компьютеры, портативные компьютеры (ноутбуки, планшеты), сервера и ТС с поддержкой виртуальных сред и технологии Windows To Go.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. СЗИ НСД может быть использовано на технических средствах (ТС), работающих под управлением операционных систем семейства Windows:

- Windows XP (SP 3) (Professional, Home, Starter) (см. п. 3.3.4 Формуляра на изделие);
- Windows Server 2003 (SP 2) (Web, Standard, Enterprise, Datacenter) (см. п. 3.3.4 Формуляра на изделие);
- Windows Server 2003 R2 (SP 2) (Web, Standard, Enterprise, Datacenter) (см. п. 3.3.4 Формуляра на изделие);
- Windows Vista (SP 2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter);
- Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server).

2.2. СЗИ НСД поддерживает как 32-битные версии ОС, архитектуры Intel x86, так и 64-битные, архитектуры AMD64 (архитектура IA64 (Itanium) не поддерживается).

2.3. Для размещения файлов СЗИ НСД требуется не менее 200 МБ пространства на системном разделе жесткого диска.

2.4. Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

2.5. СЗИ НСД может функционировать как на автономных ТС, так и на ТС в составе локальной вычислительной сети (ЛВС).

2.6. СЗИ НСД может быть использована как в сетях с доменной организацией, так и в одноранговых сетях.

2.7. Для использования аппаратных идентификаторов необходимо наличие в аппаратной части ТС USB-порта или COM-порта.

2.8. СЗИ НСД соответствует требованиям руководящих и методических документов (требования безопасности информации ФСТЭК России):

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели

защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 3 классу защищенности;

- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 2 уровню контроля;
- «Требования к системам обнаружения вторжений» (документ утвержден приказом ФСТЭК России № 638 от 6 декабря 2011 г.) – по 4 классу защиты;
- «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ;
- «Требования к средствам контроля съемных машинных носителей информации» (документ утвержден приказом ФСТЭК России № 87 от 28 июля 2014 г.) – по 2 классу защиты;
- «Профиль защиты средств контроля подключения съемных машинных носителей информации второго класса защиты» ИТ.СКН.П2.ПЗ;
- «Требования к межсетевым экранам» (документ утвержден приказом ФСТЭК России № 9 от 9 февраля 2016 г.) – по 4 классу защиты;
- «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты» ИТ.МЭ.В4.ПЗ.

2.9. При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (RU.48957919.501410-02 30), СЗИ НСД может быть использована:

- при создании защищенных автоматизированных систем до класса защищенности 1Б включительно[1] (руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- в информационных системах персональных данных до 1 уровня защищенности включительно (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»);
- в государственных информационных системах 1 класса защищённости (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);

[1] Без использования в составе изделия модулей «Межсетевой экран» и «Система обнаружения вторжений» (могут быть использованы при создании защищенных автоматизированных систем до класса защищенности 1Г включительно).

– при создании защищенных автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»).

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» RU.48957919.501410-02 91 (ТУ).

3.2. Изделие СЗИ НСД Dallas Lock 8.0-C включает в себя следующие основные функциональные модули:

- система защиты информации от несанкционированного доступа;
- средство контроля съемных машинных носителей информации;
- персональный межсетевой экран;
- система обнаружения вторжений.

3.3. Система защиты информации от несанкционированного доступа

3.3.1. Подсистема управления доступом

3.3.1.1.Изделие осуществляет контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

3.3.1.2.Изделие контролирует доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам). Для каждой пары (субъект – объект) задано явное и недвусмысленное перечисление допустимых типов доступа (чтение, запись), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту). Контроль доступа применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

3.3.1.3.Изделие содержит механизм, реализующий дискреционные правила разграничения доступа. Такой механизм применим как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под «явными» подразумеваются действия, осуществляемые с использованием системных средств системных макрокоманд, инструкций языков высокого уровня, а под «скрытыми» иные действия, в том числе с использованием собственных программ работы с устройствами.

3.3.1.4.Изделие содержит механизм, реализующий мандатный принцип контроля доступа. Для реализации этого принципа сопоставляются классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам назначаются классификационный уровни (уровни уязвимости, категории секретности и т. п.) являющиеся комбинациями иерархических и неиерархических категорий. Данные метки служат основой мандатного принципа разграничения доступа.

