

УТВЕРЖДЕН  
RU.48957919.26.20.40.142.001 31-ЛУ  
(взамен RU.48957919.501410-01 31-ЛУ)

## СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

# Dallas Lock 8.0-K

(версия 12.10.4.877)



## Описание применения

RU.48957919.26.20.40.142.001 31  
(взамен RU.48957919.501410-01 31)

## СОДЕРЖАНИЕ

<b>АННОТАЦИЯ .....</b>	<b>3</b>
<b>1 НАЗНАЧЕНИЕ.....</b>	<b>4</b>
<b>2 УСЛОВИЯ ПРИМЕНЕНИЯ.....</b>	<b>5</b>
<b>3 ОПИСАНИЕ ЗАДАЧИ.....</b>	<b>8</b>
3.1 СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА .....	8
3.2 СРЕДСТВО КОНТРОЛЯ ПОДКЛЮЧЕНИЯ СЪЕМНЫХ МАШИНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ. СРЕДСТВО КОНТРОЛЯ ОТЧУЖДЕНИЯ (ПЕРЕНОСА) ИНФОРМАЦИИ СО СЪЕМНЫХ МАШИНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ	12
3.3 ПЕРСОНАЛЬНЫЙ МЕЖСЕТЕВОЙ ЭКРАН .....	13
3.4 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ.....	16
3.5 СЕРВЕР КОНФИГУРАЦИЙ.....	20
3.6 ОБЩИЕ ЗАДАЧИ СУЩЕСТВУЮЩИХ ПОДСИСТЕМ СЗИ НСД .....	20
<b>4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ .....</b>	<b>24</b>

## 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-K**» RU.48957919.26.20.40.142.001 (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.

## 1 НАЗНАЧЕНИЕ

Изделие предназначено для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных правил разграничения доступа (ПРД) к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему (АС) и выходящими за ее пределы, обеспечения защиты информации в АС посредством ее фильтрации. Может использоваться в многопользовательских АС, информационных системах персональных данных, государственных информационных системах, автоматизированных системах управления производственными и технологическими процессами и при защите значимых объектов критической информационной инфраструктуры.

Изделие предназначено для использования на технических средствах (ТС), таких как персональные компьютеры (ПК), портативные компьютеры (ноутбуки, планшеты), сервера и ТС с поддержкой виртуальных сред и технологии Windows To Go. Может функционировать как на автономных ПК, так и на компьютерах в составе локальной вычислительной сети (ЛВС), в том числе под управлением контроллера домена.

## 2 УСЛОВИЯ ПРИМЕНЕНИЯ

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

- Windows 7 (SP1)<sup>1</sup> (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter) (см. Формуляр RU.48957919.26.20.40.142.001 30 п. 3.3.4);
- Windows Server 2008 R2 (SP1)<sup>1</sup> (Foundation, Standard, Web, Enterprise, Datacenter) (см. Формуляр RU.48957919.26.20.40.142.001 30 п. 3.3.4);
- 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);
- Windows Server 2019 (Standard, Datacenter, Essentials);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter);
- Windows Server 2025.

Модуль «Единый центр управления Dallas Lock» (далее по тексту — «**ЕЦУ Dallas Lock**», «**ЕЦУ**»), входящий в состав изделия, может быть использован на ТС, работающих под управлением ОС семейства Windows (x64):

- Windows 8.1 (Core, Pro, Enterprise);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Essentials, Standard, Datacenter);
- Windows Server 2022 (Standard, Datacenter, Datacenter: Azure Edition);

и семейства GNU Linux (x64):

- Debian 10.x;
- Debian 11.x;
- Debian 12.x;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Ubuntu 22.04 LTS;
- Ubuntu 24.04 LTS;
- Astra Linux Common Edition (Орел) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6, 1.7, 1.8;
- Альт Рабочая Станция 9.x;
- Альт Рабочая Станция 10.0, 10.1, 10.2, 10.4;
- Альт Рабочая Станция К 10.0, 10.1, 10.3, 10.4;
- Альт Сервер 9;
- Альт Сервер 10.0, 10.1, 10.2, 10.4;
- Альт 8 СП релиз 10 (Рабочая станция, Сервер);
- РЕД ОС 7.3 Муром;
- РЕД ОС 8;
- ROSA FRESH DESKTOP 12.

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

---

<sup>1</sup> С установленными обновлениями KB3033929 и KB3080149 (или пакетами обновлений, в состав которых они входят).

3. Для размещения файлов **СЗИ НСД** требуется не менее 1 Гб 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 ЛВС.
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 СОМ-порта. **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.
  - «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (документ утвержден приказом ФСТЭК России № 76 от 2 июня 2020 г.) — по 4 уровню доверия.
  - «Требования к средствам контроля съемных машинных носителей информации» (документ утвержден приказом ФСТЭК России № 87 от 28 июля 2014 г.) — по 4 классу защиты.
  - «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.
  - «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 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.
8. При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (RU.48957919.26.20.40.142.001 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));
  - в информационных системах персональных данных до 1 уровня защищенности включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
  - в государственных информационных системах до 1 класса защищенности включительно (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 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»);

- при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

### 3 ОПИСАНИЕ ЗАДАЧИ

Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» RU.48957919.26.20.40.142.001 91 (ТУ).

