УТВЕРЖДЕНО
RU.48957919.501410-01 31-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА Dallas Lock 8.0-К

Описание применения

RU.48957919.501410-01 31

Листов 16

2016 г.

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-К» RU.48957919.501410-01 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 4

2. УСЛОВИЯ ПРИМЕНЕНИЯ 5

3. ОПИСАНИЕ ЗАДАЧИ 7

3.1. Подсистема управления доступом 7

3.2. Подсистема контроля устройств 8

3.3. Подсистема преобразования информации 9

3.4. Подсистема гарантированной зачистки информации 9

3.5. Подсистема идентификации и аутентификации 9

3.6. Подсистема регистрации и учета 10

3.7. Подсистема администрирования 12

3.8. Подсистема контроля целостности 13

3.9. Подсистема восстановления после сбоев 13

3.10. Подсистема межсетевого экранирования 14

3.11. Подсистема обнаружения вторжений 14

3.12. Подсистема развертывания. 15

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ 16

4.1. Входные данные 16

4.2. Выходные данные 16

1. НАЗНАЧЕНИЕ

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) и информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС).

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

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. Формуляр RU.48957919.501410-01 п. 3.3.4);
   - Windows Server 2003 (R2) (SP 2) (Web, Standard, Enterprise, Datacenter) (см. Формуляр RU.48957919.501410-01 п. 3.3.4);
   - 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).

2. СЗИ НСД поддерживает как 32-битные версии ОС, архитектуры Intel x86, так и 64-битные, архитектуры AMD64 (архитектура IA64 (Itanium) не поддерживается).
3. Для размещения файлов СЗИ НСД требуется не менее 200 МБ пространства на системном разделе жесткого диска.
4. Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.
5. СЗИ НСД может функционировать как на автономных ТС, так и на ТС в составе локальной вычислительной сети (TCP/IP).
6. СЗИ НСД может быть использована как в сетях с доменной организацией, так и в одноранговых сетях.
7. Для использования аппаратных идентификаторов необходимо наличие в аппаратной части ТС USB-порта или COM-порта.
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 5 классу защищенности;
   - «Средства вычислительной техники. Межсетевые экраны. 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 4 уровню контроля;
   - «Требования к системам обнаружения вторжений» (документ утвержден приказом ФСТЭК России № 638 от 6 декабря 2011 г.) – по 4 классу защищенности;
   - «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 4 классу защищенности;

- «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ;
- «Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.Н4.ПЗ.

При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (RU.48957919.501410-01 30), СЗИ НСД может быть использована:

- 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» (Гостехкомиссия России, 1992));
- для обеспечения 1 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»);
- 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»);
- при создании защищенных информационных 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

Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» RU.48957919.501410-01 91 (ТУ).

В соответствии с ТУ СЗИ НСД состоит из программного ядра и следующих подсистем:

- подсистема управления доступом;
- подсистема контроля устройств;
- подсистема преобразования информации;
- подсистема гарантированной зачистки информации;
- подсистема идентификации и аутентификации;
- подсистема регистрации и учёта;
- подсистема администрирования (локального, удаленного и централизованного управления);
- подсистема контроля целостности;
- подсистема восстановления после сбоев;
- подсистема межсетевого экранирования;
- подсистема обнаружения вторжений;
- подсистема развертывания.

3.1. Подсистема управления доступом

СЗИ НСД осуществляет контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

СЗИ НСД контролирует доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.). Для каждой пары (субъект – объект) задается явное перечисление допустимых типов доступа (чтение, запись и т.д.), 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).

СЗИ НСД 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 и т.д., а под «скрытыми» – иные действия, в том числе с использованием собственных программ работы с устройствами.

Предусмотрена возможность санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

СЗИ НСД предоставляет права изменения правил разграничения доступа для выделенных субъектов (администрации, службе безопасности и т.д.).

Реализовано разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

Реализована возможность ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы.