3.3.1.5.В изделии предусмотрена возможность санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

3.3.1.6.Изделие предоставляет права изменения правил разграничения доступа для выделенных субъектов (администрации, службе безопасности).

3.3.1.7.В изделии реализовано разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

3.3.1.8.В изделии есть возможность ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя ТС.

3.3.1.9.Изделие обеспечивает поддержку и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки.

3.3.1.10. Изделие осуществляет блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.

3.3.1.11. Изделие содержит механизмы контроля состава технических средств, программного обеспечения и средств защиты информации.

3.3.1.12. Изделие предоставляет возможность управления учетными записями пользователей (добавление, удаление, блокирование, редактирование атрибутов) в т. ч. локальных, доменных, сетевых, а также возможность задания типа учетной записи пользователя:

- внутренняя;
- внешняя;
- системная;
- приложение;
- гостевая;
- временная.

3.3.1.13. Изделие осуществляет регламентацию и контроль использования в информационной системе технологий беспроводного доступа.

3.3.1.14. Изделие осуществляет регламентацию и контроль использования в информационной системе мобильных технических устройств.

3.3.1.15. В изделии реализована возможность настройки и организации замкнутой программной среды.

3.3.1.16. В изделии реализована возможность блокировки доступа к файлам по расширению.

3.3.1.17. В изделии реализована возможность разграничения доступа к буферу обмена.

3.3.1.18. В изделии реализован механизм изоляции процессов в оперативной памяти.

3.3.2. Подсистема преобразования информации

3.3.2.1.Изделие имеет механизмы исключения возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования съемных машинных носителей информации в иных информационных системах.

3.3.2.2.Изделие предоставляет возможность создания преобразованных файл-дисков и файл-контейнеров для надежного хранения защищаемой информации.

3.3.2.3.Изделие предоставляет возможность преобразования съемных машинных носителей информации.

3.3.2.4.В изделии реализовано прозрачное преобразование жестких дисков для предотвращения доступа к данным, расположенным на жестких дисках, в обход изделия.

3.3.3. Подсистема гарантированной зачистки информации

3.3.3.1.Изделие предоставляет возможность гарантированного уничтожения (стирания) и контроля уничтожения информации при полной зачистке логического диска.

3.3.3.2.В изделии осуществляется очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ТС и внешних накопителей. Очистка осуществляется однократной произвольной записью или двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). Очистка осуществляется путем записи маскирующей информации при её освобождении (перераспределении).

3.3.4. Подсистема идентификации и аутентификации

3.3.4.1.В изделии реализована возможность задания длины пароля пользователя при входе в систему.

3.3.4.2.Изделие осуществляет идентификацию и проверку подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, минимальная длина которого назначается администратором.

3.3.4.3.Изделие требует от пользователей идентифицировать себя при запросах на доступ и подвергает проверке подлинность предъявленного субъектом идентификатора. В изделии реализовано препятствие доступа к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

3.3.4.4.В изделии осуществляется идентификация терминалов, ТС, узлов сети ТС, внешних устройств ТС по логическим именам и по физическим адресам (номерам).

3.3.4.5.В изделии осуществляется идентификация программ, каталогов, файлов, по именам.

3.3.4.6.В изделии осуществляется идентификация устройств, в том числе стационарных, мобильных и портативных.

3.3.4.7.В изделии реализована возможность управления идентификаторами, в том числе создание, присвоение и уничтожение идентификаторов.

3.3.4.8.В изделии реализовано управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентифика-

ции и принятие мер в случае утраты и (или) компрометации средств аутентификации.

3.3.4.9.В изделии реализована возможность ограничения количества последовательных неудачных попыток ввода пароля (например, от 3 до 5).

3.3.4.10. В изделии реализована защита обратной связи при вводе аутентификационной информации.

3.3.4.11. В изделии реализована возможность аутентификации при помощи аппаратных идентификаторов.

3.3.4.12. В изделии реализована возможность записи авторизационных данных в аппаратный идентификатор.

3.3.4.13. В изделии реализована возможность определения принадлежности аппаратного идентификатора конкретному пользователю.

3.3.4.14. В изделии реализована возможность входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows.

3.3.5. Подсистема регистрации и учета

3.3.5.1.Изделие обеспечивает мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

3.3.5.2.Изделие содержит механизмы просмотра и анализа данных регистрации, информации о действиях отдельных пользователей в информационной системе, иметь механизмы фильтрации по заданному набору параметров.