Изделие **СЗИ НСД Dallas Lock 8.0-K** включает в себя следующие основные функциональные модули:

- система защиты информации от несанкционированного доступа;
- средство контроля подключения съемных машинных носителей информации (**СКН-П**);
- средство контроля отчуждения (переноса) информации со съемных машинных носителей информации (**СКН-Н**);
- персональный межсетевой экран (**МЭ**);
- система обнаружения вторжений (**СОВ**);
- резервное копирование (**РК**).

#### 3.1 Система защиты информации от несанкционированного доступа

##### Подсистема управления доступом

1. Изделие осуществляет контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.
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), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу средства вычислительной техники (СВТ) (объекту). Контроль доступа применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).
3. Изделие содержит механизм, реализующий дискреционные ПРД. Такой механизм применим как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (то есть 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.
4. В изделии предусмотрена возможность санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.
5. Изделие предоставляет права изменения ПРД для выделенных субъектов (администрации, службе безопасности).
6. В изделии реализовано разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
7. В изделии есть возможность ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя ТС.
8. Изделие обеспечивает поддержку и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки.
9. В изделии реализована возможность блокирования сеанса доступа после установленного времени бездействия пользователя или по его запросу через средства централизованного и удаленного администрирования **СЗИ НСД**. Событие изменения установленного времени бездействия фиксируется в журнале изменения политик. В значениях установленного времени бездействия присутствуют интервалы в 5 и 15 минут.
10. Изделие содержит механизмы контроля состава технических средств, программного обеспечения и средств защиты информации.
11. Изделие предоставляет возможность управления учетными записями пользователей (добавление, удаление, блокирование, редактирование атрибутов) в том числе локальных, доменных, сетевых, а также возможность задания типа учетной записи пользователя:
  - внутренняя;
  - внешняя;
  - системная;

- приложение;
- гостевая;
- временная.

12. Изделие осуществляет регламентацию и контроль использования в информационной системе технологий беспроводного доступа.
13. Изделие осуществляет регламентацию и контроль использования в информационной системе мобильных технических устройств.
14. В изделии реализована возможность настройки и организации замкнутой программной среды.
15. В изделии реализована возможность блокировки доступа к файлам по расширению.
16. В изделии реализована возможность разграничения доступа к буферу обмена.
17. В изделии реализована функция запрета автоматического запуска подключенных устройств.
18. В изделии реализована функция автоматического блокирования неактивных учетных записей пользователей после периода времени неиспользования более 45 дней и более 90 дней.

#### **Подсистема преобразования информации**

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.
2. Изделие предоставляет возможность создания преобразованных файл-дисков и файл-контейнеров для надежного хранения защищаемой информации.
3. Изделие предоставляет возможность преобразования съемных машинных носителей информации.

#### **Подсистема гарантированной зачистки информации**

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

#### **Подсистема идентификации и аутентификации**

1. В изделии реализована возможность задания длины пароля пользователя при входе в систему.
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. 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.
4. В изделии осуществляется идентификация терминалов, ТС, узлов сети ТС, внешних устройств ТС по логическим именам и по физическим адресам (номерам).
5. В изделии осуществляется идентификация программ, каталогов, файлов, по именам.
6. В изделии осуществляется идентификация устройств, в том числе стационарных, мобильных и портативных.
7. В изделии реализована возможность управления идентификаторами, в том числе создание, присвоение и уничтожение идентификаторов.
8. В изделии реализовано управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.
9. В изделии реализована возможность ограничения количества последовательных неудачных попыток ввода пароля (например, от 3 до 5).
10. В изделии реализована защита обратной связи при вводе аутентификационной информации.
11. В изделии реализована возможность аутентификации при помощи аппаратных идентификаторов.
12. В изделии реализована возможность записи авторизационных данных в аппаратный

идентификатор.

13. В изделии реализована возможность определения принадлежности аппаратного идентификатора конкретному пользователю.
14. В изделии реализована возможность входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows.
15. В изделии реализована функция запрета повторного использования идентификатора пользователя в течение:
  - не менее одного года;
  - не менее трех лет;
  - всего периода эксплуатации информационной системы.
16. В изделии реализована возможность аутентификации через Safe-Tech PayControl.
17. Изделие осуществляет механизм выхода из системы при извлечении аппаратного идентификатора.

#### **Подсистема регистрации и учета**

1. Изделие обеспечивает мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
2. Изделие содержит механизмы просмотра и анализа данных регистрации, информации о действиях отдельных пользователей в информационной системе, имеет механизмы фильтрации по заданному набору параметров.
3. Изделие обеспечивает защиту данных регистрации от их уничтожения или модификации нарушителем.
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.
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).
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) 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).
7. Дополнительно регистрируются все попытки доступа, все действия оператора и выделенных пользователей (администраторов защиты и т. п.).
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.
9. 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)].
10. В изделии реализована возможность определения событий безопасности, подлежащих регистрации (журналы регистрации событий имеют фиксированный размер и не имеют ограничений по срокам хранения).
11. В изделии осуществляется сигнализация попыток нарушения защиты на терминалах администратора и нарушителя.
12. В изделии осуществляется регистрация деинсталляции (не запуска) драйвера **МЭ** при активном компоненте, а также реализована функция выполнения защиты в соответствии с установленными политиками.
13. 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.