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

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

СЗИ НСД содержит механизмы контроля состава технических средств, программного обеспечения и средств защиты информации.

Реализована изоляция процессов (выполнения программ) в выделенной области памяти.

Реализована возможность ограничения количества терминальных сессий на одном ТС.

СЗИ НСД контролирует и определяет санкционированное время работы учетной записи пользователя. Реализован механизм ограничения доступа по дате и времени (расписание работы пользователей).

Реализована возможность управления учетными записями пользователей (добавление, удаление, блокирование, редактирование атрибутов), в том числе локальными, доменными, сетевыми. Также реализована возможность задания типа учетной записи пользователя:

- внутренний;
- внешний;
- системный;
- приложение;
- гостевой (анонимный);
- временный.

Реализована возможность объединения пользователей в группы, поддержка групп пользователей в правилах.

Реализована возможность настройки и организации замкнутой программной среды.

Реализована возможность блокировки доступа к файлам по расширению.

Реализована возможность разграничения доступа к буферу обмена.

3.2. Подсистема контроля устройств

СЗИ НСД осуществляет регламентацию и контроль использования в информационной системе технологий беспроводного доступа.

СЗИ НСД осуществляет регламентацию и контроль использования в информационной системе мобильных технических устройств.

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

СЗИ НСД содержит механизмы учета съемных машинных носителей информации с помощью любой маркировки. Учет защищаемых носителей производится в специальном журнале.

СЗИ НСД контролирует подключение съемных машинных носителей информации.

СЗИ НСД контролирует использование интерфейсов ввода (вывода) информации на съемные машинные носители информации.

СЗИ НСД контролирует ввод (вывод) информации на съемные машинные носители информации.

СЗИ НСД обеспечивает вывод информации на запрошенное пользователем устройство, как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки). СЗИ НСД включает в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

СЗИ НСД предоставляет возможность сохранения теневых копий файлов, записываемых на съемные машинные носители информации.

СЗИ НСД выполняет контроль аппаратной конфигурации ТС и следующих подключаемых устройств:

- Android-устройств;
- iOS-устройств;
- Bluetooth-устройств;
- DVD- и CD-ROM-дисководов;
- устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
- USB-контроллеров;
- беспроводных устройств (Wireless Communication Devices);
- биометрических устройств;
- дисководов магнитных дисков;
- звуковых, видео- и игровых устройств;
- инфракрасных устройств (IrDA);

- контроллеров магнитных дисков;
- ленточных накопителей;
- модемов;
- переносных устройств;
- портов (COM и LPT);
- сенсоров;
- сетевых адаптеров;
- сканеров и цифровых фотоаппаратов;
- принтеров;
- съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).

3.3. Подсистема преобразования информации

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

Реализована возможность создания преобразованных файл-дисков и файл-контейнеров для надежного хранения защищаемой информации.

СЗИ НСД принудительно отключает файл-диск при отключении аппаратного идентификатора.

Реализована возможность преобразования съемных машинных носителей информации.

Процесс преобразования съемных машинных носителей информации сопровождается индикацией прогресса.

3.4. Подсистема гарантированной зачистки информации

СЗИ НСД реализует и предоставляет возможность гарантированного уничтожения (стирания) и контроля уничтожения информации на съемных машинных носителях информации при полной зачистке логического диска.

Реализована возможность осуществления очистки (обнуления, обезличивания) освобождаемых областей оперативной памяти ТС и внешних накопителей. Очистка осуществляется путем записи маскирующей последовательности в освобождаемую область памяти. Вид маскирующей последовательности и число циклов записи (от 1 до 4) может настраиваться администратором безопасности.

СЗИ НСД при первоначальном назначении или при перераспределении внешней памяти предотвращает доступ субъекту к остаточной информации.

3.5. Подсистема идентификации и аутентификации

Реализована возможность задания длины пароля пользователя при входе в операционную систему.