3.3.5.3.Изделие обеспечивает защиту данных регистрации от их уничтожения или модификации нарушителем.

3.3.5.4.Изделие осуществляет регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрацию 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;
- результат попытки входа: успешный или неуспешный – несанкционированный;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке.

3.3.5.5.Изделие осуществляет регистрацию изменений полномочий субъектов доступа и статуса объектов доступа. В журнале регистрации событий, который ведется в электронном виде, указываются следующие параметры:

- дата и время изменения;
- содержание изменения с указанием идентификатора субъекта доступа, чьи полномочия подверглись изменению, или логического имени защищаемого информационного ресурса, чей статус изменился;
- идентификатор администратора информационной безопасности,

осуществившего изменение;

- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

3.3.5.6.Изделие осуществляет регистрацию выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ.

При выдаче присутствует возможность автоматической маркировки каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц).

3.3.5.7.Дополнительно регистрируются все попытки доступа, все действия оператора и выделенных пользователей (администраторов защиты и т.п.).

3.3.5.8.В изделии осуществляется регистрация создания и уничтожения объекта. Регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события;
- успешно ли осуществилось событие.

3.3.5.9. Осуществляется автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ТС, выделяемых для обработки защищаемых файлов, внешних устройств ТС, каналов связи, ТС, узлов сети ТС, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка отражает уровень конфиденциальности объекта.

3.3.5.10. В изделии осуществляется регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ТС, узлам сети, внешним устройствам ТС, программам, томам, каталогам, файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)].

3.3.5.11. В изделии реализована возможность определения событий безопасности, подлежащих регистрации (журналы регистрации событий имеют фиксированный размер и не имеют ограничений по срокам хранения).

3.3.5.12. В изделии осуществляется сигнализация попыток нарушения защиты на терминалах администратора и нарушителя.

3.3.5.13. В изделии осуществляется регистрация деинсталляции (не запуска) драйвера МЭ при активном компоненте, а также реализована функция выполнения защиты в соответствии с установленными политиками.

3.3.5.14. Для клиентской части изделия реализована функция автоматической архивации журнала регистрации событий по истечении установленного интервала времени. Границы возможного временного интервала варьируются от 1 часа до 1 года. Единицы измерения выбираются исходя из величины значения интервала – часы, дни, месяцы, год.

3.3.6. Подсистема администрирования

3.3.6.1.В изделии реализованы средства управления, ограничивающие распространение прав на доступ.

3.3.6.2.Изделие предоставляет возможность назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

3.3.6.3.Изделие содержит механизмы, позволяющие проводить периодическое тестирование функций СЗИ НСД Dallas Lock 8.0-C. Тестируются:

- реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- успешное осуществление идентификации и аутентификации, а также их средства защиты;
- очистка памяти;
- регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- работа механизма, осуществляющего контроль за целостностью изделия.

3.3.6.4.В изделии реализована возможность централизованного управления защищаемыми рабочими станциями. Осуществляется централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации, контролем целостности объектов ФС, системного реестра. Поддерживается многоуровневая иерархия групп ТС и наследование установленных параметров.

3.3.6.5.В изделии реализована возможность оповещения администратора безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях при следующих случаях:

- нарушение контроля целостности объекта;
- попытка работы после блокировки при нарушении целостности;
- попытка входа на клиентскую рабочую станцию с неправильным паролем;
- блокировка пользователя после многократного ввода неправильного пароля;

- СЗИ НСД на клиенте не отвечает (возможная причина – несанкционированная деактивация системы защиты);
- клиент недоступен долгое время (с возможностью задания периода времени);
- попытки монтирования и попытки работы с запрещенными для пользователей на клиенте устройствами.

3.3.6.6.В изделии реализована возможность создания отчета по назначенным правам, составу программного и аппаратного обеспечения.

3.3.6.7.В изделии реализована возможность удаленной установки и обновления изделия.

3.3.6.8.В изделии реализована возможность назначения администратора безопасности при удаленной установке изделия.

3.3.6.9.В изделии реализована возможность визуализации сети защищаемых ТС.

3.3.6.10.В изделии реализована возможность сохранения и применения конфигурации СЗИ НСД.

3.3.7. Подсистема контроля целостности

3.3.7.1.В изделии реализована защита архивных файлов, параметров настройки СЗИ НСД, программного обеспечения и иных данных, не подлежащих изменению в процессе функционирования ИС.