#### Подсистема администрирования

1. В изделии реализованы средства управления, ограничивающие распространение прав на доступ.
2. Изделие предоставляет возможность назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.
3. Изделие содержит механизмы, позволяющие проводить периодическое тестирование функций **СЗИ НСД Dallas Lock 8.0-K**. 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.
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.
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.
6. В изделии реализована возможность создания отчета по назначенным правам, составу программного и аппаратного обеспечения.

7. В изделии реализована возможность удаленной установки и обновления изделия.
8. В изделии реализована возможность назначения администратора безопасности при удаленной установке изделия.
9. В изделии реализована возможность визуализации сети защищаемых ТС.
10. В изделии реализована возможность сохранения и применения конфигурации **СЗИ НСД**.
11. В изделии реализована функция, позволяющая одновременно подключаться к Серверу безопасности **СЗИ НСД** нескольким консолям Сервера безопасности.
12. В изделии реализована функция ограничения количества неуспешных попыток входа и блокирование ТС, с которого предпринимаются попытки доступа, с возможностью разблокирования только администратором.
13. В изделии предустановлены шаблоны безопасности, соответствующие стандартам по защите автоматизированных систем, информационных систем персональных данных и государственных информационных систем.

#### **Подсистема контроля целостности**

1. В изделии реализована защита архивных файлов, параметров настройки **СЗИ НСД**, программного обеспечения и иных данных, не подлежащих изменению в процессе функционирования ИС.
2. В изделии реализована возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности.
3. В изделии реализован механизм создания точки восстановления при установке клиента **Dallas Lock**.
4. В изделии реализована возможность блокировки доступа к объекту файловой системы при нарушении целостности контролируемых модулей. При нарушении целостности контролируемых модулей запуск объекта файловой системы блокируется.

#### **Подсистема восстановления после сбоев**

1. **СЗИ НСД** предусматривает процедуры восстановления после сбоев и отказов оборудования, которые обеспечивают полное и оперативное восстановление свойств **СЗИ НСД**.
2. Реализована возможность возвращения всех настроек **СЗИ НСД** к исходным (установка параметров по умолчанию), что равносильно переустановке **СЗИ НСД**.

#### **Подсистема резервного копирования**

1. В изделии реализована возможность автоматизированного создания резервных копий произвольных объектов файловой системы и централизованное управление такой возможностью на уровне Сервера безопасности «**Dallas Lock 8.0**». При этом в изделии реализована возможность:
  - определения размещения сохранения резервной копии;
  - определения периодичности и расписание создания резервных копий;
  - определения количества сохраняемых резервных копий;
  - восстановления защищаемых объектов из резервной копии.
2. В изделии реализована возможность сохранения файла резервной копии и файла конфигурации Сервера безопасности в сетевую директорию.
3. В изделии реализован механизм восстановления файлов **Dallas Lock** при сбоях и повреждениях.

### **3.2 Средство контроля подключения съемных машинных носителей информации. Средство контроля отчуждения (переноса) информации со съемных машинных носителей информации**

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.
2. Изделие контролирует использование интерфейсов ввода (вывода) информации (в том числе на съемные машинные носители информации).
3. Изделие обеспечивает контроль типов подключаемых внешних программно-аппаратных

- устройств, а также конкретных съемных машинных носителей информации.
4. В изделии обеспечена возможность идентификации и аутентификации администратора **СЗИ НСД Dallas Lock 8.0-K** до предоставления ему возможности по управлению, просмотру аудита безопасности и выполнению иных действий по администрированию.
  5. В изделии осуществляется идентификация устройств, в том числе стационарных, мобильных и портативных, идентификация накопителей информации.
  6. 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.
  7. Изделие содержит механизмы генерации временных меток, и (или) происходит синхронизация системного времени в информационной системе.
  8. В изделии осуществляется разграничение доступа к управлению **СКН** и режимом выполнения функций безопасности (контроля накопителей) на основе ролей учетных записей пользователей.
  9. 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.
  10. Изделие предоставляет возможность настройки прав использования съемного машинного носителя информации с установленным специальным программным обеспечением (на конкретных средствах вычислительной техники).
  11. Изделие блокирует информационные ресурсы специализированного съемного машинного носителя информации для чтения (записи) информации при попытке подключения специализированного съемного машинного носителя информации к средству вычислительной техники, на котором не установлены компоненты средства контроля съемных машинных носителей информации (программное обеспечение взаимодействия).
  12. Изделие проверяет права использования специализированного съемного машинного носителя информации при попытке подключения специализированного съемного машинного носителя информации к средству вычислительной техники, на котором установлены компоненты средства контроля съемных машинных носителей информации (программное обеспечение взаимодействия).
  13. Изделие предоставляет доступ к информации на специализированном съемном машинном носителе информации (если проверка прав дала положительный результат) или обеспечивает недоступность (блокирование) информации на специализированном съемном машинном носителе информации для чтения (записи) информации (если проверка прав дала отрицательный результат).
  14. Изделие регистрирует события безопасности, связанные с выполнением средством контроля съемных машинных носителей информации функций безопасности, и записывает информацию аудита безопасности.
  15. Изделие обеспечивает разграничение доступа к разделам файловой системы съемных машинных носителей информации и объектам файловой системы, расположенных на них.
  16. Изделие обеспечивает блокировку автоматизированного рабочего места при подключении незарегистрированных машинных носителей информации до снятия блокировки администратором безопасности.