СЗИ НСД осуществляет идентификацию и проверку подлинности субъектов доступа при входе в операционную систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Реализована возможность идентификации и аутентификации по идентификатору (коду) и паролю временного действия.

В СЗИ НСД осуществляется аутентификация пользователей –идентификация пользователей при запросах на доступ и проверка подлинности предъявленного субъектом идентификатора.

СЗИ НСД располагает необходимыми данными для идентификации и аутентификации и препятствует входу незарегистрированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась. СЗИ НСД обладает способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

Реализовано препятствие доступа к защищаемым ресурсам незарегистрированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

Осуществляется идентификация терминалов, ТС, узлов сети ТС, каналов связи, внешних устройств ТС по логическим именам и по физическим адресам (номерам).

Осуществляется идентификация программ, томов, каталогов, файлов, записей, полей записей и иных объектов доступа по именам.

Осуществляется идентификация устройств, в том числе, стационарных, мобильных и портативных, идентификация накопителей информации.

Реализована возможность управления идентификаторами, в том числе создание, присвоение и уничтожение идентификаторов.

Реализовано управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Реализована возможность ограничения количества последовательных неудачных попыток ввода пароля (например: от 3 до 5). При превышении указанного количества, средства защиты и механизмы защиты блокируют возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности.

Реализована защита обратной связи при вводе аутентификационной информации.

Реализована возможность настройки и отображения заданного текстового уведомления пользователя при его входе в информационную систему (например, о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, о необходимости соблюдения установленных оператором правил обработки персональных данных).

Реализовано оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему.

Реализована возможность аутентификации при помощи аппаратных идентификаторов.

Реализована возможность записи авторизационных данных в аппаратный идентификатор.

Реализована возможность определения принадлежности аппаратного идентификатора конкретному пользователю.

Реализована возможность входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows.

Обеспечена возможность идентификации и аутентификации администратора СЗИ НСД до предоставления ему возможности по управлению, просмотру аудита безопасности и выполнения иных действий по администрированию.

При удаленных запросах на доступ администратора идентификация и аутентификация обеспечивается методами, устойчивыми к пассивному и активному перехвату информации.

Реализована возможность настройки приветственного сообщения при входе в операционную систему и разблокировке рабочей станции.

3.6. Подсистема регистрации и учета

СЗИ НСД обеспечивает сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

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

СЗИ НСД содержит механизмы просмотра и анализа данных регистрации, информации о действиях отдельных пользователей в информационной системе, имеет механизмы фильтрации и группировки по заданному набору параметров.

СЗИ НСД обеспечивает защиту данных регистрации от их уничтожения или модификации нарушителем.

СЗИ НСД осуществляет регистрацию входа (выхода) субъектов доступа в операционную 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.

Реализовано обеспечение регистрации входа (выхода) администратора в операционную систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения. В параметрах регистрации указываются:

- дата, время и код регистрируемого события;
- результат попытки осуществления регистрируемого события – успешная или неуспешная;
- идентификатор администратора, предъявленный при попытке осуществления регистрируемого события.

СЗИ НСД 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;
- успешность осуществления события (обслужен запрос на доступ или нет).

СЗИ НСД осуществляет регистрацию выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации должны указываться:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код);
- 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). Вместе с выдачей документа автоматически оформляется учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода), фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа фактически выданного количества листов в графе брака).

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

СЗИ НСД осуществляет регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный).

Осуществляется регистрация создания и уничтожения объекта. Регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события;
- успешность осуществления события.

Осуществляется регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ТС, узлам сети, линиям (каналам) связи, внешним устройствам ТС, программам, томам, каталогам, файлам, записям, полям записей. 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)].

В случае доступа к защищаемым файлам в параметрах регистрации также указывается вид запрашиваемой операции (например, чтение, запись, модификация, удаление).

