#### введение

Темы практических работ, представленные в данном сборнике, направлены на закрепление материала по настройке технических средств информационных систем в защищенном исполнении.

Предполагается, что обучающиеся к моменту начала выполнения практических заданий прошли дисциплины «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Криптографические методы защиты информации», «Модели нарушения безопасности и вирусология», «Защита операционных систем и систем управления базами «Защита компьютерных сетей данных», И телекоммуникаций» и знают основные угрозы безопасности информации в АС СН и способах их реализации, проблемы обеспечения безопасности информации в специальных автоматизированных системах, принципы работы СЗИ от НСД и САВЗ, инструментарием по администрированию специальных ОС, а так же владеют способами защиты специальных автоматизированных систем, навыками разработки моделей угроз и информационной безопасности специальных автоматизированных систем, способами защиты специальных автоматизированных систем, способами выявления вредоносных программ в вычислительных системах.

В ходе практических работ предполагается выполнение студентами двух видов настройки системы защиты информации автоматизированного рабочего места (персонального компьютера): настройку системы защиты информации от несанкционированного доступа и настройку средства антивирусной защиты.

В настройку системы защиты информации от несанкционированного доступа входят:

- настройка идентификации и аутентификации;

- настройка разграничения прав доступа субъектов доступа к объектам доступа;

- настройка очистки освобождаемых областей оперативной памяти;
- настройка регистрации событий;
- настройка контроля целостности;
- настройка учета внешних носителей информации.

В настройку средства антивирусной защиты входят:

- настройка файлового антивируса;
- настройка почтового антивируса;
- настройка веб-антивируса;
- настройка ІМ-антивируса;
- настройка сетевого экрана;
- настройка защиты от сетевых атак;
- настройка мониторинга системы;
- настройка обновления вирусных баз.

Настройку следует выполнять по определенным правилам, установленным нормативными или нормативно-методическими документами. Все необходимые примеры настройки находятся в приложениях сборника и могут быть использованы студентами в качестве образцов при выполнении практических работ.

Все практические работы имеют однотипное описание, включающее: название, цель, теоретические сведения, постановку задачи и последовательность действий исполнителя.

Требования к отчетам по практическим работам также типизированы:

1. Наличие титульного листа с названием работы и подписью исполнителя.

2. Описание цели работы.

3. Протокол действий по выполнению настройки средств защиты информации с комментариями исполнителя.

4. Выводы по выполненной работе.

Список использованной литературы.

# 1. НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «DALLAS LOCK»

*Цель работы.* Получить практические навыки настройки СЗИ НСД «Dallas Lock».

*Теоретические сведения.* СЗИ НСД «Dallas Lock» предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил, обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему и выходящими за её пределы. А также для обеспечения защиты информации в АС посредством её фильтрации.

Система защиты Dallas Lock представляет собой программный комплекс средств защиты информации в ОС семейства «Windows» с возможностью подключения аппаратных идентификаторов.

Использование системы защиты Dallas Lock в проектах по защите информации позволяет привести АС в соответствие требованиям законодательства РФ.

Система защиты предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (файловых, контроллерах домена и терминального доступа).

Система защиты Dallas Lock состоит из следующих основных компонентов:

Программное ядро (Драйвер защиты). Является ядром системы защиты и выполняет основные функции СЗИ НСД:

- обеспечивает мандатный (для редакции «С») и дискреционный режимы контроля доступа к объектам файловой системы и устройствам;

- обеспечивает доступ к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;

- обеспечивает работу механизма делегирования полномочий;

- обеспечивает проверку целостности СЗИ НСД, объектов ФС, программно-аппаратной среды и реестра;

- драйвер защиты осуществляет полную проверку правомочности и корректности администрирования СЗИ НСД.

Драйвер защиты автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы. Драйвер осуществляет управление подсистемами и модулями системы защиты и обеспечивает их взаимодействие. С драйвером защиты взаимодействуют защитные подсистемы, перечисленные ниже.

#### Подсистема администрирования. Включает в себя:

- подсистему локального администрирования. Обеспечивает возможности по управлению СЗИ НСД, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Включает в себя подсистему внедрения в интерфейс «Windows» Explorer («проводник»). Обеспечивает отображение пунктов в контекстном меню объектов, необходимых для назначения прав доступа к объектам ФС, вызова функции принудительной зачистки объектов ФС, преобразования;

- подсистему удаленного администрирования. Позволяет выполнять настройку системы защиты с удалённого компьютера;

- подсистему централизованного управления. Позволяет объединять защищенные компьютеры в Домен безопасности для централизованного и оперативного управления клиентами.

#### Подсистема управления доступом. Включает в себя:

- подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов;

- подсистему доступа к файловой системе, реестру и устройствам, в составе которой:

- подсистема дискреционного доступа;

- подсистема мандатного доступа (для редакции «С»).

Подсистема регистрации и учета. Включает в себя:

 подсистему аудита. Обеспечивает ведение аудита и хранение информации 8-ми категорий событий в журналах;

- подсистему печати. Обеспечивает разграничение доступа к печати, добавление штампа на документы, сохранение их теневых копий, регистрацию событий печати.

**Подсистема идентификации и аутентификации.** Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему.

**Подсистема гарантированной зачистки информации.** Обеспечивает зачистку остаточной информации.

#### Подсистема преобразования информации. Обеспечивает:

- преобразование информации в файлах-контейнерах;

- преобразование сменных накопителей для защиты от доступа в обход СЗИ НСД;

- работу с данными при одновременном их преобразовании в файлдисках;

- прозрачное преобразование жестких дисков (для редакции «С») для предотвращения доступа к данным, расположенным на жестких дисках, в обход СЗИ НСД.

Подсистема контроля устройств. Обеспечивает возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

Подсистема межсетевого экранирования. Обеспечивает контроль, а также фильтрацию потоков информации, поступающих в автоматизированную систему и выходящих за её пределы.

**Подсистема обнаружения вторжений.** Обеспечивает обнаружение и блокирование основных угроз безопасности, выполняет одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализирует некоторые отдельные сетевые протоколы.

Подсистема контроля целостности. Обеспечивает контроль целостности файловой системы, программно-аппаратной среды и реестра, периодическое тестирование СЗИ НСД, наличие средств восстановления СЗИ НСД, восстановление файлов и веток реестра в случае нарушения их целостности.

Подсистема восстановления после сбоев. 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 (установка параметров по умолчанию), что исходным равносильно переустановке СЗИ НСД.

Подсистема развертывания (установочные модули). Выполняет все необходимые функции по установке СЗИ НСД на рабочую станцию и удалению с нее. В процессе развертывания реализована возможность установки конфигурации по умолчанию и другой рабочей конфигурации СЗИ НСД. В процессе развертывания реализована возможность автоматического ввода рабочей станции под управление сервера безопасности.

В ходе данной практической работы выполняется настройка системы защиты. Выполнение работ при установке и настройке системы защиты информации для действующей информационной системы в общем случае разделяется на следующие этапы: 1) подготовка средств вычислительной технике к настройке;

2) установка и настройка общесистемного программного обеспечения;

3) установка и настройка прикладного программного обеспечения;

4) установка и настройка сетевого оборудования;

5) установка и настройка периферийного оборудования;

6) установка и настройка средств антивирусной защиты;

7) установка и настройка системы защиты информации от несанкционированного доступа.

В этой работе подробно рассмотрен последний 7-ой этап работ. В этом случае этап подготовки к установке и настройке СЗИ НСД включает в себя:

1) проверку наличия дистрибутива СЗИ НСД последней версии;

2) проверку наличия лицензионного ключа и формуляра;

3) проверку наличия матрицы доступа.

Постановка задачи. Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

#### Последовательность действий.

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать защищаемые каталоги (объект доступа).

Шаг 4. Установить объектам доступа права разграничения доступа по отношению к субъектам доступа.

Шаг 5. Выполнить настройку очистки остаточной информации.

Шаг 6. Выполнить настройку регистрации событий для объектов доступа.

Шаг 7. Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды.

Шаг 8. Выполнить настройку внешних носителей информации.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение А и приложение А.А представлен пример настройки СЗИ и настройки межсетевого экранирования. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [1].

# 2. НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «SECRET NET»

**Цель работы.** Получить практические навыки настройки СЗИ НСД «Secret Net».

*Теоретические сведения.* Система «Secret Net Studio» предназначена для обеспечения безопасности информационных систем на компьютерах, функционирующих под управлением ОС семейства «Windows».

Эффективное управление. Единая система управления продуктами для защиты Windows, Linux и платами доверенной загрузки. Система масштабируется до управления десятками тысяч рабочих станций и серверов.

*Многоуровневая защита.* Единый агент оптимально использует ресурсы компьютера для защиты от вирусов, сетевых атак, а также от несанкционированного доступа к конфиденциальным данным.

*Проверенный инструмент.* Secret Net Studio является стандартом для ряда критически важных отраслей российской экономики в области защиты конфиденциальной информации, включая защиту государственной тайны.

**Выполнение требований.** Встроенные шаблоны настроек безопасности обеспечивают и отслеживают требуемый регулятором уровень защиты ОТ-инфраструктуры с минимальными усилиями со стороны обслуживающего персонала.

Центр мониторинга Кода Безопасности.





Расширенный инструментарий для обнаружения и расследования инцидентов ИБ Команда опытных аналитиков

Рисунок 1 – Центр мониторинга Кода Безопасности





Организацию взаимодействия с НКЦКИ



Мониторинг работоспособности продуктов Кода Безопасности

# Рисунок 2 – Код Безопасности обеспечивает



Быстрое внедрение



Повышение уровня защищенности инфраструктуры



Снижение трудозатрат компании на мониторинг ИБ



Снижение урона от инцидентов ИБ и неполадок средств защиты



Поддержка 24/7



Возможность взаимодействия с дашбордами и IRP

## Рисунок 3 – Преимущества



Рисунок 4 – Сбор информации на площадке заказчика и ее обработка в Коде Безопасности

## Что входит в отчет.

1. Отчет по мониторингу событий ИБ:

- общая информация о работе заказчика;
- программно-аппаратное состояние продуктов;
- список и описание инцидентов мониторинга;
- количество подозрений на инцидент мониторинга;
- рекомендации по устранению инцидента.
- 2. Отчет по мониторингу работоспособности продуктов:
- общая информация о работе заказчика;
- наиболее опасные подозрения на инцидент;
- источник атаки и описание ее характера;
- время обнаружения инцидентов;
- рекомендации по устранению инцидента.

*Архитектура Secret Net Studio.* Secret Net Studio имеет классическую клиент-серверную архитектуру. Далее приводится описание компонентов комплекса.

*Клиент* — это программа, которая устанавливается на каждое контролируемое устройство (сервер или рабочую станцию) и реализует установленные механизмы защиты как относительно самого устройства, так и в вопросах подключения и использования корпоративных ресурсов. Клиент на устройстве может работать в двух режимах: автономном, при котором управлять защитными механизмами можно только локально, и сетевом, когда возможно и локальное, и централизованное управление механизмами защиты. Второй режим также предусматривает взаимодействие с центром управления для синхронизации информации о состоянии устройства, его изменения, а также установки различных обновлений.

Сервер безопасности решает задачи по централизованному управлению клиентскими системами при использовании Secret Net Studio в сетевом режиме работы. Так, сервер безопасности отвечает за обработку и хранение информации о состоянии других компонентов системы и клиентов,

координирует порядок взаимодействия и работы этих компонентов и реализует функции контроля и управления Secret Net Studio.

*Сервер аутентификации* реализует механизмы удостоверения подлинности пользователей и контролируемых устройств, а также обеспечивает работу механизмов межсетевого экранирования на клиентских системах и защищаемых ресурсах.

**Центр управления** — это инструмент администрирования всех компонентов Secret Net Studio, включая серверную часть и клиентские машины. Администратор может управлять пользователями, защищаемыми устройствами и ресурсами, а также просматривать информацию о состоянии контролируемых или защищаемых систем и о различных событиях в инфраструктуре.

Сервер обновлений используется для того, чтобы централизованно отправлять новые антивирусные сигнатуры, дополнения к базам правил и опасных веб-ресурсов (для межсетевых экранов и систем обнаружения вторжений) на клиентские устройства.

*Реализация масштабируемости в Secret Net Studio.* Для обеспечения хорошей горизонтальной масштабируемости Secret Net Studio можно использовать такие механизмы, как объединение лесов доменов безопасности или иерархия подчинённости сервера безопасности, а также создавать каскады серверов обновлений. Рассмотрим далее эти возможности подробнее.

Объединение лесов безопасности. Secret Net Studio позволяет организовать иерархическую структуру лесов доменов безопасности на основе связанных и несвязанных лесов доменов Windows Active Directory (AD). Леса объединяются родительским сервером и совокупно называются федерацией. Администратору, работающему с сервером, предоставляются следующие возможности по управлению защищаемыми компьютерами из дочерних лесов безопасности: - получение информации о состоянии защищаемых компьютеров,

- отправка команд оперативного управления на защищаемые компьютеры,

- получение оповещений о событиях тревоги и сбор локальных журналов с защищаемых компьютеров,

- управление параметрами безопасности этих компьютеров посредством групповых политик, заданных на родительском сервере безопасности.

подчинённости безопасности. Иерархия серверов Сервер безопасности реализует функции контроля и управления защищаемыми компьютерами при условии их подчинения. Серверу могут быть подчинены компьютеры с установленным клиентом Secret Net Studio, машины под управлением ОС семейства Linux с установленным ПО Secret Net LSP, а также другие серверы безопасности. В один лес независимо от количества серверов безопасности нём включать более 15 000 В рекомендуется не функционирующих клиентов. Одному серверу безопасности рекомендуется подчинять не более 1 500 функционирующих клиентов.

*Каскадирование серверов обновлений*. Внутри компании создаётся каскад серверов, в котором один, корневой, скачивает обновления с сервера компании «Код Безопасности», а остальные, дочерние, — с корневого или с других дочерних. Таким образом с основного сервера снимается нагрузка при обслуживании большого числа клиентов.

Системные требования Secret Net Studio. Подробные требования к аппаратному и программному обеспечению, необходимые для установки компонентов Secret Net Studio, приведены на вкладке «Системные требования» официальной страницы продукта. Отметим, что при развёртывании SNS в сетевом режиме функционирования используемые устройства должны быть введены в домен Active Directory. **Функциональные возможности Secret Net Studio.** Весь набор функциональных возможностей, реализуемых Secret Net Studio, разделяется на пять основных логических категорий. Перечислим все основные функции и механизмы защиты, реализованные в новой версии продукта, подробно рассмотрим новые возможности и внесённые изменения

*Механизмы защиты для противодействия атакующим.* В Secret Net Studio реализованы механизмы защиты, противодействующие активности потенциальных злоумышленников на разных стадиях кибератак. Рассмотрим несколько упрощённую модель атаки. Условно, она состоит из проникновения в инфраструктуру, распространения и продвижения по сети с компрометацией всё большего количества систем и устройств, а также финального этапа, когда атакующий уже достиг своих целей. Последний этап также характеризуется максимальным ущербом для организации, связанным как с репутационными рисками (например, при краже конфиденциальной секретной или информации), так и с финансовыми потерями (очевидный пример здесь — это последствия активности шифровальщиков, которые требуют выкуп за расшифровку данных). Кроме того, хакеры могут вмешиваться в бизнеспроцессы, последствия чего предсказать не так просто.

По данным компании «Код Безопасности», Secret Net Studio может выявлять кибератаки на любой стадии (в соответствии с глобальной базой знаний MITRE ATT&CK) и в некоторых случаях им противодействовать. Однако заметим, что доля отслеживаемых техник, которые используют атакующие на разных стадиях, не превышает 60 % для каждой из тактик, а для некоторых — даже 10 %.



Рисунок 5 – Обнаружение техник злоумышленников на разных стадиях кибератак с помощью Secret Net Studio

Защита данных от несанкционированного доступа. Защита информации от НСД обеспечивается широким набором функций — от ограничения прав доступа (включая различные политики по управлению доступом на основе групп, федераций и меток), различных способов аутентификации контроля устройств и печати до теневого копирования и даже намеренного уничтожения данных.

Централизованное событий. управление U мониторинг Централизованное управление и мониторинг событий как категория включает в себя обширный набор функций администрирования всей инфраструктуры, включая серверы безопасности и аутентификации, клиенты Secret Net Studio (системы под управлением операционной системы Windows) и клиенты Secret Net LSP (системы под управлением ОС Linux). Также сюда относятся задачи журналирования событий, отчётность по ним, мониторинг состояния инфраструктуры и оповещения о подозрительных компонентов или нарушающих политики безопасности событиях, правила межсетевого экранирования. В качестве ключевых функций в системе представлены возможности развёртывать компоненты Secret Net Studio, устанавливать исправления (патчи) и обновления, а также активировать механизм защиты дисков от несанкционированного доступа централизованно. Кроме того, на клиентские машины можно отправлять кумулятивные патчи и применять их пакетно (устанавливать сразу набор обновлений, как обычных, так и кумулятивных).

Оповещения о событиях «тревоги» (то есть ИБ-событиях разной степени важности) могут отображаться на панели задач Windows, а также отправляться по почте блоками на основе типов событий, а не отдельными сообщениями; на рисунке 6. представлена основная страница центра управления Secret Net Studio, на которой отображается общая статистика событий тревоги в инфраструктуре.



Рисунок 6 – Страница «Статистика» центра управления «Secret Net Studio»

Существенным достоинством системы являются шаблоны параметров безопасности, которые облегчают и упрощают процесс настройки механизмов защиты таким образом, чтобы система соответствовала требованиям законодательства России. Так, в версии 8.8 появились предустановленные шаблоны политик для:

- ИСПДн 4-го уровня защищённости (УЗ);

 информационных систем финансовых организаций до 1-го уровня защищённости в соответствии с ГОСТ 57580.1-2017;

- АСУ ТП до 1-го класса защищённости;

- ЗО КИИ до 1-й категории значимости;

ИС для обработки биометрических персональных данных как для стандартного уровня защиты информации (ЕБС-2), так и для усиленного (ЕБС-1).

Также можно самостоятельно создавать шаблоны настроек компонентов «Secret Net Studio» и параметров безопасности и проверять, соответствуют ли они требованиям регуляторов. (см. рисунки 7 ÷ 9).



Рисунок 7 – Меню «Шаблоны» центра управления Secret Net Studio



Рисунок 8 – Предустановленный шаблон для ИСПДн 1 УЗ (центр управления Secret Net Studio)

Secret Net Stud	fio	– 🗆 X		
Шаблон				
Название:	испдн уз-1			
Комментарий:	Шаблон настроек для приведения информационной системы в соответствие требованиям к обеспечению 1-го уровня защищенности персональных данных			
Сравнивается с:	computer-2.TWinfo.local			
Содержание:	<ul> <li>политики</li> </ul>	A		
	Базовая защита			
	Вход в систему	Не совпадает		
	Журнал	Не совпадает		
	Теневое копирование	Отсутствует в шаблоне		
	Ключи пользователя	Не совпадает		
	Оповещение о тревогах	Не совпадает		
	Контроль RDP подключений	Не совпадает		
	Администрирование системы защиты	Отсутствует в шаблоне		
	Локальная защита			
	Дискреционное управление доступом	Не совпадает 👻		
		Применить шаблон Отмена		

## Рисунок 9 – Сравнение созданного шаблона с предустановленным для ИСПДн 1 УЗ (центр управления Secret Net Studio)

Шифрования данных. Шифрование данных логически разделено на несколько механизмов по типу того, что нужно защитить. Реализовано шифрование файлов и папок с помощью криптоконтейнеров, то есть специально созданных файлов, подключаемых к системе в качестве логического диска с различными правами: на чтение, на полный доступ к данным и с возможностью управлять самим криптоконтейнером. Важной Secret Net Studio 8.8 особенностью версии является полнодисковое шифрование. Обычно при использовании последнего невозможно контролировать целостность объектов жёсткого диска до загрузки ОС. Отличительной особенностью Secret Net Studio 8.8 является возможность интеграции с аппаратно-программным модулем «Соболь» для доверенной загрузки и контроля целостности зашифрованных разделов. При этом доступны четыре варианта полнодискового шифрования в зависимости от кто шифрует и где хранится информация для возможности того, восстановления данных, если по каким-то причинам утерян пароль:

 – локальное шифрование пользователем с локальным хранением данных для восстановления;

 – локальное шифрование пользователем с централизованным хранением данных для восстановления;

 – локальное шифрование администратором (при этом пользователю передаётся временный пароль для доступа, который он меняет при первом входе в систему), восстановить данные может только администратор;

 централизованное шифрование администратором для группы устройств одновременно (пользователи сами устанавливают пароль на своей машине, применяется для группы устройств одновременно).

Защита сетевого взаимодействия представлена следующими механизмами:

- Межсетевое экранирование с возможностью фильтрации трафика на трёх уровнях: сети, сессий и приложений. Также можно гибко настраивать правила (включая время их действия по дням недели или даже времени суток) и шаблоны.

- Авторизация сетевых соединений, обеспечивающая аутентификацию узлов сети с использованием сертификатов для защиты от перехвата данных (атак типа «Man-in-the-Middle»).

- Программная сегментация сети без изменения топологии (используются оверлейные сети). Обеспечивает в том числе шифрование трафика между двумя сетевыми узлами.

Антивирусная защита и обнаружение вторжений. В эту категорию включены антивирусное ядро для поиска вредоносных программ и подозрительного сетевого трафика с помощью сигнатурных и поведенческих методов, эмулятор угроз (песочница), почтовый антивирус и средства по обнаружению и предотвращению вторжений. Также реализована автоматическая блокировка узлов, с которых ведётся зафиксированная вредоносная деятельность, что позволяет остановить возможного злоумышленника на начальном этапе.

#### Принцип работы «Secret Net Studio» заключается в следующем.

1. Аутентификация пользователей. При входе в систему пользователь должен ввести свои учетные данные, чтобы система могла проверить его права доступа.

2. Контроль доступа. Система отслеживает, какие пользователи имеют доступ к каким данным и какие действия они могут выполнять.

3. Шифрование данных. «Secret Net Studio» использует криптографические методы для защиты конфиденциальных данных, таких как пароли, документы и другие файлы.

4. Антивирусное сканирование. «Secret Net Studio» проверяет все файлы и документы на наличие вирусов и других вредоносных программ.

5. Мониторинг сети. «Secret Net Studio» отслеживает сетевой трафик и выявляет подозрительные активности, такие как попытки взлома или несанкционированного доступа к данным.

6. Управление правами доступа. «Secret Net Studio» позволяет администраторам настраивать права доступа для различных пользователей и групп пользователей.

7. Отчеты о событиях. «Secret Net Studio» генерирует отчеты о событиях, происходящих в системе, что позволяет администраторам отслеживать ситуацию и принимать меры по устранению проблем.

#### Достоинства:

 сертифицирован по требованиям ФСТЭК России по 4-му уровню доверия;

 наличие сертификата ФСБ России по классу АКЗ, ожидается получение сертификата по классу АК5;  – хорошая масштабируемость (один сервер безопасности поддерживает до 1,5 тысяч подключённых клиентов, один лес — 15 тысяч). Крупнейшая инсталляция — более 100 тыс. пользователей в рамках единой структуры;

 используемые механизмы защиты позволяют выявлять кибератаки на любой стадии (по классификации MITRE ATT&CK);

 возможности по быстрой настройке систем в соответствии с требованиями регуляторов в части обеспечения безопасности информационных систем с помощью предустановленных шаблонов;

– подробная техническая документация.

#### Недостатки:

– обязательная привязка к службе каталогов Microsoft Active Directory;

 – клиент для устройств под управлением OC Linux отстаёт в функциональности от клиента под Windows-системы, а клиент для устройств под управлением macOS отсутствует;

– нет планов по сертификации криптографии, используемой в Secret Net Studio.

*Постановка задачи.* Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

#### Последовательность действий.

Шаг 1. Произвести установку «Secret Net Studio».

Шаг 2. Создать пользователя системы (субъект доступа).

Шаг 3. Выполнить настройки политик безопасности.

Шаг 4. Выполнить настройки регистраций событий.

Шаг 5. Выполнить активацию новых установок.

Шаг 6. Настроить локальные журналы событий и сформировать отчёты.

Шаг 7. Сформировать для подсистемы запросов отчёты журналов тревог разного уровня.

Шаг 8. Настроить по произвольным заданным условиям новый локальный журнал событий и сформировать отчёт.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение Б представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [2, 5].

# 3. НАСТРОЙКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОС СН «ASTRA LINUX»

**Цель работы.** Получить практические навыки настройки СЗИ НСД в ОС СН «Astra Linux».

*Теоретические сведения.* ОС СН предназначена для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Основная задача, решаемая ОС в процессе своего функционирования – обеспечение интерфейса для доступа ПО к устройствам вычислительной системы посредством управления устройствами, вычислительными процессами, а также эффективное распределение вычислительных ресурсов между вычислительными процессами в соответствии с требованиями руководящих документов по обеспечению защиты информации, содержащей сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Для решения основной задачи функционирования OC она декомпозируется на следующие основные классы задач:

Идентификация и аутентификация пользователей. Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании механизма РАМ, который представляет собой набор разделяемых библиотек (модулей), с помощью которых администратор может организовывать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации. Подобный подход позволяет изменять процедуру аутентификации без изменения исходного кода и повторного компилирования РАМ. Сценарии описываются в конфигурационных файлах.

В ОС реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хэш-функции по ГОСТ Р 34.11-94 и по ГОСТ Р 34.11-2012.

Дискреционное разграничение В OC доступа. механизм обеспечивает дискреционного разграничения доступа проверку дискреционных ПРД, формируемых в виде базовых ПРД ОС семейства Linux, идентификаторов субъектов (идентификатор формируемых В виде пользователя (UID) и идентификатор группы (GID), имеющих доступ к объекту (чтение, запись, исполнение). Кроме того, для формирования дискреционных ПРД в ОС используются списки контроля доступа (ACL) и механизм системных привилегий ОС семейства Linux.

Мандатное разграничение доступа. Решение задачи мандатного разграничения доступа процессов к ресурсам основан на реализации соответствующего механизма в ядре ОС. При этом, принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом.

Правила приятия решения могут быть записаны следующим образом. Пусть контекст безопасности субъекта содержит уровень L0 и категории C0, а мандатная метка объекта содержит уровень L1 и категории C1. В ОС определены следующие операции сравнения уровней и категорий:

- уровень L0 меньше уровня L1 (L0 < L1), если численное значение L0 меньше численного значения L1;

уровень L0 равен уровню L1 (L0 = L1), если численные значения L0 и
 L1 совпадают;

- категории C0 меньше категорий C1 (C0 < C1), если все биты набора C0 являются подмножеством набора бит C1;

категории C0 равны категориям C1 (C0 = C1), если значения C0 и C1 совпадают;

Таким образом, в механизме мандатного разграничения доступа действуют следующие правила:

- операция записи разрешена, если L0 = L1 и C0 = C1;

- операция чтения разрешена, если  $L0 \ge L1$  и  $C0 \ge C1$ ;

- операция исполнения разрешена, если  $L0 \ge L1$  и  $C0 \ge C1$ .

В остальных случаях анализируются полномочия и тип мандатной метки. Тип метки может использоваться для того, чтобы изменять ее эффектные действия. Ненулевой тип метки может быть установлен только привилегированным процессом.

Изоляция адресных пространств процессов. Решение задачи изоляции адресных пространств процессов основано на архитектуре ядра ОС, которое обеспечивает для каждого процесса в системе собственное изолированное адресное пространство. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми и работает процессор) преобразуются в разные физические для разных адресных пространств. Процесс не может несанкционированным образом получить доступ к пространству процесса, непривилегированный другого так как пользовательский процесс лишен возможности работать с физической памятью на прямую.

Механизм разделяемой памяти является санкционированным способом получить нескольким процессам доступ к одному и тому же участку памяти и находится под контролем дискреционных и мандатных ПРД.

Адресное пространство ядра защищено от прямого воздействия пользовательских процессов с использованием механизма страничной

защиты. Страницы пространства ядра являются привилегированными и доступ к ним из непривилегированного кода вызывает исключение процессора, которое обрабатывается корректным образом ядром ОС. Единственным санкционированным способом доступа к ядру ОС из пользовательской программы является механизм системных вызовов, который гарантирует возможность выполнения пользователем только санкционированных действий.

**Регистрация событий.** В ОС реализована расширенная подсистема протоколирования, осуществляющая регистрацию событий в двоичные файлы с использованием сервиса parlogd.

В библиотеках подсистемы безопасности PARSEC реализован программный интерфейс для протоколирования событий с использованием расширенной подсистемы протоколирования.

Очистка оперативной и внешней памяти. Решение задачи очистки ОП основано на архитектуре ядра ОС, которое гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено ПРД. Это означает, что средства взаимодействия между процессами контролируются с помощью ПРД, и процесс не может получить неочищенную память (как оперативную, так и дисковую).

Решение задачи очистки памяти на внешних носителях основано на реализации механизма, который очищает неиспользуемые блоки ФС непосредственно при их освобождении. Работа названного механизма снижает скорость выполнения операция удаления и усечения размера файла. Механизм является настраиваемым и позволяет обеспечить работу ФС ОС в одном из следующих режимов:

- данные любых удаляемых/урезаемых файлов пределах ФС предварительно очищаются маскирующей последовательностью;

- данные ФС освобождаются обычным образом (без предварительного маскирования).

Режим работы ФС может быть выбран администратором ОС и задан в виде параметра монтирования ФС.

Контроль целостности. Решение задач контроля целостности основано на использовании библиотеки libgost, в которой реализованы функции хэширования в соответствии с ГОСТ Р 34.11- 94, ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит. Данная библиотека используется в средствах контроля целостности дистрибутива и средствах контроля целостности ФС.

Контроль целостности дистрибутива обеспечивается методом расчета его контрольной суммы и сравнения полученного значения с эталонным значением контрольной суммы.

Контроль целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств, который предоставляет возможность периодического (с использованием системного планировщика заданий сгоп) вычисления контрольных сумм файлов и соответствующих им атрибутов с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки libgost и контроль целостности связанных с файлами атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования).

Создание замкнутой программной среды. Средства создания замкнутой программной среды предоставляют возможность внедрения цифровой подписи в исполняемые файлы формата ELF, входящие в состав устанавливаемого СПО и в расширенные атрибуты файловой системы.

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра OC digsig\_verif, который является не выгружаемым модулем ядра Linux, и может функционировать в одном из следующих режимов:

1) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение запрещается (штатный режим функционирования);

2) исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в СПО);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный режим для тестирования СПО).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы также реализован в модуле ядра OC digsig\_verif и может функционировать в одном из следующих режимов:

 запрещается открытие файлов, поставленных на контроль файлов, с неверной ЭЦП или без ЭЦП;

2) открытие файлов, поставленных на контроль файлов, с неверной ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в расширенных атрибутах файловой системы);

3) ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется.

Постановка задачи. Выполнить все шаги работы, необходимые для осуществления настройки СЗИ НСД. Результаты зафиксировать в отчете.

#### Последовательность действий.

Шаг 1. Создать пользователей системы (субъект доступа).

Шаг 2. Выполнить настройки идентификации и аутентификации.

Шаг 3. Создать защищаемые каталоги (объект доступа).

Шаг 4. Установить объектам доступа права разграничения доступа по отношению к субъектам доступа.

Шаг 5. Выполнить настройку очистки остаточной информации.

Шаг 6. Выполнить настройку регистрации событий для объектов доступа.

Шаг 7. Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды.

Шаг 8. Выполнить настройку внешних носителей информации.

Шаг 9. Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Для решения задачи в приложение В представлен пример настройки СЗИ. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [3].

# 4. НАСТРОЙКА СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ «KASPERSKY ENDPOINT SECURITY ДЛЯ «WINDOWS»

*Цель работы*. Получить практические навыки настройки САВЗ «Kaspersky Endpoint Security».

*Теоретические сведения.* Существующие продукты фирмы Kaspersky можно разделить на продукты для дома, для малого бизнеса, для среднего бизнеса и корпоративные решения. Решения для дома рассчитаны на персональный домашний ПК, для малого бизнеса на 1-25 сотрудников, для среднего бизнеса 26-999 сотрудников, корпоративные решения более 1000 сотрудников. К продуктам для дома относятся: «Kaspersky Standard», «Kaspersky Plus», «Kaspersky Premium». Для малого бизнеса: «Kaspersky Standard», «Kaspersky Plus», «Kaspersky Endpoint Security Cloud». Для среднего бизнеса: «Kaspersky Endpoint Security Cloud». Для среднего бизнеса: «Kaspersky Endpoint Security Для бизнеса Стандартный», «Kaspersky Endpoint Security для бизнеса Расширенный». К корпоративным же решениям относятся: Сервисы кибербезопасности, Управление угрозами и защита от них, Защита конечных устройств, Security для виртуальных и облачных сред. Рассмотрим наиболее часто используемое решение «Kaspersky Endpoint Security».

«Kaspersky Endpoint Security» включает многоуровневую защиту от угроз, проактивные технологии, такие как Контроль программ и устройств, Веб-Контроль, средства управления уязвимостями и установкой исправлений, а также шифрование данных.

«Kaspersky Endpoint Security» обеспечивает комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак.

#### Как это работает?

**Во-первых,** средства защиты на всех уровнях линейки взаимодействуют между собой, дополняя возможности друг друга. Базовая защита рабочих мест объединяет гибкие средства контроля (с возможностями блокирования вебресурсов, приложений и устройств и установки ограничений) и мощный

движок, обнаруживающий вредоносное ПО. Начиная с уровня Расширенный, администраторам доступна функция автоматической установки исправлений и оценки уязвимостей, а также инструменты централизованной установки ПО. Таким образом, они тратят меньше времени на рутинные, но очень важные для IT-безопасности операции.

**Во-вторых,** Kaspersky Endpoint Security содержит базовые инструменты EDR, которые позволяют автоматически реагировать на сложные атаки, повышают прозрачность инфраструктуры и помогают проводить расследование атаки. Эти инструменты работают сообща и усиливают устойчивость защиты. В то же время Kaspersky Endpoint Security включает в себя средства защиты виртуальных сред, а также защиту с помощью решений для безопасности почтовых серверов и интернет-шлюзов.

В-третьих, V компаний есть возможность дополнить защиту продвинутым средством борьбы с неизвестными и маскирующимися угрозами – песочницей. Существует вредоносное ПО, которое может обходить даже самые сложные механизмы защиты рабочих мест и никак не проявляет себя, пока не появится подходящая возможность для проведения атаки. Чтобы противодействовать таким угрозам, необходимо заставить вредоносное ПО выдать себя, запустившись в безопасной, подконтрольной специалистам среде. Для этого как нельзя лучше подходит песочница. Совместное применение технологий защиты рабочих мест, базовых инструментов EDR и песочницы формирует интегрированный подход к обеспечению безопасности корпоративной сети, который серьезно увеличивает глубину защиты и помогает обнаруживать сложные угрозы, маскирующие свои действия. С помощью интегрированного решения вы сможете обнаруживать и устранять новые и неизвестные угрозы и не позволите злоумышленникам проникать в ваши корпоративные системы.

Каждый тип угроз обрабатывается отдельным компонентом. Компоненты можно включать и выключать независимо друг от друга, а также настраивать параметры их работы.

# К компонентам защиты относятся следующие компоненты программы.

• *Модуль «Обновление».* «Kaspersky Endpoint Security» загружает обновленные базы и модули программы. Это обеспечивает актуальность защиты компьютера от новых вирусов и других программ, представляющих угрозу.

• *Модуль «Базовая защита»*. Настройка модуля «Базовая защита» заключается в настройке компонентов «Защита от файловых угроз», «Защита от веб-угроз», «Защита от почтовых угроз», «Защита от сетевых угроз», «Сетевой экран», «Защита от атак BadUSB», «AMSI-защита».

• Модуль «Продвинутая защита». Настройка модуля «Продвинутая защита» заключается в настройке компонентов «Kaspersky Security Network», «Анализ поведения», «Защита от эксплойтов», «Предотвращение вторжений», «Откат вредоносных действий».

• *Модуль «Контроль безопасности»*. Настройка модуля «Контроль безопасности» заключается в настройке компонентов «Веб-Контроль», «Контроль устройств», «Адаптивный контроль аномалий», «Контроль приложений».

• *Модуль «Общие настройки»*. Настройка модуля «Общие настройки» заключается в настройке компонентов «Настройки приложения», «Настройки сети», «Угрозы и исключения», «Отчеты и хранилище», «Интерфейс», «Управление настройками».