3.3.7.2.В изделии реализована возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности.

3.3.8. Подсистема восстановления после сбоев

3.3.8.1.СЗИ НСД предусматривает процедуры восстановления после сбоев и отказов оборудования, которые обеспечивают полное и оперативное восстановление свойств СЗИ НСД.

3.3.8.2.Реализована возможность возвращения всех настроек СЗИ НСД к исходным (установка параметров по умолчанию), что равносильно переустановке СЗИ НСД.

3.4. Средства контроля съемных машинных носителей информации

3.4.1. Изделие предоставляет возможность управления использованием подключаемых произвольных съемных машинных носителей информации на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств, конкретных съемных машинных носителей информации.

3.4.2. Изделие осуществляет контроль экспорта данных пользователя на съемный машинный носитель информации.

3.4.3. Изделие контролирует использование интерфейсов ввода (вывода) информации (в т. ч. на съемные машинные носители информации).

3.4.4. Изделие обеспечивает контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

3.4.5. В изделии обеспечена возможность идентификации и аутентификации администратора СЗИ НСД Dallas Lock 8.0-C до предоставления ему возможности по управлению, просмотру аудита безопасности и выполнению иных действий по администрированию.

3.4.6. В изделии осуществляться идентификация устройств, в том числе стационарных, мобильных и портативных, идентификация накопителей информации.

3.4.7. В изделии реализованы надлежащие механизмы регистрации и предупреждения (сигнализации) о событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации предоставляют уполномоченным на это лицам возможность выборочного ознакомления с информацией о произошедших событиях.

3.4.8. Изделие содержит механизмы генерации временных меток, и (или) происходит синхронизация системного времени в информационной системе.

3.4.9. В изделии осуществляется разграничение доступа к управлению СКН и режимом выполнения функций безопасности (контроля накопителей) на основе ролей учетных записей пользователей.

3.4.10. В изделии осуществляется преобразование сменных накопителей, основанное на правах использования съемных машинных носителей информации, при задании которых используются следующие типы данных СКН:

- идентификационная информация съемных машинных носителей информации;
- идентификационная информация средств вычислительной техники.

3.5. Персональный межсетевой экран

3.5.1. Изделие обеспечивает фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций перемещения контролируемой МЭ информации к узлам информационной системы и от них.

3.5.2. Изделие обеспечивает распространение фильтрации на все операции перемещения через МЭ информации к узлам информационной системы.

3.5.3. Изделие обеспечивает фильтрацию, основанную на следующих типах атрибутов безопасности субъектов:

- сетевой адрес узла отправителя;
- сетевой адрес узла получателя.

3.5.4. Изделие обеспечивает фильтрацию, основанную на следующих типах атрибутов безопасности информации:

- сетевой протокол, который используется для взаимодействия;

- транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии);
- разрешенные (запрещенные) команды, разрешенный (запрещенный) мобильный код;
- разрешенные (запрещенные) протоколы прикладного уровня;
- разрешенное/запрещенное прикладное ПО (приложения).

3.5.5. В изделии реализована возможность явно разрешать или явно запрещать информационный поток, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации, основанном на идентифицированных атрибутах.

3.5.6. В изделии реализована возможность осуществлять политику фильтрации пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов.

3.5.7. В изделии реализована возможность осуществлять проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию.

3.5.8. В изделии реализована возможность осуществлять проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором МЭ установлены разрешительные или запретительные атрибуты безопасности. Должна быть возможность контролировать (разрешать/запрещать) использование сетевых ресурсов, содержащих следующие виды мобильного кода: ActiveX; J/VBScripts; Flash-анимация, PDF.

3.5.9. В изделии реализована возможность осуществлять проверку использования пользователями отдельных команд, для которых администратором межсетевого экрана установлены разрешительные или запретительные атрибуты безопасности; возможность контролировать (разрешать/запрещать) использование следующих команд: arp; ipconfig; getmac; nbtstat; netsh; netstat; net; nslookup; pathping; ping; route; telnet; tracert.

3.5.10. В изделии реализована возможность разрешать или запрещать информационный поток, основываясь на результатах проверок в соответствии с п. 3.5.7.

3.5.11. В изделии реализована возможность осуществлять фильтрацию пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика.