### 3.3 Персональный межсетевой экран

1. Изделие предоставляет возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций перемещения контролируемой **МЭ** информации к узлам информационной системы и от них.
2. Изделие обеспечивает распространение фильтрации на все операции перемещения через **МЭ** информации к узлам информационной системы.
3. Изделие осуществляет фильтрацию, основанную на следующих типах атрибутов безопасности субъектов:
  - сетевой адрес узла отправителя;
  - сетевой адрес узла получателя.

4. Изделие осуществляет 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).
5. Изделие предоставляет возможность явно разрешать или явно запрещать информационный поток, базируясь на устанавливаемых администратором **МЭ** наборе правил фильтрации, основанном на идентифицированных атрибутах.
6. Изделие предоставляет возможность осуществлять политику фильтрации пакетов с учетом управляющих команд от взаимодействующих с **МЭ** средств защиты информации других видов.
7. В изделии реализована возможность осуществлять проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию.
8. В изделии реализована возможность осуществлять проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором **МЭ** установлены разрешительные или запретительные атрибуты безопасности. Реализована возможность контролировать (разрешать/запрещать) использование сетевых ресурсов, содержащих PDF и следующие виды мобильного кода: ActiveX, Flash, JScript, VBScript, PostScript, Java.
9. В изделии для администратора **МЭ** предоставлена возможность модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для используемых пользователями отдельных команд. Возможность осуществлять проверку использования пользователями таких команд. Также реализована возможность контролировать (разрешать/запрещать) использование следующих команд: arp; ipconfig; getmac; nbtstat; netsh; netstat; net; nslookup; pathping; ping; route; telnet; tracer.
10. В изделии реализована возможность разрешать или запрещать информационный поток, основываясь на результатах проверок в соответствии с п.7.
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.
12. Изделие разрешает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации.
13. Изделие запрещает информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации.
14. В изделии реализована возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита. Избирательность аудита базируется на следующих возможных атрибутах:
  - идентификатор объекта;
  - идентификатор пользователя;
  - идентификатор субъекта;
  - тип события;
  - или другие атрибуты.Реализована возможность выбрать какие типы событий **МЭ** будут регистрироваться:
  - обнаружение мобильного кода (ActiveX, Flash, JScript, VBScript, PostScript, Java);
  - обнаружение запрещенных вложений (анализируется присутствие известных протоколов, рекламы, медиа-контента, PDF);
  - выполнение команд.
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.
16. В изделии возможна поддержка определенных ролей по управлению **МЭ**.

17. В изделии реализована возможность со стороны администраторов **МЭ** управлять режимом выполнения функций безопасности **МЭ**.
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.
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.
20. В изделии есть возможность ведения для каждого типа мест расположения узла с установленным **МЭ** отдельных профилей проверок.
21. В изделии есть возможность изменения области значений информации состояния соединения со стороны администраторов межсетевого экрана. У администратора есть возможность завершать сетевые соединения из таблицы соединений.
22. В изделии есть 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.
23. В изделии есть 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 межсетевым экраном по таблице состояний для определения того, не противоречит ли состояние пакета ожидаемому состоянию.
24. Реализована возможность регистрации сбоев в использовании механизма ведения таблицы состояний.
25. Для каждого соединения обеспечивается ведение таблицы состояний, основанной на информации состояния соединения и используемой при выполнении проверок для обнаружения аномальных пакетов, не соответствующих текущему состоянию соединения.
26. Реализована возможность перехвата пакетов на сетевом уровне и проверки их на предмет разрешенности по существующим правилам межсетевого экранирования. Дополнительно нужно сохранять трек каждого соединения в таблице состояний. Детали таблицы включают:
  - сетевой адрес (IP-адрес) источника;
  - сетевой адрес (IP-адрес) получателя;
  - номера портов;
  - информацию состояния соединения.
27. В изделии реализована возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата **МЭ** к штатному режиму функционирования.
28. В изделии реализована возможность тестирования (самотестирования) функций безопасности **МЭ** (контроль целостности исполняемого кода **МЭ**).
29. В изделии реализована возможность при нарушении правил **МЭ** показывать предупреждающее сообщение пользователю.
30. В изделии реализована функциональная возможность информирования (запись в журнал, всплывающее сообщение и сообщение на Сервер безопасности **СЗИ НСД**) о возможности обновления сигнатур.
31. В изделии реализована возможность задавать и анализировать командную строку (для гибкой настройки правил **МЭ**).
32. В изделии реализован вывод всплывающего детализированного уведомления при блокировке

контента.