В программе «Kaspersky Endpoint Security» предусмотрены следующие задачи:

• Полная проверка. САВЗ выполняет тщательную проверку операционной системы, включая системную память, загружаемые при старте объекты, резервное хранилище операционной системы, а также все жесткие и съемные диски.

• *Выборочная проверка*. САВЗ проверяет объекты, выбранные пользователем.

• *Проверка важных областей.* «Kaspersky Endpoint Security» проверяет объекты, загрузка которых осуществляется при старте операционной системы, системную память и объекты заражения руткитами.

• *Проверка съемных дисков.* Задача по проверке, проверяющая все файлы подключаемых съемных дисков.

• *Проверка из контекстного меню*. Специальный вид проверки, позволяющий запустить задачу по проверке выбранных файлов минимальным количеством действий.

• **Фоновая проверка**. Режим проверки САВЗ без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов средства ВТ, чем другие виды проверок.

• *Проверка целостности.* Задача проверяет модули «Kaspersky Endpoint Security для Windows», находящиеся в папке установки программы, на наличие повреждений или изменений. Если модуль программы имеет некорректную цифровую подпись, то такой модуль считается поврежденным.

## Последовательность действий.

Шаг 1. Выполнить настройку модуля «Обновление».

Шаг 2. Выполнить настройку модуля «Базовая защита».

Шаг 3. Выполнить настройку модуля «Продвинутая защита».

Шаг 4. Выполнить настройку модуля «Контроль безопасности».

Шаг 5. Выполнить настройку модуля «Общие настройки».

Шаг 6. Выполнить настройку модуля «Задачи».

Для решения задачи в приложение Г представлен пример настройки средства антивирусной защиты. Более конкретная информация представлена в источниках, указанных в списке рекомендуемой литературы [4].

# СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Конфидент Система защиты информации от несанкционированного доступа Dallas Lock 8.0 Руководство по эксплуатации RU.48957919.501410-02 92, 2017

2. Код безопасности Средство защиты информации Secret Net Studio Руководство администратора Настройка и эксплуатация RU.88338853.501400.001 91 3, 2019

3. Справочный центр Astra Linux https://wiki.astralinux.ru

4. Kaspersky Endpoint Security 10 для «Windows», 2017

5. Код безопасности Средство защиты информации Secret Net Studio Руководство администратора Установка, обновление, удаление RU.88338853.501400.001 91 2, 2020

## ПРИЛОЖЕНИЕ А

## Пример настройки СЗИ НСД «Dallas Lock»

#### Создание пользователя системы

Открыть оболочку администратора системы защиты и выбрать категорию «Учетные записи» (см. рисунок А.1.).

Учетные записи         Параметры безопасности         Контроль ресурсов         СКН         ИЗ         СОВ         Журналы           Учетные         Сессии         Сессии </th
Учетные записи         Сессии исключения ссессии исключения субъекты доступа         Группы Заблокированные пользователи         Эвблокированные удалить удалить         Сеобиства Фоновить удалить         Свойства Фоновить удалить         Гринадл. исинификатора Действия           Учетная запись СЗИ         Полное имя         Описание         Тип учетной за         И           Учетная запись СЗИ         Полное имя         Описание         Тип учетной за         И           Учетная запись СЗИ         Полное имя         Описание         Не указан         И           Учетная запись СЗИ         Арминистратор безопасности         Администратор безопасности         Не указан           Э John         Арминистратор безопасности         Администратор безопасности         Не указан           Э secServer         secServer user         Используется для сетевых входов с незащищенных компь         Не указан           Э nonymous         Аполутоиз user         Используется для сетевых входов с незащищенных компь         Не указан
Учетная запись СЗИ         Полное имя         Описание         Тип учетной за         I           В John         Администратор безопасности         Администратор безопасности         Не указан            SecServer         secServer user         Используется для синхронизации с сервером безопасности         Не указан            anonymous         Anonymous user         Используется для сетевых входов с незащищенных компь         Не указан            -         -         -         -         -         -         -
Доhn         Администратор безопасности         Администратор безопасности         Не указан           SecServer         secServer user         Используется для синхронизации с сервером безопасности         Не указан           anonymous         Anonymous user         Используется для сетевых входов с незащищенных компь         Не указан           -
SecServer       SecServer user       Используется для синхронизации с сервером безопасности       Не указан         anonymous       Anonymous user       Используется для сетевых входов с незащищенных компь       Не указан
Anonymous user Используется для сетевых входов с незащищенных компь Не указан

Рисунок А.1. – Окно оболочки администратора системы защиты

Нажать кнопку создать в категории действия, или в контекстном меню,

открывающимся по нажатию на правую кнопку мыши (см. рисунок А.2.).

Создание учет	тной записи	×
Размещение	Локальный (JOHN-PC) 🔻	Q
Логин	1	Q
	ОК Отмен	на

Рисунок А.2. – Окно создания учетной записи

В открывшемся окне в поле размещения выбрать локальный и указать логин регистрируемого пользователя (см. рисунок А.З.).
Создание уче	тной записи	×
Размещение	Локальный (JOHN-PC) 🔻	
Логин	user_1	Q
	ОК ОТМ	ена

Рисунок А.3. – Заполненной окно создания учетной записи

При вводе имени в системе существуют следующие правила:

• максимальная длина имени - 20 символов;

 имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ []: | <> + =;,?
 (a) \*); разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами);

• после нажатие кнопки «ОК» откроется меню создания учетной записи пользователя. Здесь можно указать «Полное имя» и «Описание» для пользователя, установить различные параметры для учетной записи пользователя и пароля (см. рисунок А.4.).

Создание учетной записи Общие Аппаратная идентификация	Изменение о	сновных параметров пользов	вателя
Группы	Домен Логин Полное имя Описание Параметры Отключена У Запретить работу пр Служебный пользов Не синхронизируемы Пароль Запретить смену пар Пароль без ограниче	иser_1 Иванов Иван пользователь_1 ри нарушенной целостности атель ий пользователь пароля при следующем входе роля пользователем ения срока действия	Тип учетной записи Не указан Мандатный доступ Настроить Число разрешенных сеансов Не используется Расписание работы Настроить
		ОК	Cancel Apply

Рисунок А.4. – Окно редактирования параметров учетной записи

При нажатии кнопки «ОК» откроется окно для задания пароля пользователя, можно либо написать пароль вручную (см. рисунок А.5.).

Пароль пользователя 'JOHN-PC	\user_1'
Генерация пароля	
Пароль	•••••
Подтверждение	•••••
	ОК Отмена

Рисунок А.5. – Окно создания пароля пользователя

Либо воспользоваться функцией генерации пароля (см. рисунок А.б.):

Пароль пользователя 'JOHN-PC	\user_2'	<b>—</b> ×
Генерация пароля	pqwhgn	
Пароль	pqwhgn	
Подтверждение		
	ОК	Отмена

Рисунок А.б. – Пример создания пароля при помощи генерации

После создания пользователя он добавиться в список учетных записей (см. рисунок А.7.).

	Dallas Lock 8.0-C [John, 0 (O	ткрытые данные), метка не выбрана]	_ = ×
Учетные записи Параметр	ры безопасности Контроль ресу	осов СКН МЭ СОВ Журналы	
Учетные записи Ссссии Ссссии Ссссии- исключения Субъекты доступа	а Заблокированные пользователи 😳 Создать В Заблокированные сользователи	Свойства ать № Обновить № Задать пароль Действия Доп. функции	
Учетная запись СЗИ 🔍	Полное имя 🔍	Описание	Тип учетной за
🤱 John	Администратор безопасности	Администратор безопасности	Не указан
â secServer	secServer user	Используется для синхронизации с сервером безопасности	Не указан
anonymous	Anonymous user	Используется для сетевых входов с незащищенных компь	Не указан
<mark>▲ user_1</mark>	Иванов Иван	пользователь_1	Не указан
1			

Рисунок А.7. – Окно учетной записи с новым пользователем

Из списка учетных записей можно изменить основный параметры пользователя. При этом откроется окно, аналогичное окну при создании.

Здесь необходимо изменить включить параметр учетной записи «Запретить работу при нарушенной целостность» и параметр пароля «Запретить смену пароля пользователем» (см. рисунок А.8.).

user_1			×
Общие Аппаратная идентификация	Изменение о	сновных параметров пользов	ателя
Группы	Домен		
	Логин	user_1	
	Полное имя	Иванов Иван	
	Описание	пользователь_1	
	Параметры		Тип учетной записи
	Отключена		Не указан 🔻
	📝 Запретить работу п	ри нарушенной целостности	Мандатный доступ
	Служебный пользов	Настроить	
	Не синхронизируемь	ій пользователь	Число разрешенных сеансов
	Пароль		Не используется 🔹
	Потребовать смену	пароля при следующем входе	Расписание работы
	📝 Запретить смену пар	ооля пользователем	Настроить
	🔲 Пароль без ограниче	ения срока действия	
		ОК	Cancel Apply

Рисунок А.8. – Окно редактирования основных параметров пользователя

Также, здесь во вкладке «Группы» можно настроить группы, в которые входит пользователь (см. рисунок А.9.).

user_1		٢
Общие	🚯 Группы, в которые входит пользователь	
Аппаратная идентификация		
Группы		
	Группы	
	- Users	
	Добавить Удалить	
	OK Cancel Apply	

Рисунок А.9. – Окно редактирования групп пользователя

#### Настройка идентификации и аутентификации

Открыть оболочку администраторы системы защиты и перейти во вкладку «Параметры безопасности» (см. рисунок А.10.).

Dallas Lock 8.0-C [John	, 0 (Открытые данные), метка не выб	ірана] —	= x
Учетные записи Параметры безопасности Контроль	ресурсов СКН МЭ СОВ	Журналы	
Корании Вход Аудит Права пользователей Доступ информации целости Контр информации иностаточной Контр Контр	оль Блокируемые Изолированные ности расширения процессы	Свойства     Обновить     Основить     Основить     Основить     Основить     Основить	
Параметр	Значение		-
	P		
Вход: запрет смены пользователя без перезагрузки	DBIK/I.		- 11
Вход: отображать имя последнего пользователя	Дa		_
Вход: максимальное количество ошиоок ввода пароля	15		_
Вход: время олокировки учетной записи в случае ввода неправил	ТЭ мин.		
Вход: отооражать информацию о последнем успешном входе	Per une		=
Вход: запрет одновременной расоты пользователей с различным	BBIK/I.		
Вход, выоор мандатной метки при входе в ОС	Her		
	Her		
Вход, запретить использование парольного илерфейса входа	Her		
Вход, автоматический высор аннаратного идентификатора при ав	42 лн		
Пароли: минимальный срок действия пароля	Не используется		
Пароли: напоминать о смене пароля за	14 лн.		
Пароли: минимальная длина	бсимв		
Пароли: необходимо наличие цифр	Нет		
во Пароли: необходимо наличие спец символов	Нет		
Пароли: необходимо наличие строчных и прописных букв	Нет		
Пароли: необходимо отсутствие цифры в первом и последнем си	Нет		
Пароли: необходимо изменение пароля не меньше чем в	Не используется		-

Рисунок А.10. – Список параметров входа

Здесь можно настроить различные параметры безопасности, включая различные отображения информации, сроки действия и параметры паролей и т.д. Пример настройки на рисунке A.11.:

Учетные записи         Параметры безопасности         Контроль ресурсов         CKH         M3         COS         Журналы <ul></ul>
Права       Мандатный Очистка остаточной Контроль Блокируеные Изолированные Загрузчик       Основить         Аудит       Права       Мандатный Очистка остаточной Контроль Блокируеные Изолированные Загрузчик       Основить         Категории       Категории       Волод       Основить       Действия         Параметр       Значение       Действия         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Да         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Выкл.         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Выкл.         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Выкл.         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Выкл.         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Выкл.         В Вход: запрет смены пользователя без перезагрузки       Выкл.       Выкл.         В Вход: запрет одновреки учетной записи в случае ввода неправил       30 мин.       Выкл.         В Вход: запрет одновременной работы пользователей с различным       Выкл.       Выкл.       Выкл.         В Вход: запрет одновременной работы пользователей с различным       Выкл.       Выкл.       Выкл.         В Вход: запрет одновременной работы пользователей с различным       Выкл. <td< td=""></td<>
Параметр         Значение           Параметр         Значение           В Код: запрет смены пользователя без перезагрузки         Выкл.           В Код: отображать имя последнего пользователя         Да           В Код: время блокировки учетной записи в случае ввода нароля         3           В Код: отображать информацию о последнем успешном входе         Нет           В Код: запрет одновременной работы пользователей с различным         Выкл.           В Код: запрет одновременной избор аппаратного интерфейса входа         Нет           В Код: запретить использование смарт-карт         Нет           В Код: запретить использование парольного интерфейса входа         Нет           В Код: запретить использование парального интерфейса входа         Нет           В Код: запретить использование парального интерфейса входа         Нет           В Код: запретить использование парального интерфейса входа         Нет
Выкл.         Выкл.           Вакла:         Сображать имя последнего пользователя         Да           Вакла:         Сображать имя последнего пользователя         Да           Вакла:         Вакла:         Сображать имя последнего пользователя         Да           Вакла:         Вакла:         Сображать имя последнего пользователя         Да           Вакла:         Вакла:         Сображать имформацию о последнем успешном входе         Нет           Вакла:         Вакла:         Выкл.         Выкл.         Выкл.           Вакла:         Вакла:         Выкл.         Выкл.         Выкл.         Выкл.           Вакла:         Вакла:         Выкл.         Выкл.         Выкл.         Выкл.         Выкл.           Вакла:         Вакла:         Выкл.
Вход: отображать имя последнего пользователя         Да           Вход: максимальное количество ошибок ввода пароля         3           Вход: время блокировки учетной записи в случае ввода неправил         30 мин.           Вход: отображать информацию о последнем успешном входе         Нет           Вход: запрет одновременной работы пользователей с различным         Выкл.           Вход: выбор мандатной метки при входе в ОС         Выкл.           Вход: запретить использование смарт-карт         Нет           Вход: запретить использование парольного интерфейса входа         Нет           Вход: запоматический выбор аппаратного идентификатора при ав         Нет
Вход: максимальное количество ошибок ввода пароля       3         Вход: время блокировки учетной записи в случае ввода неправил       30 мин.         Вход: отображать информацию о последнем успешном входе       Нет         Вход: запрет одновременной работы пользователей с различным       Выкл.         Вход: выбор мандатной метки при входе в ОС       Выкл.         Вход: запретить использование смарт-карт       Нет         Вход: запретить использование парольного интерфейса входа       Нет         Вход: запоматический выбор аппаратного идентификатора при ав       Нет
<ul> <li>Вход: время блокировки учетной записи в случае ввода неправил 30 мин.</li> <li>Вход: отображать информацию о последнем успешном входе</li> <li>Нет</li> <li>Вход: запрет одновременной работы пользователей с различным</li> <li>Вкод: запрет одновременной работы пользователей с различным</li> <li>Вкод: выбор мандатной метки при входе в ОС</li> <li>Вкод: разрешить использование смарт-карт</li> <li>Вкод: запретить использование парольного интерфейса входа</li> <li>Нет</li> <li>Вход: автоматический выбор аппаратного идентификатора при ав</li> <li>Нет</li> </ul>
Вход: отображать информацию о последнем успешном входе         Нет           Вход: запрет одновременной работы пользователей с различным         Выкл.           Вход: запрет одновременной работы пользователей с различным         Выкл.           Вход: зыбор мандатной метки при входе в ОС         Выкл.           Вход: запретить использование смарт-карт         Нет           Вход: запретить использование парольного интерфейса входа         Нет           Вход: затоматический выбор аппаратного идентификатора при ав         Нет
<ul> <li>В Вход: запрет одновременной работы пользователей с различным Выкл.</li> <li>В вход: выбор мандатной метки при входе в ОС</li> <li>В вход: разрешить использование смарт-карт</li> <li>Нет</li> <li>В ход: запретить использование парольного интерфейса входа</li> <li>Нет</li> <li>В ход: автоматический выбор аппаратного идентификатора при ав</li> </ul>
Выкл.         Выкл.           В выкл.         Выкл.           В выкл.         Нет
Вход: разрешить использование смарт-карт         Нет           Вход: запретить использование парольного интерфейса входа         Нет           Вход: автоматический выбор аппаратного идентификатора при ав         Нет
Вход: запретить использование парольного интерфейса входа Вход: автоматический выбор аппаратного идентификатора при ав Нет
🛃 Вход: автоматический выбор аппаратного идентификатора при ав Нет
В Пароли: максимальный срок действия пароля 90 дн.
В Пароли: минимальный срок действия пароля Не используется
Тароли: напоминать о смене пароля за 14 дн.
Тароли: минимальная длина         6 симв.
📆 Пароли: необходимо наличие цифр Нет
📆 Пароли: необходимо наличие спец символов Нет
Тароли: необходимо наличие строчных и прописных букв Нет
📆 Пароли: необходимо отсутствие цифры в первом и последнем си Нет
Эта Пароли: необходимо изменение пароля не меньше чем в         Не используется

Рисунок А.11. – Пример настройки списка параметров входа

### Установка прав разграничения доступа

Открыть оболочку администраторы системы защиты и перейти во вкладку «Контроль ресурсов» - «Дискреционный доступ» (см. рисунок А.12.).

	Dallas Lock 8.0-С [John, 0 (Открытые данные), метка не выбрана] 🛛 🗕 🗖 🛪							
	Учетные записи	Параметры	безопасности	Контроль р	оесурсов СКН		Журналы	
Bce	Дискреционный М доступ Контр	Дандатный Ауди доступ роль файловой с	Контроль целостности	Глобальные	Устройства Контроль устрой	СТВ Добавить ( Ф. Добавить ( Ф. Добавить ( Ф. Добавить ( Стве	ФС) 🚰 Свойства Реестр) 🦓 Обновить Действия	
Имя и па	араметры							
Mapa C:\DL C:\DL	метры фиксирован LOCK80\Logs LOCK80\Passports	ных дисков по	• • • • • • • • • • • • • • • • • • •					

Рисунок А.12. – Окно дискреционного доступа

В контекстном меню или во вкладке «Действия» выбрать «Добавить (ФС)» (см. рисунок А.13.).

	👩 Dallas Lock 8.0-С [John, 0 (Открытые данные), метка не выбрана] 🛛 💶 🛪							
	Учетные записи	Параметры	безопасности	Контроль р	есурсов	СКН	МЭ СОВ Журналы	
Bce	Дискреционный доступ Контро	цатный Ауди доступ по файловой (	Контроль целостности	Глобальные	Устр	ойства о устройств	<ul> <li>Добавить (ФС)</li> <li>Добавить (Реестр)</li> <li>Удалить</li> <li>Действия</li> </ul>	а гь
Имя и па	араметры							
i Tapa C:\DI	метры фиксированн .LOCK80\Logs .LOCK80\Passports	ых дисков по . Доб. Доб. Удал Своі Обн	звить (ФС) звить (Реестр) ить іства овить					
,								

Рисунок А.13. – Пример вызова контекстного меню

В результате откроется окно выбора ресурса (см. рисунок А.14.).

Выбор ресурса		×
C:\[fixed]		<ul> <li>E</li> </ul>
Имя	/ Размер	
📂 \$Recycle.Bin		
E DLLOCK80		
📂 PerfLogs		
📂 Program Files		
📂 Program Files (x86)		
📂 ProgramData		
100 Recovery		
📂 System Volume Information		
🛅 Users		
🗁 Windows		
pagefile.sys	3 Gb	
Все файлы (*)	▼ (Q)	Выбрать Отмена

Рисунок А.14. – Меню выбора ресурса

Выбрать нужный ресурс и нажать кнопку «Выбрать» (см. рисунок А.15.).

выбор ресурса		
C:\[fixed] • C:\		🔿 🗈 🖻
Имя	🛆 Разм	lep
📂 \$Recycle.Bin		
E DLLOCK80		
🗁 PerfLogs		
📂 Program Files		
📂 Program Files (x86)		
📂 ProgramData		
Recovery		
System Volume Information		
TestFolder		
🗁 Users		
Windows		
pagefile.sys	3 Gb	
все фаилы (*)	▼ 😡	Выбрать Отмена

Рисунок А.15. – Пример выбора ресурса

В результате откроется окно настроек безопасности, в котором необходимо выбрать вкладку «Дискреционный доступ» (см. рисунок А.16.).

Безопасность: TestFolder	
Общие Дискреционный доступ	Изменение прав дискреционного доступа
Мандатный доступ	Назначенные права
Аудит доступа	
Контроль целостности	
	Пользователи Группы Все Удалить
	Автоматический поиск пользователей/групп
	Разрешить Запретить Полный доступ Только чтение Запись Удаление Чтение разрешений Закрыть доступ Чтение разрешений Запись разрешений Выполнение
	OK Cancel Apply

Рисунок А.16. – Окно настройки дискреционного доступа

Здесь необходимо назначить права доступа. Сделать это можно либо посредством выбора отдельных пользователей, либо групп (см. рисунок А.17.).

Безопасность: TestFolder		×
Общие Дискреционный доступ	Изменение прав дискреционного доступа	
Мандатный доступ	Назначенные права	
Аудит доступа Контроль целостности	suser_1 & user_2	
	Пользователи Группы Все Удалить ✓ Автоматический поиск пользователей/групп	
	Разрешить Запретить Полный доступ Только чтение Запись Удаление Чтение разрешений Закрыть доступ Выполнение Разрешить Запретить Удаление Чтение разрешений Выполнение	
	OK Cancel App	oly

Рисунок А.17. – Пример настройки дискреционного доступа

Для выбранных субъектов необходимо задать набор разрешений и запретов, определяющий права доступа к данному объекту. Например, как рисунке А.18.:

Безопасность: TestFolder		×
Общие Дискреционный доступ	Изменение прав дискреционного доступа	
Мандатный доступ Аудит доступа Контроль целостности	Назначенные права	
	Разрешить Запретить Разрешить Запретить Полный доступ Чтение Запись Удаление Чтение разрешений Запись разрешений Запись разрешений Выполнение	
	OK Cancel App	ly

Рисунок А.18. – Пример настройки набора разрешений

После завершения работы с дискреционным доступ, необходимо применить изменения и нажать кнопку «ОК». В результате окно закроется, а в список объектов добавится выбранный (см. рисунок А.19.).

				Dallas Loc	k 8.0-C [John, (	) (Открыт	ые данные),	метка не выбра	іна]	_ = ×
у у	четные записи	Параме	тры бе	зопасности	Контроль р	есурсов	СКН		Журналы	
Bce A	искреционный доступ Контр	Церод Іандатный доступ роль файлов	Аудит вой сис	Контроль целостности темы	Глобальные	Устр Контрол	ойства ы устройств	<ul> <li>Добавить (</li> <li>Добавить (</li> <li>Удалить</li> </ul>	ФС) 🚰 Свойства Реестр) 🦓 Обновить Действия	
Имя и пара	метры									
🛒 Парамет	тры фиксирован	ных дисков	по							
C:\DLLO	CK80\Logs									
C:\DLLO	CK80\Passports									
The second secon										
1										

Рисунок А.19. – Результат создания настройки дискреционного доступа

### Настройка очистки остаточной информации

Открыть оболочку администраторы системы защиты и перейти во вкладку «Параметры безопасности» - «Очистка остаточной информации» (см. рисунок А.20.).

		Dalla	s Lock 8.0-C [Johr	, 0 (Открытые данны	іе), метка не выб	брана]	_ = X
	Учетные записи	Параметры безопасное	ти Контрол	ь ресурсов СКН		Журналы	
Вход	Аудит Права пользователи	Мандатный Очистка ос вй доступ	таточной мации Контр целост Категории	оль Блокируемые ности расширения	Изолированные процессы	<ul> <li>Свойства</li> <li>Свойства</li> <li>Свойства</li> <li>Обновит</li> <li>Обновит</li> <li>Действия</li> </ul>	
Парамет	rp			Значение			
<b>1</b> 0чи	цать освобождаемо	е дисковое пространство		Нет			
🔮 Очиц	цать файл подкачки	виртуальной памяти		Нет			
0чи	цать данные в конфі	иденциальных сеансах доо	тупа	Нет			
📴 Пров	зерять очистку инфо	рмации		Нет			
Коли	чество циклов затир	ания		1			
Зати	рающая последоват	ельность		00 00 00 00			
-							
-							
-							
-							
							.:

Рисунок А.20. – Окно очистки остаточной информации

Изменить стандартное значение на «Да» для параметров: «Очищать освобождаемое дисковое пространство», «Очищать файл подкачки виртуальной памяти», «Проверять очистку информации». Изменение параметра происходит посредством окна «Редактирование параметров безопасности» (см. рисунок А.21.).

Редактирование параметров безопасности	×
Очищать освобождаемое дисковое пространство	
Да	
© Нет	
	ОК Отмена

Рисунок А.21. – Окно настройки очистки дискового пространства Количество циклов затирание установить в соответствии с требованиями политики безопасности (см. рисунок А.22.).

Dallas Lock 8.0-C [John	, 0 (Открытые данные), метка не выбрана] 💷 📼 🗙
Учетные записи Параметры безопасности Контроль	ресурсов СКН МЭ СОВ Журналы
	оль Блокируемые Изолированные Загрузчик юсти расширения процессы DL Действия
Параметр	Значение
🧟 Очищать освобождаемое дисковое пространство	Да
ダ Очищать файл подкачки виртуальной памяти	Да
Очищать данные в конфиденциальных сеансах доступа	Her
Проверять очистку информации	Да
СПКОЛИЧЕСТВО ЦИКЛОВ ЗАТИРАНИЯ	1
аранирающая последовательность	
<u> </u>	

Рисунок А.22. – Пример настройки очистки остаточной информации

### Настройка регистрации событий

Открыть оболочку администраторы системы защиты и перейти во вкладку «Параметры безопасности» - «Аудит» и установить значение «Вкл.» для необходимых параметров (см. рисунок А.23.).

Dallas Lock 8.0-C [John	п, 0 (Открытые данные), метка не выбрана] 🛛 💶 🛪
Учетные записи Параметры безопасности Контроль	ь ресурсов СКН МЭ СОВ Журналы
Категории	<ul> <li>Свойства</li> <li>Обновить</li> <li>Вагрузчик</li> <li>Осль Блокируемые Изолированные Загрузчик</li> <li>Основить</li> <li>Основить</li> <li>Действия</li> </ul>
Параметр	Значение
💵 Журнал входов в систему	Вкл.
🔡 Журнал ресурсов	Вкл.
📄 Журнал управления политиками безопасности	Вкл.
🤽 Журнал управления учетными записями	Вкл.
👼 Журнал печати	Вкл.
📟 Журнал запуска/завершения процессов	Вкл.
Фиксировать в журнале входов неправильные пароли	Нет
Заносить в журнал исходящие попытки входа на удаленные комп	Her
💐 Заносить в журнал события запуска и остановки ОС	Да
🖸 💭 Заносить в журнал события запуска и остановки модулей админи	Да
Аудит устройств	Выкл.
Аудит событий зачистки	Вкл.
Аудит доступа: Заносить в журналы ошибки ОС	Выкл.
Аудит доступа/запуска: Вести аудит системных пользователей	Выкл.
🍝 Печатать/редактировать штамп	Нет
🚔 Создавать теневые копии распечатываемых документов	Нет
🖶 Разрешить печать из-под уровней доступа	Все уровни
🚑 Добавлять штамп при печати под уровнями	Все уровни
📖 Выгрузка журналов	Выкл.

Рисунок А.23. – Окно настройки аудита

Для настройки аудита глобальных параметров перейти в категорию «Глобальные» на вкладке «Контроль ресурсов» (см. рисунок А.24.).

			Dallas Lock 8	.0-C [John, 0 (	(Открыть	іе данные),	метка не выбран	ia]	_ = = X
	Учетные записи	Параметры без	опасности	Контроль ре	сурсов	СКН		Журналы	
Bce	Дискреционный М доступ Конт	Мандатный Аудит доступ роль файловой сис	Контроль целостности темы	лобальные	Устро Контроль	риства устройств	🚰 Свойства Действия		
Парамет	гры								
🗾 Пара	метры ФС по умол	чанию							
🗾 Пара	метры фиксирован	ных дисков по умо	лчанию						
🗾 🗐 Пара	метры сети по умо	лчанию							
🗾 🗐 Пара	метры преобразов	анных файл-диско	в по умолчани.						
🗾 Пара	метры открытых см	менных накопителе	ей по умолчан						
🗾 Пара	метры CD-ROM ди	сков по умолчанин	0						
📑 Пара	іметры открытых U	SB-Flash накопител	ей по умолча						
📑 Пара	іметры открытых FC	DD-дисков по умол	чанию						
📑 Пара	метры преобразов	анных сменных на	копителей по						
📑 Пара	метры преобразов	анных USB-Flash на	копителей по						
📑 Пара	метры преобразов	анных FDD-дисков	по умолчанию						
📑 Пара	метры реестра по у	умолчанию							
L									
-									
L									
L									
L									
1									

Рисунок А.24. – Глобальные параметры

Выбрать глобальный параметр и нажать «Свойства» (см. рисунок А.25.).

	E	)allas Lock 8.0-С [John, 0 (Откры	гые данные), метка не выбран	на]	_ = ×
Учетные за	писи Параметры безопа	сности Контроль ресурсов	СКН МЭ СОВ	Журналы	
Все Дискрецио достуг Параметры ФС п Параметры ФС п Параметры откре Параметры откре Параметры откре Параметры откре Параметры откре Параметры откре Параметры прео Параметры прео Параметры прео Параметры прео	Параметры ФС по умолчани Общие Дискреционный доступ Аудит доступа	ню Свойства Имя Тип Дискреционный доступ Аудит	Параметры ФС по умолчанию Глобальный дескриптор Выкл. Вкл.		
			OK	Cancel Apply	

Рисунок А.25. – Свойства глобального параметра

Открыть вкладку «Аудит доступа» и отметить необходимые события, нажать «ОК» (см. рисунок А.26.).

		Dallas Lock 8	3.0-С [John, 0 (Открытые	данные	е), метка не вы	брана]		- =	
Учетные заг	писи Параметры безопа	сности	Контроль ресурсов	СКН		Журналы			
	Параметры ФС по умолчан	ию	ю 💌						
Все Дискрецио достуг	Общие Дискреционный доступ	۲	Назначение аудита						
Параметры	Аудит доступа	🛛 Аудит	включен						
Параметры ФС п Параметры фикс Параметры сети Параметры прео Параметры откре Параметры ОС-R Параметры откре Параметры откре Параметры прео Параметры прео		⊂ Событи	я Открытие объект Закрытие объект. Чтение данных Запись данных Создание Удаление Выполнение	a	Успех	Отказ 9 9 9 9 9 9 9 9 9 9 9			
Параметры преог Параметры реест			Изменение разрец Полный аудит	јений		V V			
			Теневое копирова	ние					
					ОК	Cancel	Apply		



Для настройки аудита локальных объектов ФС необходимо перейти в категорию «Аудит» на вкладке «Контроль ресурсов» см. (см. рисунок А.27.).

Dallas Lock 8.0-С [John, 0 (Открытые данные), метка не выбрана] — 🗖 🗶									
	Учетные записи	Параметры бе	зопасности	Контроль р	есурсов	СКН		Журналы	
Bce	Дискреционный М доступ Контри	андатный доступ оль файловой си	Контроль целостности стемы	Глобальные	Устр Контроль	ойства ь устройств	<ul> <li>Добавить</li> <li>Добавить</li> <li>Добавить</li> <li>Удалить</li> </ul>	(ФС) 🚰 Свойства (Реестр) 🦓 Обновить Действия	
Имяип	араметры								-
🗐 Пара	эметры ФС по умолч	анию							
Пара	метры реестра по ум	иолчанию							
C:\D	LLOCK80\Admshell.ex	e							
C:\D	LLOCK80\DLEncrypt.e	xe							=
C:\D	LLOCK80\BlockIcon.e	xe							
C:\D	LLOCK80\ExitWin.exe								
C:\D	LLOCK80\TestProg.ex	e							
C:\D	LLOCK80\DIInst.exe								
🖲 C:\DI	LLOCK80\DIIpsService	.exe							
🖲 C:\DI	LLOCK80\DIIpsEngine	.dll							
🖲 C:\DI	LLOCK80\SaveCfg131.	.dll							
🦲 C:\W	/indows\SysWOW64\E	DIGDIPrint.dll							
🦲 C:\W	/indows\SysWOW64\E	OClipboard.dll							
🦲 C:\W	/indows\SysWOW64\E	DIIps.dll							
🦲 C:\W	/indows\SysWOW64\E	)IThunk.dll							
🦲 C:\W	/indows\System32\DIA	AutP.dll							
🧧 C:\W	/indows\System32\DIk	(erber.dll							
🧧 C:\W	/indows\System32\DIL	.ives.dll							
🦲 C:\W	/indows\System32\DIS	ShExt.dll							-

Рисунок А.27. – Настройка аудита для локальных объектов ФС

Нажать «Добавить (ФС)» и выбрать ресурс для назначения аудита. В данном примере – папка TestFolder (см. рисунок А.28.).

		Dallas Lo	ock 8.0-С [John, 0 (Открыть	іе данные), метка	не выбрана]	_ = X
	Учетные записи	Параметры безопасности	Контроль ресурсов	CKH MB	сов Журналы	
		Выбор ресурса	)[		· · · · · · · · · · · · · · · · · · ·	
Bce	Дискреционный N доступ	C:\[fixed]			I I I I I I I I I I I I I I I I I I I	
<u> </u>	Контр	Имя	/	Размер		
Имя и па Пара Пара С:\DL С:\DL С:\DL С:\DL С:\DL С:\DL С:\DL С:\DL	араметры метры ФС по умол метры ресстра по у LOCK80\Admshell.e LOCK80\DLEncrypt. LOCK80\DlockIcon.e LOCK80\ExitWin.exe LOCK80\Dlinst.exe LOCK80\Dlinst.exe	\$Recycle.Bin     DLLOCK80     PerfLogs     Program Files     Program Files (x86)     ProgramData     Recovery     System Volume Information     TestFolder     Users	1		•	
<ul> <li>C:\DL</li> <li>C:\DL</li> <li>C:\W</li> <li>C:\W</li> <li>C:\W</li> <li>C:\W</li> <li>C:\W</li> </ul>	LOCK80\DIIpsEngin LOCK80\SaveCfg131 indows\SysWOW64\ indows\SysWOW64\ indows\SysWOW64\	pagefile.sys		3 Gb		
C:\W	indows\System32\DI indows\System32\DI	Все файлы (*)	•		Выбрать Отмена	
C:\W	indows\System32\DII	Lives.dll				
] 🖲 C:\W	indows\System32\DIS	ShExt.dll				₹ ,

Рисунок А.28. – Выбор ресурса для назначения аудита

Открыть вкладку «Аудит доступа», перед выбором событий включить аудит, отметив флажком поле «Аудит включен». После этого отметить необходимые события и нажать «ОК» (см. рисунок А.29.).

		Dallas Lock 8.0-0	С [John, 0 (Отк	рытые данные), метка не выб	рана]		-	. = x
9	Учетные записи Пара	метры безопасности Ко	нтроль ресурс	ов СКН МЭ СОВ	Журналы			
	-	Безопасность: TestFolder					×	
Bce	Дискреционный Мандатнь	Общие	(D)	азначение аудита				
	доступ доступ Контродь фай	Дискреционный доступ						
Имяипа	араметры	Мандатный доступ	🔽 Аудит в	ключен				<u> </u>
🚚 Пара	метры ФС по умолчанию	Аудит доступа	-События					
🗐 Пара	метры реестра по умолчани	Контроль целостности	0000011101		Успех	Отказ		
	LOCK80\Admsnell.exe			Открытие объекта		$\checkmark$		=
	LOCK80\BlockIcon.exe			Закрытие объекта	<b>V</b>	<b>V</b>		
C:\D	LOCK80\ExitWin.exe			Чтение данных	<b>V</b>	$\checkmark$		
C:\D	LOCK80\TestProg.exe			Запись данных	<b>V</b>	$\checkmark$		
C:\DI	LOCK80\DIInst.exe			Создание	<b>V</b>	<b>V</b>		
C:\DI	LOCK80\DIIpsService.exe			Удаление	<b>V</b>	$\checkmark$		
C:\DI	LOCK80\DIIpsEngine.dll			Выполнение	<b>V</b>	$\checkmark$		
C:\DI	LOCK80\SaveCfg131.dll			Изменение разрешений		$\checkmark$		
🦲 C:\W	indows\SysWOW64\DIGDIPrir				_			
🦲 C:\W	indows\SysWOW64\DIClipbo			Полный аудит	$\checkmark$	$\checkmark$		
🦲 C:\W	indows\SysWOW64\DIIps.dll							
🦲 C:\W	indows\SysWOW64\DIThunk			Теневое копирование				
🔟 C:\W	indows\System32\DIAutP.dll							
🧧 C:\W	indows\System32\DIKerber.dl		]					
🧧 C:\W	indows\System32\DILives.dll				ОК	Cancel	Apply	
🖲 C:\W	indows\System32\DIShExt.dll							-
_								

Рисунок А.29. – Настройка аудита доступа для ресурса ФС

Для настройки аудита объектов реестра необходимо перейти в категорию «Аудит» на вкладке «Контроль ресурсов» и нажать кнопку «Добавить реестр» ( см. рисунок А.30.).