3.5.12. Изделие разрешает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации.

3.5.13. Изделие запрещает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты

информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации.

3.5.14. В изделии реализована возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита. Избирательность аудита должна базироваться на следующих возможных атрибутах:

- идентификатор объекта;
- идентификатор пользователя;
- идентификатор субъекта;
- тип события;
- или другие атрибуты.

Возможность выбрать какие типы событий МЭ будут регистрироваться (чекбокс):

- обнаружение мобильного кода;
- обнаружение запрещенных вложений;
- выполнение команд.

3.5.15. В изделии реализована регистрация и учет следующих событий:

- запуск и завершение выполнения функций аудита;
- результаты выполнения проверок информации сетевого трафика;
- запись нового значения любой изменяемой политики/параметра.

3.5.16. В изделии реализована поддержка определенных ролей по управлению МЭ.

3.5.17. В изделии реализована возможность со стороны администраторов МЭ управлять режимом выполнения функций безопасности МЭ.

3.5.18. Для администратора МЭ реализована возможность модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления МЭ фильтрации.

3.5.19. Для администратора МЭ реализована возможность назначать модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для прикладного программного обеспечения (приложений) с целью последующего осуществления фильтрации.

3.5.20. Для администратора МЭ реализована возможность модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для используемых пользователями отдельных команд.

3.5.21. В изделии реализована возможность ведения для каждого типа мест расположения узла с установленным МЭ отдельных профилей проверок.

3.5.22. В изделии реализована возможность изменения области значений информации состояния соединения со стороны администраторов межсетевого

экрана. Для администратора реализована возможность завершать сетевые соединения из таблицы соединений.

3.5.23. В изделии реализована возможность присвоения профилям проверок допустимых значений, таких как профиль проверок для использования внутри информационной системы, профиль проверок для использования за пределами информационной системы и других допустимых профилей проверок. Реализованы:

- возможность создания профилей, выбора и назначения профиля настроек определенным (найденным) сетям, в том числе при обнаружении новой сети;
- возможность редактирования профилей настроек;
- аудит сбоев в использовании механизма ведения отдельных профилей проверок (пример сбоя: профиль не найден и применен профиль по умолчанию).

Профили выбираются как минимум по IP-адресу текущего адаптера. Количество профилей, равное 8, можно считать достаточным. Профили (кроме профиля по умолчанию) могут переименовываться.

3.5.24. В изделии реализована возможность присвоения информации состояния соединения допустимых значений. В качестве основных состояний для сетевого трафика используются следующие:

- установление соединения;
- использование соединения;
- завершение соединения.

При этом каждый новый пакет проверяется МЭ по таблице состояний для определения того, не противоречит ли состояние пакета ожидаемому состоянию.

3.5.25. В изделии реализована возможность регистрации сбоев в использовании механизма ведения таблицы состояний.

3.5.26. В изделии обеспечивается для каждого соединения ведение таблицы состояний, основанной на информации состояния соединения и используемой при выполнении проверок для обнаружения аномальных пакетов, не соответствующих текущему состоянию соединения.

3.5.27. В изделии реализована возможность перехвата пакетов на сетевом уровне и проверки их на предмет разрешенности по существующим правилам межсетевого экранирования. Дополнительно сохраняется трек каждого соединения в таблице состояний. Детали таблицы включают:

- сетевой адрес (IP-адрес) источника;
- сетевой адрес (IP-адрес) получателя;
- номера портов;
- информацию состояния соединения.

3.5.28. В изделии реализована возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования.

3.5.29. В изделии реализована возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ).

3.5.30. В изделии реализована возможность при нарушении правил МЭ показывать предупреждающее сообщение пользователю.

3.6. Система обнаружения вторжений

3.6.1. В изделии имеются средства автоматизированного обновления базы решающих правил.

3.6.2. В изделии предоставляется возможность обновления базы решающих правил только администраторам и пользователям.

3.6.3. Модуль СОВ имеет графический интерфейс администрирования.

3.6.4. В изделии реализованы механизмы локального и удалённого администрирования СОВ.

3.6.5. В изделии администраторам безопасности (и только им) предоставляется возможность модифицировать режим выполнения функций, связанных с внутренним представлением времени, со сбором данных о системе ИТ, их анализом и ответными реакциями.