33. В изделии реализована функциональная возможность «пакетного» управления правилами **МЭ**, которая позволяет формировать и применять отдельные группы правил **МЭ**.
34. В изделии реализован фильтр HTTP заголовка, который позволяет выполнять журналирование, блокировку соединения с аномальными HTTP заголовками.
35. В изделии реализована функциональная возможность активации более жестких правил **МЭ** при отсутствии на защищаемом ТС антивируса, обновлений или при нарушении контроля целостности.
36. В изделии реализована функциональная возможность использования DNS-имени вместо правил IP-адреса при настройке правил **МЭ** для обеспечения работы правила при смене IP-адреса ресурса.
37. В изделии реализован интерактивный режим обучения при формировании правил **МЭ**.
38. В изделии реализована политика «**Блокировка QUIC**».
39. В изделии реализован механизм фильтрации сетевого трафика с поддержкой команд протоколов: HTTP, SMTP, FTP, IMAP, POP3, DNS. Факты срабатывания фильтров с поддержкой команд протоколов фиксируются в «**Журнале трафика**».
40. В изделии реализован профиль межсетевого экрана, позволяющий логически изолировать автоматизированное рабочее место от сети передачи данных и поддерживать соединение только с Единым центром управления Dallas Lock.

### 3.4 Система обнаружения вторжений

1. В изделии имеются средства автоматизированного обновления базы решающих правил.
2. В изделии предоставляется возможность обновления базы решающих правил только администраторам и пользователям.
3. Модуль **СОВ** имеет графический интерфейс администрирования.
4. В изделии реализованы механизмы локального и удалённого администрирования **СОВ**.
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.
6. В изделии уполномоченным администраторам безопасности (и только им) предоставляется возможность задания, а также запроса, изменения, модификации, удаления и очистки значений по умолчанию.
7. В изделии поддерживаются следующие роли для управления модулем **СОВ**:
  - администратор безопасности;
  - пользователь ИС;
  - администратор сервера.
8. В изделии обеспечена возможность ассоциировать пользователей с ролями.
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.
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.
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;
  - заблокировать IP-адрес атакующего в течении заданного времени.
- 12.В изделии реализована возможность определения ограничений следующих данных только администратором безопасности:
- размер хранимых журналов;
  - время блокировки IP-адреса атакующего.
- 13.В изделии предпринимаются следующие действия при достижении или превышении данными ограничений **СОВ**, установленных в требовании 12:
- ротация журналов при превышении размера хранимых журналов;
  - разблокировка IP-адреса атакующего при истечении времени блокировки IP-адреса атакующего.
- 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**.
- 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, регистрируются 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.
- 16.В изделии реализована возможность предоставлять администратору безопасности право читать все данные аудита из записей аудита.
- 17.В изделии реализована возможность записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.
- 18.В изделии реализована возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.
- 19.В изделии реализована возможность запрета всем пользователям доступа к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ для чтения.
- 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.
- 21.В изделии выполняется функция самотестирования при запуске, по запросу уполномоченного пользователя для демонстрации правильного выполнения функций безопасности **СОВ**.
- 22.Изделие предоставляет возможность уполномоченным пользователям верифицировать целостность данных функций безопасности **СОВ**.
- 23.В изделии предоставляется возможность уполномоченным пользователям верифицировать

целостность программного кода функций безопасности **СОВ**.

24. Обеспечена возможность собирать информацию о сетевом трафике, проходящем через узлы сети:
  - информация о сетевых адресах;
  - информация об используемых портах;
  - информация о значениях полей сетевого пакета;
  - информация об аппаратных адресах устройств;
  - информация об идентификаторах протоколов;
  - информация о размерах пакетов.
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.
26. В изделии реализована возможность собирать и регистрировать следующую информацию:
  - дату и время события;
  - тип события;
  - идентификатор субъекта.
27. В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием сигнатурных и эвристических методов.
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.
29. В изделии реализована возможность выполнять анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов на заданном уровне.
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.
31. В изделии реализована возможность определения подмены IP-адреса и блокировка IP-флуда.
32. В изделии реализована возможность блокировки узлов, сканирующих ПК в сети.
33. В изделии реализована возможность выявления атак, направленных на отказ в обслуживании.
34. В изделии реализована возможность определения списка типов атак, которые будут блокироваться.
35. В изделии реализована возможность создания собственных сигнатур **СОВ**.
36. В изделии реализована возможность блокировать недоверенные приложения, не имеющие цифровой подписи.
37. В изделии реализована возможность доверия приложениям, имеющим цифровую подпись.
38. В изделии реализована возможность настройки списка уязвимых портов.
39. В изделии реализована возможность выбора компонентов, разрешенных для использования на ПК.
40. В изделии реализована возможность выявления попыток ПО записывать данные в системный реестр и обращения к критическим объектам ОС.
41. В изделии реализована возможность настройки «чувствительности» определения атак.
42. В изделии реализована возможность настройки исключений для доверенных узлов, с которых не будет обнаруживаться атака.
43. В изделии реализовано маскирование датчиков **СОВ**.
44. В изделии реализован контроль целостности базы решающих правил **СОВ** (сигнатур журналов, трафика).
45. В изделии реализована возможность сохранения отфильтрованной информации из журналов после применения фильтрации.
46. В изделии реализована функциональная возможность «Безопасная среда» (БС), позволяющая запускать и производить работы с программным обеспечением в изолированной, защищенной среде без внесения изменений в основную ОС, проверять ПО на опасные действия с целью определения степени доверия к нему и формировать отчет о деятельности программы. Отчет составляется с правами доступа, исключающими возможность редактирования файла. В отчете отображено следующее:

- краткая сводка о потенциально-вредоносных действиях;
  - оценка безопасности приложения, файла или ссылки;
  - полное наименование о системе;
  - подробное составление отчетов/журналов о результатах проверки.
47. В изделии реализована возможность импорта и последующего обновления «черного списка» URL адресов из внешнего «\*.txt» файла.
48. В изделии реализована возможность защиты службы **СОВ** от неавторизованного останова.
49. В изделии реализована функциональная возможность задавать и анализировать командную строку для процессов для гибкой настройки правил журналов приложений **СОВ**.
50. В изделии реализован вывод из кэша DNS-имени внешнего респондента при наличии такой информации в отправленных или принятых данных.
51. В изделии реализована функция самотестирования контроля приложений.
52. В изделии реализована функция автоматического запуска приложений в БС в случае, если они получены с сайтов сети Интернет.
53. В изделии реализован детектор вредоносной активности вирусов-шифровальщиков.
54. В изделии реализован детектор подозрительных файловых операций.
55. В изделии реализован транзакционный режим для минимизации потери данных от действий вируса-шифровальщика:
- ведение списка удаляемых файлов и маскирование этих операций таким образом, как будто эти файлы уже удалены;
  - создание теневых копий изменяемых файлов в скрытом каталоге и маскирование их таким образом, как будто этих файлов нет.
56. В изделии реализовано принятие решений по событиям, связанным с активностью вирусов-шифровальщиков.
57. В изделии реализовано реагирование на события, связанные с активностью вирусов-шифровальщиков.
58. В изделии реализована регистрация событий, связанных с активностью вирусов-шифровальщиков.
59. В изделии реализована возможность блокировки отправки телеметрии Windows.
60. В изделии реализована возможность выявления атак типа DHCP Flooding, DHCP Starvation и Rogue DHCP Server.
61. В изделии предусмотрена предустановленная база IoC-объектов<sup>1</sup> с возможностью ручного и автоматизированного обновления.
62. В изделии реализована возможность добавления пользовательских IoC-объектов.
63. В изделии реализована возможность просмотра, удаления, активации, деактивации, экспорта и поиска объектов в базе IoC-объектов.
64. В изделии реализован механизм обнаружения IoC автоматизированном рабочем месте по расписанию и по запросу уполномоченного лица.
65. В изделии реализована регистрация следующих событий, связанных с индикаторами компрометации:
- изменение базы IoC-объектов (добавление, удаление, активация, деактивация, экспорт индикаторов компрометации);
  - обновление базы IoC-объектов;
  - изменение значений политик, связанных с индикаторами компрометации;
  - обнаружение IoC.
66. В изделии реализована возможность управления правилами автоматического реагирования СОВ, в том числе создание, удаление, просмотр, редактирование, активация, деактивация и изменение приоритета.
67. В изделии реализована регистрация следующих событий, связанных с правилами автоматического реагирования СОВ:

---

<sup>1</sup> IoC-объект — JSON-объект, который содержит описание индикатора компрометации. Индикаторы компрометации (IoC) — цифровые артефакты, которые с большой долей вероятности указывают на несанкционированный доступ к системе (то есть ее компрометацию).

- редактирование списка правил автоматического реагирования СОВ (создание, копирование, редактирование, удаление, изменение приоритета, активация и деактивация правил автоматического реагирования СОВ);
- изменение значений политик, связанных с правилами автоматического реагирования СОВ;
- срабатывание правил автоматического реагирования СОВ.

68. Изделие выполняет одно из следующих действий при срабатывании условий правила автоматического реагирования СОВ:

- блокировка учетной записи;
- блокировка автоматизированного рабочего места;
- включение профиля межсетевого экрана «Изоляция узла».

### 3.5 Сервер конфигураций

1. В изделии реализована функция сбора по сети и обработки информации о программном обеспечении ПК с установленным **Dallas Lock 8.0**.
2. В изделии реализована функция отслеживания изменений в установленном программном обеспечении на клиентах.
3. В изделии реализована функция фиксации событий подсистемы сканирования клиентской части в журнале **СК**. Фиксируются следующие типы событий:
  - сканирование;
  - редактирование параметров;
  - загрузка Паспорта ПО со съемного машинного носителя;
  - синхронизация Паспортов клиента.
4. В изделии реализована функция фильтрации событий, зафиксированных в журнале управления политиками, по типу и результату.
5. В изделии выполняется контроль и фиксация состояния программной среды.
6. В изделии реализована функциональная возможность сравнения Проекта паспорта и заверенного Паспорта, заверенных паспортов в рамках одного клиента.
7. В изделии реализована функция формирования Проекта паспорта ПО, Паспорта ПО.
8. В изделии реализована функция утверждения Паспорта ПО с помощью установки простой электронной подписи.
9. В изделии реализована функция создания и редактирования прав учетных записей СК.
10. В изделии реализована функциональная возможность хранения данных о состоянии ПО клиентов в базе данных программного модуля. Изделие обеспечивает хранение следующих данных:
  - сведения о клиентах;
  - сведения о персонале комплекса:
  - паспорта ПО клиентов с электронной подписью Контролеров (информация об изменениях состава ПО и исполняемых файлах);
  - информация о ПО.