		Dallas Loc	k 8.0-C [John, 0	(Открытые данные),	метка не выбрана]		 х
	Учетные записи Пара	метры безопасности	Контроль р	есурсов СКН	МЭ СОВ Журн	алы	
Bce	Дискреционный Мандатны доступ доступ	й Аудит Контроль целостности	Глобальные	Устройства	<ul> <li>Добавить (ФС)</li> <li>Добавить (Реестр)</li> <li>Удалить</li> </ul>	管 Свойства . 🝓 Обновить	
	Контроль фай	ловой системы		Контроль устройств	Действи	R	
Имя и па	араметры	Выбор ветки реестра				×	*
C:\W     E:\W      E:\W	Има и параметры       Interception         © C:\Windows\System32\DIFlashDiri       Interception         © C:\Windows\System32\DIESMAR       Interception         © C:\Windows\System32\DIESMOS       Interception         © C:\Windows\System32\Dieses\Univers\dfl       Interception         © C:\Windows\System32\Dirivers\dfl       Interception         © C:\Windows\System32\Dirivers\dfl </td <td></td>						
HKEY	LOCAL_MACHINE\SYSTEM				Выбрать Отмена	3	
C:\Te	estFolder						-

Рисунок А.30. – Выбор ветки реестра

Выбрать нужный ключ реестр; в примере выбран HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (см. рисунок 31).

Выбор ветки реестра	×
PhotoPropertyHandler	*
🕀 💼 PnPSysprep	
🕀 💼 Policies	
PreviewHandlers	
😥 💼 PropertySystem	
🕀 💼 Reliability	
😥 💼 RenameFiles	
🛅 Run	
RunOnce	
🕀 🧰 🧰 Setup	
🕀 🦲 Shell Extensions	
🕀 🦲 ShellCompatibility	
🕀 🧰 Sidebar	
i ⊡ ⊡ SideBySide	-
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	
Выбрать	Отмена

Рисунок А.31. – Выбор реестра

Выбрать действия для аудита в разделе «Аудит доступа» (см. рисунок А.32.).

Безопасность: Run				<b>—</b> ———————————————————————————————————
Общие	Назначение аудита			
Дискреционный доступ				
Аудит доступа	📝 Аудит включен			
Контроль целостности	События			
	У	(cnex	Отказ	
	Открытие объекта			
	Закрытие объекта			
	Чтение данных			
	Запись данных	1	$\checkmark$	
	Создание	1		
	Удаление	<b>v</b>		
	Изменение разрешений			
	Полный аудит			
		ОК	Cancel	Apply

Рисунок А.32. – Назначение аудита доступа для выбранного реестра

Результат добавление элементов аудита (см. рисунок А.33.):

			Dallas Loc	:k 8.0-C [John, 0	(Открыть	ле данные),	метка не выбр	ана]			_ = X
	Учетные записи	Параме	етры безопасности	Контроль р	есурсов	СКН		Журн	алы		
Bce	Дискреционный I доступ Конт	Щандатный доступ	Аудит Контроль целостности	Глобальные	Устр	ойства	<ul> <li>Добавить</li> <li>Добавить</li> <li>Добавить</li> <li>Удалить</li> </ul>	, (ФС) (Реестр) Действи	🚰 Свойства 🍓 Обновить 19		
		pono quinto	bon chereina		literitpent	, jeipenere,		Action		)	
C:\W     C:\W	/indows\System32\D /indows\Syste	DLESMART.dl DIDS9097.dll DIDS9097.U.dl DIDS9097.U.dl Drivers\dlflt.sj Drivers\dlflt.sj Drivers\dlfirev Drivers\dlfirev Drivers\dlfwc Drivers\d	II I ys pt.sys wall.sys csys ctrl.sys sys urrentControlSet\Serv urrentControlSet\Serv urrentControlSet\Serv urrentControlSet\Serv urrentControlSet\Serv urrentControlSet\Serv urrentControlSet\Serv \Microsoft\Windows'	ices\DIFirewall\ ices\DIFirewall\ ices\DIFirewall\ ices\DIFirewall\ ices\DIFirewall\ ices\DIFirewall\ \CurrentVersion	Parameter Parameter Parameter Parameter Parameter Parameter	s\Default s\Active\-> s\Active\-> s\Active\-> s\Active\->' s\Active\->'	\dlIdsLogRules \dlIdsNetRules \AppRules \RegKeysCtrl \Heuristics				Ш
1											·

Рисунок А.33. – Результат добавления элементов аудита

# Настройка контроля целостности файловой системы и программноаппаратной среды

Для настройки общих параметров необходимо перейти в категорию «Контроль целостности» на вкладке «Параметры безопасности» (см. рисунок А.34.).

Dallas Lock 8.0-C [John	, 0 (Открытые данные), метка не выбрана] 🛛 💶 🛪
Учетные записи Параметры безопасности Контроль	ресурсов СКН МЭ СОВ Журналы
Контр Вход Аудит Права пользователей доступ информации Категории	оль Блокируемые Изолированные Загрузчик расширения Изолированные Загрузчик DL DL Прогр. апп. среда Подкатегории Действия
Параметр	Значение
💽 Проверять целостность ΦС при загрузке ОС	Вкл.
Периодический контроль ФС	Не используется
🔀 Контроль ΦС по расписанию	Выкл.
🛍 Проверять целостность прогр.апп. среды при загрузке ОС	Вкл.
👩 Периодический контроль прогр.апп. среды	Не используется
💑 Контроль прогр.апп. среды по расписанию	Выкл.
📕 Проверять целостность реестра при загрузке ОС	Вкл.
🖸 Периодический контроль реестра	Не используется
🕁 Контроль реестра по расписанию	Выкл.
Изменение файлов с назначенным контролем целостности	Разрешить
1	

Рисунок А.34. – Настройка общих параметров среды

Изменить параметр «Периодический контроль» в соответствии с требованиями политики безопасности (см. рисунок А.35.).

Dallas Lock 8.0-C [John,	0 (Открытые данные), метка не выбра	ана] — 🗆 🗙
Учетные записи Параметры безопасности Контроль	ресурсов СКН МЭ СОВ	Журналы
Вход         Аудит         Права         Мандатный         Очистка остаточной         Контри контр           пользователей         доступ         информации         целостн	Блокируемые Изолированные Зап ости расширения процессы	Свойства Грузчик DL DL
Категории		Подкатегории Действия
Параметр	Значение	
🛃 Проверять целостность ФС при загрузке ОС	Вкл.	
🛃 Периодический контроль ФС	1 ч.	
🔀 Контроль ΦС по расписанию	Выкл.	
Я Проверять целостность прогр.апп. среды при загрузке ОС	Вкл.	
💑 Периодический контроль прогр.апп. среды	Не используется	
💑 Контроль прогр.апп. среды по расписанию	Выкл.	
📕 Проверять целостность реестра при загрузке ОС	Вкл.	
💽 Периодический контроль реестра	1ч.	
🔂 Контроль реестра по расписанию	Выкл.	
У Изменение файлов с назначенным контролем целостности	Разрешить	
,		12

Рисунок А.35. – Результат изменения параметра

Для настройки контроля целостности объектов ФС необходимо выбрать объект и нажать кнопку «Свойства» в категории «Аудит» на вкладке «Контроль ресурсов» (см. рисунок А.36.).

			Dallas Loc	k 8.0-C [John, 0	(Открытые данные	, метка не выбрана]		 x
۷	Учетные записи	Параме	тры безопасности	Контроль р	есурсов СКН	МЭ СОВ Журн	налы	
Bce	Дискреционный М доступ Конта	андатный доступ	Аудит Аудит контроль целостности вой системы	Срединие Глобальные	Устройства Контроль устройств	<ul> <li>Добавить (ФС)</li> <li>Добавить (Реестр).</li> <li>Удалить</li> <li>Действ</li> </ul>	🚰 Свойства 🥘 Обновить ия	
Имана								
COM	indows System 22 D	ECMART AL	1					-
	indows\System32\Di	DS0007 dil	1					
C.W	indows\System32\D	DS9097.01						
C:W	indows\System32\D	rivers\dlflt.s\	vs					
C:\W	indows\System32\D	rivers\DICrvr	pt.svs					
C:\W	indows\System32\D	rivers\dlfirev	vall.sys					
💽 C:\W	indows\System32\Di	rivers\dldisk	.sys					
🧵 C:\W	indows\System32\D	rivers\dlhwc	trl.sys					
🗵 C:\W	indows\System32\D	rivers\dllwf.s	sys					
🧵 C:\W	indows\ZPSSHELL.e>	e						
🛃 HKEY	LOCAL_MACHINE	SYSTEM\Cu	rrentControlSet\Servi	ces\DIFirewall\	Parameters\Default			
HKE\	LOCAL_MACHINE	SYSTEM\Cu	rrentControlSet\Servi	ces\DIFirewall\	Parameters\Active\->	•\dlIdsLogRules		- m.
HKE)	LOCAL_MACHINE	SYSTEM\Cu	rrentControlSet\Servi	ces\DIFirewall\	Parameters\Active\->	\dlIdsNetRules		
HKE\	LOCAL_MACHINE	SYSTEM\Cu	rrentControlSet\Servi	ces\DIFirewall\	Parameters\Active\->	•\AppRules		- 11
HKEY	LOCAL_MACHINE	SYSTEM\Cu	rrentControlSet\Servi	ces\DIFirewall\	Parameters\Active\->	RegKeysCtrl		Ξ
HKEY	LOCAL_MACHINE	SYSTEM\Cu	irrentControlSet\Servi	ces\DIFirewall\	Parameters\Active\->	•\Heuristics		- 11
C:\Te	estFolder							- 11
HKEY	LOCAL_MACHINE	SOFTWARE	\Microsoft\Windows\	CurrentVersion	i\Run			
1								

Рисунок А.36. – Выбор объекта для настройки контроля целостности

Перейти в раздел «Контроль целостности». отметить флажком поле «Контроль целостности включен», выбрать алгоритм расчета контрольной суммы (CRC32, ГОСТ Р 34.11-94, MD5) и нажать кнопку «Пересчитать», нажать кнопки «Применить» и «ОК» (см. рисунок А.37.).



Рисунок А.37. – Настройка контроля целостности для директории

Аналогично контроль целостности настроить и для файлов, регистров (см. рисунки А.38., А.39.):

Имя и параметры			Назначенные права		
🧧 стали страность: Run			· "		
© С Общие © С	Расчет и конт	гроль целостности			
Дискреционныи доступ С Аудит доступа	📝 Контроль целостност	ги включен			
С Контроль целостности С С	Свойства Параметр		•		
	Алгоритм расчета	Хэш ГОСТ Р 34.11-94	▼		
	Контрольная сумма	B2-47-92-2A-40-44-27 C9-2C-53-C2-2A-DD-7	7-6E-35-0F-64-EC-28-D0-A9-8A- IC-CE-58-AD-CF-1D-91-A9-8F-12		
	Расчетная КС	B2-47-92-2A-40-44-27 C9-2C-53-C2-2A-DD-7	'-6E-35-0F-64-EC-28-D0-A9-8A- 'C-CE-58-AD-CF-1D-91-A9-8F-12		
	Восстанавливать в Включая вложенны	: случае нарушения цело ые ветки	Пересчитать		
🗁 C					
🖻 d   🖻 d			OK Cancel Apply		
инкеу_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Аудит; Контроль целостности С CD(00000000-EC22351B):\ Дискр. доступ					

# Рисунок А.38. – Настройка контроля целостности для регистра

	0001.00	Аудин, контроль целостности
🧧 Безопасность: test.file		
Общие	Расчет и конт	роль целостности
🧧 Дискреционный доступ		
🧧 Мандатный доступ	🖊 Контроль целостност	и включен
🧧 Аудит доступа	Свойства	
Контроль целостности		
<b>©</b>	Алгоритм расчета	Хэш ГОСТ Р 34.11-94 💌
8	Контрольная сумма	F9-A7-59-73-0A-22-B5-EF-0B-D9-4A-73-CB-9E-C4-D7- BD-00-1B-D6-C5-42-01-CD-D8-51-D8-69-D1-26-59-61
	Расчетная КС	F9-A7-59-73-0A-22-B5-EF-0B-D9-4A-73-CB-9E-C4-D7- BD-00-1B-D6-C5-42-01-CD-D8-51-D8-69-D1-26-59-61
	Восстанавливать в Проверять целостн	случае нарушения целостности юсть при доступе Пересчитать
		OK Cancel Apply
C:\Users\John\Desktop\test.file		Контроль целостности

Рисунок А.39. – Настройка контроля целостности для файла

# Настройка прав разграничения доступа для внешних носителей информации

Перейти на вкладку «СКН» (см. рисунок А.40.).

Dallas Lock 8.0-С [John, 0 (Открытые данные), метка не выбрана] -						
Учетные записи Параметры 6	безопасности Контроль ресурсов	СКН МЭ СОВ Журналы				
Сменные Описание для Преос накопители сменных накопителей сменных Система контроля накопителей	<ul> <li>Фобавить Мо Обно</li> <li>Удалить</li> <li>Удалить</li> <li>Удалить</li> <li>Свойства</li> <li>Действия</li> </ul>	вить				
Сменные накопители	Назначенные права					
1						

Рисунок А.40. – Окно настроек сменных накопителей

Выбор ресурса × 🏓 🖻 🖻 D:\[cd-rom] Имя Размер 1 📂 boot 📂 efi 📂 sources 📂 support 🚞 upgrade autorun.inf 122 b bootmgr 374 Kb bootmgr.efi 653 Kb setup.exe 104 Kb - Все файлы (\*) Выбрать Отмена

Выбрать внешний носитель (см. рисунок А.41.).

Рисунок А.41. – Выбор внешнего носителя

После нажатия кнопки выбрать откроется окно настройки безопасности внешнего носителя (см. рисунок А.42.).

Безопасность: D:\		х
Общие	Сбщая информация	
Мандатный доступ	Свойства	
Аудит доступа	Имя СD(0000000-EC22351B) Тип CD-ROM диск Дискреционный доступ Выкл. Мандатный доступ Выкл. Аудит Выкл.	
	OK Cancel Apply	

Рисунок А.42. – Окно настройки безопасности внешнего носителя

Перейти во вкладку дискреционный доступ и настроить права для различных пользователей/групп (см. рисунки А.43., А.44.).

Безопасность: D:\		x
Общие Дискреционный доступ	Изменение прав дискреционного доступа	
Мандатный доступ Аудит доступа	Назначенные права	
	<ul> <li>▲ втоматическии поиск пользователей/групп</li> <li>Разрешить Запретить</li> <li>Полный доступ</li> <li>Обзор папки</li> <li>Изменение содержимого</li> <li>Удаление вложенных объектов</li> <li>Удаление вложенных объектов</li> <li>Закрыть доступ</li> <li>Закрыть доступ</li> <li>Чтение разрешений</li> <li>Запись разрешений</li> <li>Изкоуровневое чтение</li> <li>Изкоуровневая запись</li> </ul>	
	OK Cancel Apply	

Рисунок А.43. – Настройка для пользователя «user\_1»

Безопасность: D:\	×
Общие Дискреционный доступ	Изменение прав дискреционного доступа
Мандатный доступ	Назначенные права
Аудит доступа	
	Разрешить Запретить
	Обзор папки П И Изменение содержимого V Удаление вложенных объектов V Выполнение вложенных объектов V
	Закрыть доступ     Чтение разрешений     Г       Запись разрешений     Г       Низкоуровневое чтение     Г       Низкоуровневая запись     Г
	OK Cancel Apply

Рисунок А.44. – Настройка для пользователя «user\_2»

Результат добавление дискреционного доступа для сменного накопителя (см. рисунок А.45.).

	Dallas Lock 8.0-С [John, 0 (Открыты	ые данные), метка не выбрана]	_ = X
Учетные записи Параметры безо	опасности Контроль ресурсов	СКН МЭ СОВ Журналы	
Сменные накопители сменных накопителей сменных накопителей система контроля накопителей	В Добавить № Обне © Удалить № Свойства Действия	овить	
Сменные накопители	Назначенные права		
CD(0000000-EC22351B):\	Дискр. доступ		
1			

Рисунок А.45. – Результат добавления настройки

### Проверка настроек

Зашли в user\_1 (см. рисунок А.46.).:

				6	
	Librario	25 🕨		<ul> <li>Search Libraries</li> </ul>	٩
	Organize 🔻 New lib	orary			
	Favorites	Libraries Open a library to see your files an	d arrange them by folder, date, and other prope	rties.	
	Recent Places	Documents Library	Music Library	Pictures Library	
Getting Started	ints	Videos Library			
Windows Media Center					
Calculator	Иванов Иван				
Sticky Notes	Documents				
Spinning Tool	Pictures				
	Music				
Paint	Games				
Remote Desktop Connection	Computer				
Magnifier	Control Panel				
Solitaire	Devices and Printers				
	Default Programs				
All Programs	Help and Support				

Рисунок А.46. – Вход в систему от лица «user\_1»



Попытка записи в защищенную папку «TestFolder» (см. рисунок А.47.).

Рисунок А.47. – Попытка записи

Результат выполнения операции – ошибка записи (см. рисунок А.48.).

😗 User	r Account	: Control			×			
Ŷ	Do you want to allow the following program to make changes to this computer?							
		Program name: Verified publisher: File origin:	File Operation Microsoft Wind Hard drive on th	<b>ows</b> is computer				
Тос	ontinue, f	type an administrato	r password, and t	hen click Yes.				
Lo	Looking for credential tiles							
	S The file or directory is corrupted and unreadable.							
🕑 s	how detai	ls	[	Yes	D			

Рисунок А.48. – Результат выполнения операции

Аналогичная попытка записи, с использованием учетной записи администратора безопасности (см. рисунок А.49.).

😌 User Account	😯 User Account Control 🛛 💌						
Do you want to allow the following program to make changes to this computer?							
	Program name: File Operation Verified publisher: <b>Microsoft Windows</b> File origin: Hard drive on this computer						
To continue,	type an administrator password, and then click Yes.						
	John						
	JOHN-PC						
	Аппаратные идентификаторы: 0						
	Апп. идентификатор не выбран 🔻						
	•••••						
The file or directory is corrupted and unreadable.							
Show <u>d</u> eta	ils <u>Y</u> es <u>N</u> o						

Рисунок А.49. – Повторная попытка с использованием прав администратора безопасности

Получилось создать файл (см. рисунок А.50.).

Comput	er 🕨 Local Dis	sk (C:) 🕨 TestFol	der			•	<b>∳</b> Se	arch TestFolder	. 🗆	×
Organize   Include	n library 🔻	Share with 🔻	New folder							0
☆ Favorites	Name	<u>^</u>		Date modified	Туре	Size				
🔜 Desktop 🚺 Downloads 🗐 Recent Places	123			25.10.2018 22:13	Text Document		0 KB			
<ul> <li>□ Libraries</li> <li>□ Documents</li> <li>□ Music</li> <li>□ Pictures</li> <li>□ Videos</li> </ul>										
🖳 Computer										
1 item										

Рисунок А.50. – Созданный файл

Уведомления об нарушение целостности контролируемого ресурса (см. рисунок А.51.).



Рисунок А.51. – Уведомление о нарушение целостности папки

Запись в журнале о попытке нарушения целостности отслеживаемого объекта (см. рисунок А.52.)

				Dallas Lock 8	.0-С [John, 0 (Отк	рытые даннь	іе), метка не выбра	іна]			_ = X
	Учетные записи	Параметры безоп	асности Контроль ре	сурсов СКН		Журналы					
Журнал входов	журнал упр. журнал упр. уч.записями ресурсов	Журнал Журнал у печати политика Категории	пр. Журнал Журнал ми процессов из файла	<ul> <li>Обновить</li> <li>Архивировать</li> <li>Экспорт</li> </ul>	[ Открыть папк 📄 Права для фаі 🚔 Теневая копи: ействия	у(и) йла(ов) я	6 Применить филь Настроить фильт руппировать заг	тр 📻 Настрої р 🛄 Сохрані писи 🥅 Автообі Фильтр	ить группировку ить выборку новление		
	Время	Пользовател	Компьютер	Объект доступа		Результат	Операция	Доступ	Мандатная метка	Права	Процесс
66	25.10.2018 22:14:12	user 1		C:\TestFolder		OK	Открытие кат	0 (Открытые	Без метки	LRA	C:\Windows\explorer.exe
66	25.10.2018 22:14:12	user 1		C:\TestFolder		OK	Открытие кат	0 (Открытые	Без метки	L RA	C:\Windows\explorer.exe
6 66	25.10.2018 22:14:12	John		C:\TestFolder		OK	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\Svstem32\dllh
66	25.10.2018 22:14:12	John		C:\TestFolder		OK	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\TestFolder		OK	Открытие кат	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\TestFolder\N	ew Text Docume.	ОК	Закрытие объ	0 (Открытые	Без метки	D RA	C:\Windows\System32\dllhi
66	25.10.2018 22:14:12	John		C:\TestFolder\N	ew Text Docume.	OK	Закрытие объ	0 (Открытые	Без метки	D RA	C:\Windows\System32\dllhi
66	25.10.2018 22:14:12	John		C:\TestFolder\		OK	Закрытие объ	0 (Открытые	Без метки	W	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\TestFolder\		OK	Закрытие объ	0 (Открытые	Без метки	W	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\TestFolder\N	ew Text Docume.	OK	Переименова	0 (Открытые	Без метки		C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\TestFolder\		OK	Открытие кат	0 (Открытые	Без метки	AF	C:\Windows\System32\dllhi
66	25.10.2018 22:14:12	John		C:\TestFolder\N	ew Text Docume.	OK	Открытие фай	0 (Открытые	Без метки	D RA	C:\Windows\System32\dllhi
66	25.10.2018 22:14:12	user_1		C:\TestFolder		OK	Закрытие объ	0 (Открытые	Без метки	R RA	C:\Windows\explorer.exe
66	25.10.2018 22:14:12	user_1		C:\TestFolder		OK	Закрытие объ	0 (Открытые	Без метки	R RA	C:\Windows\explorer.exe
66	25.10.2018 22:14:12	user_1		C:\TestFolder		OK	Закрытие объ	0 (Открытые	Без метки	R RA	C:\Windows\explorer.exe
66	25.10.2018 22:14:12	user_1		C:\TestFolder		OK	Закрытие объ	0 (Открытые	Без метки	R RA	C:\Windows\explorer.exe
66	25.10.2018 22:14:12	John		C:\Windows\sys	tem32\propsys.dl	I OK	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\sys	tem32\propsys.dl	I OK	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\sys	tem32\propsys.dl	I OK	Открытие фай	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\Sys	WOW64\propsys	ОК	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\Sys	sWOW64\propsys	ОК	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\Sys	sWOW64\propsys	ОК	Открытие фай	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\Sys	WOW64\propsys	ОК	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\Sys	sWOW64\propsys	ОК	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\Sys	WOW64\propsys	ОК	Открытие фай	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
66	25.10.2018 22:14:12	John		C:\Windows\sys	tem32\propsys.dl	I OK	Закрытие объ	0 (Открытые	Без метки	RA	C:\Windows\System32\dllh
1									-		
Всего за	писей: 8832									_	

## Рисунок А.52. – Журнал ресурсов

# Запись в журнале входов о нарушении целостности (см. рисунок А.53.).

				Dallas Lock 8.0	-C [John, 0 (Открытые,	данные), метка не выбрана]	_ = ×
	Учетные записи	Параметры безоп	асности Контроль ресу	рсов СКН М	ИЭ СОВ Журн	алы	
5				🔄 Обновить	🔏 Применить фильтр	🛃 Настроить группировку	
				🖳 Архивировать	🖐 Настроить фильтр.	. 🛄 Сохранить выборку	
Журнал вхолов	Журнал упр. Журнал уч.записями ресурсов	Журнал Журнал у печати политика	упр. Журнал Журнал	Экспорт	👼 Группировать запи	си 🕅 Автообновление	
	,,	Категории		Действия		Фильтр	
	Время	Пользовател	Источник	Доступ	Мандатная метка	Результат	Неверный пар
<u>A</u> 7	25.10.2018 22:15:22	John	Разблокировка рабочей ст	та		Нарушена целостность контролируемых файлов.	
<b>()</b> 6	25.10.2018 22:14:45	John	Выход из ОС	0 (Открытые	. Без метки	OK	
<u>A</u> 5	25.10.2018 22:14:45	John	Вход в ОС	0 (Открытые	. Без метки	Нарушена целостность контролируемых файлов.	
1 4	25.10.2018 22:14:17	John	Выход из ОС	0 (Открытые	. Без метки	ОК	
<u>A</u> 3	25.10.2018 22:14:12	John	Вход в ОС	0 (Открытые	. Без метки	Нарушена целостность контролируемых файлов.	
🕸 <u>2</u>	25.10.2018 22:13:37	user_1	Вход в ОС	0 (Открытые.	. Без метки	Нарушена целостность контролируемых файлов.	
01	25.10.2018 22:12:10	user_1	Вход в ОС	0 (Открытые	. Без метки	OK	
0	25.10.2018 17:47:46	John	Вход в ОС	0 (Открытые	. Без метки	OK	
-							
Всего зап	исей: 8						

Рисунок А.53. – Журнал входов

Блокирование пользователя «user\_2» (см. рисунок А.54.)

user_2 Общие Аппаратная идентификация	Изменение о	сновных параметров пользо	<b>ж</b> ателя
Группы	Домен Логин Полное имя Описание Параметры У Отключена У Запретить работу п Служебный пользов Не синхронизируемь Пароль Потребовать смену пај Пароль без ограничи	изег_2 Антон Антонов пользователь_2 ри нарушенной целостности атель ый пользователь пароля при следующем входе роля пользователем ения срока действия	Тип учетной записи Не указан Мандатный доступ Настроить Число разрешенных сеансов Не используется Расписание работы Настроить
		ОК	Cancel Apply

Рисунок А.54. – Блокировка учетной записи «user\_2»

Попытка входа от лица заблокированной учетной записи (см. рисунок А.55.).



Рисунок А.55. – Попытка входа от лица заблокированной записи

Результат попытки (см. рисунок А.56.).



Рисунок А.56. – Результат входа с заблокированной записи

Многократные попытки входа в учетную запись с использованием неверного пароля (см. рисунок А.57.).



Рисунок А.57. – Вход в учетную запись «user\_1» с неправильным паролем

Результат – учетная запись заблокирована из-за превышения допустимого количества попыток (см. рисунок А.58.).



Рисунок А.58. – Блокировка записи

Записи о вышеперечисленных попытках входа отражены в журнале (см. рисунок А.59.).

	🔊 Dallas Lock 8.0-С [John, 0 (Открытые данные), метка не выбрана] 💷 📼 🗴							
	Учетные записи	Параметры безоп	асности Контроль ресу	<b>урсов СКН</b> МЕ	сов Журна	лы		
				🔄 Обновить	Применить фильтр	🚍 Настроить группировку		
				🕰 Архивировать 🛛 🤊	🖁 Настроить фильтр	Сохранить выборку		
Журнал	Журнал упр. Журнал	Журнал Журнал ј	пр. Журнал Журнал	Экспорт	👼 Группировать запис	и Автообновление		
входов	уч.записями ресурсов	Категории	лии процессов из файла	Действия		Фильтр		
	Bneug	Пользовател	Истолник	/loctrin	Maugaruan Herra	Pazyattat	Нарарцый дэр	
A 14	25 10 2018 22:20:05	lohn	Выход из ОС	Доступ	Без метки	OK	Певернай пар	
A 13	25.10.2018 22:20:05	John	Byon a OC	0 (Открытые	Без метки			
£12	25 10 2018 22:19:47	user 1	Вход в ОС	0 (Открытые	Без метки	Лостигнуто допустимое количество оцинбок ввода пародя. Уче		
@11	25.10.2018 22:19:36	user 1	Вход в ОС	0 (Открытые	Без метки	Указан неверный пародь.		
<b>1</b> 0	25.10.2018 22:19:35	user 1	Вход в ОС	0 (Открытые	Без метки	Указан неверный пароль.		
<b>63</b> 9	25.10.2018 22:19:31	user 2	Вход в ОС	0 (Открытые	Без метки	Учетная запись заблокирована.		
<b>3</b> 8	25.10.2018 22:18:44	user 2	Вход в ОС	0 (Открытые	Без метки	Учетная запись заблокирована.		
<u>A</u> 7	25.10.2018 22:15:22	John	Разблокировка рабочей с	та		Нарушена целостность контролируемых файлов.		
6	25.10.2018 22:14:45	John	Выход из ОС	0 (Открытые	Без метки	ОК		
<u>A</u> 5	25.10.2018 22:14:45	John	Вход в ОС	0 (Открытые	Без метки	Нарушена целостность контролируемых файлов.		
4	25.10.2018 22:14:17	John	Выход из ОС	0 (Открытые	Без метки	ОК		
<u>A</u> 3	25.10.2018 22:14:12	John	Вход в ОС	0 (Открытые	Без метки	Нарушена целостность контролируемых файлов.		
😮 2	25.10.2018 22:13:37	user_1	Вход в ОС	0 (Открытые	Без метки	Нарушена целостность контролируемых файлов.		
1	25.10.2018 22:12:10	user_1	Вход в ОС	0 (Открытые	Без метки	OK		
0	25.10.2018 17:47:46	John	Вход в ОС	0 (Открытые	Без метки	OK		
Brano 220	Mcaŭ: 15							

Рисунок А.59. – Записи в журнале входов

## ПРИЛОЖЕНИЕ А.А

### Настройка межсетевого экранирования

### Создание сетевого профиля

Перейти на вкладку «МЭ» - «Сетевые профили» (см. рисунок А.А.1.).

Dalias Lock 0.0-C (John) o (Orkphilible Jannale), Merka ne biopanaj	= - ~
Учетные записи Параметры безопасности Контроль ресурсов СКН МЭ СОВ Ж	Курналы
Адреса Сетевые профили Категории Сединения Параметры Правила Профили Фильтрация Статистика Отключить МЭ МЭ МЭ МЭ Действия	
ID Описание Локальный адрес IP v4 Локальный адрес IP v6 Сетевой интерфейс	
О1 Доверенная сеть не используется не используется любой сетевой адаптер	
2 Недоверенная сеть не используется не используется любой сетевой адаптер	
Э не используется не используется любой сетевой адаптер	
4 не используется не используется любой сетевой адаптер	
5 не используется не используется любой сетевой адаптер	
6 не используется не используется любой сетевой адаптер	
7 не используется не используется любой сетевой адаптер	
8 По умолчанию любой любой любой сетевой адаптер	
	· · ·

Рисунок А.А.1 – Окно настройки сетевых профилей

Включить сетевой профиль «Доверенная сеть» и установить параметры в соответствии с используемой сетью (см. рисунок А.А.2.).

Учетные записи Параметры безопасности Контроль ресурсов СКН МЭ СОВ Журналы Адреса Сетевые Соединения Параметры Правила Профили Фильтрация Статистика Отключить МЭ МЭ МЭ МЭ МЭ Категории В Описание Свойства сетевого профиля МЭ Свойства сетевого профиля Р-адреса 4 Свойства сетевого профиля: Доверенная сеть Р-адреса 1 Доверенная сеть Р-адреса 1 ПР v4 192 . 168 . 0 . 0 / 24 Далтер адаптер			Dallas Lock 8.0-C [J	ohn, 0 (Открытые данные),	метка не вы	ыбрана]	- =
Адреса       Сетевые соединения Параметры Правила Профили Фильтрация Статистика Отключить МЭ       № Обновить Себойства         И       Описание       Свойства сетевого профиля       № Свойства сетевого профиля         №       1       Доверенная сеть       Аалтер         0       3	Y	Учетные записи	Параметры безопасности	Контроль ресурсов	СКН	МЭ СОВ Жур	налы
ID       Описание       Свойства сетевого профиля       рейс	Дреса	Сетевые профили	Гараметры Правила Проф МЭ М Категории	з 🦻 🏹 📑 рили Фильтрация Статисти Э МЭ	ка Отключит МЭ	№ Обновить Свойства… Действия	
О1       Доверенная сеть       название профиля:       Доверенная сеть       адаптер         2       Недоверенная сеть       По умолчанию       ПР v4       192 . 168 . 0 . 0 / 24       адаптер         6       Пр v4       192 . 168 . 0 . 0 / 24       адаптер       адаптер         7       По умолчанию       Сетевой интерфейс:       побой сетевой адаптер       адаптер         ОК       Отмена       Отмена       Отмена       Отмена	ID	Описание	Свойства сетевого про	филя		<b>рейс</b>	
OK OTMEHA	<ul> <li>1</li> <li>2</li> <li>3</li> <li>4</li> <li>5</li> <li>6</li> <li>7</li> <li>8</li> </ul>	Доверенная сеть Недоверенная сеть По умолчанию	Название профиля: IP-адреса IP v4 IP v4 IP v6 Сетевой интерфейс:	Доверенная сеть 192 . 168 . 0 . 0 :: любой сетевой адалтер	/ 24	адаптер адаптер адаптер адаптер адаптер адаптер адаптер адаптер	
	•				UTM	244	

Рисунок А.А.2. – Настройка доверенной сети

Перейти во вкладку «Параметры» и открыть свойства параметра «Режим обучения МЭ» (см. рисунок А.А.З.).

	Dallas Lock 8.0-С [John, 0 (Открытые	данные), метка не	выбрана]		_ = X
Учетные записи Параме	тры безопасности Контроль ре	сурсов СКН	МЭ СОВ	Журналы	
Адреса Сетевые Соединения Параме профили	ры Правила Профили Фильтрация МЭ МЭ Категории	Статистика Отключ МЭ МЭ	Каралови Кить Свойств Действи	ить ва я	
Параметр	Режим обучения МЭ				
<ul> <li>Доверенные правила МЭ</li> <li>Отключать GZIP для анализа HTTP т</li> <li>Сохранять локальные правила M3 п</li> <li>Режим обучения МЭ</li> <li>Список разрешенных драйверов пр</li> <li>Протоколирование событий измен</li> <li>Периодичность проверки защищен</li> <li>Уведомления по событиям отсутств</li> <li>Отключать локальные правила МЭ</li> <li>Порты сторонних программ</li> </ul>	<ul> <li>Включить режим обучения</li> <li>Режим после обучения</li> <li>Пропускать пакеты</li> <li>Запрещать пакеты</li> <li>Запрещать пакеты</li> <li>Скончание обучения</li> <li>Время: 18:18:52</li> <li>Дата: 25,10.2018</li> <li>Макс. кол-во портов в Макс. кол-во адресов в</li> <li>Макс. кол-во созда</li> </ul>	Период обучения ④ День ○ Неделя ○ Месяц Установить одном правиле: 5 одном правиле: 5 ваемых правил: 5 ОК От			

Рисунок А.А.З. – Свойства режима обучения

# Настроить режим обучения, как показано на рисунке А.А.4.:

	Dallas Lock 8.0-С [John, 0 (Открыть	іе данные), метка не	выбрана]		_ = X
Учетные записи Параме	тры безопасности Контроль р	оесурсов СКН	МЭ СОВ	Журналы	
Адреса Сетевые Соединения Параме	гры Правила Профили Фильтраци: МЭ МЭ Категории	а Статистика Отключ МЭ МЭ	№ Обно инть Дейст	обить ства бия	
Параметр	Режим обучения МЭ				
<ul> <li>Доверенные правила МЭ</li> <li>Отключать GZIP для анализа HTTP т</li> <li>Сохранять локальные правила МЭ и</li> <li>Режим обучения МЭ</li> <li>Список разрешенных драйверов пр</li> <li>Протоколирование событий измен</li> <li>Периодичность проверки защищея</li> <li>Уведомления по событиям отсутств</li> <li>Отключать локальные правила МЭ</li> <li>Порты сторонних программ</li> </ul>	<ul> <li>Включить режим обучения</li> <li>Режим после обучения</li> <li>Пропускать пакеты</li> <li>Запрещать пакеты</li> <li>Окончание обучения</li> <li>Время: 18:22:06</li> <li>Дата: 01.11.2018</li> <li>Макс. кол-во портов и Макс. кол-во адресов и Макс. кол-во созд</li> </ul>	Период обучения День Неделя Месяц Установить в одном правиле: 30 в одном правиле: 40 аваемых правил: 50 ОК От	а а а а а а а а а а а а а а		
ј Глобальные настройки МЭ					.:i

Рисунок А.А.4. – Настройка свойства режима обучения

В данном режиме автоматически формируются правила для посещенных доменов (см. рисунки А.А.5., А.А.6.).