3.6.6. В изделии уполномоченным администраторам безопасности (и только им) предоставляется возможность задания, а также запроса, изменения, модификации, удаления и очистки значений по умолчанию.

3.6.7. В изделии поддерживаются следующие роли для управления модулем СОВ:

- администратор безопасности;
- пользователь ИС;
- администратор сервера.

3.6.8. В изделии обеспечена возможность ассоциировать пользователей с ролями.

3.6.9. В изделии обеспечена возможность выполнять анализ собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени. Обеспечена возможность по результатам анализа фиксировать следующую информацию:

- дату и время, результат анализа, тип данных, идентификатор источника данных;
- протокол (механизм), используемый для проведения вторжения;
- идентификатор субъекта вторжения, идентификатор объекта вторжения.

3.6.10. В изделии реализована возможность выполнять следующие функции по анализу всех полученных данных СОВ:

- обнаруживать вторжения в режиме, близком к реальному масштабу времени на уровне отдельных хостов (локальных узлов ИС) путем

анализа сетевого трафика без потери данных для анализа;

– обнаруживать вторжения на уровне отдельных хостов (локальных узлов ИС) путем анализа журналов событий ОС и прикладного ПО.

3.6.11. В случае обнаружения вторжений и нарушений безопасности, изделие предпринимает следующие действия:

– осуществить фиксацию факта обнаружения вторжений или нарушений безопасности в журналах аудита;
– уведомить администратора безопасности об обнаруженных вторжениях и нарушениях безопасности с помощью визуального отображения соответствующего сообщения на консоли управления и подачи звукового сигнала, а также сообщения по электронной почте;
– блокировать IP-адрес атакующего в течении заданного времени.

3.6.12. В изделии реализована возможность определения ограничений следующих данных только администратором безопасности:

– размер хранимых журналов;
– время блокировки IP-адреса атакующего.

3.6.13. В изделии предпринимаются следующие действия при достижении или превышении данными СОВ, установленных в требовании 1.4.4.12:

ротация журналов при превышении размера хранимых журналов;

– разблокировка IP-адреса атакующего при истечении времени блокировки IP-адреса атакующего.

3.6.14. В изделии реализована возможность генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

– запуск и завершение выполнения функций аудита;
– все события, потенциально подвергаемые аудиту, на неопределённом уровне аудита (минимальный, базовый, детализированный);
– доступ к СОВ;
– чтение информации из записей аудита;
– неуспешные попытки читать информацию из записей аудита;
– все модификации режима выполнения функций, связанных со сбором данных о системе ИТ, их анализом и ответными реакциями;
– все модификации данных СОВ, данных аудита и всех прочих данных СОВ;
– модификация группы пользователей – исполнителей роли;
– выполнение и результаты самотестирования компонентов СОВ.

3.6.15. В изделии реализована возможность регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

– дата и время, тип события, идентификатор субъекта и результат события (успешный или неуспешный);
– для каждого типа событий, потенциально подвергаемых аудиту, из числа определённых в функциональных компонентах, регистрируют-

ся следующие параметры: идентификатор объекта, вид запрашиваемого доступа при событии запуска и завершения выполнения функций аудита, при доступе к СОВ;

– идентификатор пользователя при событии модификации группы пользователей – исполнителей роли.

3.6.16. В изделии реализована возможность предоставлять администратору безопасности право читать все данные аудита из записей аудита.

3.6.17. В изделии реализована возможность записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

3.6.18. В изделии реализована возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

3.6.19. В изделии реализована возможность запрета всем пользователям доступа к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ для чтения.

3.6.20. В изделии предоставляется возможность выполнять поиск, упорядочивание, сортировку данных аудита, основанную на следующих атрибутах:

– дата и время;
– идентификатор субъекта;
– тип события;
– результат события (успешный / неуспешный);
– действие.

3.6.21. В изделии выполняется функция самотестирования при запуске, по запросу уполномоченного пользователя для демонстрации правильного выполнения функций безопасности СОВ.

3.6.22. Изделие предоставляет возможность уполномоченным пользователям верифицировать целостность данных функций безопасности СОВ.

3.6.23. В изделии предоставляется возможность уполномоченным пользователям верифицировать целостность программного кода функций безопасности СОВ.

3.6.24. Обеспечена возможность собирать информацию о сетевом трафике, проходящем через узлы сети:

– информация о сетевых адресах;
– информация о используемых портах;
– информация о значениях полей сетевого пакета;
– информация о аппаратных адресах устройств;
– информация о идентификаторах протоколов;
– информация о размерах пакетов.