### 3.6 Общие задачи существующих подсистем СЗИ НСД

1. Изделие может контролировать и определять санкционированное время работы учетной записи пользователя. Реализован механизм ограничения доступа по дате и времени (расписание работы пользователей).
2. Изделие способно принудительно отключать файл-диск при отключении аппаратного идентификатора.
3. В изделии реализована возможность контроля функций гарантированной зачистки информации.
4. В изделии реализована возможность настройки и отображения заданного текстового уведомления пользователя при его входе в информационную систему (напоминание о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных).
5. В изделии реализовано оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему, о количестве неуспешных попыток входа в информационную систему за период, об изменении сведений, относящихся к учетной

- записи пользователя.
6. В изделии осуществляется регистрация событий, связанных с действиями по зачистке остаточной информации.
  7. В изделии реализован механизм гибкой настройки штампа, предоставляемого при отчуждении информации на твердую копию.
  8. При сетевом использовании изделие обеспечивает (силами сервера безопасности) синхронизацию времени.
  9. В изделии реализован модуль управления лицензиями для сервера безопасности и на ограничение числа терминальных сессий.
  10. В изделии реализована возможность дублирования серверов безопасности при сетевом развертывании, для повышения отказоустойчивости изделия.
  11. В изделии реализована возможность установки конфигурации по умолчанию, удовлетворяющей требованиям ограничений по эксплуатации, указанным в подразделе 3.3 формуляра на изделие.
  12. В изделии реализована возможность автоматического экспорта журналов **СБ** и журналов, собираемых с клиентов **ДБ**, во внешнюю SQL базу данных.
  13. Изделие обеспечивает явное выведение клиентской рабочей станции из-под управления сервера безопасности.
  14. В изделии реализована возможность перемещения групп клиентов сервера безопасности в другие группы через их контекстное меню, соответствующее существующей иерархии групп.
  15. Изделие обеспечивает автоматическое обновление информации в режиме реального времени о клиентах, техническая поддержка которых закончилась.
  16. В изделии реализована функция отображении информации об активных компонентах **СЗИ НСД** в окне «**О программе**».
  17. В изделии реализована авторизация по смарт-карте через удостоверяющий центр MS Windows для 64-разрядных операционных систем.
  18. При функционировании в домене Active Directory **СЗИ НСД** при настроенной авторизации по смарт-карте изделие обеспечивает возможность отключения парольного интерфейса входа.
  19. При обновлении изделие автоматически проверяет электронные подписи исполняемых модулей и запрещает установку не прошедших проверку ЭП исполняемых модулей.
  20. При совместном использовании на одной клиентской рабочей станции **СЗИ НСД** и **СДЗ Dallas Lock** обеспечиваются:
    - возможность сквозной авторизации в ОС – передача введенных авторизационных данных из **СДЗ Dallas Lock** в **СЗИ НСД**;
    - возможность заимствования временных отметок из **СДЗ Dallas Lock** для регистрации событий безопасности.
  21. Расширена интеграция с клиентами домена под управлением изделия **СЗИ НСД Dallas Lock Linux**. Обеспечиваются:
    - синхронизация политик безопасности;
    - выгрузка журналов клиентов под управлением изделия **СЗИ НСД Dallas Lock Linux** в MS SQL;
    - полноценная синхронизация учетных записей групп (по аналогии с **СЗИ НСД**);
    - удаленное развертывание **СЗИ НСД Dallas Lock Linux**;
    - централизованное управление ролями администрирования **СЗИ НСД Dallas Lock Linux**.
  22. При удалении **СЗИ НСД** изделие предлагает сохранить произведенные настройки.
  23. В изделии реализована базовая интеграция с антивирусом «**Kaspersky Endpoint Security**»:
    - определение наличия установленного антивируса на клиентских рабочих станциях;
    - предоставление информации об актуальности антивирусных баз;
    - анализ журналов антивируса с реакцией на заданный разработчиком перечень событий.
  24. В изделии реализована графическая панель мониторинга защищенности системы (защищаемого контура).
  25. В изделии реализована функция теневого копирования, обеспечивающая копирование информации, которую пользователь записывает на сменные или сетевые накопители, в специальную папку на локальном жестком диске с возможностью задавать максимальный размер хранилища теневых копий и время их жизни. Доступ пользователя к теневой копии автоматическим образом ограничивается.