Рисунок А.А.5. – Посещение домена

		Dallas Loc	:k 8.0-C [John, (	) (Открытые данные), метка не выбрана, Период тех. подд	ержки истек]				
<b>9</b>	Учетные записи Параметры безопасности	Контроль ресурсов СКН МЭ СОВ 2	Журналы						
Agpeca	Сетевые Соединения Параметры Правила Профили Категории	или Фильтрация Статистика Отключить МЭ МЭ	Редактир (2) Активир (3) Деактиви Действия,	новать 🔂 Копировать 💾 Сохранить овать 🕞 Увеличить приоритет 🗧 Загрузить ировать 🚍 Уменьшить приоритет Профиль правил По умолчанию					
<u>n</u>	Описание	Маски пути	С Пользов	Протоколы и поля	Расписан	3an	Уровень доступа	Направлен	Сетевые профили
1	DNS клиент	C:\WINDOWS\system32\svchost.exe	Everyone	Внешний TCP порт = 53, Внешний UDP порт = 53	Всегда		Все уровни	Любое	Bce
2 🜔	ARP	System	Everyone	ARP	Всегда		Все уровни	Любое	Bce
3	DHCP клиент	C:\WINDOWS\system32\svchost.exe	Everyone	Локальный UDP порт = 68 Внешний UDP порт = 67	Всегда		Все уровни	Любое	Bce
) 4	HTTP/HTTPS клиент		Everyone	Внешний ТСР порт = 80, 443	Всегда		Все уровни	Исходящи	Bce
) 5	Internet Explorer HTTP/HTTPS	C:\Program Files\Internet Explorer\IEXPLORE.EXE;C:\	Everyone	Внешний ТСР порт = 80, 443	Всегда		Все уровни	Любое	Bce
) 6	IGMP	System	Everyone	IGMP	Всегда		Все уровни	Любое	Bce
7	www.yandex.ru		Everyone	Внешний IPv4 = www.yandex.ru	Всегда		Все уровни	Исходящи	Bce
8 (	Внешние сетевые папки		Everyone	Внешний TCP порт = 139, 445, 135, Локальный UDP п	Всегда		Все уровни	Любое	Bce
9	Локальные сетевые папки	System	Everyone	Локальный TCP порт = 139, 445, 135, Локальный UDP	Всегда		Все уровни	Любое	Bce
10	Dallas Lock удаленное управление (входящее)	C:\WINDOWS\system32\Isass.exe	Everyone	Локальный ТСР порт = 17490	Всегда		Все уровни	Входящие	Bce
11	Dallas Lock удаленное управление (исходящее)	C:\WINDOWS\system32\Isass.exe;C:\DLLOCK80\*	Everyone	Внешний ТСР порт = 17490, 17491, 17498, 17499	Всегда		Все уровни	Исходящи	Bce
12	Dallas Lock проверка доступности клиентов (І		Everyone	ICMP сообщение = Эхо ответ, Эхо запрос	Всегда		Все уровни	Любое	Bce
13	Dallas Lock СБ (входящее)	C:\WINDOWS\system32\Isass.exe;C:\DLLOCK80\DISe	Everyone	Локальный ТСР порт = 17490, 17491, 17492, 17493	Всегда		Все уровни	Входящие	Bce
14	Dallas Lock СБ (исходящее)	C:\WINDOWS\system32\Isass.exe;C:\DLLOCK80\*	Everyone	Внешний ТСР порт = 17490, 17491, 17492, 17493, 17498	Всегда		Все уровни	Исходящи	Bce
15	Dallas Lock СЛ (входящее)	C:\DLLOCK80\DILicServer\DILicModule.exe	Everyone	Локальный ТСР порт = 17498, 17499	Всегда		Все уровни	Входящие	Bce
) 16	ICMP по умолчанию (исходящее)		Everyone	ICMP сообщение = Адресат недоступен, Эхо запрос,	Всегда		Все уровни	Исходящи	Bce
17	ICMP по умолчанию (входящее)		Everyone	ІСМР сообщение = Эхо ответ, Адресат недоступен, З	Всегда		Все уровни	Входящие	Bce
18	Правило на использование сети Интернет		Everyone	IPv4	Всегда		Все уровни	Любое	Доверенная сеть
2 19	Автоматическое правило 1 (режим обучения)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	John	Внешний IPv4 = 104.16.249.249, www.yandex.ru, yande	Всегда		Все уровни	Исходящи	Bce
20	Автоматическое правило 2 (режим обучения)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	John	Внешний IPv4 = www.yandex.ru, yandex.ru, pki-goog.l	Всегда		Все уровни	Исходящи	Bce
21	Автоматическое правило 3 (режим обучения)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	John	Внешний IPv4 = favicon.yandex.net; Внешний TCP по	Всегда		Все уровни	Исходящи	Bce
22	Автоматическое правило 4 (режим обучения)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	John	Внешний IPv4 = a1887.dscq.akamai.net, a19.dscg10.aka	Всегда		Все уровни	Исходящи	Bce
Э По	Действие с пакетами не попавшими ни под о								

Рисунок А.А.б. – Добавленные правила

## Настройка фильтрации

Перейти во вкладку «Фильтрация» - «Фильтры», выбрать один из параметров и настроить его в соответствии с требованиями политики безопасности (см. рисунок А.А.7.).

			Dallas Lock 8.0-C [John, 0	(Открытые данные), метка не вы	брана, Период тех. поддержки
Учетные записи	Параметры безопасности	Контроль ресурсов СКН	ИЭ СОВ Журналы		
Адреса Сетевые Соединения профили	Гараметры Правила Проф МЭ М Категории	рили <mark>бильтрация</mark> Статистика Отключит МЭ	настройки <mark>Фильтры</mark> Веб-кон Параметр	28 Констрацию птроль Исключения Выключить фильтрацию ы фильтрации	Обновить Свойства Действия
Имя	Действие	Действия по профилям			
ActiveX	Отключено				
<ul> <li>Flash</li> </ul>	Отключено				
<ul> <li>JScript</li> </ul>	Отключено				
O VBScript	Отключено				
💂 НТТР	По профилю	0 Доверенная сеть: Жур	оналировать; 7 По умолчанию: В	Блокировать	
ONS	Отключено			-	
○ SSH	Отключено	Свойства фильтра	<b>X</b>		
TELNET	Отключено				
○ RDP	Отключено	Имя фильтра: НПР			
HttpProxy	Отключено	П Действие для всех профилей:	По профилю 👻		
IFrame	Отключено				
HTTP:Referers	Отключено	Профили			
HTTP:HeaderSize	Отключено	Установить действие на все профили:	Отключено 🔻		
O PDF	Отключено				
PostScript	Отключено	1. Доверенная сеть	Журналировать 👻		
Java	Отключено				
OpenVPN	Отключено	2. педиверенная сеть	Блокировать 👻		
		3.	Блокировать 👻		
		4,	Блокировать 👻		
		5,	Блокировать 👻		
		6.	Блокировать 👻		
		7.	Блокировать 👻		
		8. По умолчанию	Блокировать 💌		
			ОК Отмена		
				-	

Рисунок А.А.7. – Настройка фильтрации

## Настройка почты

Перейти во вкладку «Правила МЭ» и создать новое правило (см. рисунок

A.A.8.).

Информация Общие Протоколы Пользователи Дополнительно Описание правила: Тонтовый сервис Действие: Разрешить  Действие: Разрешить  Действие: Разрешить Действие: Обзор Обзо	Настройки правила М	мэ	x
Протоколы       Описание правила: iouroвый сервис         Пользователи       Действие: Разрешить • Расписание работы         Дополнительно       Запустить приложение: • Обзор         Запустить приложение: • Оповещение о запрете пакета (при настроенном аудите в журнале пакетов МЭ)         Применить правило только для указанных приложений (ножно указать наску пути)         Параметры:         Параметры:         Добавить         Удалить	Информация	Общие настройки	
Удалить	Общие Протоколы Пользователи Дополнительно	Описание правила: Почтовый сервис Действие: Разрешить Расписание работы Действие: Разрешить Пастроить Запустить приложение: (от ОС, не интерактивно) Оповещение о запрете пакета (при настроенном аудите в журнале пакетов МЭ) Применить правило только для указанных приложений (можно указать маску пути) Параметры: Добавить И	
		Правило активно Покальное правило	

Рисунок А.А.8. – Создание нового правила МЭ

# Настроить протоколы (см. рисунок А.А.9.).

Настройки правила I	MЭ	×
Информация	Сетевые протоколы	
Общие		
Протоколы	Направление передачи: Любое направление передачи 💌	
Пользователи	Список протоколов	
Дополнительно	Ethernet 🔹	
	Добавить С ТСР Удалить	
	Параметры выбранного протокола (должны выполняться все указанные условия - "логическое И")	
	<ul> <li>Покальный IPv4</li> <li>✓ Внешний IPv4 (= 77.88.21.249)</li> <li>✓ Внешний протокол</li> </ul>	
	<ul> <li>□ Локальный ТСР порт</li> <li>□ Внешний ТСР порт ( = 25, 110, 143)</li> </ul>	
	ОК	Cancel

Рисунок А.А.9. – Настройка протоколов

Настроить порты (см. рисунки А.А.10., А.А.11.).

Настройки правила І	МЭ	×
Информация	Сетевые протоколы	
Общие		
Протоколы	Направление передачи: Любое направление передачи 🔻	
Пользователи	Список протоколов	
Дополнительно	Ethernet 🔹	
	Добавить Удалить	
	Параметры выбранного протокола (должны выполняться все указанные условия - "логическое И")	
	🔲 Локальный ТСР порт	
	І Внешний ТСР порт ( = )	
	Параметры поля "Внешний ТСР порт"	
	Операция сравнения Номер порта в формате 1, 2-64, 88	
	Равно 💌 == 25, 110, 143	
	Наборы портов Таблица значений Применить	
	OK	cel

Рисунок А.А.10. – Настройка портов для ТСР

Настройки прави	іла МЭ		23
Информация		Сетевые протоколы	
Общие	Наборы порт	08	
Протоколы			-
Пользователи	Порт 🛆	Описание	
Лополнительно	20	FTP data	
дополнительно	22	SSH	-
	23	Telnet	
	25	SMTP	1
	53	DNS	
	67	DHCP	
	68	DHCP	- I
	69		
	81	нтр	
	110	POP3	
	123	NTP	
	135	MSRPC	
	137	SMB-NS	5
	138	SMB-DGM	
	139	SMB-SSN	
	143	IMAP	
		ОК Отмена	
	I	OK	Cancel

Рисунок А.А.11. – Выбор используемых портов

Настроить пользователей, взаимодействующих с правилом (см. рисунок А.А.12.).

Настройки правила I	мэ	×
Информация Общие	настройки учетных записей пользователей	
Протоколы Пользователи Дополнительно	Выбранные пользователи Suser_1 Suser_2 Пользователи Группы Все Удалить Vдалить Латонатический поиск пользователей/групп	
	Выбрать все Снять все	
	т	Cancel

Рисунок А.А.12. – Настройка пользователей

Настроить сетевые профили, использующие правило (см. рисунок А.А.13.).

Настройки правила М	ИЭ					×
Информация	∎т∎ д	ополнительные наст	гройки			
Общие						
Протоколы	Список сетевых адаптеров					
Пользователи	Local Area Connection (Intel(R) PRO/1000 MT Desktop Adapter)					
Дополнительно					<b>Добавить</b> Удалить	
	Выбранные сетевые профили					
		Описание	192,168.0.0/24	не используется	сетевои интерфеис	
		Недоверенная сеть	не используется	не используется	любой сетевой ад	
	3		не используется	не используется	любой сетевой ад	
			не используется	не используется	любой сетевой ад	
			не используется	не используется	любой сетевой ад	
			не используется	не используется	любой сетевой ад	
	0 8 📀 🗉	По умолчанию	любой	любой	любой сетевой ад	
	Выбрать все Снять все					
					OK	Cancel

Рисунок А.А.13. – Настройка сетевых профилей

В результате будет создано следующее правило (см. рисунок А.А.14.).



Рисунок А.А.14. – Результат создания правила
### Настройка анализа SSL трафика

Перейти во вкладку «Фильтрация» - «Настройки» и включить параметр «Анализ SSL трафика» (см. рисунок А.А.15.).

Dallas Lock 8	.0-С [John, 0 (Открытые данные), метка не	выбрана, Перис	од тех. поддержки истек]	_ = X
Учетные записи Параметры безопасно	ости Контроль ресурсов СКН	МЭ СОВ	Журналы	
Сородина Соединения Параметры Правила Профили МЭ Категори	и радила развита статистика Отключи МЭ	ть Настройки	Фильтры Веб-контроль Исключения Параметры фильтрации	Карания Выключить фильтрацию
Параметр	Значение			
Список перехватываемых исходящих портов	80,443,3128,8080			
Режим работы	Фильтровать все, кроме исключений			
😣 Анализ SSL трафика	Нет			
💌 Максимальный размер http-заголовка	2048			
Включить уведомление в трей при блокировк Ан	ализ SSL трафика			
	Анализ SSL трафика			
	Да			
	Het			
		ОК	Отмена	
Всего записей: 24 Текущий профиль МЭ: По умолчани	0			

Рисунок А.А.15. – Включение анализа SSL трафика

## Настройка сбора информации (журналов)

Перейти во вкладку «Параметры безопасности» - «Аудит» (см. рисунок А.А.16.).

Dallas Lock 8.0-С [John, 0 (Отк	рытые данные), метка не выбрана, Период тех. поддержки истек] 💷 🗖 💈
Учетные записи Параметры безопасности Контро.	ль ресурсов СКН МЭ СОВ Журналы
Код Аудит Права Пользователей Мандатный Очистка остаточной Конг пользователей доступ информации целос Категории	<ul> <li>Свойства</li> <li>Свойства</li> <li>Свойства</li> <li>Сбоюкуучные Изолированные Загрузчик</li> <li>Обновить</li> <li>Действия</li> </ul>
Параметр	Значение
Хурнал входов в систему	Вкл.
Журнал ресурсов	Вкл.
Журнал управления политиками безопасности	Вкл.
Журнал управления учетными записями	BKn.
🖷 Журнал печати	Выкл.
Журнал запуска/завершения процессов	BKn.
🔄 Служебный журнал МЭ (заблокированные пакеты в формате Рсар	а) Выкл.
👑 Журнал пакетов МЭ	Вкл
🞯 Журнал соединений МЭ	Выкл.
👳 Журнал трафика фильтрации МЭ	Bion.
🔕 Журнал событий ОС	Bion.
👳 Журнал трафика СОВ	Bkn.
Журнал контроля приложений СОВ	Bkn.
🛃 Фиксировать в журнале входов неправильные пароли	Her
Заносить в журнал исходящие попытки входа на удаленные комп.	Her
💐 Заносить в журнал события запуска и остановки ОС	Да
🔍 Заносить в журнал события запуска и остановки модулей админи.	Да
🔄 Аудит устройств	Выкл.
🔄 Аудит событий зачистки	Вкл.
Аудит доступа: Заносить в журналы ошибки ОС	Выкл.
Аудит доступа/запуска: Вести аудит системных пользователей	Выкл.
🍝 Печатать/редактировать штамп	Нет
Создавать теневые копии распечатываемых документов	Нет
Разрешить печать из-под уровней доступа	Все уровни
Добавлять штамп при печати под уровнями	Все уровни
📖 Выгрузка журналов	Выкл.

Рисунок А.А.16. – Параметры аудита

Открыть свойства параметра «Настройки журнала пакетов» и настроить его аналогично правилу МЭ (см. рисунок А.А.17.).

проики журнала на	KETOB IVIJ		
нформация	Пиформация		
бщие			
ротоколы	Свойства		
ользователи	Параметр	Значение	
ополнительно	Действие	Правило не инвертировано, активно	
	Журналирование	Всех пакетов	
	Маски пути	Все пути	
	Сетевые интерфейсы	Все сетевые интерфейсы	
	Пользователи	Everyone	
	Протоколы и поля	IPv4	
		- Внешний IPv4 = dzen.ru, yandex.ru	
	Расписание	Всегда	
	Мандатный уровень	Все уровни	
	Направление	Любое	
	Сетевые профили	Доверенная сеть, По умолчанию	
	Включить запись out-of-state T	Выключено	

Рисунок А.А.17. – Настройка журнала пакетов

Открыть свойства параметра «Настройки журнала соединений» и настроить его аналогично правилу МЭ (см. рисунок А.А.18.).

	Dallas L	ock 8.0-C [John,	0 (Открытые данны	е), метка не выб	рана, Пер	иод тех. подд	ержки истек]		_	= X
Учетные записи	и Параметры безо	пасности К	онтроль ресурсов	СКН МЭ	СОВ	Журналы				
2	<u> </u>	<b>1</b>	i i i				Свойства Обновить			
Вход Аудит Прав	Настройки журнала	соединений МЭ							×	
	Информация									
Параметр	Общие		рормация							
🖳 Журнал входов в сист	Протоколы	- Свойства								
🔡 Журнал ресурсов	-	Cooncroa		2						
📗 Журнал управления г	Пользователи	Параметр		Значение						
🌋 Журнал управления у	/•	Действие		Правило не и	нвертиров	ано, активно				
🛲 Журнал печати	_	Пользова	тепи	Everyone						
🥮 Журнал запуска/заве	P	Протокол	ы и поля	IPv4						
Служеоный журнал м	<b>^</b>			- Внешний If	v4 = dzen.r	u, yandex.ru				
журнал пакетов M3		Расписани	1e	Всегда						
урнал соединении г	Y I	Мандатны	ий уровень	Все уровни						
🖤 Журнал трафика фил	6	Направле	ние	Любое						
Журнал событии ОС		Сетевые г	профили	Bce						
Паринал прафика СОВ	·									=
Фиксировать в холона										
Заносить в холонал ис										
Заносить в журнал со	1									
Ваносить в журнал со										
Аулит устройств										
Аудит событий зачист	T									
Аудит доступа: Занос	и									
Аудит доступа/запуск	a									
🐣 Печатать/редактиров	a									
🕀 Создавать теневые ко	r									
🔒 Разрешить печать из-	r							OK	Cancel	
🕹 Добавлять штамп при	и печати под уровнями		Все уровн	4						-
🔊 Выгрузка журналов			Выкл.							-
	•		20000 2000		20000 2000		00000 00000	20000		•

Рисунок А.А.18. – Настройка журнала соединений

## Результаты настроек на рисунках А.А.19. и А.А.20..

							Dallas Loc	k 8.0-C	[John, 0 (Открытые да	нные), метка не	е выбрана, Пери	юд тех. поддержки исте	<]				_ = = >
۲	Учетные записи	Параметры безоп	асности	Контроль рес	урсов СКН	MЭ	сов Х	Курналі	ы								
Журна входо	л Журнал упр. Журнал в уч.записями ресурсов	Журнал Журнал у печати политика	упр. Журн ами проце	нал журнал пакетов МЭ Категории	Журнал соединений МЭ	Журнал трафика с	Журнал Журнал обытий ОС	Журна прил	л контроля Журнал южений из файла	<ul> <li>Обновить</li> <li>Архивиров</li> <li>Экспорт Действия</li> </ul>	вать 🐺 Прим Вать 👼 Настр 🍮 Групп	енить фильтр 📑 Нас юить фильтр 🛄 Сох иировать записи 🥅 Авт Фильтр	троить группировку ранить выборку ообновление				
ID 🗸	Время	Локальный а	Локаль	Внешний ад	Внешнее имя	Внешн	Направ	Пр	Информация		Пользователь	Доступ	Процесс	PID	Дли	Правило	Результат
0 25	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	тср	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	54		ОК
0 24	17.04.2023 20:53:15	10.0.2.15	10003	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	204	(Доверенные	ОК
023	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	54		OK
0 22	17.04.2023 20:53:15	10.0.2.15	54860	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	54	(Доверенные	OK
0 21	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	204		OK
0 20	17.04.2023 20:53:15	10.0.2.15	10003	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	89	(Доверенные	OK
19	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	89		OK
18	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	60		OK
017	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	60		ОК
16	17.04.2023 20:53:15	10.0.2.15	54860	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	1703	(Доверенные	OK
0 15	17.04.2023 20:53:15	10.0.2.15	10003	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	54	(Доверенные	OK
14	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	86		ОК
13	17.04.2023 20:53:15	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	тср	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	1671		OK
12	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	54		OK
011	17.04.2023 20:53:11	10.0.2.15	10003	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	346	(Доверенные	ОК
10	17.04.2023 20:53:11	10.0.2.15	54860	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	54	(Доверенные	ОК
09	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	311		OK
08	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	89		OK
07	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	60		ОК
06	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Прием	тср	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	60		OK
05	17.04.2023 20:53:11	10.0.2.15	54860	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	1727	(Доверенные	OK
04	17.04.2023 20:53:11	10.0.2.15	10003	5.255.255.70	www.yandex	12098	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	54	(Доверенные	ОК
03	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	488		OK
02	17.04.2023 20:53:11	10.0.2.15	54859	5.255.255.70	www.yandex	HTTPS	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	1293		OK
01	17.04.2023 20:53:10	10.0.2.15	10003	62.217.160.2	dzen.ru	12062	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	LOCAL_SYST	0 (Открытые данные)	C:\DLLOCK80\DIIpsService.exe	1400	66	(Доверенные	OK
0	17.04.2023 20:53:10	10.0.2.15	60637	62.217.160.2	dzen.ru	HTTPS	Отпра	TCP	Ethernet: 08:00:27:C2:	67:8B, 52:54:	John	0 (Открытые данные)	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2560	55		OK

## Рисунок А.А.19. – Журнал пакетов МЭ после настроек

							Dallas	Lock 8.0	)-С [John, 0 (Откр	оытые дан	ные), метка не	е выбрана, Период те	х. подде	ржки истек]				
۲	Учетные записи	Тараметры безог	асности	Контроль рес	урсов СКН	MЭ	СОВ	Журі	налы									
	<b>2 =</b> 0			888						7	Обновить	🛛 👔 Применить	фильт	о 📑 Настроить	группировку			
Ľ							M.				🕮 Архивиров	вать 🖥 Настроить	фильтр	🔲 Сохранить	выборку			
Журна	л Журнал упр. Журнал	Курнал Журнал	упр. Журн	ал Журнал	Журнал	Журнал	Журна.	т Жуј	онал контроля 🔾	Курнал	Экспорт	Бруппиров	ать запи	или 🔲 Автообнов	ление			
входо	в учізаписями ресурсов	печати политик	ами проце	CCOB Hakerob WD	соединении мэ	трафика с	ровнии	OC II	риложении и	s wanna		29 · P) · · · · P						
				NALPI ODM/							/ Гемствия			W0/1510				
		1		категории							Деиствия			фильтр		J		
ID 🗸	Время	Локальный а	Локаль	Внешний ад	Внешнее имя	Внешн	IP 8	Пр	Пользователь	Доступ	Деиствия	Процесс	PID	Событие	Отправлено	Получено	Правило	Результат
ID \\ 1	Время 17.04.2023 20:55:43	Локальный а 10.0.2.15	Локаль 60591	Внешний ад 77.88.55.60	Внешнее имя www.yandex	Внешн HTTPS	IP в IPv4	Пр ТСР	Пользователь John	Доступ 0 (Откры	деиствия атые данные)	Процесс C:\Program Files (	PID 2560	Событие Закрытие исх	Отправлено 57 Кб	Получено 81 Кб	Правило Автоматическ	Результат ОК
ID \\ 101 100	Время 17.04.2023 20:55:43 17.04.2023 20:55:38	Локальный а 10.0.2.15 10.0.2.15	Локаль 60591 60569	Внешний ад 77.88.55.60 77.88.55.60	Внешнее имя www.yandex www.yandex	Внешн HTTPS HTTPS	IP в IPv4 IPv4	Пр ТСР ТСР	Пользователь John John	Доступ 0 (Откры 0 (Откры	деиствия атые данные) атые данные)	Процесс C:\Program Files ( C:\Program Files (	PID 2560 2560	Событие Закрытие исх Закрытие исх	Отправлено 57 Кб 6 Кб	Получено 81 Кб 24 Кб	Правило Автоматическ Автоматическ	Результат ОК ОК
ID \ 1 1 0	Время 17.04.2023 20:55:43 17.04.2023 20:55:38	Локальный а 10.0.2.15 10.0.2.15	Локаль 60591 60569	Внешний ад 77.88.55.60 77.88.55.60	Внешнее имя www.yandex www.yandex	Внешн HTTPS HTTPS	IP в IPv4 IPv4	Пр ТСР ТСР	Пользователь John John	Доступ 0 (Откры 0 (Откры	деиствия атые данные) атые данные)	Процесс C:\Program Files ( C:\Program Files (	PID 2560 2560	Событие Закрытие исх Закрытие исх	Отправлено 57 Кб 6 Кб	Получено 81 Кб 24 Кб	Правило Автоматическ Автоматическ	Результат ОК ОК
ID \ 1 1 0	Время 17.04.2023 20:55:43 17.04.2023 20:55:38	Локальный а 10.0.2.15 10.0.2.15	Локаль 60591 60569	категории Внешний ад 77.88.55.60 77.88.55.60	Внешнее имя www.yandex www.yandex	Внешн HTTPS HTTPS	IP в IPv4 IPv4	Пр ТСР ТСР	Пользователь John John	Доступ 0 (Открь 0 (Открь	Деиствия итые данные) итые данные)	Процесс C:\Program Files ( C:\Program Files (	PID 2560 2560	Событие Закрытие исх Закрытие исх	Отправлено 57 Кб 6 Кб	Получено 81 Кб 24 Кб	Правило Автоматическ Автоматическ	Результат ОК ОК
ID \ 1 1 0	Время 17.04.2023 20:55:43 17.04.2023 20:55:38	Локальный а 10.0.2.15 10.0.2.15	Локаль 60591 60569	категории Внешний ад 77.88.55.60 77.88.55.60	Внешнее имя www.yandex www.yandex	Внешн HTTPS HTTPS	IP в IPv4 IPv4	Пр TCP TCP	Пользователь John John	Доступ 0 (Откры 0 (Откры	Деиствия итые данные) итые данные)	Процесс C:\Program Files ( C:\Program Files (	PID 2560 2560	Событие Закрытие исх Закрытие исх	Отправлено 57 Кб 6 Кб	Получено 81 Кб 24 Кб	Правило Автоматическ Автоматическ	Результат ОК ОК

Рисунок А.А.20. – Журнал соединений МЭ после настроек

#### ПРИЛОЖЕНИЕ Б

#### Пример настройки СЗИ НСД «Secret Net»

#### Установка «Secret Net Studio»

Установку компонентов «Secret Net Studio» можно выполнять при работе на компьютере как в локальной сессии, так и в терминальной. Установка любого компонента должна выполняться пользователем, входящим в локальную группу администраторов компьютера. С помощью программы управления следует подключиться к серверу безопасности и сформировать список устанавливаемого ПО и заданий развертывания. После этого на СБ (сервер безопасности) И компьютерах установка ΠО выполняется автоматически в фоновом режиме. При этом происходит оповещение о начале и завершении процесса установки, а после окончания установки выполняется перезагрузка компьютер.

1) Начало установки «Secret Net Studio» приведено на рисунках Б.1. иБ.2..C3И«Secret Net Studio»:ссылка на демо-версию(https://www.securitycode.ru/products/secret-net-studio/).

Дождитесь появления окна программы автозапуска и запустите установку с помощью команды «Защитные компоненты».



Рисунок Б.1. – Запуск «Secret Net Studio»

На экране появится диалог принятия лицензионного соглашения. Ознакомьтесь с содержанием лицензионного соглашения и нажмите кнопку «Принимаю».

Вас приветствует программа установки Secret Net Studio версии 8.5.5329.0.	
Пожалуйста, внимательно прочитайте лицензионное соглашение. Для продолжения установки необходимо принять лицензионное соглашение.	e
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ	
С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ ПО ИСПОЛЬЗОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ООО «КОД БЕЗОПАСНОСТИ»	
Редакция документ	а от <u>10.09.2015</u>
. ОБЩИЕ ПОЛОЖЕНИЯ	
астоящее лицензионное соглашение (далее - Соглашение) является Лицензионным Д бществом с ограниченной ответственностью «Код Безопасности», расположенным по Москва, Мурманский проезд, дом 14, корпус 1 (далее - Правообладатель), и вами, ользователь), правомерно владеющим экземпляром лицензионного программного о Код Безопасности» (далее - ЛПО).	Договором между адресу: 129075, , лицом (далее - беспечения ООО
ПО, производимое и распространяемое Правообладателем, - это комплекс прогр (окументации, которые являются объектами авторского права и охраняются законом од словом «Документация» подразумеваются печатные материалы и файлы с текст писание компонентов ЛПО и являющиеся его неотъемлемой частью.	оамм для ЭВМ и в Везде в тексте гом, содержащие
се права на интеллектуальную собственность в отношении ЛПО (равно как в от бновлений и дополнений, распространяемых Правооблателем для ЛПО), сключительные права на коры, алгоритимы и т.д., содержадилеся в нем, принадлежат и равообладателем и его лицензиарами. ЛПО защищено в соответствии конопательством. межлинародными соглашениями в области авторского по	тношении любых в том числе и сохраняются за с российским ава и другими

Рисунок Б.2. – Лицензионное соглашение

2) Последовательность выбора режима работы, загрузки ключа и компонентов защиты представлена на рисунках Б.3. ÷ Б.7. После выбора соответствующих параметров в окне действия подтверждаются и продолжаются нажатием кнопок «Далее»/ «Загрузить»/ «Открыть».

На экране появился диалог для выбора режима работы компонента.

Автономный режим	~	
	∨ Обновить	
ые ниже имя и пароль		
	Автономный режим ключения учетную запись текущег ые ниже имя и пароль	Автономный режим Обновить ключения учетную запись текущего пользователя ые ниже имя и пароль

Рисунок Б.З. – Выбор режима работы

В поле «Режим работы» укажите — «Автономный режим». Нажмите кнопку «Далее >». На экране появится диалог для выбора лицензий и формирования списка устанавливаемых защитных подсистем.

редъявите лицензию и становки.	выберите компоненты си	стемы	защиты	, которые будут включены	после	C.
РЕЖИМ РАБОТЫ 2 КОМПОНЕНТЫ		защи	ты	4 установка		
іля добавления лицензи	й нажмите кнопку "Загру	зить"	Загру	зить 🔻		
Компонент		Лицен	нзия	Примечание		
Базовая защита		Отсу	тствует	Обязательный компонент		
Дискреционное упра	вление доступом	Отсу	тствует			
Затирание данных		Отсу	тствует			
Контроль устройств		Отсу	тствует			
Замкнутая программ	ная среда	Отсу	тствует			
Полномочное управл	ение доступом	Отсу	тствует			
🗌 Контроль печати		Отсу	тствует			
Защита дисков и ши	фрование данных	OTCY	тствует			
Персональный межс	етевой экран	Отсу	тствует			
Обнаружение и пред	отвращение вторжений	OTCY	тствует			
Антивирус		Отсу	тствует			
Паспорт ПО		Отсу	тствует			
Доверенная среда		Отсу	тствует			

Рисунок Б.4. – Окно выбора компонентов защиты

Для загрузки ключа (лицензии) из файла — нажать кнопку «Загрузить» → «Из файла».

	The DAMMA		
ля добавления лицензий нажните кнопку "За	грузить*	Загрузить 🗸	T
Компонент	Лицен	С сервера безопасности Из файла	-
Базовая защита	Отсут	твует Обязательный компонент	
Дискреционное управление доступом	Отсуто	твует	
Затирание данных	Отсуто	твует	
Контроль устройств	Отсут	твует	
Замкнутая программная среда	Отсут	твует	
Полномочное управление доступом	Отсуто	твует	
Контроль печати	Отсуто	твует	
Защита дисков и шифрование данных	Отсут	твует	
Персональный межсетевой экран	Отсуто	твует	
Обнаружение и предотвращение вторжен	ий Отсут	твует	
Антивирус	Отсуто	твует	
Паспорт ПО	Отсуто	твует	
Доверенная среда	Отсут	твует	

Рисунок Б.5. – Загрузка ключа (лицензии)

🖲 Открытие				$\times$
	8_5 > sns_key ∨	õ	Поиск: sns_key	Q
Упорядочить 🔻 Нова	ая папка		8== -	2
	Имя		Дата изменения	Тип
Рабочий стол 🖈	KE000068297 14E68C_key.lic		24.10.2018 10:03	Файл
<ul> <li>Загрузки</li> <li>Документы</li> <li>Дображения</li> <li>Изображения</li> <li>Этот компьютер</li> <li>Рабочий стол</li> <li>Локальный диск (С</li> <li>DVD-дисковод (D:)</li> <li>Сеть</li> </ul>				
	<			>
Имя с	файла: КБ000068297 14E68C_key.lic	:	Открыть Отме	~ на

Выберите нужный файл в появившемся диалоге.

Рисунок Б.б. – Выбор файла для загрузки ключа

После загрузки данных в диалоге появятся сведения о лицензиях. Отметьте в списке устанавливаемые подсистемы, для которых имеются свободные лицензии (установку компонента "Базовая защита" отключить нельзя). При наличии нескольких групп лицензий для компонента можно выбрать нужную группу в раскрывающемся списке.

редъявите лицензию и вы становки.	берите компоненты си	істемы защиті	ы, которые будут включень	после	C
РЕЖИМ РАБОТЫ	2 компоненты	защиты	З параметры	4 установка	
іля добавления лицензий н	нажмите кнопку "Загру	зить" Загр	узить 👻		
Компонент		Лицензия	Примечание		
🛛 Базовая защита		15000 экз,.	• Обязательный компонент	r.	
Дискреционное управл	ение доступом	15000 экз,.	•		
🗹 Затирание данных		15000 экз,.	•		
И Контроль устройств		15000 экз,.			
Замкнутая программна	я среда	15000 экз,.			
Полномочное управлен	ние доступом	15000 экз,.			
Контроль печати		15000 экз,.	•		
🗹 Защита дисков и шифр	ование данных	15000 экз,.	•		
Персональный межсети	евой экран	15000 экз,.	•		
Обнаружение и предот	гвращение вторжений	Отсутствует	r -		
Антивирус		Отсутствует			
Паспорт ПО		Отсутствует			
🗌 Доверенная среда		Отсутствует			

Рисунок Б.7. – Выбор компонентов защиты

3) Процесс завершения установки «Secret Net Studio» последовательно приведен на рисунках Б.8. ÷ Б.12: для подтверждения и продолжения действий в соответствующем окне нажимаем кнопки «Готово»/ «Далее»/ «Закрыть». По завершению установки на экране блокировки компьютера появится логотип «Secret Net Studio».

После завершения действий, приведенных на рисунке Б.7., на экране появится диалог для выбора папки установки и настройки параметров подключений. В поле "Установить в папку" оставьте заданную по умолчанию папку установки или укажите другую папку назначения. При необходимости используются ссылки в разделе «Дополнительно» (по требованию).

адайте дополнительные	е параметры для установки системы	защиты.		
РЕЖИМ РАБОТЫ	2 компоненты защиты	3 параметры	4 установка	
/становить в папку:				
C: \Program Files \Secret Ne	t Studio\Client\	Обзор		
Дополнительно:				
Сохранить сценарий уста	ановки			
Ввести учетную информа	and the reserve and the part of the			
ввести учетную информа Выбрать пакеты исправл	тений для установки			

#### Рисунок Б.8. – Окно параметров установки

По окончании настройки параметров нажмите кнопку «Готово». Начнется процесс установки защитных подсистем в соответствии с заданными параметрами.