В СЗИ НСД реализована возможность определения событий безопасности, подлежащих регистрации, и сроков их хранения (журналы регистрации событий должны иметь фиксированный размер и не должны иметь ограничений по срокам хранения).

В СЗИ НСД реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.

СЗИ НСД содержит механизмы генерации временных меток. Возможна синхронизация системного времени в информационной системе.

Осуществляется сигнализация попыток нарушения защиты на терминалах администратора и нарушителя.

Осуществляется регистрация событий, связанных с действиями по зачистке остаточной информации.

3.7. Подсистема администрирования

В СЗИ НСД реализованы средства управления, ограничивающие распространение прав на доступ.

В СЗИ НСД реализовано управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе учетными записями внешних пользователей.

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

СЗИ НСД содержит механизмы, позволяющие проводить периодическое тестирование функций СЗИ НСД. Тестируются следующие функции:

- 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.

В СЗИ НСД реализован механизм гибкой настройки штампа, проставляемого при отчуждении информации на твердую копию.

При сетевом использовании СЗИ НСД обеспечивает (за счет сервера безопасности) синхронизацию времени.

Реализован модуль управления лицензиями для сервера безопасности и на ограничение числа терминальных сессий.

Реализована возможность дистанционного управления компонентами изделия, в том числе возможности конфигурирования параметров и фильтров, проверки взаимной согласованности всех настроек и фильтров, анализа регистрационной информации.

Реализована возможность централизованного управления защищаемыми рабочими станциями. Осуществляется централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями

информации. Поддерживается многоуровневая иерархия групп ТС и наследование установленных параметров.

Реализована возможность распределения функций централизованного управления на несколько рабочих станций – реплицированных серверов информационной системы. Между серверами безопасности, находящимися в репликации, обеспечивается синхронизация по требованию всех настроек централизованного управления.

Реализована возможность средствами централизованного управления активации и деактивации модуля МЭ, СОВ для компьютера или группы компьютеров, входящих в состав информационной сети (посредством изменения серийного номера СЗИ НСД).

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 СЗИ НСД);
- клиент недоступен долгое время (с возможностью задания периода времени);
- попытка монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами;
- попытка нарушения правил фильтрации межсетевого экрана;
- модификация функций безопасности СОВ.

Реализована возможность создания отчета по назначенным правам, настройкам МЭ, настройкам СОВ, составу программного и аппаратного обеспечения.

Реализована возможность удаленной установки и обновления изделия.

Реализована возможность визуализации сети защищаемых ТС.

Реализована возможность сохранения и применения конфигурации СЗИ НСД.

3.8. Подсистема контроля целостности

СЗИ НСД обеспечивает целостность программных средств изделия, а также неизменность программной среды. При этом:

- целостность проверяется при загрузке операционной системы по контрольным суммам компонент изделия и динамически в процессе работы АС;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

В СЗИ НСД реализованы средства периодического контроля за целостностью программной и информационной части изделия.

Реализована защита архивных файлов, параметров настройки СЗИ НСД, программного обеспечения и иных данных, не подлежащих изменению в процессе функционирования ИС (обработки персональных данных).

Реализована возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности.

3.9. Подсистема восстановления после сбоев

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

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

3.10. Подсистема межсетевого экранирования

СЗИ НСД обеспечивает фильтрацию сетевого трафика. Решение по фильтрации принимается для каждого сетевого пакета независимо, на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

СЗИ НСД обеспечивает фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.

СЗИ НСД обеспечивает фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов.

СЗИ НСД обеспечивает фильтрацию с учетом любых значимых полей сетевых пакетов.

Реализовано обеспечение фильтрации на установление виртуальных соединений на транспортном уровне запросов (при этом, по крайней мере, учитываются транспортные адреса отправителя и получателя).

Реализовано обеспечение фильтрации на прикладном уровне запросов к прикладным сервисам (при этом, по крайней мере, учитываются прикладные адреса отправителя и получателя).