26. В изделии реализована функция автоматического сохранения нескольких файлов конфигурации Сервера безопасности по установленному расписанию с возможностью задать путь сохранения файла конфигурации **СЗИ НСД** на жестком диске, сетевом диске или съемном машинном носителе.
27. В изделии реализована функция агрегации событий несанкционированного доступа по разнородным клиентам домена безопасности с унифицированной возможностью обработки для любого узла или группы узлов (вне зависимости от типа).
28. В изделии реализована функция проверки цифровой подписи объектов файловой системы, находящиеся под контролем целостности, при их обновлении. В случае наличия у нового исполняемого файла цифровой подписи замена разрешается, в противном – запрещается.
29. В изделии реализована возможность просмотра в журнале Сервера безопасности параметра, при синхронизации которого возникает ошибка.
30. В изделии реализована функция, позволяющая включать контроллеры домена ОС Windows в Домен безопасности **СЗИ НСД**.
31. В изделии реализована функция, позволяющая создавать учетные записи доменных пользователей из консоли администрирования **СЗИ НСД**.
32. В изделии реализована функция, позволяющая включать Серверы безопасности **СЗИ НСД** в Домен безопасности **СЗИ НСД**.
33. В изделии реализована функция, позволяющая включить клиентскую часть **СЗИ** в домен безопасности **СЗИ НСД** по IP-адресу.
34. Для консоли Сервера безопасности **СЗИ НСД** реализована возможность настройки глобальных параметров дискреционного доступа на уровне групп клиентов.
35. В изделии реализована возможность распределения групп пользователей по клиентам и группам дерева консоли Сервера безопасности **СЗИ НСД**.
36. В изделии реализована индикация «неактивного режима» в дереве клиентов консоли Сервера безопасности.
37. В изделии реализована возможность отображения сообщения об окончании удаленной установки клиентской части **СЗИ НСД** (с указанием необходимости выполнения перезагрузки) для персонального компьютера, на который была произведена удаленная установка. Для консоли Сервера безопасности реализована возможность произвольного редактирования (задания) текста данного сообщения.
38. Для Сервера безопасности **СЗИ НСД** реализована репликация настроек **СДЗ «Dallas Lock»** при кластеризации.
39. В изделии реализована возможность добавления произвольного комментария в электронном виде к событиям **НСД**.
40. В изделии реализована функция выгрузки отчета о действиях пользователя (учетной записи пользователя) на защищаемых ТС из базы данных SQL.
41. В изделии реализован сервис сбора аналитической информации (журнал информационно-технологического сопровождения). Сервис хранит и отображает в консоли Сервера безопасности:
  - события по работе с заявками пользователя в службу технической поддержки;
  - информационные сообщения, отправленные производителем.
42. В изделии реализована возможность отображения информации о состоянии ПО Kaspersky Endpoint Security в консоли Сервера безопасности с использованием Open API, журналирования, фильтрации, настройки приоритетов событий, происходящих с Kaspersky Security Center, выполнения принудительного сканирования клиентских ТС с предустановленным ПО Kaspersky Endpoint Security, обновления антивирусных баз.
43. В Сервере безопасности реализована регистрация подключенных к АРМ клиентов сменных накопителей.
44. В изделии реализован механизм подстановки учетной записи пользователя при выборе токена в интерфейсе входа в Консоль сервера безопасности **Dallas Lock**.
45. В изделии реализована возможность аудита отключения/подключения разрешенных/запрещенных USB-накопителей.
46. В изделии реализована возможность присваивать одному пользователю более одного аппаратного идентификатора (с возможностью авторизации по любому из них).
47. В изделии реализована интеграция с Единым центром управления **Dallas Lock** в части:

- контроля сессий пользователя;
  - отображения состояния **СЗИ НСД**;
  - управления учетными данными;
  - управления политиками безопасности;
  - контроля устройств
  - сбора информации с клиентов **СЗИ НСД** в журналы Единого центра управления **Dallas Lock**;
  - формирования заданий и управление зданиями для клиентов **СЗИ НСД**;
  - отправки сигнализации об инцидентах безопасности;
  - настройки лицензирования;
  - управления межсетевым экраном (добавление и редактирование правил **МЭ**);
  - управления СОВ, в том числе правилами автоматического реагирования СОВ и индикаторами компрометации;
  - управления СКН уровня подключения и уровня отчуждения;
  - удаленной разблокировки автоматизированного рабочего места;
  - перераспределения терминальных сессий;
  - удаленной регистрации аппаратных идентификаторов.
48. В изделии реализован механизм отображения в журнале Сервера безопасности событий всех серверов безопасности (при использовании SQL).
49. В изделии реализована поддержка SSL/TLS на Сервере безопасности для отправки почтовых уведомлений о событиях **НСД** с использованием внешних smtp-серверов.
50. В изделии реализована возможность выгрузки списка пользователей и клиентов с Сервера безопасности в текстовом виде.

## 4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

### Входные данные

#### 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;
  - файлы IoC-объектов (для **СОВ**);
  - резервные копии программных компонентов **СЗИ НСД**;
  - объекты, на которые установлен контроль целостности;
  - объекты, в которых ведется поиск индикаторов компрометации (для **СОВ**);
  - сетевой трафик (для **МЭ, СОВ**);
  - установленные соединения (для **МЭ**);
  - события, регистрируемые в журналах аудита ОС и приложений (для **СОВ**).
2. Логин может служить набор любых символов, введенных с клавиатуры, длиной от 1 до 20, за исключением: "/", "\", "[", "]", ":", "|", "<", ">", "+", "=", ";", " ", "?", "@", "\*\*".
3. Паролем может служить набор любых символов, введенных с клавиатуры, длиной от 1 до 31. Допустимые специальные символы: "`", "~", "!", "@", "#", "\$", "%", "^", "&", "\*\*", "(, ")", "\_", "-", "+", "{", "}", "[", "]", "\\", "|", ":", ";", "'", " ", "<", ">", " ", ".", "?", "/".
4. Минимальная длина и состав символов пароля регулируются соответствующими параметрами безопасности в **СЗИ НСД**.

### Выходные данные

#### 1. 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 и аппаратной конфигурации;
  - файлы IoC-объектов;
  - сообщения **СЗИ НСД** в случае сигнализации при попытках несанкционированного доступа.
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.