Secret Net Studio			×
Установка			
Дождитесь окончания уста	ановки. Это может занять нескольк	ю минут.	
1 режим работы	2 компоненты защиты	З параметры	4 установка
Создание точки восстанов	вления		
<ul> <li>Обновление хранилища д</li> </ul>	истрибутивов		
Secret Net Studio - Базо	овая защита		
🗸 Secret Net Studio - Локалы	ный центр управления		
🗸 Secret Net Studio - Локалы	ная защита		
Secret Net Studio - Контрол	ль печати		
🧹 Secret Net Studio - Защита	дисков и шифрование данных		
<ul> <li>Secret Net Studio - Сетева:</li> </ul>	я защита		
<ul> <li>Установка пакетов исправ</li> </ul>	влений		

## Рисунок Б.9. – Процесс установки

Secret Net Studio			×
Установка			
Дождитесь окончания устан	овки. Это может занять нескольк	ю минут.	
1 режим работы	2 компоненты защиты	З параметры	4 установка
<ul> <li>Создание точки восстановл</li> <li>Обновление хранилища дис</li> <li>Secret Net Studio - Базовая з</li> <li>Secret Net Studio - Локальнь</li> <li>Secret Net Studio - Локальна</li> <li>Secret Net Studio - Контроль</li> <li>Secret Net Studio - Защита д</li> <li>Secret Net Studio - Сетевая з</li> <li>Установка пакетов испр</li> </ul>	ения трибутивов ащита ий центр управления и аащита печати исков и шифрование данных защита жавлений		
			Далее

## Рисунок Б.10. – Завершение процесса установки

На экране появится завершающий диалог со сведениями о выполненных

операциях и предложением перезагрузить компьютер.



Рисунок Б.11. – Окно завершения установки

Проверьте состав подключенных к компьютеру устройств. Если подключены устройства, которые в дальнейшем должны быть запрещены к использованию — отключите их.

Перезагрузите компьютер и дождитесь загрузки системы.



Рисунок Б.12. – Экран блокировки после установки «Secret Net»

Итоговый состав компонентов:

– значок «Secret Net Studio» в области трея Windows;

– дополнительная вкладка «Secret Net Studio» в диалоговом окне настройки свойств ресурса (файла, папки или устройства);

 программа настройки подсистемы полномочного управления доступом;

– диалоговое окно «Управление Secret Net Studio» в Панели управления Windows;

- программа «Локальный центр управления»;

программа «Управление пользователями» (для настройки параметров локальных пользователей);

– программа «Контроль программ и данных» в локальном режиме работы.

#### Создание пользователя системы

Создание пользователя может выполняться как функциями ОС, так и с помощью СЗИ НСД. Процесс создания нового пользователя последовательно приведен на рисунках Б.13. ÷ Б.18: для подтверждения и продолжения действий в соответствующем окне нажимаем кнопку «Создать».

Открыть «Secret Net Studio» и войти в систему под учётной записью администратора. В меню «Пуск» ОС выбрать пункт «Управление пользователями» (см. рисунок Б.13.). Она предназначена для настройки параметров работы пользователей в системе защиты и позволяет выполнять действия как с доменными пользователями, так и с локальными. Далее перейти на вкладку «Управления параметрами безопасности пользователей» (см. рисунок Б.14.) → нажать кнопку «Добавить пользователя» в верхней части страницы, используйте предложенные варианты пользователей и групп, с разрешёнными правами → Создать → Пользователь.





DESKTOP-526S021	Имя /	Тип	Описание	Уровені
	🔐 Криптограф	Группа	Членам разрешено выполнение операций криптогра	
	🔐 Операторы	Группа	Операторы архива могут переопределять ограничени	
	😣 Операторы	Группа	Члены этой группы могут иметь некоторые админист	
	😣 Операторы	Группа	Члены этой группы могут удаленно запрашивать атр	
	😣 Опытные п	Группа	Категория опытных пользователей оставлена для обр	
	😣 Пользовате	Группа	Пользователи не имеют прав на изменение параметр	
	용 Пользовате	Группа	Члены этой группы могут запускать, активизировать	
	😣 Пользовате	Группа	Члены этой группы могут планировать ведение журн	
	😣 Пользовате	Группа	Члены данной группы имеют как местный, так и удал	
	용 Пользовате	Группа	Члены этой группы имеют право на выполнение удал	
	🚨 Пользовате	Группа	Члены этой группы могут получать доступ к ресурса	
	🚨 Репликатор	Группа	Поддержка репликации файлов в домене	
	🚨 Управляема	Группа	Члены этой группы управляются системой.	
	🎎 Читатели ж	Группа	Члены этой группы могут читать журналы событий с	
	🔏 DefaultAcco	Польз	Учетная запись пользователя, управляемая системой.	Неконф
	🔏 WDAGUtility	Польз	Учетная запись пользователя, которая управляется и	Неконф
	👗 windows	Польз		Неконф
	👗 Администр	Польз	Встроенная учетная запись администратора компьют	Неконф
	🐍 Гость	Польз	Встроенная учетная запись для доступа гостей к комп	Неконф
	< C	мена паро	ля	>
	G	войства		
	ر لا	далить		
	-			

Рисунок Б.14. – Окно управления параметрами безопасности пользователей

В открывшемся окне для нового пользователя – ввести имя пользователя и пароль, в описание можно добавить нужную информацию (например адрес электронной почты), подтвердить требование смены пароля.

Новый пользовате	аль Х
Пользователь:	stud
Полное имя:	stud
Описание:	
Пароль:	•
Подтверждение:	•
🗹 Требовать смену	у пароля при следующем входе пользователя
Отключить учет	тную запись
	Создать Отмена

Рисунок Б.15. – Окно добавления пользователя



Для добавленного пользователя произвести смену пароля.

Рисунок Б.16. – Вход от лица добавленного пользователя



Рисунок Б.17. – Сообщение о требовании изменения пароля



Рисунок Б.18. – Изменение пароля

## Настройка Политик безопасности

1) Загрузите OC Windows под учетной записью администратора.

2) Откройте "Локальный центр управления" ("Пуск → Все программы → Код Безопасности → Secret Net Studio → Локальный центр управления").
(см. рисунок Б.19.). Откроется окно центра управления в автономном режиме.
(см. рисунок Б.20.)



Рисунок Б.19. – Меню «Пуск», локальный центр управления



Рисунок Б.20. – Окно центра управления «Secret Net Studio»

Локальный центр управления – это плиточная панель настроек.

3) После запуска окна приложения выберите вкладку «НАСТРОЙКИ» (см. рисунок Б.21.). В левой части окна располагается список настроек по

разделам. В центральной части окна находятся параметры безопасности. Если нажать левой кнопкой мыши на знак «i», который располагается рядом с параметром, можно увидеть описания параметра (см. рисунок Б.22.).

🔳 Лока	альный режим : Secret Net Studio	- Центр управления				- 6	J X
$\equiv$	$\textcircled{\begin{tabular}{ccc} \hline \hline$					<ul> <li>✓</li> </ul>	
ھ	СОСТОЯНИЕ НАСТРОЙК	ИНФОРМАЦИЯ	💡 ЛИЦЕНЗИИ				
		21					
0	🖉 Шаблоны 👻	-					
8	политики	<u>_</u>	🛱 Базовая заш	ита			
	Базовая защита		• Вазовал защ	ma			
Ê	Вход в систему		Вход в систему				-
	Журнал						
	Теневое копирование		Максимальный период неактивности д	о блокировки	10		
T	Ключи пользователя		экрана		то минут		
16	Оповещение о тревог	ax					
$ \rightarrow $	Контроль RDP подклю	чений			Duran		
$\sim$	Администрирование с	истемы защиты	запрет вторичного входа в систему		ВКЛЮЧИТЬ		
> )	Локальная защита						
	Дискреционное управ	вление доступом	Реакция на изъятие идентификатора		Не блокировать		
I [	Затирание данных		·				
	Полномочное управл	ение доступом					
F9   1	Замкнутая программн	ая среда 🚽					-
<u>,</u> \_	• • • • • • • • • • • • • • • • • • •	•	<u>ال</u>				►
12						Применить	Отмена
	Тип Дата и время 🗸	Событие		Описание	:		49/50 ^
	09.04.2023 18:11:14	Запрос конфигурации		Конфигура	ация загружена.		
$\int_{0}^{\infty}$	09.04.2023 18:10:32	Запрос конфигурации		Конфигура	ация загружена.		
e 6//	09.04.2023 18:10:32	Открытие сессии в ло	кальном режиме.	Запрос отп	правлен агенту.		
EV / -	09.04.2023 18:10:32	Открытие сессии в ло	кальном режиме.	Сессия отк	срыта.		
. m		Закрытие сессии.		Сессия зак	правлен агенту.		
/¥	09.04.2023 18:09:33	Запрос конфигурации	h	Конфигура	ация загружена.		
					and a province	Окно событий 🔗	80 0

#### Рисунок Б.21. – Окно настройки



Количество попыток аутентификации не ограничено

## Рисунок Б.22. – Кнопка информация ((«i») в окне приложения

4) Выберите интересующую группу из раздела «Политики» в левой части окна приложения. Политики безопасности в «Secret Net Studio» разделены на группы (модули).

#### Настройка модуля «Базовая защита»

Базовая защита («Вход в систему», «Журнал», «Теневое копирование», «Оповещение о тревогах», «Контроль «Ключи пользователя», RDP подключений», «Администрирование системы защиты») — объединяет параметры функционирования механизмов базовой защиты клиента. Перейдите в группу «Базовая защита» и выполните настройки в соответствии заданием. Последовательная настройка модуля «Базовая с защита» представлена на рисунках Б.23. ÷ Б.39., для фиксации настроек в системе после выбора параметров нажать кнопку «Применить» в правом нижнем углу окна приложения.

#### Вход в систему

политики	👼 Базовая зашита		
Базовая защита	S Dabo Dan Da Anta		
Вход в систему	Вход в систему		Аудит
Журнал			
Теневое копирование	Максимальный период неактивности до блокировки		
Ключи пользователя	экрана	15 минут	
Оповещение о тревогах			
Контроль RDP подключ			
Администрирование си	Запрет вторичного входа в систему	Включить	(I)
Локальная защита			
Дискреционное управл	Реакция на изъятие идентификатора	Не блокировать	- (i)
Затирание данных	·		
Полномочное управлен			
Замкнутая программная 👻			
•	Количество неудачных попыток аутентификации	3 🚔 попытки	(i)
		Данные изменены Применит	ь Отмена

### Рисунок Б.23. – Настройка входа в систему

=	политики		👼 Базовая зашита			
	Базовая защита		• BaseBan Ballina			
	Вход в систему		Вход в систему		Аудит	4
	Журнал		······································	3 попытки		
	Теневое копирование					
	Ключи пользователя					
	Оповещение о тревогах		Режим идентификации пользователя	Смешанный 👻	i	
	Контроль RDP подключ					
	Администрирование си					
	Локальная защита		Режим аутентификации пользователя	• Стандартная аутентификация		
	Дискреционное управл		, crani cy comprised in the second		U	
	Затирание данных			О Эсиленная аутентификация по паролю		
	Полномочное управлен			данные		
	Замкнутая программная	Ŧ				
•	• • • • • • • • • • • • • • • • • • •					٦
				Данные изменены Применить	Отмена	]

Рисунок Б.24. – Настройка входа в систему: режим идентификации и аутентификации пользователя

Вход в систему	Вход в систему		Аудит
Журнал			
Теневое копирование			
Ключи пользователя	Парольная политика	Брать значения из парольной политики Windows	i
Оповещение о тревога	Политика активна, если в эффективной политике клиента включен режим «усиленная аутентификация по паролю»	• Задать свои значения	
Контроль RDP подключ		Минимальная длина пароля:	
Администрирование си		П не ограничена	
Покальная защита			
Дискреционное управл		• не менее 6 символов (от 1 до 16)	
Затирание данных			
Полномочное управлен		Срок действия пароля:	
Замкнутая программна 👻		неограниченный	
►			

## Рисунок Б.25. – Настройка входа в системы: парольная политика

•	ПОЛИТИКИ Базовая защита	Î	🐯 Базовая защита			
	Вход в систему Журнал Теневое копирование Ключи пользователя Оповещение о тревога: Контроль RDP подключ Администрирование си Локальная защита		Вход в систему	Срок действия пароля: неограниченный не более 60 дней (от 1 до 999) Сложность пароля:	Аудит	
< ■	Дискреционное управл Затирание данных Полномочное управлен Замкнутая программна	Ŧ	Оповещение пользователя	Рекомендуем установить минимальную длину пароля не менее 6 символов Оповещение пользователя о последнем успешном	(i)	-
				Данные изменены Применить	Отмена	1

Рисунок Б.26. – Настройка входа в системы: парольная политика, продолжение

	ПОЛИТИКИ Базовая защита		🐯 Базовая защита			
	Вход в систему		Вход в систему		Аудит	
	Журнал					
	Теневое копирование			Сложность пароля:		
	Ключи пользователя			с ограничениями на содержание символов		
	Оповещение о тревога:			Рекомендуем установить минимальную длину		
	Контроль RDP подключ	1		пароля не менее 6 символов		
	Администрирование си					
	Локальная защита					
	Дискреционное управл		Оповещение пользователя	<ul> <li>Оповещение пользователя о последнем успешном входе в систему</li> </ul>	(i)	
	Затирание данных			Предупреждение пользователя о мерах защиты		
	Полномочное управлен			информации до входа в систему		
	Замкнутая программна	Ŧ				
٠	• • • •					Ŧ
				Данные изменены	Отмена	

Рисунок Б.27. – Настройка входа в системы: оповещение пользователя



Рисунок Б.28. – Уведомление о принятых мерах защиты на экране блокировки

### Настройка журнала

🛛 👘 🛣 Базовая зашита	
азовая защита	
Вход в систему Журнал	
Журнал	
Теневое копирование Максимальный размер журнала системы защит	ы 2240 K5
Ключи пользователя	
Оповещение о тревогах	
Контроль RDP подключи	-
Администрирование си-	По достижении максимального размера журнала:
Іокальная защита	<ul> <li>Затирать события по мере необходимости</li> </ul>
Дискреционное управл	<ul> <li>Затирать события старее: 3 дней</li> </ul>
Затирание данных	
Полномочное управлен	Не затирать события (очистка журнала вручную)
Замкнутая программная 👻	
	BUILTIN\Администраторы

Рисунок Б.29. – Настройка журнала: максимальный размер журнала системы защиты, политика перезаписи событий

-	политики	🗎 🐯 Базовая защита					
	Базовая защита		Вазовал защина				
	Вход в систему		Журнал			1	
	Журнал		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	PLULTING A second second second			
	Теневое копирование		Учетные записи с привилегией просмотра журнала	вотстичадминистраторы		(i)	
	Ключи пользователя		системы защиты				
	Оповещение о тревогах						
	Контроль RDP подключ	-					
	Администрирование си						
	Локальная защита				( <del>+</del> )		
	Дискреционное управл				00		
	Затирание данных		Учетные записи с привилегией управления журналом системы защиты	BUILTIN\Администраторы		$(\mathbf{i})$	
	Полномочное управлен						
	Замкнутая программная	Ŧ					
	•						Ŧ
				Данные изменены	Применить	Отмена	1

Рисунок Б.30. – Настройка журнала: учётные записи с привилегией просмотра и управления журнала системы защиты

#### Настройка теневого копирования

-	политики		🖾 Базовая защита			
	Базовая защита		С вазовал защита			
	Вход в систему		Теневое копирование		Аудит	4
	Журнал					
	Теневое копирование		Размер хранилища	Укажите количество дискового пространства, отводимое для хранилища подсистемы теневого копирования.	(i)	
	Ключи пользователя			Размер задается в процентах от размера раздела, на		
	Оповещение о тревогах			котором размещено хранилище.		
	Контроль RDP подключ			5% 80%		
	Администрирование си			20%		
	Локальная защита			<ul> <li>Автоматически перезаписывать старые данные</li> </ul>		I
	Дискреционное управл			при переполнении хранилища		ľ
	Затирание данных					
	Полномочное управлен		Ключи пользователя		Аудит	
	Замкнутая программная	Ŧ				
<	• •		M	360		1
				Данные изменены Применить	Отмена	1

Рисунок Б.31. – Настройка теневого копирования

#### Настройка ключей пользователя

ПОЛИТИКИ	🐯 Базовая защита					
Вход в систему	Ключи пользователя				Аудит	
Журнал						
Теневое копирование	Максимальный срок действия ключа	60	дней		(j)	
Ключи пользователя	4		Anen			
Оповещение о тревогах						
Контроль RDP подключ	Минимальный срок действия ключа	7	дней		<u>Аудит</u> (j (j	
Администрирование си						
Локальная защита						
Дискреционное управл	Предупреждение об истечении срока действия ключа	3	дня		(j)	
Затирание данных						
Полномочное управлен						
Замкнутая программная 🔻	Оповещение о тревогах					
•						Ŧ
		Да	нные изменены	Применить	Отмена	٦

Рисунок Б.32. – Настройка ключей пользователя

Настройка оповещения о тревогах



Оповещение о тревогах

Локальное оповещение о тревогах

Определяется пользователем

i

Рисунок Б.33. – Настройка оповещения о тревогах

Настройка контроля RDP подключений

## 🐯 Базовая защита

Контроль RDP подключений					.4
Перенаправление устройств в RDP-подключениях	СОМ-портов	Запрещено	*	(j)	
	LPT-портов	Запрещено	•		
	Дисков	Запрещено	•		
	Устройств Plug and Play	Запрещено подключать удал	*		
Перенаправление буфера обмена в RDP-подключениях	Запрещено		•	(j)	
	Данные изменены Применит			Отмена	1

Рисунок Б.34. – Настройка контроля RDP подключений

# 🐯 Базовая защита

Контроль RDP подключений			
Перенаправление буфера обмена в RDP-подключениях	Запрещено	Ŧ	i
Перенаправление принтеров в RDP-подключениях	Запрещено	•	i

# Рисунок Б.35. – Настройка контроля RDP подключений, продолжение

Настройка администрирования системы защиты

# 🐯 Базовая защита

Администрирование системы защиты		Аудит
Самозащита продукта	И Включить	(j)
	Включить контроль административных привилегий После изменения политики потребуется перезагрузка	
PIN администратора	Изменить	(j)
Учетные записи с привилегией управления механизмом самозащиты	BUILTIN\Администраторы	(j)
	Данные изменены Применить	Отмена

Рисунок Б.36. – Настройка администрирования системы защиты

#### Подтверждение

?

При включенном контроле административных привилегий для изменения параметров системы защиты необходим ввод PIN администратора. Перед включением контроля рекомендуется сменить PIN администратора в политике «Администрирование системы защиты». Хотите продолжить?