СЗИ НСД позволяет выполнить фильтрацию регистрируемых событий МЭ с учетом даты/времени.

Реализовано разграничение сетевого доступа пользователей к узлам сети.

Реализовано разграничение доступа к сети для приложений. Реализована возможность идентификации и аутентификации по идентификатору (коду) и паролю временного действия.

Реализована возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

При удаленных запросах на доступ администратора идентификация и аутентификация обеспечиваются методами, устойчивыми к пассивному и активному перехвату информации.

Реализована регистрация действий администратора по изменению правил фильтрации МЭ.

Реализована возможность регистрации и учета фильтруемых пакетов. В параметрах регистрации указываются, по крайней мере, адрес, время и результат фильтрации.

Реализована возможность регистрации и учета запросов на установление виртуальных соединений.

Реализована локальная сигнализация попыток нарушения правил фильтрации.

Реализована дистанционная сигнализация попыток нарушения правил фильтрации.

Реализована программируемая реакция на события в МЭ.

Реализована возможность оповещения администратора безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях при попытках нарушения правил фильтрации межсетевого экрана.

Реализована возможность создания отчета по правилам фильтрации межсетевого экрана.

Реализована возможность сохранения и применения конфигурации СЗИ НСД, в том числе межсетевого экрана.

3.11. Подсистема обнаружения вторжений

В СЗИ НСД реализована возможность сбора информации о сетевом трафике, проходящем через контролируемые узлы ИС.

В СЗИ НСД реализована возможность сбора информации о событиях, регистрируемых в журналах аудита ОС.

Реализована возможность выполнения анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксации информации о дате и времени события, о типе события, об идентификаторе субъекта.

Реализована возможность обнаружения вторжения по отношению к контролируемым узлам ИС в режиме, близком к реальному масштабу времени, на уровне отдельных узлов.

Реализована возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов.

В СЗИ НСД реализована возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика и аномалий в действиях пользователя ИС, на заданном уровне эвристического анализа.

В СЗИ НСД реализована возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита.

Реализована возможность уведомления администратора СОВ об обнаруженных вторжениях и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления.

Реализована возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем (OSI).

В СЗИ НСД реализована возможность автоматизированного обновления базы решающих правил.

В СЗИ НСД реализован интерфейс администрирования.

Реализована возможность уполномоченным администраторам (ролям) управлять режимом выполнения функций безопасности СОВ.

Реализована возможность уполномоченным администраторам (ролям) управлять данными (данными СОВ), используемыми функциями безопасности СОВ.

Реализована возможность поддержки определённых ролей для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС.

Реализована возможность управления данными функций безопасности СОВ (данными СОВ) в части установления и контроля ограничений на эти данные.

В СЗИ НСД реализована возможность тестирования (самотестирования) функций безопасности СОВ (контроль целостности исполняемого кода СОВ).

Реализована возможность генерации записей аудита для событий, потенциально подвергаемых аудиту.

В СЗИ НСД реализована возможность чтения информации из записей аудита.

В СЗИ НСД реализована возможность выполнения поиска, упорядочивания, сортировки данных аудита.

3.12. Подсистема развертывания.

Выполняет все необходимые функции по установке СЗИ НСД на рабочую станцию и удалению с нее.

В процессе развертывания реализована возможность установки конфигурации по умолчанию (удовлетворяющей требованиям ограничений по эксплуатации, указанным в разделе 3.3. формуляра на изделие, RU.48957919.501410-01 30) и другой рабочей конфигурации СЗИ НСД.

В процессе развертывания реализована возможность автоматического ввода рабочей станции под управление сервера безопасности.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

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).

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

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

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

4.2. Выходные данные

Выходными данными являются:

- сообщения СЗИ НСД на действия пользователей;
- журналы событий, создаваемые СЗИ НСД в процессе работы;
- теневые копии распечатываемых документов и копии файлов, записываемых на отчуждаемые носители информации;
- 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.

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.