3.6.25. В изделии обеспечена возможность собирать информацию о следующих событиях на узлах сети:

- события, регистрируемые в журналах аудита: ОС, прикладного программного обеспечения;
- вызов функций;
- обращение к ресурсам.

3.6.26. В изделии реализована возможность собирать и регистрировать следующую информацию:

- дату и время события;
- тип события;
- идентификатор субъекта.

3.6.27. В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием сигнатурных и эвристических методов.

3.6.28. В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика, методах выявления аномалий в действиях пользователя ИС.

3.6.29. В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов на заданном уровне.

3.6.30. Изделие имеет механизмы обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня (ICMPv4, ICMPv6, IPv4, IPv6) и транспортного уровня (UDP, TCP) базовой эталонной модели взаимосвязи открытых систем.

3.6.31. В изделии реализована возможность определения подмены IP-адреса и блокировка IP-флуда.

3.6.32. В изделии реализована защита IP-адреса от ложных сообщений «IP-адрес уже занят».

3.6.33. В изделии реализована возможность блокировки узлов, сканирующих ПК в сети.

3.6.34. В изделии реализована возможность выявления атак, направленных на отказ в облуживании.

3.6.35. В изделии реализована возможность определения списка типов атак, которые будут блокироваться.

3.6.36. В изделии реализована возможность создания собственных сигнатур СОВ.

3.6.37. В изделии реализована возможность блокировать недоверенные приложения, не имеющие цифровой подписи.

3.6.38. В изделии реализована возможность доверия приложениям, имеющим цифровую подпись.

3.6.39. В изделии реализована возможность настройки списка уязвимых портов.

3.6.40. В изделии реализована возможность выбора компонентов, разрешенных для использования на ПК.

3.6.41. В изделии реализована возможность выявления попыток ПО записывать данные в системный реестр и обращения к критическим объектам ОС.

3.6.42. В изделии реализована возможность настройки «чувствительности» определения атак.

3.6.43. В изделии реализована возможность настройки исключений для доверенных узлов, с которых не будет обнаруживаться атака.

3.6.44. В изделии реализовано маскирование датчиков СОВ.

3.6.45. В изделии реализован контроль целостности базы решающих правил СОВ (сигнатур журналов, трафика).

3.6.46. В изделии реализована возможность сохранения отфильтрованной информации из журналов после применения фильтрации.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

4.1.1. Входными данными являются:

- файлы конфигураций модулей СЗИ НСД, используемые при установке;
- уникальные для каждого пользователя логин, пароль и серийный номер аппаратного идентификатора;
- пароль при преобразовании/обратном преобразовании объекта файловой системы;
- формализованные правила политик безопасности, реализуемые с помощью механизмов СЗИ НСД и преобразованные в значения атрибутов и полномочий;
- сетевой трафик (для МЭ, СОВ);
- установленные соединения (для МЭ);
- события, регистрируемые в журналах аудита ОС и приложений (для СОВ).

4.1.2. Логином может служить набор любых символов, введенных с клавиатуры, длиной от 1 до 20, за исключением: "/", "\", "[", "]", ":", "|", "<", ">", "+", "=", ";", ",", "?", "@", "*".

4.1.3. Паролем может служить набор любых символов, введенных с клавиатуры, длиной от 6 до 31. Допустимые специальные символы: "`", "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/".

4.1.4. Минимальная длина и состав символов пароля регулируются соответствующими параметрами безопасности в СЗИ НСД.

4.2. Выходные данные

4.2.1. Выходными данными являются:

- сообщения СЗИ НСД на действия пользователей;
- журналы событий, создаваемые СЗИ НСД в процессе работы;
- значения контрольных сумм объектов, на которых установлен контроль целостности;
- резервные копии программных компонентов СЗИ НСД;
- файлы конфигураций модулей СЗИ НСД;
- отчеты результатов автоматического тестирования функционала по назначенным правам и конфигурациям, отчеты по спискам установленного ПО;
- сообщения СЗИ НСД в случае сигнализации при попытках несанкционированного доступа.

4.2.2. В журналах событий отслеживаются и отображаются такие данные, как дата, время, имя пользователя, имя объекта, тип операции, результат попытки доступа, характер ошибки и иная информация.