Да	Нет
~~~ I	

Рисунок Б.37. – Настройка администрирования системы защиты: предупреждение о необходимости PIN

# 🐯 Базовая защита

Администрирование системы защиты		Аудит
Самозащита продукта	<ul> <li>Включить</li> </ul>	(j)
	<ul> <li>Включить контроль административных привилегий</li> <li>После изменения политики потребуется перезагрузка</li> </ul>	
PIN администратора	Изменить	(j)
Учетные записи с привилегией управления механизмом самозащиты	BUILTIN\Администраторы	(i)
	Данные изменены Применить	Отмена

Рисунок Б.38. – Настройка администрирования системы защиты, продолжение

## 🐯 Базовая защита

Администрирование системы защиты			Аудит	4
PIN администратора	Изменить		i	
Учетные записи с привилегией управления механизмом самозащиты	BUILTIN\Администраторы		i	
		<b>(</b>		ļ
	Данные изменены	Пріхенить	Отмена	•

Рисунок Б.39. – Настройка администрирования системы защиты, завершение

#### Настройка модуля «Локальная защита»

Локальная защита («Дискреционное управление доступом», «Затирание данных», «Полномочное управление доступом», «Замкнутая программная среда», «Защита диска и шифрование данных») — объединяет параметры функционирования механизмов локальной защиты клиента. Перейдите в группу «Локальная защита» и выполните настройки в соответствии с заданием. Последовательная настройка модуля «Локальная защита» представлена на рисунках Б.40. ÷ Б.49., для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.



#### Рисунок Б.40. – Выбор настройки локальной защиты

Настройка дискреционного управления доступом

## 🗟 Локальная защита



Рисунок Б.41. – Настройка дискреционного управления доступом

Предоставление привилегии для изменения прав доступа на любых ресурсах и назначение администраторов ресурсов. Для параметра «Учетные записи с привилегией управления правами доступа» отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.

Настройка затирания данных

## 🐯 Локальная защита

Затирание данных		Аудит
Количество циклов затирания на локальных дисках	9	i
Количество циклов затирания на сменных носителях	9	i
Количество циклов затирания оперативной памяти	2	i
Количество циклов затирания по команде "Удалить безвозвратно"	9	i
	Данные изменены Применить	Отмена

Рисунок Б.42. – Настройка затирания данных

Укажите нужные значения для параметров затирания. Если параметру присвоено значение «0», затирание не выполняется. Для гарантированного уничтожения данных в большинстве случаев достаточно 2 проходов затирания (для государственных организаций предусмотрено не менее 7). Для просмотра справочной информации о параметре нажмите кнопку «i».

## 🐯 Локальная защита

Затирание данных		Аудит	d
Количество циклов затирания при уничтожении данных на дисках	9	i	ļ
Список исключений	%WINDIR% (> `   * ?	i	
	Путь		
			,
	Данные изменены Применить	Отмена	1

Рисунок Б.43. – Настройка затирания данных, продолжение

Для добавления объекта в список исключений укажите полный путь к объекту и нажмите кнопку . При необходимости используйте переменные среды окружения из раскрывающегося списка, нажав кнопку . Для изменения пути к объекту выберите его в списке исключений и нажмите кнопку ; • для удаления объекта из списка исключений нажмите кнопку .

Настройка полномочного управления доступом

# 🗟 Локальная защита

Полномочное управление доступом		Аудит	4
Названия уровней конфиденциальности	Неконфиденциально	i	
	Конфиденциально		
Строго конфиденциально			
Режим работы	<ul> <li>Контроль потоков отключен</li> <li>Контроль потоков включен</li> </ul>	i	
	Данные изменены Применить	Отмена	1

Рисунок Б.44. – Настройка полномочного управления доступом

В механизме полномочного управления доступом используется принцип наследования категорий конфиденциальности. Методы наследования различаются в зависимости от типов ресурсов. Устройства наследуют категорию конфиденциальности от классов, к которым они относятся. При этом для класса разрешено указывать только категорию для общедоступной информации (по умолчанию — «Неконфиденциально») или включить режим доступа «без учета категории конфиденциальности». За счет этого исключается возможность копирования конфиденциальной информации на неразрешенное подключенное устройство (при работе механизма в режиме контроля потоков и отсутствии у пользователя привилегии на вывод конфиденциальной информации).

### 🕸 Локальная защита

Полномочное управление доступом		Аудит
Режим работы	Контроль потоков отключен	(j)
	• Контроль потоков включен	
	<ul> <li>Строгий контроль терминальных подключений</li> </ul>	
	<ul> <li>Автоматический выбор максимального уровня сессии</li> </ul>	
	После изменения политики потребуется перезагрузка	

# Рисунок Б.45. – Настройка полномочного управления доступом, продолжение

#### Настройка замкнутой программной среды

## 🐯 Локальная защита

Замкнутая программная среда			Аудит
Учетные записи, на которые не действуют правила замичитой прогламичой спелы	BUILTIN\Администраторы		i
Summing on the pumming spectre			
		(+)	

Рисунок Б.46. – Настройка замкнутой программной среды

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии (скрипты).

Настройка защиты диска и шифрования данных

#### 🐯 Локальная защита

Защита диска и шифрование данных			Аудит	1
Учетные записи с привилегией на создание	BUILTIN\Администраторы		i	
криптоконтейнера	BUILTIN\Пользователи			
		<b>(</b>		
				2
	Данные изменены	Применить	Отмена	

Рисунок Б.47. – Настройка защиты диска и шифрования данных

			-		
кальные диски		Хранение данных восс	тановле	ния: лок	аль
🔓 Зашифровать	🔍 Сменить ключ				
циох Новый тон (Е:) ) (С:) Новый том (F:) \\?\Volume(6a8b649a-0a58-497a-9eff-0f66df1aa340) Восстановить	Статус Зашифрован Не зашифрован Не зашифрован Не поддерживается Не поддерживается	Ключ шифрования 08.02.2021 20:30:54			
Сменить пароль					
Сменить пароль Для доступа ко всем жестким дискам задается од	цин пароль				

Рисунок Б.48. – Мастер шифрования дисков Secret Net Studio



Рисунок Б.49. – Загрузчик Secret Net Studio (запрос пароля для доступа к зашифрованному диску)

### Настройка модуля «Сетевая защита»

Сетевая защита («Персональный межсетевой экран») — объединяет параметры функционирования механизмов сетевой защиты клиента. Перейдите в группу «Сетевая защита» и выполните настройки в соответствии с заданием. Последовательная настройка модуля «Сетевая защита» представлена на рисунках Б.50. ÷ Б.56., для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.

Контроль RDP подключ	濛(	Сетевая защ	ита				
Локальная защита	Персо	ональный межсете	вой экран				
Дискреционное управля Затирание данных	Правил	а доступа	·				
Полномочное управлен	Правила, регламентирующие доступ к <u>сетевым сервисам</u> (TCP/IP v4) данного компьютера.						
Замкнутая программная Защита диска и шифров	Вкл	Субъект	Сетевой сервис	Тип доступа	Направление	Удаленный адре	
Сетевая защита	~	everyone Secret Net Studio	DNS-sanpoc	Разрешен	Исходящее	*	
Персональный межсете Контроль устройств	~	everyone Secret Net Studio	DHCP-ответ	Разрешен	Входящее	*	
Контроль печати	~	everyone Secret Net Studio	DHCP-sanpoc	Разрешен	Исходящее		
Антивирус	~	everyone Secret Net Studio	NetBIOS (служба имен)	Разрешен	Входящее	*	
•		auaniana Sacrat Nat Studia	NotDIOS (calorfo approxim)	Daapaulou	Prostilico		

# Рисунок Б.50. – Настройка персонального межсетевого экрана: правила доступа

## 🐯 Сетевая защита

Персональный межсетевой экран							
Настройки							
Протоколы				(i)	l		
Протокол	Доступ	Аудит	По умолчанию		ľ		
Internet Protocol, version 4(IPv4)	~	~					
Internet Protocol, version 6(IPv6)							
Novell IPX							
Протоколы с устаревшим форматом Ethernet-кадра							
					-		

# Рисунок Б.51. – Настройка персонального межсетевого экрана: настройка протоколов

## 🐯 Сетевая защита

Пе	Персональный межсетевой экран									4
Hac	тройки									
	Разрешить следующие типы ІСМР-(	сооби	цений:							
	Описание	Ŧ	Тип 🔻	Код 🔻	Получение	Отправка		Добавить		i.
	Эхо-ответ		0	Любой	~					
	Адресат недоступен		3	Любой	~	~			1	
	Перенаправление		5	Любой			Ľ			
	Альтернативный адрес узла		6	Любой						
	Эхо-запрос		8	Любой		~	١.,			-
					Данные	изменены		Применить	Отмена	1

Рисунок Б.52. – Настройка персонального межсетевого экрана: типы ICMP-сообщений

#### Настройки

Перенаправление	5	Любой			По умолчанию
Альтернативный адрес узла	6	Любой			
Эхо-запрос	8	Любой		~	
Ходатайство маршрутизатора	10	Любой	~	~	
Превышение временного интервала	11	Любой	~		-

Заблокировать остальные типы ICMP-сообщений

# Рисунок Б.53. – Настройка персонального межсетевого экрана: типы ICMP-сообщений, продолжение

Контроль RDP подключ	🐯 Сетевая защита		
Локальная защита	Персональный межсетевой экран		-
Дискреционное управля Затирание данных	Режим обучения		
Полномочное управлен	• Выключен	(j	
Замкнутая программная			
Защита диска и шифров	О Постоянное обучение с		
Сетевая защита Персональный межсете	Задать интервал обучения: 09.04.2023 21:03 ▼ - 16.0	4.2023 21:03 💌	1
Контроль устройств Контроль печати	<ul> <li>Активировать правила после окончания обучения</li> </ul>		
Антивирус	Направление	<ul> <li>Входящие</li> <li>Исходящие</li> <li>По умолчанию</li> </ul>	
∧ć		40000	

Рисунок Б.54. – Настройка персонального межсетевого экрана: режим обучения

# 🐯 Сетевая защита

#### Персональный межсетевой экран

			-
Направление	<ul> <li>Входящие</li> </ul>	<ul> <li>Исходящие</li> </ul>	По умолчанию
Максимальное количество генерируемых правил	10000	10000	
Максимальное количество генерируемых правил для приложения	15	15	
Сохранить информацию о процессе	•	~	
Сохранить информацию об адресах локального хоста	~	~	

Рисунок Б.55. – Настройка персонального межсетевого экрана: режим обучения, продолжение

# 🐯 Сетевая защита

Персональный межсетевой экран

Режим обучения							
сохранить информацию оо адресах локального хоста	v	v					
Сохранить информацию о портах локального хоста	~	✓					
Сохранить информацию об адресах удаленного хоста	~	✓					
Сохранить информацию о портах удаленного хоста	✓	~					

Рисунок Б.56. – Настройка персонального межсетевого экрана: режим обучения, завершение

#### Настройка модулей «Контроль устройств» и «Контроль печати»

Контроль устройств — содержит параметры функционирования механизмов контроля подключения и изменения устройств и разграничения доступа к устройствам; контроль печати — содержит параметры для настройки маркировки документов, теневого копирования, списка используемых принтеров и политик прямой печати. Перейдите в группы «Контроль устройств» и «Контроль печати» и выполните настройки в соответствии с заданием. Последовательная настройка модулей «Контроль устройств» и «Контроль печати» и выполните настройки в соответствии с заданием. Последовательная настройка модулей «Контроль устройств» и «Контроль печати» представлена на рисунках Б.57. ÷ Б.63, для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.

	Затирание данных	\land Контроль устройств					
	Замкнутая программная	Настройки	Аудит				
	Защита диска и шифрое Сетевая защита Персональный межсете	Теневое копирование Определяется настройками устройства 💌					
	Контроль устройств						
	Контроль печати Антивирус	Устройства	Аудит				
	Обнаружение вторжений Обновление		i				
	Паспорт ПО	🕂 🗴 🖉 🗇 🗋 🕞 🚠 🔲 🎼 Колонки таблицы т					
•	РЕГИСТРАЦИЯ СОБЫТИЙ 🖵	Устройства Параметры контроля	Параметр				
		Применить					

Рисунок Б.57. – Настройка контроля устройств: настройки (теневое копирование)

Механизм теневого копирования предназначен для создания в системе дубликатов данных, выводимых на отчуждаемые носители информации. Действие механизма распространяется на те устройства, для которых включен режим теневого копирования.

	Затирание данных 🔶 Полномочное управлен	🚓 Контроль устройств	Í
	Замкнутая программная	Настройки	Аудит
	Сетевая защита Персональный межсете	Теневое копирование Определяется настройками устройства 👻	i
	Контроль устройств		
	Контроль печати Антивирус	Устройства	Аудит
	Обнаружение вторжений Обновление		i
	Паспорт ПО	🕂 💼 🥒 🕞 🖆 🕞 🚠 🔲   ↓ Колонки таблицы 👻	
•	РЕГИСТРАЦИЯ СОБЫТИЙ 🚽	Устройства Параметры контроля	Параметр
		Применить	

Рисунок Б.58. – Настройка контроля устройств: теневое копирование, продолжение

Для параметра «Теневое копирование» укажите нужное значение: «Отключено для всех устройств» — теневое копирование при записи информации на устройства не выполняется; «Определяется настройками устройства» — теневое копирование выполняется для устройств с включенным режимом теневого копирования.

# 🖍 Контроль устройств

Устройства			Аудит		
			i		
+ 🗊 🖉 🔂 🗇 🛧 🔳 📖 Колони	ки таблицы 👻				
Устройства	Параметры контроля	0 0	Параметры		
😑 📀 🍠 Последовательные порты	Наследуются (Постоянно подключен	Ø	;		
🐵 🍠 Последовательный порт (COM1)	🐵 🝠 Последовательный порт (COM1) Постоянно подключено (без блокир 🤨				
💿 🍠 Параллельные порты	Наследуются (Постоянно подключен	Ø	¢		
4			Þ		
	Данные изменены	Трименить	Отмена		

Рисунок Б.59. – Настройка контроля устройств: устройства

Загрузите список устройств. — Выберите строку с нужным элементом (группа, класс, модель, устройство). — При необходимости введите

дополнительные сведения об элементе в ячейке колонки «Комментарий»: для этого нажмите кнопку в правой части ячейки. → Примечание: по умолчанию колонка «Комментарий» не отображается. Для включения отображения нажмите кнопку «Колонки таблицы», которая расположена над списком устройств. Дополнительные сведения, указанные для устройства, сохраняются в журнале при регистрации событий, связанных с этим устройством. → Укажите нужные параметры в ячейке колонки «Параметры контроля». Для этого нажмите кнопку в правой части ячейки. Если для данного объекта требуется отключить наследование параметров от вышестоящего объекта и явно задать политику контроля, удалите отметку из поля «Наследовать настройки контроля от родительского объекта» и настройте параметры контроля.

В локальной политике в список устройств автоматически добавляются все обнаруженные устройства компьютера. Также в этот список помещаются сведения об устройствах, подключенных на терминальных клиентах данного компьютера во время терминальных сессий. Подключенные в данный момент устройства отображаются в нормальном виде, отключенные — с зачеркнутыми именами.

Для удобного просмотра списка устройств и оперативного получения основных сведений о текущей конфигурации параметров предусмотрены специальные пиктограммы статуса, перечисленные в таблице Б.1..

Пиктограмма	Описание
0	Параметры контроля для устройства наследуются от вышестоящего элемента списка устройств
🔘 (серый цвет)	Режим контроля для устройства отключен
۲	Для устройства включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру
😑 (зеленый цвет)	Для устройства включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать
兽 (красный цвет)	Для устройства включен режим контроля, при котором устройство запрещается подключать к компьютеру

Таблица Б.1. – Пиктограммы статуса

Управление принтерами осуществляется в программе управления Secret Net Studio, которая может устанавливаться как отдельный компонент «Secret Net Studio — Центр управления» — для работы в централизованном режиме или как составная часть клиента Secret Net Studio — для работы в локальном режиме. Для компьютеров с установленным клиентом в автономном режиме функционирования недоступны возможности управления с использованием групповых политик.

Локальная защита Дискреционное управл Затирание данных	嶜 Контроль печ	ати	
Полномочное управлен	Настройки		Аудит
Замкнутая программная Защита диска и шифров	Маркировка документов	Отключена -	(j)
Сетевая защита		Вид маркировки: По умолчанию	
Персональный межсете		$\bigcirc \bigcirc \bigcirc$	
Контроль устройств		00	
Контроль печати		Приложения, включенные в расширенную обработку	
Антивирус			
Обнаружение вторжений	Теневое копирование	Отключено для всех принтеров 👻	(i)
Обновление			
Паспорт ПО 🚽			
•	Принтеры		Аулит
		Применить	

Рисунок Б.60. – Настройка контроля печати: настройки

Локальная защита	A	🗟 Контроль пецати	
Дискреционное управл			
Затирание данных		Harran Xuu	A
Полномочное управлен		пастроики	Аудит
Замкнутая программная			
Защита диска и шифров		Маркировка документов Стандартная обработка 👻	0
Сетевая защита		Вид маркировки: По умолчанию	
Персональный межсете		$\bigcirc \bigcirc \bigcirc \bigcirc$	
Контроль устройств			
Контроль печати		Приложения, включенные в расширенную обработку	
Антивирус			
Обнаружение вторжений		Теневое копирование Определяется настройками принтера 🔹	(i)
Обновление			
Паспорт ПО	Ŧ		
•		Принтеры	Аулит
		Данные изменены Применить	Отмена

Рисунок Б.61. – Настройка контроля печати: настройки, продолжение

Локальная защита	🔄 🙀 Контроль п	іечати			
Затирание данных	Принтеры				Аудит
Замкнутая программная Защита диска и шифрог					i
Сетевая защита	+ 🗊				
Контроль устройств	Имя принтера	Имя компьютера	Категории конфиденциаль	ности 🥝 🗓	
Контроль печати Антивирус	настроики по умолчанию		Любой категорий		
Обнаружение вторжений					
Паспорт ПО					
	B.J.	Д	анные изменены	Применить	Отмена

Рисунок Б.62. – Настройка контроля печати: принтеры

Список принтеров изначально состоит из одного элемента «Настройки по умолчанию». Параметры использования принтеров, заданные для этого элемента, применяются ко всем принтерам, кроме тех, которые в явном виде присутствуют в списке принтеров. Добавление принтеров в список политики осуществляется с помощью специальной программы-мастера. Явно заданные параметры для конкретных принтеров имеют приоритет перед параметрами элемента «Настройки по умолчанию».

Локальная защита Дискреционное управл	嶜 Контроль печати	
Затирание данных Полномочное управлен	Прямая печать	Аудит
Замкнутая программная Защита диска и шифров	Включить политику контроля прямой печати	i
Сетевая защита	Политика контроля прямой печати	
Персональный межсете	Путь к исполняемому файлу 🔻 Все устройства разрешены 🔻 Разрешенные устройства	
Контроль устройств		1
Контроль печати		
Антивирус		
Обнаружение вторжений		
Обновление		
Паспорт ПО 🚽		
• • •		
	Данные изменены Применить	Отмена

Рисунок Б.63.- Настройка контроля печати: прямая печать

Политики контроля прямого вывода на печать определяют процессы (приложения), которым разрешен прямой вывод на печать, минуя запрет на это действие.

#### Настройка модулей «Антивирус» и «Обнаружение вторжений»

Антивирус — содержит параметры для настройки постоянной защиты, режимов сканирования, списка исключений и сканирования по расписанию; обнаружение вторжения — содержит параметры для настройки детекторов сетевых атак и сигнатурных анализаторов. Перейдите в группы «Антивирус» и «Обнаружение вторжений» и выполните настройки в соответствии с заданием. Последовательная настройка модуля «Антивирус» представлена на рисунках Б.64. ÷ Б.72.. Последовательная настройка модуля «Обнаружение вторжений» представлена на рисунках Б.73. ÷ Б.80.. Для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.

Затирание данных	Постоянная защита		Аудит.
Замкнутая программна: Защита диска и шифрог Сетевая защита Персональный межсете Контроль устройств Контроль печати	Настройки постоянной антивирусной защиты, применяемые для сканирования файлов, к которым осуществляется доступ.	<ul> <li>Максимальная защита (проверка сигнатур, углубленная звристи</li> <li>Оптимальная защита (проверка сигнатур, звристика в обычном</li> <li>Быстрое сканирование (только проверка сигнатур)</li> <li>Пользовательская</li> <li>Отключена</li> </ul>	(i)
Антивирус Обнаружение вторжений Обновление Паспорт ПО	Действия при обнаружении зараженных файлов:	<ul> <li>Лечить зараженные файлы</li> <li>Удалять зараженные файлы</li> <li>✓ Удаляемые файлы поместить в карантин</li> </ul>	

## Рисунок Б.64. – Настройка антивируса: постоянная защита

Локальная защита Дискреционное управл	*	🛞 Антивирус		
затирание данных		Постоянная защита		Аудит
Замкнутая программная		Настройки постоянной антивирусной защиты,	• Максимальная защита (проверка сигнатур, углубленная эвристи	(j)
Защита диска и шифров	ni.	применяемые для сканирования файлов, к которым осуществляется доступ.	Оптимальная защита (проверка сигнатур, эвристика в обычном	
Сетевая защита			Быстрое сканирование (только проверка сигнатур)	
Персональный межсете				
Контроль устройств			Пользовательская	
Контроль печати			Отключена	
Антивирус		Действия при обнаружении	<ul> <li>Лечить зараженные файды</li> </ul>	
Обнаружение вторжений		зараженных файлов:		
Обновление			<ul> <li>Удалять зараженные фаилы, если не удалось лечение</li> </ul>	
Паспорт ПО	-		<ul> <li>Удаляемые файлы поместить в карантин</li> </ul>	
•				
			Данные изменены Применить	Отмена

Рисунок Б.65. – Настройка антивируса: постоянная защита, продолжение

Локальная защита 🔺 Дискреционное управл	🛞 Антивирус		
Затирание данных	Сканирование подключаемых носителей		Аудит
Полномочное управлен			
Замкнутая программная	при их подключении к защищаемому	• сканировать подолочаемые посители	U
Защита диска и шифров	компьютеру.		
Сетевая защита	Эвристика:	<ul> <li>Углубленная эвристика</li> </ul>	
Персональный межсете			
Контроль устройств			
Контроль печати		Выключена	
Антивирус	Исключения по файлам:	Пропускать архивы	
Обнаружение вторжений			
Обновление		Пропускать файлы более 500 МБ	
Паспорт ПО 🚽		<ul> <li>Проверять только файлы с расширениями:</li> </ul>	
•			
		Данные изменены Применить	Отмена

Рисунок Б.66. – Настройка антивируса: сканирование подключаемых носителей

Локальная защита Дискреционное управл	*	🛞 Антивирус		
Затирание данных		Сканирование подключаемых носителей		Аудит
Полномочное управлен				
Замкнутая программная		Исключения по фаилам:	Пропускать архивы	
Защита диска и шифров			Пропускать файлы более 500 МБ	
Сетевая защита			<ul> <li>Проверять только файлы с расширениями:</li> </ul>	
Персональный межсете				
Контроль устройств				
Контроль печати			Пример ввода: .ext,.ext2,.ext3	
Антивирус		Действия при обнаружении	<ul> <li>Лечить зараженные файлы</li> </ul>	
Обнаружение вторжений		зараженных файлов:		
Обновление			• Удалята зараженные файлы, сели не удалось лечение	
Паспорт ПО	-		<ul> <li>Удаляемые файлы поместить в карантин</li> </ul>	
•		17		
			Данные изменены Применить	Отмена

# Рисунок Б.67. – Настройка антивируса: сканирование подключаемых носителей, продолжение



# Рисунок Б.68.– Настройка антивируса: контекстное сканирование



Рисунок Б.69. – Настройка антивируса: полное сканирование
Локальная защита Дискреционное управл	🛞 Антивирус		
Затирание данных Полномочное управлен Замкногая програминая	Быстрое сканирование Настройки быстрого сканирования, запуст	аемого администратором из программы управления или по расписанию.	<u>Аудит</u>
Защита диска и шифров	Эвристика:	Углубленная эвристика	
Сетевая защита		• Обычный режим	
Персональный межсете		🔵 Выключена	
Контроль устройств			
Контроль печати	Действия при обнаружении зараженных файлов:	<ul> <li>Лечить зараженные файлы</li> </ul>	
Антивирус	Separatinisit germout	<ul> <li>Удалять зараженные файлы, если не удалось лечение</li> </ul>	
Обнаружение вторжений		<ul> <li>Удаляемые файлы поместить в карантин</li> </ul>	
Обновление			
Паспорт ПО 🚽		Дополнительная настройка	
		Данные изменены Применить	Отмена

### Рисунок Б.70. – Настройка антивируса: быстрое сканирование

Локальная защита 🌰 Дискреционное управл	🛞 Антивирус	
Затирание данных	Сканирование по расписанию	Аудит
Полномочное управлен Замкнутая программная	Расписание сканирования:	i
Защита диска и шифров	Профиль 🔻 Расписание 🔻	
Сетевая защита	Быстрое сканирование Еженедельно, суббота в 3:00	
Персональный межсете		
Контроль устройств		
Контроль печати		
Антивирус		
Обнаружение вторжений		
Обновление		
Паспорт ПО 🚽		
•	Профили	5
	Данные изменены Применить	Отмена

Рисунок Б.71. – Настройка антивируса: сканирование по расписанию



Рисунок Б.72. – Настройка антивируса: исключения

Локальная защита Дискреционное управл	^	🏶 Обнаружение вторжений		
Затирание данных		Детекторы сетевых атак		Аудит
Полномочное управлен				
Замкнутая программная		<ul> <li>Включить детекторы атак</li> </ul>		(i)
Защита диска и шифров		<ul> <li>Блокировка атакующего хоста при обнаружении атак</li> </ul>		
Сетевая защита		Врама блокировки: 15 минит		
Персональный межсете		время олокировки.		
Контроль устройств		<ul> <li>Использовать черный список IP-адресов</li> </ul>		
Контроль печати				
Антивирус		Белый список IP-адресов:		
Обнаружение вторжений			(-	Ð
Обновление		Указанные IP-адреса не будут блокироваться		×
Паспорт ПО	-			_
↓		Путь		
			Применить	Отмена

### Рисунок Б.73. – Настройка обнаружения вторжений: начало

Дискреционное управл	обнаружение вторжении	
Затирание данных	Детекторы сетевых атак	Аудит
Полномочное управлен		
Замкнутая программная	<ul> <li>Включить детекторы атак</li> </ul>	Û
Защита диска и шифров	<ul> <li>Блокировка атакующего хоста при обнаружении атак</li> </ul>	
Сетевая защита		
Персональный межсете	ыремя олокировки. 25 минут	
Контроль устройств	<ul> <li>Использовать черный список IP-адресов</li> </ul>	
Контроль печати		
Антивирус	Белый список IP-адресов:	
Обнаружение вторжений		+)
Обновление	Указанные IP-адреса не будут блокироваться	
Паспорт ПО 🚽		_
• •	Путь	

Рисунок Б.74. – Настройка обнаружения вторжений: детекторы сетевых атак

Локальная защита Дискреционное управл	🏶 Обнаружение вторжений			
Затирание данных	Детекторы сетевых атак			Аудит
Полномочное управлен	Детекторы			
Замкнутая программная				
Защита диска и шифров	<ul> <li>Сканирование портов</li> </ul>			
Сетевая защита	Период обнаружения:	60	секунд	
Персональный межсете				
Контроль устройств	Максимальное количество обращений к портам за указанный период:	150		
Контроль печати				
Антивирус	ARD-specifing			
Обнаружение вторжений	▼ Arc-spooling			
Обновление	Время после ARP-запроса, в течение которого ожидается ARP-ответ:	1500	миллисекунд	
Паспорт ПО 🚽				
•	Действие с ARP-ответами, полученными без ARP-запросов:	Активное г	противодействи 👻	
	Данные из	менены	Применить	Отмена

Рисунок Б.75. – Настройка детекторов сетевых атак: детекторы

Дискреционное управл	🏶 Обнаружение вторжении			
Затирание данных Полномочное управлен	Детекторы сетевых атак <ul> <li>✓ SYN-FLOOD</li> </ul>			<u>Аудит</u>
Защита диска и шифров	Время, за которое учитываются полуоткрытые соединения:	30	секунд	
Персональный межсете	Количество полуоткрытых соединений, после которых хост считается атакующим:	20		
Контроль устроиств Контроль печати	Блокировать пакет, если детектор сработал:	$\checkmark$		
Антивирус Обнаружение вторжений	<ul> <li>Аномальный трафик</li> </ul>			
Обновление	ьлокировать пакет, если детектор сработал:	$\checkmark$		
	V DDoS			

# Рисунок Б.76. – Настройка детекторов сетевых атак: детекторы, продолжение

Локальная защита	🗎 🤀 Обцаружение вторжений				4
Дискреционное управл	• Обнаружение вторжении				
Затирание данных	Детекторы сетевых атак			Аудит І	
Полномочное управлен					
Замкнутая программная	✓ DDoS				
Защита диска и шифров	Максимальное количество активных удаленных хостов, при	1000			
Сетевая защита	превышении которого срабатывает детектор:	1000			
Персональный межсете					h
Контроль устройств	✓ DoS				I
Контроль печати	Отрезок времени, за который учитывается обращение к порту:	60	секунд		I
Антивирус					
Обнаружение вторжений	Максимальное количество пакетов, при превышении которого будет	52428			
Обновление	detectupobana ataka.				
Паспорт ПО	Максимальный размер данных, при превышении которого будет детектирована атака:	76800	КБ		
					4
	Данные и:	зменены	Применить	Отмена	1

# Рисунок Б.77. – Настройка детекторов сетевых атак: детекторы, завершение

	етекторы сетевых атак			A		
Замкнутая программна:	Замедлять трафик с атакую	Замедлять трафик с атакующего хоста:				
Защита диска и шифров	Сервис	Макс. к-во пакетов	Макс. размер (КБ)			
етевая защита Персональный межсете	Получатель ІСМР	200	23			
онтроль устройств онтроль печати	RDP-сервер	1310720	1536000			
тивирус	SMB-сервер	6710886	7864320			
5наружение вторжений 5новление						

Рисунок Б.78. – Настройка детекторов сетевых атак: сервис (продолжение)

Локальная защита	A	🖶 Обнаружение вторжений	
Дискреционное управл			
Затирание данных			
Полномочное управлен		Сигнатурные анализаторы	Аудит
Замкнутая программная Защита диска и шифров	ł.	<ul> <li>Включить сигнатурные анализаторы</li> </ul>	i
Сетевая защита		Анализаторы	
Персональный межсете		✓ Анализатор НТТР	
Контроль устройств		<ul> <li>Контроль входящего трафика</li> </ul>	
Контроль печати		<ul> <li>Контроль исходящего трафика</li> </ul>	
Антивирус		Список портов:	
Обнаружение вторжений	۰.	80; 8080; 3128	
Обновление			
Паспорт ПО	-		
		Данные изменены Применить	Отмена

# Рисунок Б.79. – Настройка обнаружения вторжений: сигнатурные анализаторы

Локальная защита	🏶 Обнаружение вторжений		A
дискреционное управл Затирание данных Полномочное управлен	Сигнатурные анализаторы	Аудит	
Замкнутая программна: Защита диска и шифрог	<ul> <li>Блокировать фишинговые URL-адреса</li> <li>Блокировать ботнет сети</li> </ul>		
Сетевая защита Персональный межсете	Белый список URL-адресов:		
Контроль устройств Контроль печати	(		
Антивирус Обнаружение вторжений	указанные вео-аареса не будут олокироваться Путь		l
Обновление			
hachop no			1
	Данные изменены Применить	Отмена	l

Рисунок Б.80. – Настройка обнаружения вторжений: сигнатурные анализаторы. продолжение

#### Настройка модулей «Обновления» и «Паспорт ПО»

Обновление — содержит параметры автоматической проверки обновлений антивирусных баз и базы правил; паспорт ПО — содержит параметры настройки сбора данных о состоянии программной среды (СПС) по расписанию, выбранных каталогов и расширения файлов. Перейдите в группы «Обновления» и «Паспорт ПО» и выполните настройки в соответствии с заданием. Последовательная настройка модулей «Обновления» и «Паспорт ПО» представлена на рисунках Б.81. ÷ Б.87., для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.

Обновление				
Настройки обновления.				(i)
Расписание запуска проверки обновлений:	Частота запуска:	Еженедельно	•	
	День недели:	Пятница	*	
	Время:	23:00	•	
Размешение сервера обновлений:	• Обновлять с с	ервера Secret Net Studio		
, , ,	0.5			
	• Без прокси	ñ		
	Настройки обновления. Расписание запуска проверки обновлений: Размещение сервера обновлений:	Настройки обновления. Расписание запуска проверки Частота запуска: обновлений: День недели: Время: Размещение сервера обновлений: • Обновлять с с • Без прокси	Настройки обновления. Расписание запуска проверки обновлений: День недели: Время: 23:00 Размещение сервера обновлений: • Обновлять с сервера Secret Net Studio • Без прокси	Настройки обновления.           Расписание запуска проверки обновлений:         Частота запуска:         Еженедельно         ▼           День недели:         Пятница         ▼           Время:         23:00         ▼           Размещение сервера обновлений:         •         Обновлять с сервера Secret Net Studio           •         Без прокси

### Рисунок Б.81. – Настройка обновлений

Локальная защита Аискреционное управл	🕵 Обновление					
Затирание данных	Обновление					
Замкникая прогозимная	Настройки обновления.					(i)
Защита лиска и шифроз						
Сетевая защита	Расписание запуска проверки	Частота запуска:	Еженедельно	*		
Персональный межсете	соповлении.	День недели:	Пятница	-		
Контроль устройств						
Контроль печати		Время:	22:00	*		
Антивирус						
Обнаружение вторжений	Размешение сервера обновлений:		rensena Secret Net Studio			
Обновление	Газмещение сервера обновлении.					
Паспорт ПО 🚽		• Без прокси	1			
•		Использов	ать системные настройки п	прокси		
			Данные изменены	При	именить	Отмена

### Рисунок Б.82. – Настройка обновлений, продолжение

Локальная защита Аискреционное управл	🗧 Паспорт ПО	
Затирание данных Полномочное управлен Замкнутая программная Защита диска и шифрог	Сбор данных СПС по расписанию Не задано т	<u>Аудит</u> і
Сетевая защита Персональный межсете	Каталоги и файлы	Аудит
Контроль устройств Контроль печати Антивирус Обнаружение вторжений	По выбранным каталогам и файлам проводится сбор данных о состоянии программной среды (СПС). Проводить сбор данных СПС: По всем локальным дискам компьютера Выбранным узгалогам и лискам:	(j)
Обновление Паспорт ПО	Запрещенные символы: < > *   * ?	
	Применить	

Рисунок Б.83. – Настройка паспорта ПО

В группе параметров "Каталоги и файлы" настройте область сканирования при сборе данных: установите отметки в соответствующих полях ( по требованию).

## 🖪 Паспорт ПО

Сбор данных СПС по расписанию	Аудит
Периодическое 👻	i
Начиная с <u>01.11.2022 18:57</u> каждые 3 📩 дней 👻	

Рисунок Б.84. – Настройка паспорта ПО: сбор данных СПС по расписанию

Если запуск процесса сбора данных о состоянии программной среды должен выполняться в определенные моменты времени, настройте расписание запуска: выберите нужный режим в раскрывающемся списке группы параметров «Сбор данных СПС по расписанию» – «Периодическое» / «Еженедельное»

Локальная защита Дискреционное управл	🕯 🖪 Паспорт ПО			4
Затирание данных	Каталоги и файлы		Аудит	l
Замкнутая программная	По выбранным каталогам и файлам проводится сбор данных о состоянии программной среды (СПС	).		l
Защита диска и шифров	Проводить сбор данных СПС:		i	1
Сетевая защита	• По всем локальным дискам компьютера			
Персональный межсете	Выоранным каталогам и дискам:			
Контроль устройств		$\equiv \oplus$		
Контроль печати	Запрещенные символы: < > "   * ?			
Антивирус Обнаружение вторжений	Путь			
Обновление				
Паспорт ПО	v			
				1
	Данные изменены	Применить	Отмена	1

Рисунок Б.85. – Настройка паспорта ПО: каталоги и файлы

Локальная защита		
Дискреционное управл		
Затирание данных	Каталоги и файлы	Аудит І
Полномочное управлен	Исключать каталоги. диски и файлы:	
Замкнутая программная		$\bigcirc$
Защита диска и шифров		Ð
Сетевая защита	Запрещенные симвалы: < > "   * ?	
Персональный межсете	Путь	
Контроль устройств		
Контроль печати		
Антивирус		
Обнаружение вторжений		
Обновление		
Паспорт ПО 🚽		
	Данные изменены Применить	Отмена

## Рисунок Б.86. – Настройка паспорта ПО: каталоги и файлы, продолжение

Локальная защита Дискреционное управл	\$		Паспорт ПО		1
Затирание данных		Расши	ирения файлов	Аудит	
Полномочное управлен Замкнутая программная Защита диска и шифрог	l	Пров	одить сбор данных СПС: По всем расширениям файлов Выбранным:	(j)	
Сетевая защита			= A		
Персональный межсете	1				
Контроль устройств			Запрещенные символы: < > : "   * ?		
Контроль печати	н		Расширение		h
Антивирус					l
Обнаружение вторжений			exe		l
Обновление			com		ŀ
Паспорт ПО	-				
• • •			dii		1
			Данные изменены Применить	Отмена	]

Рисунок Б.87. – Настройка паспорта ПО: расширения файлов

### Настройка Регистраций событий

Настройка регистрации событий, относящихся к работе политик соответствующих модулей (см. рисунок Б.88.). По умолчанию включена регистрация всех событий. С помощью значка <sup>(1)</sup> («i») ознакомьтесь с описаниями событий и установите аудит успеха и отказа в разделе «Регистрация событий» (см. рисунок Б.89.), все параметры не относящиеся к аудиту успеха и отказа устанавливаются в соответствии с заданием или на свое усмотрение (предпочтительней по умолчанию): поставьте «галочку», напротив события, если нужно установить аудит и уберите если нужно снять аудит.

Ŧ	политики		🗱 Регистрация событий		
Э	РЕГИСТРАЦ 况 СОБЫТИЙ		м спистрации соовнии		
	Администрирование		Администрирование		-
	Администрирование систег				
	Антивирус		Включена защитная подсистема	<ul> <li>Включить</li> </ul>	(j)
	Вход в систему				
	Дискреционное управлени				
	Замкнутая программная ср		Групповые политики успешно применены	<ul> <li>Включить</li> </ul>	i
	Затирание данных	1			
	Защита диска и шифровани				
	Ключи пользователя		Добавлен пользователь	<ul> <li>Включить</li> </ul>	Ū
	Контроль печати				
	Контроль приложений		Закрыта докальная программа управления	Вклюцить	(i)
	Контроль устройств	Ŧ			
	• • •				
				Применить	

### Рисунок Б.88. – Окно настройка регистрации событий

Администрирование	
Включена защитная подсистема	🗸 Включить
Групповые политики успешно применены	Определяет режим регистрации события "Включена защитная подсистема", тип события Аудит успехов
Добавлен пользователь	Событие регистрируется в случае, если включен механизм защиты системы Secret Net Studio.
	Значение по умолчанию: <b>"Включено"</b>

#### Рисунок Б.89. – Окно информации о событии

Аудит безопасности Windows - это технические средства и мероприятия, направленные на регистрацию и систематический регулярный анализ событий, влияющих на безопасность информационных систем. Технически, аудит безопасности в Windows peaлизуется через настройку политик аудита и настройку аудита объектов. Политика аудита определяет какие события и для каких объектов будут генерироваться в журнал «Событий Безопасность». Настройку регистрации событий относящихся к работе политик конкретной группы можно настроить дискретно для конкретной группы через ссылку «Аудит» в окне выбора параметров в правой части заголовка группы (правая верхняя часть; см. рисунок Б.23.); при этом в левой части окна регистрации событий будет отображаться выбранная конкретная группа, а в центральной части – отображаться настройки этой группы.

Перейдите в группу «Регистраций событий» и выполните настройки в соответствии с заданием. Последовательная настройка группы «Регистрация

событий» представлена на рисунках Б.90. ÷ Б.142., для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.

#### Настройка администрирования

### политики регистрацуз событий Вегистрация событий

-N0-						
Администрирование		Администрирование				
Администрирование систе						Ľ.
Антивирус		Включена защитная подсистема	$\checkmark$	Включить	(i)	
Вход в систему						
Дискреционное управлени						
Замкнутая программная ср	1	Групповые политики успешно применены	$\checkmark$	Включить	i	
Затирание данных						
Защита диска и шифрованы			_			
Ключи пользователя		Добавлен пользователь	<ul> <li>Включить</li> </ul>	(i)		
Контроль печати						
Контроль приложений				Pressources		
Контроль устройств	-	Закрыта локальная программа управления	v	БКЛЮЧИТЬ	U	
•						-
			Γ	Пониманить		
	Администрирование Администрирование систеи Антивирус Вход в систему Дискреционное управлени Замкнутая программная ср Затирание данных Зацита диска и шифровань Ключи пользователя Контроль печати Контроль приложений Контроль устройств	Администрирование Администрирование систег Антивирус Вход в систему Дискреционное управлени Замкнутая программная ср Затирание данных Защита диска и шифрован Ключи пользователя Контроль приложений Контроль устройств	Администрирование Администрирование систе Антивирус Вход в систему Дискреционное управлени Замкнутая программная ср Затирание данных Защита диска и шифровани Ключи пользователя Контроль печати Контроль устройств	Администрирование Администрирование систет Антивирус Вход в систему Дискреционное управлени Замкнутая программная ср Затирание данных Защита диска и шифровани Ключи пользователя Контроль печати Контроль устройств	Администрирование Администрирование систе Антивирус Вход в систему Дискреционное управлени Замкнутая программная ср Затирание данных Защита диска и шифровани Ключи пользователя Контроль печати Контроль устройств Контроль устройств	Администрирование Администрирование систет Антивирус Вход в систему Дискреционное управлени Замкнутая программная ср Затирание данных Защита диска и шифровани Ключи пользователя Контроль печати Контроль устройств Контроль устройств

### Рисунок Б.90. – Настройка администрирования, начало

### 🐯 Регистрация событий

Администрирование				
Запущена локальная программа управления		✔ Включить	(j)	
Изменен пароль пользователя		✓ Включить	i	
Изменен режим работы агента		✔ Включить	(i)	
Изменены параметры действующей политики безопасности		✔ Включить	i	
	Данные изменены	Применить	Отмена	]

Рисунок Б.91. – Настройка администрирования, продолжение первое

Ð	ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ		🐯 Регистрация событий		
	Администрирование		Администрирование		1
	Администрирование систег				* H
	Антивирус		Изменены параметры пользователя	<ul> <li>Включить</li> <li>і</li> </ul>	
	Вход в систему				
	Дискреционное управлени				
	Замкнутая программная ср		Не удалось изменить режим работы агента	✓ Включить (i)	
	Затирание данных				
	Защита диска и шифровани		Отключена зашитная полсистема	У Вклюцить	
	Ключи пользователя				
	Контроль печати				
	Контроль приложений		Ошибка применения групповых политик	<ul> <li>Включить</li> <li>і</li> </ul>	
	Контроль устройств	Ŧ			
•	•				-

# Рисунок Б.92. – Настройка администрирования, продолжение второе

Данные изменень

Отмена

### ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ

### 🐯 Регистрация событий

ибка синхронизации учетной информации с персональным межсетевым экраном	<ul> <li>Включить</li> </ul>	(j
ибка синхронизации учетной информации с персональным межсетевым экраном	<ul> <li>Включить</li> </ul>	(i)
	REPORT	
дупреждение при применении групповых политик		U
хронизация учетной информации с персональным межсетевым экраном	<ul> <li>Включить</li> </ul>	(j)
лен пользователь	<ul> <li>Включить</li> </ul>	(i)
e,	дупреждение при применении групповых политик хронизация учетной информации с персональным межсетевым экраном лен пользователь	дупреждение при применении групповых политик кронизация учетной информации с персональным межсетевым экраном лен пользователь Включить Включить Включить Включить

### Рисунок Б.93. – Настройка администрирования, завершение

### Настройка администрирования системы защиты

политики		📾 Регистрация событий				
РЕГИСТРАЦИЯ СОБЫТИЙ		ал стистрации соовний				
Администрирование		Администрирование системы защиты				
Администрирование системы заг						
Антивирус		Запрет несанкционированного вызова		Включить	(i)	1
Вход в систему						
Дискреционное управление дост						
Замкнутая программная среда	1	Попытка доступа к защищенному процессу		<ul> <li>Включить</li> </ul>	(i)	
Затирание данных						
Защита диска и шифрование дан						
Ключи пользователя		Попытка модификации или отключения защитного механизма		<ul> <li>Включить</li> </ul>	(i)	
Контроль печати						
Контроль приложений		Польтиз молификации или улаления параметоря системы защиты		Preserver	$\odot$	
Контроль устройств	-	попытка модификации или удаления параметров системы защиты		• включить	U	
• • • • • • • • • • • • • • • • • • •						w
			Данные изменены	Применить	Отмена	1

Рисунок Б.94. – Настройка администрирования системы защиты

### 🕸 Регистрация событий

### Рисунок Б.95. – Настройка антивируса

### Настройка входа в систему

политики

РЕГИСТРАЦИЯ СОБЫТИЙ

### 🐼 Регистрация событий

Администрирование		Вход в систему				
Администрирование системы за						
Антивирус		Вход пользователя в систему		Включить	(i)	
Вход в систему		,				
Дискреционное управление дост	1					
Замкнутая программная среда		Завершение работы пользователя		<ul> <li>Включить</li> </ul>	i	
Затирание данных						
Защита диска и шифрование дан						
Ключи пользователя		Запрет входа пользователя		<ul> <li>Включить</li> </ul>	(i)	
Контроль печати						
Контроль приложений				Pressure		
Контроль устройств	-	запрет сетевого подключения под другим именем		• ВКЛЮЧИТЬ	U	
↓						Ŧ
			Данные изменены	Применить	Отмена	1

### Рисунок Б.96. – Настройка входа в систему, начало

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ	🐯 Регистрация событий			
Администрирование	Вход в систему		1	.4
Администрирование системы зас	Идентификатор не зарегистрирован	И Вилюцить	(i)	
Антивирус		• 00104018	Ū	
Вход в систему				
Дискреционное управление дост	Компьютер заблокирован системой защиты	<ul> <li>Включить</li> </ul>	i	
Замкнутая программная среда				
Затирание данных				
Защита диска и шифрование дан	Компьютер разблокирован	<ul> <li>Включить</li> </ul>	(i)	
Слючи пользователя				
Контроль печати			$\odot$	
Контроль приложений	Ошибка выполнения функционального контроля	<ul> <li>Включить</li> </ul>	Û	
Контроль устройств				
	Ошибка создания контекста пользователя	READURATE	•	-
	Данные изменены	Применить	Отмена	1

Рисунок Б.97. – Настройка входа в систему, продолжение первое

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ		🐯 Регистрация событий				
Администрирование		Вход в систему			1	4
Администрирование системы за						
Антивирус		Ошибка создания контекста пользователя	~	Включить	i	
Вход в систему						
Дискреционное управление дост			_	7 -		
Замкнутая программная среда		Пароль пользователя не соответствует требованиям безопасности	~	Включить	(i)	
Затирание данных	1					
Защита диска и шифрование дан		Пользователь возобновил сеанс работы на компьютере		Включить	(j)	
Ключи пользователя			-			
Контроль печати						
Контроль приложений		Пользователь приостановил сеанс работы на компьютере	~	Включить	(i)	
Контроль устройств	-					
•						1
		Ланные изм	енены	Применить	Отмена	1

# Рисунок Б.98. – Настройка входа в систему, продолжение второе

## 🐯 Регистрация событий

Вход в систему		
Система инициировала блокировку сессии пользователя	✓ Включить	(i)
Успешное завершение функционального контроля	✔ Включить	i

### Рисунок Б.99. – Настройка входа в систему, завершение

### Настройка дискреционного управления доступом

политики		📾 Регистрация событий				
РЕГИСТРАЦИЯ СОБЫТИЙ		А стистрации соовнии				
Администрирование		Дискреционное управление доступом				A
Администрирование системы за						
Антивирус		Доступ к файлу или каталогу		Включить	(i)	
Вход в систему		·····				ľ
Дискреционное управление дост						
Замкнутая программная среда	1	Запрет доступа к файлу или каталогу		<ul> <li>Включить</li> </ul>	(i)	
Затирание данных						
Защита диска и шифрование дан				_		
Ключи пользователя		Изменение прав доступа		<ul> <li>Включить</li> </ul>	(i)	
Контроль печати						
Контроль приложений		-				
Контроль устройств	$\overline{\mathbf{v}}$	Замкнутая программная среда				
↓						1
			Данные изменены	Применить	Отмена	1

Рисунок Б.100. – Настройка дискреционного управления доступом

Настройка замкнутой программной среды

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ	🐯 Регистрация событий		
Администрирование	Замкнутая программная среда		
Администрирование системы за			
Антивирус	Загрузка библиотеки	Включить	(i)
Вход в систему			
Дискреционное управление дост			
Замкнутая программная среда	Запрет загрузки библиотеки	✓ Включить	i
Затирание данных			
Защита диска и шифрование дан			
Ключи пользователя	Запрет запуска программы	<ul> <li>Включить</li> </ul>	(i)
Контроль печати			
Контроль приложений		A Branchurzh	
Контроль устройств 🗸 👻	Souper actionmental newspectrum o expanse		
4			
	Данные изменены	Применить	Отмена

Рисунок Б.101. – Настройка замкнутой программной среды

### 🕸 Регистрация событий

Замкнутая программная среда		
Запуск программы	<ul> <li>Включить</li> </ul>	i
Исполнение скрипта	✓ Включить	i

# Рисунок Б.102. – Настройка замкнутой программной среды, продолжение

### Настройка затирания данных

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ	Î	🐯 Регистрация событий			
Администрирование		Затирание данных			
Администрирование системы за					
Антивирус		зратное удаление файлового объекта јение операции безвозвратного удаления	$\checkmark$	Включить	(j)
Вход в систему					Ŭ
Дискреционное управление дост					
Замкнутая программная среда	1	авершение операции безвозвратного удаления	$\checkmark$	<ul> <li>Включить</li> </ul>	i
Затирание данных					
Защита диска и шифрование дан			_	_	
Ключи пользователя		Начало операции безвозвратного удаления	$\checkmark$	Включить	Û
Контроль печати					
Контроль приложений		Ошибка безвозвратного улаления файлового объекта	1	BERNOLINTE	
Контроль устройств	Ŧ		•	DIDITIONITE	
↓					
		Данные изменены		Применить	Отмена

Рисунок Б.103. – Настройка затирания данных, начало

#### политики РЕГИСТРАЦИЯ СОБЫТИЙ

### 📔 🐯 Регистрация событий

Администрирование		Затирание данных			1	
Администрирование системы за						
Антивирус		Для файла включены потоки целостности ReFS	~	Включить	i	
Вход в систему						
Дискреционное управление дост						1
Замкнутая программная среда	1	Добавление файлового объекта в очередь отложенной обработки	~	Включить	(i)	
Затирание данных						
Защита диска и шифрование дан		23PADILIAU/A VASAAU/A OCTATOLULIV ASUULIV US AOVAALUON AI/CVA		Pressure	÷	
Ключи пользователя		Завершение удаления остаточных данных на локальном диске	v	• ВКЛЮЧИТЬ	U	
Контроль печати						
Контроль приложений		Завершение удаления остаточных данных на съемном диске	~	Включить	i	
Контроль устройств	$\overline{\mathbf{v}}$			-		
← →						1
		Данные измене	ны	Применить	Отмена	1

### Рисунок Б.104. – Настройка затирания данных, продолжение первое

#### политики РЕГИСТРАЦИЯ СОБЫТИЙ

### 🐯 Регистрация событий

Администрирование		Затирание данных			1	A
Администрирование системы за						
Антивирус					~	
Вход в систему		Начало удаления остаточных данных на локальном диске	l	<ul> <li>Включить</li> </ul>	Ū	
Дискреционное управление дост						1
Замкнутая программная среда		Начало удаления остаточных данных на съемном диске		Включить	(j)	
Затирание данных						
Защита диска и шифрование дан						
Ключи пользователя		Ошибка помещения файла в очередь отложенной обработки		<ul> <li>Включить</li> </ul>	(j	
Контроль печати						
Контроль приложений						
Контроль устройств	-	Ошибка удаления имени файлового объекта		<ul> <li>Включить</li> </ul>	(i)	
4 · · · · · · · · · · · · · · · · · · ·						-
			Данные изменены	Применить	Отмена	1

### Рисунок Б.105. – Настройка затирания данных, продолжение второе

#### политики РЕГИСТРАЦИЯ СОБЫТИЙ

### 🕸 Регистрация событий

Администрирование		Затирание данных		1	
Администрирование системы за					
Антивирус		Ошибка удаления остаточных данных	✓ Включить	(i)	
Вход в систему					
Дискреционное управление дост		Vазление остаточных данных прерывается	- Brabouuth		
Замкнутая программная среда	1	удаление остаточных данных прерывается		U	
Затирание данных	-				
Защита диска и шифрование дан					
Ключи пользователя		Завершение удаления данных на диске	<ul> <li>Включить</li> </ul>	(i)	
Контроль печати					
Контроль приложений			Pressure		
Контроль устройств	Ŧ	пачало удаления данных на диске		Û	
•					4
		Данные изменены	Применить	Отмена	1

Рисунок Б.106. – Настройка затирания данных, продолжение третье

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ		🐯 Регистрация событий				
Администрирование		Затирание данных			1	4
Администрирование системы заг						
Антивирус		Операция удаления данных на диске прервана пользователем	$\checkmark$	Включить	(i)	
Вход в систему						
Дискреционное управление дост						l.
Замкнутая программная среда		Ошибка в процессе сбора информации о системе	$\checkmark$	Включить	(i)	
Затирание данных						
Защита диска и шифрование дан			_			
Ключи пользователя		Сбой при подготовке устроиства к удалению данных на диске	$\checkmark$	Включить	U	
Контроль печати						
Контроль приложений		Сбой при удалении данных на диске	×	Включить	(i)	
Контроль устройств	T.		•	00000000	U	
4 · · · · · · · · · · · · · · · · · · ·						7
		Ланные	изменены	Применить	Отмена	٦

### Рисунок Б.107. – Настройка затирания данных, завершение

### Настройка защиты диска и шифрования данных

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ

### 📔 🐯 Регистрация событий

Синстидии совытии						
Администрирование		Защита диска и шифрование данных				i.
Администрирование системы заг						
Антивирус		Добавление криптоконтейнера в список криптоконтейнеров пользователя	~	Включить	(i)	
Вход в систему			-			
Дискреционное управление дост						l
Замкнутая программная среда	1	Добавление пользователя в список доступа к криптоконтейнеру	$\checkmark$	Включить	i	l
Затирание данных						
Защита диска и шифрование дан			_			
Ключи пользователя		Запрет операции подключения криптоконтейнера	$\checkmark$	Включить	(i)	
Контроль печати						
Контроль приложений		Изменение базового клюца шифорвания криптоконтейнера	1	BRADUMETE		
Контроль устройств	Ŧ	изменение обзового ключа шифрования криптокоптеннера	•	ылючить		
• • • • • • • • • • • • • • • • • • •						2
		Данные изменен	ы	Применить	Отмена	

# Рисунок Б.108. – Настройка защиты диска и шифрования данных, начало

### ПОЛИТИКИ

### 🐯 Регистрация событий

стисти Ации совытии					
Администрирование		Защита диска и шифрование данных		1	
Администрирование системы за					
Антивирус		Изменение уровня доступа пользователя к криптоконтейнеру	<ul> <li>Включить</li> </ul>	(j)	
Вход в систему					
Дискреционное управление дост					
Замкнутая программная среда		Исключение криптоконтейнера из списка криптоконтейнеров пользователя	<ul> <li>Включить</li> </ul>	i	
Затирание данных					
Защита диска и шифрование дан		Q		$\odot$	
Ключи пользователя		Отключена защита для диска	• ВКЛЮЧИТЬ	U	
Контроль печати					
Контроль приложений		Удаление пользователя из списка доступа к криптоконтейнеру	<ul> <li>Включить</li> </ul>	(i)	
Контроль устройств	$\overline{\mathbf{v}}$				
↓					
		Данные изменены	Применить	Отмена	1
					- E -

Рисунок Б.109. – Настройка защиты диска и шифрования данных, продолжение

### 🐯 Регистрация событий

Защита диска и шифрование данных		
Успешное отключение криптоконтейнера из системы	✓ Включить	i
Успешное подключение криптоконтейнера в системе	✓ Включить	i
Установлена защита для диска	✓ Включить	i

# Рисунок Б.110. – Настройка защиты диска и шифрования данных, завершение

Настройка ключей пользователя

### 🐯 Регистрация событий

Ключи пользователя			d
Изменен ключ пользователя	✓ Включить	(j)	
Удален ключ пользователя	🖌 Включить	i	1
Контроль печати			

### Рисунок Б.111. – Настройка ключей пользователя

### Настройка контроля печати

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ		🐯 Регистрация событий				
Администрирование		Контроль печати				4
Администрирование системы за						
Антивирус		Запрет печати документа		Включить	(i)	
Вход в систему						
Дискреционное управление дост						
Замкнутая программная среда		Запрет прямого обращения к принтеру		<ul> <li>Включить</li> </ul>	i	
Затирание данных						
Защита диска и шифрование дан				✓ Включить		
Ключи пользователя		Начало печати документа			(i)	
Контроль печати						
Контроль приложений				A Pressure		
Контроль устройств	-	пачало печати экземпляра документа		СКЛЮЧИТВ	U	
↓						1
			Данные изменены	Применить	Отмена	]

Рисунок Б.112. – Настройка контроля печати, начало

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ		🐯 Регистрация событий				
Администрирование		Контроль печати			1	
Администрирование системы за						
Антивирус		Ошибка при печати документа	$\checkmark$	Включить	i	
Вход в систему						
Дискреционное управление дост						
Замкнутая программная среда		Ошибка при печати экземпляра документа	$\checkmark$	Включить	i	
Затирание данных						ľ
Защита диска и шифрование дан		D		0	$\odot$	
Ключи пользователя		Печать документа	$\checkmark$	включить	Ū	
Контроль печати						
Контроль приложений		Сохранение копии напечатанного документа	~	Включить	(i)	
Контроль устройств	-					
4						-
		Даннь	ые изменены	Применить	Отмена	٦

Рисунок Б.113. – Настройка контроля печати, продолжение

## 🐯 Регистрация событий

Контроль печати		
Успешное завершение печати документа	<ul> <li>Включить</li> </ul>	i
Успешное завершение печати экземпляра документа	✔ Включить	i

Рисунок Б.114. – Настройка контроля печати, завершение

### Настройка контроля приложений

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ		🐯 Регистрация событий				
Администрирование		Контроль приложений				.4
Администрирование системы за						
Антивирус		Аудит системных процессов (в дополнение к пользовательским)		Включить	(i)	
Вход в систему		· · · · · · · · · · · · · · · · · · ·				
Дискреционное управление дост						
Замкнутая программная среда	1	Запуск процесса		<ul> <li>Включить</li> </ul>	i	
Затирание данных						
Защита диска и шифрование дан			авершение процесса			
Ключи пользователя		Завершение процесса		<ul> <li>Включить</li> </ul>	(j)	
Контроль печати						
Контроль приложений		Doctors & Burbany of Maria		Pressource		
Контроль устройств	-	доступ к буферу обмена		• БКЛЮЧИТЬ	U	
<						-
			Данные изменены	Применить	Отмена	1

Рисунок Б.115. – Настройка контроля приложений, начало

политики		🗱 Регистрация событий			
РЕГИСТРАЦИЯ СОБЫТИЙ					
Администрирование		Контроль приложений		1	4
Администрирование системы за					
Антивирус		Запрет доступа к буферу обмена	<ul> <li>Включить</li> </ul>	(i)	
Вход в систему					
Дискреционное управление дост			Pressure		
Замкнутая программная среда		доступ к содержимому окна процесса	• БКЛЮЧИТЬ	U	
Затирание данных					1
Защита диска и шифрование дан		Запрет доступа к содержимому окна процесса	<ul> <li>Включить</li> </ul>	i	
Ключи пользователя					
Контроль печати					
Контроль приложений		Операция перетаскивания (drag-n-drop) между процессами	<ul> <li>Включить</li> </ul>	i	
Контроль устройств	Ŧ				
					1
		Ланные изменен	Применить	Отмена	1

Рисунок Б.116. – Настройка контроля приложений, продолжение

### 🐯 Регистрация событий

Контроль приложений					
Запрет операции перетаскивания (drag-n-drop) между процессами	<ul> <li>Включить</li> </ul>	i			

Рисунок Б.117. – Настройка контроля приложений, завершение

### Настройка контроля устройств

ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ	Î	🐯 Регистрация событий				
Администрирование		Контроль устройств				4
Администрирование системы за						
Антивирус		Выход из спяшего режима		READURE		
Вход в систему		выход из спищего режима		• БКЛЮЧИТЬ	U	
Дискреционное управление дост						
Замкнутая программная среда		Доступ к устройству		<ul> <li>Включить</li> </ul>	i	
Затирание данных	-					
Защита диска и шифрование дан						ľ
Ключи пользователя		Запрет доступа к устройству		<ul> <li>Включить</li> </ul>	i	
Контроль печати						
Контроль приложений		2				
Контроль устройств	-	запрет подключения устроиства		<ul> <li>Включить</li> </ul>	0	
↓						4
			Данные изменены	Применить	Отмена	1

Рисунок Б.118. – Настройка контроля устройств, начало

политики		🕾 Регистрация событий			
РЕГИСТРАЦИЯ СОБЫТИЙ		Сперация соовний			
Администрирование		Контроль устройств			4
Администрирование системы за					
Антивирус		Изменены параметры устройства	Включить	i	
Вход в систему					
Дискреционное управление дост					
Замкнутая программная среда		Обнаружено новое устройство	<ul> <li>Включить</li> </ul>	i	
Затирание данных	۰.				
Защита диска и шифрование дан				$\odot$	1
Ключи пользователя		Обнаружены изменения в процессе контроля аппаратной конфигурации	<ul> <li>Включить</li> </ul>	Û	
Контроль печати					
Контроль приложений		Отключение устройства	Включить	(i)	
Контроль устройств	Ŧ				
€ →					-
		Данные изме	нены Применить	Отмена	1

# Рисунок Б.119. – Настройка контроля устройств, продолжение первое

политики		🖾 Регистрация событий				
РЕГИСТРАЦИЯ СОБЫТИЙ	II.	Сперация соовний				
Администрирование	II.	Контроль устройств				4
Администрирование системы за	II.					
Антивирус	II.	Переход в спящий режим		<ul> <li>Включить</li> </ul>	i	
Вход в систему	II.					
Дискреционное управление дост	II.			_		
Замкнутая программная среда		Подключение устройства		✓ Включить	(i)	
Затирание данных						
Защита диска и шифрование дан		Успешное завершение контроля аппаратной конфигурации		Включить	(i)	ł
Ключи пользователя		sentence soccase concentration and a new sorter spagning				
Контроль печати						
Контроль приложений		Устройство удалено из системы		<ul> <li>Включить</li> </ul>	i	
Контроль устройств	Ŧ					
← →						1
			Данные изменены	Применить	Отмена	1

Рисунок Б.120. – Настройка контроля устройств, продолжение второе

## 🐯 Регистрация событий

Контроль устройств		
Утверждение аппаратной конфигурации компьютера	<ul> <li>Включить</li> </ul>	i

Рисунок Б.121. – Настройка контроля устройств, завершение

### Настройка контроля целостности

РЕГИСТРАЦИЯ СОБЫТИЙ	A	📾 Регистрация событий				
Администрирование		Спетрации соовнии				
Администрирование системы заг		Контроль целостности				
Антивирус						
Вход в систему		Выполнен перерасчет эталона ресурса	1	Вклюцить		
Дискреционное управление дост		bulloniteri repepar let stanona perspea	L		÷	
Замкнутая программная среда						
Затирание данных		Для ресурса отсутствует эталонное значение	[	<ul> <li>Включить</li> </ul>	(j)	
Защита диска и шифрование дан						
Ключи пользователя						
Контроль печати		Добавление учетной записи к заданию ЗПС	[	<ul> <li>Включить</li> </ul>	(i)	
Контроль приложений						
Контроль устройств		Management and the second	r	C Durante		
Контроль целостности	-	изменение группы ресурсов	• БКЛЮЧИТЬ	U		
4 · · · · · · · · · · · · · · · · · · ·						Ŧ
			Данные изменены	Применить	Отмена	]

### Рисунок Б.122. – Настройка контроля целостности, начало

#### РЕГИСТРАЦИЯ СОБЫТИЙ Администрирование

### 🐯 Регистрация событий

Администрирование системы за		Контроль целостности				A
Антивирус						
Вход в систему		Изменение задания	~	Включить	i	
Дискреционное управление дост				-		
Замкнутая программная среда						
Затирание данных		Изменение задачи	~	Включить	i	
Защита диска и шифрование дан						
Ключи пользователя		14			$\odot$	i.
Контроль печати		Исправление ошибок в базе данных	~	Включить	Û	1
Контроль приложений						
Контроль устройств		Нарушение целостности ресурса	~	Включить	(i)	
Контроль целостности	-					
▲						4
			Данные изменены	Применить	Отмена	1

### Рисунок Б.123. – Настройка контроля целостности, продолжение первое

#### РЕГИСТРАЦИЯ СОБЫТИЙ

### 🐯 Регистрация событий

Администрирование			
Администрирование системы за	Контроль целостности		1
Антивирус			
Вход в систему	Начало обработки задания на контроль целостности	<ul> <li>Включить</li> </ul>	i
Дискреционное управление дост			
Замкнутая программная среда			
Затирание данных	Обнаружено нарушение целостности при обработке задания	<ul> <li>Включить</li> </ul>	Û
Защита диска и шифрование дан			
Ключи пользователя	Ошибка при восстановлении ресурса по эталонному значению	REPORT	
Контроль печати	emine in second and perpet to statements and termo		
Контроль приложений			
Контроль устройств	Ошибка при открытии базы данных контроля целостности	<ul> <li>Включить</li> </ul>	i
Контроль целостности 🚽			
	Данные изменены	Применить	Отмена

Рисунок Б.124. – Настройка контроля целостности, продолжение второе

#### 🕸 Регистрация событий РЕГИСТРАЦИЯ СОБЫТИЙ Администрирование Администрирование системы за Контроль целостности Антивирус Вход в систему **i** Ошибка при принятии текущего значения ресурса в качестве эталонного Включить Дискреционное управление дост Замкнутая программная среда Затирание данных i Ошибка при расчете эталона Включить Защита диска и шифрование дан Ключи пользователя Ошибка синхронизации локальной базы данных с центральной Включить i Контроль печати Контроль приложений Контроль устройств i Ресурс восстановлен по эталонному значению Включить Контроль целостности 🚽 b. Данные изменены Отмена

# Рисунок Б.125. – Настройка контроля целостности, продолжение третье

#### РЕГИСТРАЦИЯ СОБЫТИЙ Администрирование

### 🐯 Регистрация событий

Администрирование системы за		Контроль целостности				A
Антивирус						
Вход в систему		Синуронизация докальной базы данных с центральной	1	Brainguiste	(i)	
Дискреционное управление дост		синкропизация локальной база данных с центральной	•	• включить		
Замкнутая программная среда						
Затирание данных	1	Снятие задания КЦ с контроля	~	Включить	i	
Защита диска и шифрование дан						
Ключи пользователя						
Контроль печати		Создание группы ресурсов	~	Включить	i	×.
Контроль приложений						
Контроль устройств		CORRENT		Preserver	÷	
Контроль целостности	-	создание задания	•	выночить	U	
<						-
		Данны	е изменены	Применить	Отмена	1

# Рисунок Б.126. – Настройка контроля целостности, продолжение четвёртое

#### РЕГИСТРАЦИЯ СОБЫТИЙ

Администрирование

## 🍵 🐯 Регистрация событий

Администрирование системы за	Контроль целостности			4
Антивирус				
Вход в систему	Создание задачи	<ul> <li>Включить</li> </ul>	i	
Дискреционное управление дост				
Замкнутая программная среда				
Затирание данных	Текущее значение ресурса принято в качестве эталонного	<ul> <li>Включить</li> </ul>	i	
Защита диска и шифрование дан				
Ключи пользователя	V		$\odot$	
Контроль печати	Удаление группы ресурсов	<ul> <li>Включить</li> </ul>		i.
Контроль приложений				
Контроль устройств	Удаление задания	Включить	(i)	
Контроль целостности 🚽				
				4
	Данные изменены	Применить	Отмена	1

Рисунок Б.127. – Настройка контроля целостности, продолжение пятое

РЕГИСТРАЦИЯ СОБЫТИЙ	^	🚟 Регистрация событий				
Администрирование	11	ал спистрации соовнии				
Администрирование системы за		Контроль целостности				4
Антивирус						
Вход в систему		Удаление задачи		Включить	i	
Дискреционное управление дост						
Замкнутая программная среда			_			
Затирание данных		Удаление устаревших эталонных значений	•	Включить	(i)	
Защита диска и шифрование дан						
Ключи пользователя		Vлаление учетной записи из залания 3ПС		READURE		
Контроль печати		s designed a service as addenia one		быючить	U	L
Контроль приложений						ľ
Контроль устройств		Успешная проверка целостности ресурса	•	Включить	i	
Контроль целостности	-					
€						4
		Д	анные изменены	Применить	Отмена	1

# Рисунок Б.128. – Настройка контроля целостности, продолжение шестое

### 🐯 Регистрация событий

Контроль целостности		
Успешное завершение задания на контроль целостности	✓ Включить	i
Установка задания КЦ на контроль	✔ Включить	i

### Рисунок Б.129. – Настройка контроля целостности, завершение

#### Настройка обнаружения вторжений

Вся информация об активности механизма обнаружения и предотвращения вторжений регистрируется в журнале Secret Net Studio.

Администрирование	📾 Регистрация событий			
Администрирование системы за	ал стистрации соовнии			
Антивирус	Обнаружение вторжений			ļ
Вход в систему				
Дискреционное управление дост	Сработал детектор вторжений	<ul> <li>Включить</li> </ul>	Û	
Замкнутая программная среда				
Затирание данных	СОВ заблокировала удаленный узел	<ul> <li>Включить</li> </ul>		
Защита диска и шифрование дан	Обнаружена сигнатура СОВ. Доступ заблокирован	✓ Включить		
Ключи пользователя	COB กระชากบายการสาว พระกอมมาณี พระก	Включить		
Контроль печати	сов разолокировала удаленный узел			
Контроль приложений	Обнаружен IP из черного списка, доступ заблокирован	<ul> <li>Включить</li> </ul>		
Контроль устройств	Обнаружен IP из черного списка, доступ не заблокирован	<ul> <li>Включить</li> </ul>		ł
Контроль целостности		A Process		
Обнаружение вторжений	Обнаружен ОКЕ из черного списка, доступ заблокирован	• БКЛЮЧИТЬ		
• • • • • • • • • • • • • • • • • • •	Обнаружены устаревшие базы СОВ	<ul> <li>Включить</li> </ul>		1
	Данные изменены	Применить	Отмена	1

Рисунок Б.130. – Настройка обнаружения вторжений

### Настройка общих событий

Администрирование системы за	📾 Регистрация событий			
Антивирус	ал стистрации соовтний			
Вход в систему	Общие события			4
Дискреционное управление дост				
Замкнутая программная среда	Информационное событие	READURE		
Затирание данных	Phyophic counter	• DK/RO4VITB	U	
Защита диска и шифрование дан				
Ключи пользователя	Несанкционированное действие	<ul> <li>Включить</li> </ul>	(i)	
Контроль печати				
Контроль приложений				
Контроль устройств	Ошибка	<ul> <li>Включить</li> </ul>	(i)	
Контроль целостности				
Обнаружение вторжений	Desturbance	Discussion of the second se		
Общие события	предупреждение	• ВКЛЮЧИТЬ	U	
4 · · · · · · · · · · · · · · · · · · ·				1
	Ланные изменены	Применить	Отмена	1

### Рисунок Б.131. – Настройка общих событий

## 🐯 Регистрация событий

Общие события		
Событие	✓ Включить	(j)

### Рисунок Б.132. – Настройка общих событий, продолжение

Настройка паспорта ПО

## 🐯 Регистрация событий

## Паспорт ПО Запуск сбора данных СПС Ошибка в процессе сбора данных СПС Сбор данных СПС завершен Сохранены данные СПС

Рисунок Б.133. – Настройка паспорта ПО

### Настройка полномочного управления доступом

Вход в систему	📾 Регистрация событий		
Дискреционное управление дост	от спистрация соовнии		
Замкнутая программная среда	Полномочное управление доступом		
Затирание данных			
Защита диска и шифрование дан	Вывол конфиленциальной информации на внешний носитель	REPORT	$\odot$
Ключи пользователя	вывод конфиденциольной информации на внешний носитель	выючить	Ū
Контроль печати			
Контроль приложений	Доступ к конфиденциальному ресурсу	<ul> <li>Включить</li> </ul>	i
Контроль устройств			
Контроль целостности			
Обнаружение вторжений	Запрет вывода конфиденциальной информации на внешний носитель	<ul> <li>Включить</li> </ul>	(i)
Общие события			
Паспорт ПО		. Preserver	
Полномочное управление достуг	запрет доступа к конфиденциальному ресурсу	ВКЛЮЧИТЬ	U
↓			
	Данные изменены	Применить	Отмена

## Рисунок Б.134. – Настройка полномочного управления доступом, начало

Вход в систему	🗱 Регистрация событий		
Дискреционное управление дост	ан спистрации соовнии		
Замкнутая программная среда	Полномочное управление доступом		1.1
Затирание данных	······································		
Защита диска и шифрование дан	Запрет изменения параметров конфиденциальности ресурса	<ul> <li>Включить</li> </ul>	i
Ключи пользователя			
Контроль печати			
Контроль приложений	Запрет перемещения конфиденциального ресурса	<ul> <li>Включить</li> </ul>	i
Контроль устройств			
Контроль целостности	M		0
Обнаружение вторжений	изменение параметров конфиденциальности ресурса	<ul> <li>Включить</li> </ul>	Ū
Общие события			
Паспорт ПО	Использование механизма исключений	<ul> <li>Включить</li> </ul>	(i)
Полномочное управление достуг 🚽			
€ →			
	Данные изменены	Применить	Отмена

## Рисунок Б.135. – Настройка полномочного управления доступом, продолжение

### 🐯 Регистрация событий

Полномочное управление доступом		
Конфликт категорий конфиденциальности	✓ Включить	(j)
Перемещение конфиденциального ресурса	✔ Включить	i
Удаление конфиденциального ресурса	<ul> <li>Включить</li> </ul>	i

## Рисунок Б.136. – Настройка полномочного управления доступом, завершение

### Настройка теневого копирования

Дискреционное управление дост	🐯 Регистрация событий			
Замкнутая программная среда	степрации соовнии			
Затирание данных	Теневое копирование			4
Защита диска и шифрование дан	······			
Ключи пользователя	Завершена запись на сменный лиск	READULIET		
Контроль печати	Successful survey to calculate gree		U	
Контроль приложений				
Контроль устройств	Завершена запись образа CD/DVD/BD	<ul> <li>Включить</li> </ul>	(j)	
Контроль целостности				
Обнаружение вторжений				
Общие события	Запрет записи на сменный диск	<ul> <li>Включить</li> </ul>	i	
Паспорт ПО				
Полномочное управление достуг	20000 00000 CD/D/D/PD	Duran Internet		h
Теневое копирование 🚽	Sanper Sanucu oopasa CD/DVD/BD	• ВКЛЮЧИТЬ	U	
↓				4
	Данные изменены	Применить	Отмена	1

### Рисунок Б.137. – Настройка теневого копирования

Дискреционное управление дост	📾 Регистрация событий		
Замкнутая программная среда	Затегистрация соовний		
Затирание данных	Теневое копирование		
Защита диска и шифрование дан			
Ключи пользователя	Начата запись на сменный диск	Включить	(i)
Контроль печати			
Контроль приложений			
Контроль устройств	Начата запись образа CD/DVD/BD	<ul> <li>Включить</li> </ul>	i
Контроль целостности			
Обнаружение вторжений			
Общие события	Ошибка записи на сменный диск	<ul> <li>Включить</li> </ul>	(i)
Паспорт ПО			
Полномочное управление достуг	Ошибка записи образа CD/DVD/RD	READURE	•
Теневое копирование		• оклочить	
• • • • • • • • • • • • • • • • • • •			
	Ланные изменены	Применить	Отмена

### Рисунок Б.138. – Настройка теневого копирования,

#### продолжение

### Настройка ЦУ КЦ-ЗПС

Замкнутая программная среда	<b></b>	📾 Регистрация событий
Затирание данных		Сперация соовний
Защита диска и шифрование дан		ЦУ КЦ-ЗПС
Ключи пользователя		
Контроль печати	1	Лобавление субъекта
Контроль приложений		Hanne d'anne

Контроль печати	1	Лобавление субъекта	Включить	(i)
Контроль приложений				
Контроль устройств				
Контроль целостности Добавление учетной записи к заданию ЗПС		<ul> <li>Включить</li> </ul>	i	
Обнаружение вторжений				
Общие события				
Паспорт ПО		Изменение группы ресурсов	<ul> <li>Включить</li> </ul>	(i)
Полномочное управление достуг				
Теневое копирование		Изменение заланию	REPORT	
ЦУ КЦ-ЗПС	Ŧ	Powerenie objenia	выночить	
•				
		Данные изменены	Применить	Отмена

Рисунок Б.139. – Настройка ЦУ КЦ-ЗПС, начало

Замкнутая программная среда	*	📾 Регистрация событий				
Затирание данных		Спострация соовний				
Защита диска и шифрование дан		11V K11-30C				4
Ключи пользователя						
Контроль печати		Изменение задачи	~	Включить	(j)	
Контроль приложений						
Контроль устройств						
Контроль целостности		Изменение субъекта	$\checkmark$	Включить	i	
Обнаружение вторжений						
Общие события						
Паспорт ПО		Снятие задания КЦ с контроля	$\checkmark$	Включить	(i)	
Полномочное управление достуг						
Теневое копирование	-			Pressure		
цу кц-зпс	-	создание группы ресурсов	v	выночить	U	
4 <b>•</b>						4
		Данные изм	енены	Применить	Отмена	1

### Рисунок Б.140. – Настройка ЦУ КЦ-ЗПС, продолжение первое

Замкнутая программная среда 🔶	📾 Регистрация событий		
Затирание данных	одат стистрация соовтний		
Защита диска и шифрование дан	11Y KU-30C		
Ключи пользователя			
Контроль печати			
Контроль приложений	Создание задания	<ul> <li>Включить</li> </ul>	i
Контроль устройств			
Контроль целостности		Press	
Обнаружение вторжений	создание задачи	• БКЛЮЧИТЬ	
Общие события			
Паспорт ПО	Удаление группы ресурсов	<ul> <li>Включить</li> </ul>	i
Полномочное управление достуг			
Теневое копирование			
цу кц-зпс 🚽	Удаление задания	<ul> <li>Включить</li> </ul>	i
4 <b>•</b>			
	Данные изменены	Применить	Отмена

### Рисунок Б.141. – Настройка ЦУ КЦ-ЗПС, продолжение второе

Замкнутая программная среда 👘	📾 Регистрация событий		
Затирание данных	Сперации соовнии		
Защита диска и шифрование дан	ШУ КШ-ЗПС		1.1
Ключи пользователя			
Контроль печати	N .		
Контроль приложений	Удаление задачи	<ul> <li>Включить</li> </ul>	Û
Контроль устройств			
Контроль целостности	Удаление субъекта	<ul> <li>Включить</li> </ul>	(j)
Обнаружение вторжений			
Общие события			
Паспорт ПО	Удаление учетной записи из задания ЗПС	<ul> <li>Включить</li> </ul>	(i)
Полномочное управление достуг			
Теневое копирование			
цу кц-зпс 🚽	Установка задания КЦ на контроль	<ul> <li>Включить</li> </ul>	(i)
4 <b>•</b>			
	Данные изменены	Применить	Отмена

Рисунок Б.142. – Настройка ЦУ КЦ-ЗПС, завершение

### Настройка группы «Параметры»

Настройка этого блока представлена на рисунке Б.143. (используется по необходимости), для фиксации настроек в системе после выбора нажать кнопку «Применить».

±	ПОЛИТИКИ РЕГИСТРАЦИЯ СОБЫТИЙ	🐯 Парамет	ры			
	ПАРАМЕТРЫ Управление трассировкой	Управление трасс	ировкой		i	
		Каталог для файлов трасс	сировки:			l
		: Шаблон настроек трасси	Использовать общий лог-файл Выключена		v	
			Перекрывать настройки модулей			
		Общие	Категории отладочных событий:			
		Настройки модулей	Расширенная регистрация			
1	• • •		Обычные события			
				Применить		

Рисунок Б.143. – Настройка параметров: управления трассировкой

#### Активация новых установок

Для завершения процедуры активации новых установленных значений параметров безопасности на вкладке «НАСТРОЙКИ», нажмите кнопку "Применить". → Дождитесь завершения операции сохранения изменений и обратите внимание на появившуюся запись об изменении политик в панели событий. → Перезагрузите ОС/ компьютер/ «Secret Net Studio» и вновь запустите программу управления. → Во вкладке «контроля административных привилегий» ввести РІN администратора безопасности (пароль). Последовательный порядок действия при завершении процедуры активации представлен на рисунках Б.144. ÷ Б.147..



Рисунок Б.144. – Запуск «Secret Net Studio»



Рисунок Б.145. – Запуск ОС



Рисунок Б.146. – Запуск «Локальный центр управления»

Secret Ne	Secret Net Studio: контроль административных привилегий				
Для запуска программы в режиме администрирования - введите PIN администратора. В случае отказа от ввода PIN программа будет запущена в режиме просмотра.					
PIN админи	истратора	[			
		ОК	Режим просмотра		

Рисунок Б.147. – Окно запроса PIN администратора безопасности

### Просмотр локальных Журналов и Запросов

#### Журналы

В «Secret Net Studio» присутствуют четыре типа журналов:

1) Secret Net Studio — события генерируемые самим комплексом;

2) Безопасности — события связанные с безопасностью системы;

3) Системный — общесистемные события;

4) Приложений — события возникающие во время эксплуатации различного ПО.

В данном окне можно создавать новый журнал или загружать из файла. Чтобы открыть сохранный журнал выберите «Открыть журнал с диска» и откройте файл журнала (необязательно).

Просмотр сведений, содержащихся в локальных журналах (в журналах по умолчанию) в программе управления «Secret Net Studio»: в окне программы управления «Secret Net Studio» в панели навигации выберите «Журналы» ( ) двойным нажатием левой клавиши мыши. → В левом окне вкладки находиться перечень доступных для просмотра локальных журналов и запросы. (см. рисунок Б.148.).

🔳 Лока	альный режим : Secret Net Studio - Центр упра	вления			- 0	×
=	(i) ← → Q		*	Q <b>T</b>	$\checkmark$	
읊	🚺 Новый 👻 🔳 Открыть 🥂					-
	ЖУРНАЛЫ © Secret Net Studio © Безопасности © Системный © Приложений		Добро пожаловать в раздел журналов!			
	запросы	-@-	Начните работу с создания нового запроса. В случае н	необходимости		
T	🖸 Все тревоги		обратитесь за дополнительной информацией в раздел	1 справки.		
5	🖸 Тревоги повышенного уровня		Новый Открыть журнал с диска			
	ВНЕШНИЕ ЖУРНАЛЫ					
R						

Рисунок Б.148. – Интерфейс «Журналы»

Для просмотра полного содержания любого из журналов достаточно выбрать его двойным щелчком мыши. — Выбрать журнал приложений. — Параллельно при открытии вкладки просмотра записей в правой части окна должны появиться активные иконки (кнопки), позволяющие распечатать или сохранить журнал в файл на диске (см. рисунки Б.149. ÷ Б.153.). Сформировать отчёты в соответствии с заданными условиями.

$= \textcircled{\textbf{B}} \leftrightarrow \rightarrow \textbf{Q}$	р управле	10.9					- Q <b>T</b>	
🖸 Новый 👻 🖿 Открыть		события	УГРОЗЫ					
	\$	Дата 🔺	Журнал	Событие	Категор	Источник	🖵 Комп	Домен
журналы	٩	09.04.2023	Secret Net St	Старт служ	Регистрация	LocalProtec	DESKTOP-526	NT AUTHO
C Secret Net Studio	×	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
🕼 Безопасности	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
🕼 Системный	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
🕼 Приложений	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
ЗАПРОСЫ	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
🖸 Все тревоги	9	09.04.2023	Secret Net St.	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
🕼 Тревоги повышенного уровня		09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
ВНЕШНИЕ ЖУРНАЛЫ	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
)-	٩	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
	9	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
11	٩	09.04.2023	Secret Net St	Изменены	Управление	LocalProtec	DESKTOP-526	NT AUTHO
	4							
×								1/2035

Рисунок Б.149. – Отчёт журнала «Secret Net Studio»

В нижнем поле указывается полная информация о событии. События, отмеченные знаком ключик ( ) отмечаются как разрешенные. События, отмеченные знаком замок ( ) отмечаются как запрещенные.

	<ul><li>↔ Q</li></ul>								- Q Y	<ul> <li>✓</li> </ul>	
По но	вый 🔻 📕 Открыть			события	УГРОЗЫ						
-			尊	Дата 🔺	Журнал	Событие	Категор	Источник	🖵 Комп	Домен	
ЖУРНАЛ	лы		٩	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		4
D s	ecret Net Studio		•	20.02 2022	Feronachoczy	Процесси и	Process Cre	Microsoft-	WIN-FTO/TC		
D 6	езопасности	×	-	25.05.2025	Desonachociu	процессу н	FIDCESS CIE	WICLOSOIC	Will Crosten		
			~	29.03.2023	Безопасности	Загружены	Other Policy	Microsoft	WIN-ETOJIC		
20 C	истемныи		٩	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
10 n	Іриложений		9	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
ЗАПРОС	ы		9	29.03 2023	Безопасности	Создан нов	Process Cre	Microsoft-	WIN-FTO/TC		
D B	се тревоги			20.00.0000	-	cospan noon	notess cital	Microsoft in			
10 T			~	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-EIOJIC		
322	ревоги повышенного	уровня	٩	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
внешни	ИЕ ЖУРНАЛЫ		٩	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
			9	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
				20.02.2022		C	Dana Car	Marrie			
			-	29.03.2025	везопасности	Создан нов	Process Cre	MICrosoft	WIN-EIUJIC		
			٩	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
			٩	29.03.2023	Безопасности	Создан нов	Process Cre	Microsoft	WIN-ETOJTC		
			4							•	
										1/2339	)
Тип	Дата и время	Событие					Описани	re		1	110
2	10.04.2023 20:30:23	Запрос жур	нала	событий.			Журнал	получен.			
8	10.04.2023 20:29:54	Запрос жур	нала	событий.			Журнал	получен.			
2	10.04.2023 20:29:52	Запрос жур	нала	событий.			Журнал	получен.			
8	10.04.2023 20:29:12	Запрос кон	фигур	ации.			Конфигу	рация загружен	a.		
2	10.04.2023 20:29:02	Запрос кон	фигур	ации.			Конфигу	рация загружен	a.		
28	10.04.2023 20:29:02	Открытие с	ессии	в локальном ре	жиме.		Sanpoc o	тправлен агент	у.		
840	10.04.2023.20-20-02	OTVOLITING		R ROKARLUOM DO			Corcus	TYPLITS			

Рисунок Б.150. – Отчёт журнала безопасности



Рисунок Б.151. – Запуск системного журнала: процесс «выполнить запрос»

97	тьный режим : Secret Net Studio - Центр упр	авлен	ия						- 0
	(■) ← → Q							- Q Y	$(\checkmark)$
	🚺 Новый 👻 🔳 Открыть		события	УГРОЗЫ					
		尊	Дата 🔺	Журнал	Событие	Категор	Источник	🖵 Комп	Домен
	журналы	0	19.11.2020	Системный	109	(103)	Microsoft	WIN-ETOJTC	<b>^</b>
	C Secret Net Studio X	6	19 11 2020	Системный	13	(2)	Microsoft-	WIN-FTO/TC	
	Безопасности 🛛		20.02.2022	Систоприй	12	(1)	Microsoft	WIN FTOITC	
	Системный Х	0	29.03.2023	Системный	12	(1)	WICTOSOTE	WIN-EIG/IC	NTAUTHO
		0	29.03.2023	Системный	153	(62)	Microsoft	WIN-ETOJTC	NT AUTHO
	Триложении	0	29.03.2023	Системный	20	(31)	Microsoft	WIN-ETOJTC	NT AUTHO
	ЗАПРОСЫ	0	29.03.2023	Системный	238	(101)	Microsoft	WIN-ETOJTC	NT AUTHO
	😨 Все тревоги	0	29.03.2023	Системный	25	(32)	Microsoft	WIN-ETOJTC	NT AUTHO
	💭 Тревоги повышенного уровня	0	29.03.2023	Системный	27	(33)	Microsoft	WIN-ETOJTC	NT AUTHO
			20.03.2023	Системный	18	(57)	Microsoft-	WIN-FTOITC	NT AUTHO
			20.02.2022	CHETCHILDIN	22	(57)	Wierosofe		NT AUTUO
		0	29.03.2023	Системныи	32	(58)	Microsoft	WIN-EIOJIC	NTAUTHO
		0	29.03.2023	Системный	20	(6)	Microsoft	WIN-ETOJTC	NT AUTHO
		0	29.03.2023	Системный	16		Microsoft	WIN-ETOJTC	NT AUTHO
		0	29.03.2023	Системный	6		Microsoft	WIN-ETOJTC	NT AUTHO
		4							2
									1/977
	Тип Дата и время 🗸 Событие					Опис	ание		11
	💈 10.04.2023 20:31:15 Запрос жур	нала	событий.			Журна	ал получен.		
	💈 10.04.2023 20:30:23 Запрос жур	нала	событий.			Журна	ал получен.		
	💈 10.04.2023 20:29:54 Запрос жур	нала	событий.			Журна	ал получен.		
	💈 10.04.2023 20:29:52 Запрос жур	нала	событий.			Журна	ал получен.		
	💈 10.04.2023 20:29:12 Запрос кон	фигур	ации.			Конфи	игурация загружен	a.	
	💈 10.04.2023 20:29:02 Запрос кон	фигур	ации.			Конфи	игурация загружен	a.	
	10.04.2023 20:29:02 Открытие с	ессии	в локальном ре	жиме.		Запро	с отправлен агент	/.	

Рисунок Б.152. – Отчёт системного журнала

(		<ul><li>↔ → Q</li></ul>								- Q T	
ľ	To Hos	ый т 🖿 Открыт			события	УГРОЗЫ					
	12	- onput		₫	Дата 🔺	Журнал	Событие	Категор	Источник	🖵 Комп	Домен
ж	курнал	Ы		0	29.03.2023	Приложений	1531		Microsoft	WIN-ETOJTC	NT AUTHO
	C Se	cret Net Studio		6	29.03.2023	Приложений	5615		Microsoft	WIN-FTO/TC	NT AUTHO
	🖸 Бе	зопасности			20.02.2022	Почложений	1004		Missoroft		
	C CH	истемный		0	29.03.2023	приложении	1004		WICTOSOIL"	WIN-EIO/IC	
	10 n.			0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
	962 UP	риложении	^	0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
3	АПРОСЬ	bl		0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
	D Bc	е тревоги		0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
	🖸 Тр	евоги повышенного	о уровня	0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
в	НЕШНИ	Е ЖУРНАЛЫ		0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
				0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
				0	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
				6	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
				6	29.03.2023	Приложений	1004		Microsoft	WIN-ETOJTC	
											-
											1/2231
т	ип	Лата и время	7 Событие					Описа	ние		11
۲	2	10.04.2023 20:31:38	3 Запрос жу	рнала	событий.			Журна	л получен.		
	2	10.04.2023 20:31:15	Запрос жу	рнала	событий.			Журна	л получен.		
	2	10.04.2023 20:30:23	Запрос жу	рнала	событий.			Журна	л получен.		
	8	10.04.2023 20:29:54	4 Запрос жу	рнала	событий.			Журна	л получен.		
	2	10.04.2023 20:29:52	Запрос жу	рнала	событий.			Журна	л получен.		
	2	10.04.2023 20:29:12	2 Запрос ко	нфигур	ации.			Конфи	гурация загружен	a,	
эйки	n 👷	10.04.2023 20:29:02	Запроско	нфигур	ации.			Конфи	гурация загружен	a.	

Рисунок Б.153. – Отчёт журнала приложений

При переходе на вкладку «Угрозы» просматриваются потенциальные угроза системы (см. рисунок Б.154.).

	события	УГРОЗЫ		
	Угроза		Дата	Компьютер
۲	Контроль	аппаратной конфигурации заверше	27.11.2019 10:50:	START
۰	🌗 Контроль	аппаратной конфигурации заверше	27.11.2019 10:54:	START
۲	🌗 Контроль	аппаратной конфигурации заверше	27.11.2019 10:56:	START
۲	🌗 Контроль	аппаратной конфигурации заверше	27.11.2019 11:03:	START
۲	🌗 Контроль	аппаратной конфигурации заверше	27.11.2019 16:19:	START
۲	🌗 Контроль	аппаратной конфигурации заверше	27.11.2019 18:57:	START
۰	🌗 Контроль	аппаратной конфигурации заверше	03.12.2019 9:33:26	START
۲	🌗 Контроль	аппаратной конфигурации заверше	03.12.2019 9:56:48	START
۲	🌗 Контроль	аппаратной конфигурации заверше	04.12.2019 6:30:38	START
	ДЕТАЛЬНО	ОБЩЕЕ		
	Угроза			

🕒 Контроль аппаратной конфигурации завершен с ошибками

Рисунок Б.154. – Журнал угроз

#### Запросы

Подсистема запросов позволяет формировать выборки по заданным развернутым условиям, включая записи из любых локальных журналов: на панели инструментов нажмите кнопку «Новый» ( Новый ) → установите произвольные (заданные) правила фильтра → нажмите кнопку «Получить журнал» → результат.

В случае необходимости получить конкретную выборку записей журнала запускается режим фильтрации журнала – правила фильтра: можно составить запрос на формирование выборки по определенным условиям: в правой части окна кнопка «Запрос»  $\rightarrow$  открылась панель  $\rightarrow$  С помощью кнопки «Добавить правило» ввести следующие сведения (по заданию): «Дата»  $\rightarrow$  «Интервал»  $\rightarrow$  «За последние 24 часа»  $\rightarrow$  «Агент»  $\rightarrow$  «Содержит»  $\rightarrow$  «Secret Net Studio» (см. рисунок Б.155.). Параметр логического условия должен быть установлен в положение «И» (зеленый фон). В результате

получится журнал содержащий все события отказа по заданным условиям (см. рисунок Б.156.).

KO	нструктор Ф	ильтри	Приложен	чий				
жу	рналы	Secret N Gesonaci	et Studio 📝	Прила	ожений мный			
Пр	авила фильтр	a						
	Правило		Onepatop		Условие			
¢								
< ~	Дата		Интервал	٠	За последние 24 часа	٠	И	или

### Рисунок Б.155. – Окно настройки выборки журнала

=	(a) ← → Q								- Q	т ( 🗸		
읊	🚺 Новый 👻 🔳 Открыть		события	УГРОЗЫ								
		礮	Дата 🔻	Журнал	Событие	Категория	Источник	🖵 Комп	Домен	👤 Польз		肉
0	журналы	8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin	^	۳ ا
	Secret Net Studio	8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		<u>ه</u>
8	Безопасности Х	8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		18
- 141	Системный	8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		
75	апросы	8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		I –
		8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		L
R		8	27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		L
	* 🕞 Новый фильтр 🛛 🖯 С 🗙		27.11.2019	Secret Net St	Запрет изменения парамет	Полномочное управл	LocalProtec	START	START	Admin		L
÷.),		<b>.</b>	27 11 2019	Secret Net St	Запрет изменения парамет	Полномонное управл	LocalProtec	START	START	∆dmin	Ŧ	
	внешние журналы	Д	етально	ОБЩЕЕ ПАР/	АМЕТРЫ					1/24	0 🕑	
77) h		Имя	1	Значение								
		Жур	нал (код)	4							1	L
$\gamma \sim$		жур	нал	Secret Net Studio								L
		SID	агента	S-1-5-21-3065691	637-4221373225-3210272325							L
		Area	нт	Secret Net Studio								L
. [o] /		Тип	(код)	16								L
		Тип		Аудит отказов								
ø		Дата	a	04.12.2019 6:33:32								
/		-									$\nabla$	

### Рисунок Б.156. – Окно журнала из выборки по заданным условиям

Для событий безопасности особой важности в СЗИ «Secret Net Studio» предусмотрен отдельный тип сообщений — тревоги, они регистрируются в специальном журнале. События тревоги различаются по уровню угрозы, который определяется степенью значимости самого события и уровнем важности того компьютера, на котором они произошли. Сервер безопасности накапливает сведения о событиях тревоги в отдельном журнале, который формируется из уведомлений, направляемых серверу от защищаемых компьютеров. Состав отслеживаемых событий может редактироваться

посредством создания правил фильтрации на основе уведомлений о событиях тревоги (см. рисунки Б.157. и Б.158.): перейдите в раздел «ЗАПРОСЫ» → двойным нажатием левой клавиши мыши выберите нужный пункт из представленных готовых вариантов раздела — «Все тревоги» или «Тревоги повышенного уровня» → взаимодействуйте с ними такое же как с журналами (см. выше).

альный режим : Secret Net Studio - Центр упр	равлени	19						- 0	
(iii) ← → Q							- Q Y	<ul> <li>✓</li> </ul>	
🖸 Новый 👻 🖿 Открыть		события	УГРОЗЫ						
	\$	Дата 🔺	Журнал	Событие	Категор	Источник	🖵 Комп	Домен	
журналы		29.03.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		4
🕼 Secret Net Studio 🛛 🛛 🛛 🖉		29.03.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
Безопасности Х	-	20.02 2022	Easonacuactu	05003000	Surtam Into	Microsoft	DESKTOR 526		
Системный 🛛		29.05.2025	везопасности	Операция	System inte	MICTOSOIL	DESKIOP-320		
	-	29.03.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
нриложении А		29.03.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
ЗАПРОСЫ		29.03.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
🕼 Все тревоги 🛛 🗙		29.03.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
🕼 Тревоги повышенного уровня	•	09.04.2023	Безопасности	Учетной за	Logon	Microsoft	DESKTOP-526		
ВНЕШНИЕ ЖУРНАЛЫ		09.04.2023	Безопасности	Учетной за	Logon	Microsoft	DESKTOP-526		
		09.04.2023	Безопасности	Учетной за	Logon	Microsoft	DESKTOP-526		
		09.04.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
		09.04.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
		09.04.2023	Безопасности	Операция	System Inte	Microsoft	DESKTOP-526		
	4							Þ	
								1/424	0
Тип Дата и время 🛛 Событие					Описан	ие		1	113
10.04.2023 20:33:28 Запрос жур 10.04.2023 20:31:28 Запрос жур	рнала с	обытий.			Журнал	получен.			
<ul> <li>10.04.2023 20:31:38 3anpoc xy</li> <li>10.04 2023 20:31:15 3anpoc xy</li> </ul>	рнала с рнала с	обытий.			<u>журнал</u>	получен.			
2 10.04.2023 20:31:13 Sampoc xv	рнала с	обытий.			Журнал	получен.			
10.04.2023 20:29:54 Запрос жу	рнала с	обытий.			Журнал	получен.			
🕱 10.04.2023 20:29:52 Запрос жу	рнала с	обытий.			Журнал	получен.			
2 10.04.2023 20:29:12 Запрос кон	нфигура	ации.			Конфигу	пация заглужен	a		

Рисунок Б.157. – Отчёт запросов «Журнал всех тревог»

shan pecini secret recistado qemp yn	Jubricii	na						
(iii) ← → Q							- Q <b>Y</b>	$\checkmark$
<b>Го</b> Новый - Покрыть	1	события	УГРОЗЫ					
	礅	Дата 🔺	Журнал	Событие	Katerop	Источник	🖵 Комп	Домен
ЖУРНАЛЫ		10.04.2023	Secret Net St	Обнаружен	Регистрация	LocalProtec	DESKTOP-526	NT AUTHO
Secret Net Studio		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
Безопасности Х		10.04.2023	Secret Net St	Попытка д	Самозашита	LocalProtec	DESKTOP-526	NT AUTHO
🖸 Системный 🛛 👋	-	10.04 2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
Приложений ×	-	10.04.2022	Corret Not St		Caucasaura	LocalProtes	DESKTOR 526	
ЗАПРОСЫ		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtect	DESKTOP-520	NT AUTHO
Все тревоги Х		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKIOP-526	NTAUTHO
		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
ar these in the semicine to Abound a the		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
внешние журналы	6	10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
	8	10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
		10.04.2023	Secret Net St	Попытка д	Самозащита	LocalProtec	DESKTOP-526	NT AUTHO
	4							Þ
								1/404
Тип Дата и время 🔻 Событие					Описан	ие		1
🙎 10.04.2023 20:34:00 Запрос жур	рнала (	событий.			Журнал	получен.		
10.04.2023 20:33:28 Запрос жур 10.04.2023 20:33:28 Запрос жур	рнала (	событий.			<u>Журнал</u>	получен.		
10.04.2023 20:31:58 Запрос жур	онала (	событии.			журнал	получен.		
10.04.2023 20:31:15 Sanpoc жур	рнала (	событии.			журнал	получен.		
<ul> <li>10.04.2023 20:30:23 3anpoc жур</li> <li>10.04.2023 20:30:54 2</li> </ul>	рнала (	событии.			журнал	получен.		
апрос жур	инала (	сооытии.			журнал	получен.		

## Рисунок Б.158. – Отчёт запросов «Журнал тревог повышенного уровня»

Администратор безопасности оповещается о тревогах с помощью уведомлений в панели мониторинга или по e-mail. Также для оповещения могут использоваться звуковые сигналы. Для обработки полученных оповещений администратору безопасности доступна функция квитирования событий, которая позволяет подтверждать получение информации с описанием принятых мер.
## ПРИЛОЖЕНИЕ В

# Пример настройки ОС СН «Astra Linux» 1.7.3

🕕 Информация о системе		×
📔 Справка \vee 🕐 Выход		
і О системе                Ш Энергопотребление                 Энергопотребление                 Устройства                 Ш ЦП                 О Гиисок устройств                 ДГ                 Устройства USB                 Дрерывания                 Прерывания                 Преть Сать	О системе АSTRA LINUX° Аstra Linux Special Edition Уровень защищенности: максимальный Обновление: 1.7.3 https://astralinux.ru	
— 💭 Сервер Samba — 🗣 Сетевые интерфейсы ✓- 🗶 Графика — 🖵 OpenGL (GLX) — 💥 Сервер Х	Имя компьютера: astra Архитектура: x86, 64-разрядная Ядро: 5.15.0-33-generic Графическая платформа: X11	
└─़॑॑॑॑॑ Vulkan └─॑ ॑ ♥ OpenGL (EGL)	Оборудование Процессор: 1 × Intel® Соге™ i7-7700HQ CPU @ 2.80GHz Память: 3,8 ГиБ ОЗУ Графический процессор: Ilvmpipe Производитель: innotek GmbH Название изделия: VirtualBox	

Параметры системы показаны на рисунке В.1..

Рисунок В.1. – Параметры системы Astra Linux 1.7.3

# Создание пользователя системы:

Открыть «Управление политикой безопасности» (см. рисунок В.2.).



Рисунок В.2. – Окно управления политикой безопасности

Перейти во вкладку «Группы» (см. рисунок В.3.).

🤠 Управление политикой безопасности	- Группы пользователей	×
Файл Правка Настройки Помо	щь	
	С 📀 🖉 Обычные	~
∽ 🖵 astra	Группы пользователей	
>- 🛒 Аудит		
>- 🚨 Группы	Наименование V GID	Системная
>- 🚰 Замкнутая программная с	astra-admin 1001	нет
— 🔍 Мандатное управление до	administrator 1000	нет
>- 🥡 Мандатные атрибуты		
>- 🕅 Мандатный контроль цело		
— 🖸 Монитор безопасности		
>- 📊 Настройки безопасности		
>- 🔚 Политики учетной записи		
✓ 🖾 Пользователи		
administrator		
>- 🚵 Привилегии		
>- 🛃 Управление квотами		
> 🛃 Устройства и правила		
	Подстановка 🗸	Фильтр

Рисунок В.3. – Окно управления группами

Нажать на кнопку «Создать новый элемент» (либо знак «+», либо через контекстное меню Группы), заполнить наименование и GUID (Globally Unique Identifier) для создаваемой группы. Подтвердить создание (см. рисунок В.4.).

😼 Управление политикой безопасности		×
Файл Правка Настройки Помоще		
- astra	Создание группы пользователей	
>- 🛒 Аудит		
>- 🖾 Группы	Haumehobahue: users_group	GID: 1002
>- 📴 Замкнутая программная с	Пользователи	
Мандатное управление до	Имя V UID GECOS Группа Системный	
Мандатные атрибуты Мандатные контрадь нада		
П Монитор безоласности		
>- І Настройки безопасности		
>- 🐴 Политики учетной записи		
∽ 🕮 Пользователи		
administrator		
>- 🚠 Привилегии		
>- 🛃 Управление квотами		
> 🔄 Устройства и правила		
		+ -

# Рисунок В.4. – Создание группы пользователей

Перейти во вкладку пользователи (см. рисунок В.5.).

🤕 Управление политикой безопасности -	Пользователи						_ 0 ×
Файл Правка Настройки Помощ	ь						
0000+- 3	$\odot \oslash$	Обычные	~				
v 📮 astra	Пользователи						
>- 🐨 Аудит	Имя ∨	UID	GECOS	Группа	Системный	Дом. каталог	Оболочка
>- 🍲 Труппы >- 🍞 Замкнутая программная с	🌲 administ	1000	administrato	administrator	нет	/home/admi	/bin/bash
— 🔘 Мандатное управление до							
>- 🕡 Мандатные атрибуты							
>- 🖲 Мандатный контроль цело							
П Монитор безопасности							
>- 11 Настроики безопасности							
Пользователи							
💷 administrator							
>- 🪵 Привилегии							
>- 🖸 Управление квотами							
>- 🤌 Устройства и правила							
	Подстановка	~	Фильтр				

# Рисунок В.5. – Список пользователей

Аналогично добавлению группы, нажать на кнопку создать новый элемент и заполнить соответствующие поля: «Имя», «Домашний каталог», «Оболочка», «GECOS», выбрать первичную группу пользователя из

существующих в системе. Подтвердить создание пользователя (см. рисунок В.6.).

🤯 Управление политикой безопасности			_ 🗆 ×
Файл Правка Настройки Помощ	ь   📀 ⊘    Ос	бычные 🗸	
v- 🖬 astra	Создание пользоват	геля	
>- 🛒 Аудит ~- 🚨 Группы	Имя:	user_1	UID:
administrator	Первичная группа:	🚨 users_group 🗸 🗌 Hoba:	а Пароль
- 🚔 astra-admin - 🛱 users_group	Дом. каталог:	/home/user_1	Изменить
>- 🚰 Замкнутая программная с	Оболочка:	/bin/bash	Печатать
— 🕲 Мандатное управление до	GECOS:	user_1	
>- 🔘 Мандатный контроль цело		Группы	
🔳 Монитор безопасности	Наименование ∨ G	ID Системная	
<ul> <li>П Настройки безопасности</li> <li>Политики учетной записи</li> <li>Пользователи</li> <li>administrator</li> <li>Привилегии</li> <li>Управление квотами</li> <li>Устройства и правила</li> </ul>	video  4.    users_group  10.    users  10.    plugdev  4.    floppy  2.    dialout  20.	4 да 202 нет 20 да 6 да 5 да 0 да	+ -
ι			

Рисунок В.6. – Создание пользователя

После этого автоматически появится окно для смены пароля (см. рисунок В.7.).

<ul> <li>Управление политикой безопасности</li> <li>Файл Правка Настройки Помош</li> <li>         О         О         + -         О     </li> </ul>	Пользователь: user_1	×
∽- 🔽 astra ≻ 🛒 Аудит	Пользователь: user_1 🚨 Общие  Блокировка 📫 Аудит 🏹 Привилегии 🍱 МРД 🛸 Срок д	аействия 💧 Графический ки < >
∽ 🖬 Группы — 🚨 administrator — 📮 astra-admin	Имя: user_1 Первичная группа: Смена пароля: user_1 ×	UID: 1001 🗘
<ul> <li>users_group</li> <li>Замкнутая программная с</li> <li>Мандатное управление до</li> <li>Мандатное управление до</li> </ul>	Дом. каталог: /h Новый пароль : Оболочка: /b •••••••	Изменить Изменить Печатать
<ul> <li>Мандатные атриоуты</li> <li>Мандатный контроль цело</li> <li>Монитор безопасности</li> <li>Цастройки безопасности</li> </ul>	GECOS: us Да Отмена Группы	
<ul> <li>- Настроики осезопасности</li> <li> Политики учетной записи</li> <li> Пользователи</li> </ul>	22 video 44 да ⊐ users_group 1002 нет 22 video 44 да	
- 🕹 administrator user_1 >- 🛅 Привилегии	2 plugdev 46 да 22 floppy 25 да	
<ul> <li>Э Управление квотами</li> <li>Устройства и правила</li> </ul>		+-

Рисунок В.7. – Смена пароля пользователя

В результате выполнения данных действий, будет создан пользователь. При необходимости, в дальнейшем, пароль можно сменить из списка пользователей, нажав кнопку пароль (см. рисунок В.8.)

😻 Управление политикой безопасности -	Пользователь: user_1	- 🗆 ×
Файл Правка Настройки Помош	5	
◎ ◎ ◎ ◎   + -   3	Обычные ~	
v- 🖵 astra	Пользователь: user_1	
>- 🛒 Аудит У- 🚨 Группы	🚨 Общие 💊 Блокировка 🛍 Аудит 🔁 Привилегии 🛄 МРД 🛸 Срок действия 🚊 Гра	афический ки < >
administrator	Имя: user_1	UID: 1001 🗘
astra-admin	Первичная группа: 📮 users_group 🗸 🗸	Пароль
— 🥁 users_group >- 🚰 Замкнутая программная с	Дом. каталог: /home/user_1	Изменить
🛛 🔕 Мандатное управление до	Оболочка: /bin/bash	Печатать
>- 🕡 Мандатные атрибуты	GECOS: User 1	
>- 📕 Мандатный контроль цело		
— 🗋 Монитор безопасности	Группы	
>- 📔 Настройки безопасности	Наименование V GID Системная	
>- 🔚 Политики учетной записи	video 44 ga	
∨- ጁ Пользователи	users_group 1002 Het	
- 🚨 administrator	users 100 ga	
user_1	Plugdev 46 ga	
>- 🚉 Привилегии	🐱 порру 25 да	
>- 🖸 Управление квотами		
>- 🛃 Устройства и правила		

Рисунок В.8. – Общие настройки пользователя

Для безопасности, помимо этого, необходимо настроить блокировку, аудит, МРД, и срок действия.

Во вкладке «Блокировка», установить максимальное количество попыток входа, отметить поля «Удаление пароля и блокировка входа», «Блокировать учетную запись» (см. рисунок В.9.).

🤕 Управление политикой безопасности	- Политика блокировки пользователя: user_1	_ 🗆 ×
Файл Правка Настройки Помоц	Įb	
	<b>B</b> ce ~	
- 📮 astra	Пользователь: user_1	1
> 🛒 Аудит	🗳 Общие 💊 Блокировка 🖾 Аудит 🖏 Привилегии 🖬 МРД 🔩 Срок де	йствия 🚊 Графический ки < 🗲
administrator	Счетчик неудачных входов: 0/8	Сброс
— 🚨 astra-admin	Максимальное количество неудачных попыток входа: 3 🗘 Значение "0" соотве	етствует глобальному значению.
<ul> <li>users_group</li> <li>Замкнутая программная с</li> <li>Мандатное управление до</li> <li>Мандатные атрибуты</li> <li>Мандатный контроль цело</li> <li>Монитор безопасности</li> <li>Настройки безопасности</li> <li>Политики учетной записи</li> <li>Пользователи</li> <li>аdministrator</li> <li>Привилегии</li> <li>Угравление квотами</li> <li>Устройства и правила</li> </ul>	<ul> <li>Удаление пароля и блокировка входа</li> <li>Блокировать пароль</li> <li>Блокировать учетную запись</li> </ul>	

Рисунок В.9. – Настройка блокировки пользователя

Во вкладке «Аудит» можно настроить отдельный аудит действий для пользователя. В данном примере, были выбраны настройки аудита по умолчанию (см. рисунок В.10.).

Управление политикой безопасности	- Настройки ау	дита пользовател:	a: user_1			- 0
	; 000	Bce	~			
🖵 astra	Пользовате	ль: user_1				
>- 🛒 Аудит	🔔 Общие	la Блокировка	🙁 Аудит	🤼 Привилег	ии 🍱 МРД 🖾 Срок действия 🚨 Графический к	и<>
🗸 📮 Группы	Инастрой			- ,		
administrator	• пастрои	ки аудита по умол	ГЧАНИЮ			
astra-admin	Averation			А	удит	
users_group	Аудит у	тказов:				
— В Замкнутая программная с	Danage	A Know	Coferma	Veneu	07//02	
>- 🕡 Мандатные атрибуты	16	V NJIO4	net	ychex		Ш
> 📕 Мандатный контроль цело	15	e	rename			
🗕 🖹 Монитор безопасности	14	h	chroot			
>- 🚺 Настройки безопасности	13	p	cap			
>- 👆 Политики учетной записи	12	m	mac			
∨- 🏯 Пользователи	11	r	acl			
administrator	10	a	audit			
user_1	9	g	gid			
>- 🚵 Привилегии	8	i	uid			
>- 🛃 Управление квотами	7	L	module			
🚈 🗹 устроиства и правила						

Рисунок В.10. – Настройка аудита пользователя

Во вкладке «МРД» настроить уровни и категории доступа. (см. рисунок . .

В.	l	1	.)

🤯 Управление политикой безопасности	мРД атрибуты пользователя: user_1 _ 🗆	×
Файл Правка Настройки Помоц	b	
$  \odot \odot \odot \odot   + -   \odot$	; Sce ~	
- astra	Пользователь: user_1	
>- Ш Аудит	🚨 Общие 🖾 Блокировка 🛍 Аудит 🗟 Привилегии 🚺 MPA 🗟 Срок действия 🏛 Графический ки < >	
∽ 🖾 Группы		
- administrator	уровни	
astra-admin		
users_group		
Памкнугая программная с	Максимальный: 🖻 1:Уровень_1 🔍 🖻 63:Высокий 🗸	
Мандатное управление до	Категории	
>- Мандатные агрибуты	Разряд У Наименование Мин. Макс.	
П Монитор безопасности	1 Категория 2	
>- Т. Настройки безопасности	0 Категория 1	
>- 🚈 Политики учетной записи		
∨- ﷺ Пользователи		
- 🔔 administrator		
.≭_user_t		
>- 🚞 Привилегии		
>- 💽 Управление квотами		
>- 🕼 Устройства и правила		

Рисунок В.11. – Настройка МРД пользователя

«Срок действия» настраиваются Bo вкладке минимальное И максимальное число дней между сменами пароля для пользователя, а также число дней до смены пароля, за которое необходимо выдать предупреждение. Здесь же можно настроить число дней, через которое учетная запись с устаревшим паролем будет заблокирована, и, при необходимости, установить дату, по истечению которой учетная запись будет заблокирована (см. рисунок B.12.):



Рисунок В.12. – Настройка срока действия учетной записи пользователя

### Настройка идентификации и аутентификации

Открыть управление политикой безопасности и открыть вкладку «Политики учетной записи» (см. рисунок В.13.)



Рисунок В.13. – Окно политик учетной записи

Выполнить необходимые выполнить необходимые настройки во вкладке «Блокировка». В примере, были выбраны индивидуальные настройки, задано максимальное количество неуспешных попыток – 3, а период блокировки 30 секунд (см. рисунок В.14.)

😼 Управление политикой безопасности	- Политика блокировка учетной заг	писи: настройки pam_tally	_ 🗆 ×
Файл Правка Настройки Помоц	ць		
<b>◎ ● ● ●   + -   ○</b>	Bce	$\checkmark$	
∽ ≞ Группы	Политика блокировка учетной з	записи: настройки pam_tally	
<ul> <li>administrator</li> <li>astra-admin</li> <li>users_group</li> <li>Замкнутая программна</li> </ul>	<ul> <li>Индивидуальные настройки</li> <li>Не сбрасывать счетчик</li> <li>Не использовать счетчик дл</li> </ul>	і ія пользователя с ціd=0	
— 🕲 Мандатное управление >— 🕡 Мандатные атрибуты	<ul> <li>Неуспешных попыток:</li> <li>Период блокировки:</li> </ul>	3 Секунд С	
≻ 🔘 Мандатный контроль ц — 🔝 Монитор безопасности	Период разблокирования:	\$	
>> 🚹 Настройки безопасности >> 🐴 Политики учетной записи			
<ul> <li>В поссерания</li> <li>Политика локальног</li> </ul>			
>- S Политика паролей Политика создания			
<ul> <li>&gt; Пользователи</li> <li>&gt; Привилегии</li> <li>&gt; Привилегии</li> </ul>			
<ul> <li>Управление квотами</li> <li>Устройства и правила</li> </ul>			

Рисунок В.14. – Настройка блокировки учетной записи

Выполнить необходимые настройки во вкладке «Политика паролей».

В разделе сложность: настраиваются необходимые ограничения для создаваемых паролей.

В примере была установлены минимальная длина пароля – 8 символов, минимальное количество цифр – 4 (см. рисунок В.15.):

🤯 Управление политикой безопасности	и - Политика сложности пароля: настройки pam_cracklib	_ = >
Файл Правка Настройки Помо	иць С Все ~	
🗸 🖾 Группы	Политика паролей	
administrator	📓 Сложность 🖾 Срок действия 🕤 Шаблоны устаревания 🗍 История	
users group	Проверка имени пользователя (только для pam_cracklib)	
>- 🚱 Замкнутая программна	Проверка GECOS	
<ul> <li>Мандатное управление</li> </ul>	Применять для пользователя root	
> 🕡 Мандатные атрибуты	Минимальная длина пароля (минимум 6 символов):	
>- 🖲 Мандатный контроль ц	8	Ŷ
Монитор безопасности	Иинимальное количество строчных букв в новом пароле:	
>- Т. Настройки безопасности		0
Политики учетной записи	Минимальное количество заглавных букв в новом пароле:	
Блокировка		^
<ul> <li>Политика локальног</li> </ul>		~
Политика паролей	Минимальное количество цифр в новом пароле:	
История	4	Ŷ
<b>Ш</b> Сложность	Минимальное количество других символов в новом пароле:	
— 🛲 Срок действия		\$
🔄 Шаблоны устаре		
🐴 Политика создания		

Рисунок В.15. – Настройка сложности пароля

В разделе срок действия устанавливается параметры по умолчанию, касающиеся смены пароля.

В примере было установлено максимальное количество дней между сменами пароля – 90, число дней выдачи предупреждения до смены пароля – 15 (см. рисунок В.16.):

🤝 Управление политикой безопасности -	политика срока действия пароля: настройки passwd	_ 🗆 ×
Файл Правка Настройки Помощ	lþ	
$\odot \odot \odot \odot + - \odot$	; O O Bce ~	
🗸 🚍 Группы	Политика паролей	
administrator	🖽 Сложность 📧 Срок действия 🖾 Шаблоны устаревания 🚹 История	
a users_group	Минимальное количество дней между сменами пароля:	
>- 📴 Замкнутая программна	0 дней	0
— 🚇 Мандатное управление	Максимальное количество дней между сменами пароля:	
>- 🕡 Мандатные атрибуты	90 дней	0
>- 🕅 Мандатный контроль ц	Число дней выдачи предупреждения до смены пароля:	
Монитор безопасности	15 дней	
Н Настроики безопасности 	Число дней неактивности после устаревания пароля	
— 🕮 Блокировка	облокировки учетной записи:	
— 🗵 Политика локальног		
∽ 🔄 Политика паролей	Срок действия учетной записи пользователя:	
— 🛣 История		~
— 🖩 Сложность	θ	
🔤 Срок действия		
🔤 Шаблоны устаре		
— 📲 Политика создания 🕖		

Рисунок В.16. – Настройка срока действия пароля

### Установка прав разграничения доступа

Для установки прав разграничения доступа необходимо открыть менеджер файлов с правами администратора. Например, это можно сделать, открыв окно ввода команд комбинацией клавиш «Win+R» (см. рисунок B.17.).



Рисунок В.17. – Окно ввода команд

В появившемся окне ввести команду «sudo fly-fm», и отметить пункт «Выполнить в терминале» (см. рисунок В.18.).



Рисунок В.18. – Ввод команды

После выполнения команды необходимо ввести пароль для учетной записи администратора (см. рисунок В.19.).



Рисунок В.19. – Ввод пароля для «sudo»

В результате откроется «Менеджер файлов» AstraLinux (см. рисунок В.20.).



Рисунок В.20. – Окно менеджера файлов

Для настройки прав доступа к папке, необходимо, щёлкнув по ней правой кнопкой мыши, открыть контекстное меню и среди пунктов выбрать «Свойства» (см. рисунок В.21.).



Рисунок В.21. – Контекстное меню папки

В открывшемся окне перейти во вкладку дискреционные атрибуты (см. рисунок В.22.).

Свойства							×
tmp							
Общие Яр.	Общие Ярлык Дискреционные атрибуты				Мандатная м	иетка Подпись	
Пользователь:	root			```		-бит	
Группа:	root			```	SGID-	-бит	
					🗹 Sticky	/-бит	
Субъект			Обычн	ble		По умолчанию	
(S) Пользов	ватель	,		☑ 🖻	🗸 🌠	Создать	
(S) Группа				<b>P</b>	🗹 🚀	Создать	
(S) Осталы	ные			<b>I</b>	🗹 🚀	Создать	
Маска				Создат	ь	Создать	
🗹 Пользователи 🗹 Группы 🗹 Основные			5			Добавить субъект АС	:L
IOSITIOUIU						Да Отмен	la

Рисунок В.22. – Дискреционный атрибуты папки

И настроить права доступа на папку выбранную папку для пользователей и групп (см. рисунок В.23.).

Свойства						×
Общие Яр.	пык	Дискреционные атр	ибуты	Аудит	Мандатная м	иетка Подпись
Пользователь: Группа:	Пользователь: user_1					
Субъект			Обычные			По умолчанию
(S) Пользон	ватель	,	🗹 💕	☑ 🖻	🕶 💅	Создать
(S) Группа			🗹 📑	🗹 🂾	🕶 🌮	Создать
(S) Осталы	ные				🗌 🚀	Создать
Маска	Маска			Создат	ь	Создать
🗹 Пользователи 🗹 Группы 🗹 Основные						Добавить субъект ACL
						Да Отмена

Рисунок В.23. – Настройка дискреционных атрибутов

## Настройка очистки остаточной информации

Открыть управление политикой безопасности

Открыть вкладки: «Настройки безопасности» - «Политика очистки памяти» (см. рисунок В.24.).

🤕 Управление политикой безопасности - Пол	тика очистки памяти		×
Файл Правка Настройки Помощь			
3 0 0 0   + -   3	Bce ~		
🗸 📮 astra	Политика очистки памяти		
>- 🛒 Аудит			
>- 🚨 Группы		Очистка разделов подка	чки
>- 🚰 Замкнутая программная среда		Игнорировать разделы подк	ачки
<ul> <li>Фандатное управление доступ</li> </ul>	Устройство		~
>- 🕡 Мандатные атрибуты			
>- () Мандатный контроль целостно			
Монитор безопасности			
			+ -
Политика консоли и интерп	-		
🖣 Политика очистки памяти	F	арантированное удаление файло	випапок
🖳 Системные параметры	Устройство Точка монтиров: Тип	Очистка Количест	BO
>- 🚑 Политики учетной записи	1 /dev/sda1 / ext4	выключен ~	
>- 🎩 Пользователи			
>- 选 Привилегии			
>- 💽 Управление квотами			
>- 👂 Устройства и правила			

Рисунок В.24. – Окно политики очистки памяти

Настроить очистку разделов подкачки и установить параметры для гарантированного удаления файлов и папок, в частности тип, способ очистки и количество повторения (см. рисунок В.25.).

Управление политикой безопасности - Пол	итика очистки пам	яти				- 🗆 >	×
Файл Правка Настройки Помощь							
$  \odot \odot \odot \odot   + -   \Im  $	S 🖉 Bce	2	$\sim$				
- astra	Политика очисти	ки памяти					٦
>- 🛒 Аудит							í.
>- 🖾 Группы			<b>v</b> 0	нистка раздел	юв подкачки		
>- ি Замкнутая программная среда			Игнор	ировать разде	елы подкачки		
— 🔘 Мандатное управление доступ	Устройство					~	
>- 🕡 Мандатные атрибуты							
>- 🕅 Мандатный контроль целостно							
— 🗈 Монитор безопасности							
Настройки безопасности							
— 🛕 Глобальные настройки киоска							
>- 😤 Параметры ядра							
— 🔼 Политика консоли и интерп			Гарантиров	анное удален	ие файлов и па	пок	
💐 Политика очистки памяти	Verpoverpo		Tue	0	Konuuoczno		
🖳 🕎 Системные параметры		/			количество		
>- 🟝 Политики учетной записи	1 /dev/sda1	/	ext4	Случайно 🗸	1		
>- 🏯 Пользователи							
≻ 🚵 Привилегии							
>- 🛃 Управление квотами							
> 🕼 Устройства и правила							

Рисунок В.25. – Настройка гарантированного удаления

## Настройка регистрации событий

Настройка регистраций событий пользователя выполнялась при создании пользователя.

Для настройки регистрации событий по отношению к объектам доступа нажать сочетание клавиш «Win+R» и в появившемся окне ввести команду «sudo fly-fm», а также установить пункт «Выполнить в терминале» (см. рисунок B.26.)

🚀 Выполн	ить команду	_ 🗆 ×			
>_	Введите имя программы, которую Вы ресурса, который хотите посмотреть	хотите запустить, или адрес			
Команда:	sudo fly-fm	✓ … F			
Выполнить в терминале					
Дополнит	гельно >>	Выполнить Отмена			

Рисунок В.26. – Ввод команды

Для настройки прав доступа к папке, необходимо, щёлкнув по ней правой кнопкой мыши, открыть контекстное меню и среди пунктов выбрать «Свойства» (см. рисунки В.27. и В.28.).







Рисунок В.28. - Контекстное меню

зойства			\$
tmp			
Общие Ярлык Ді	искреционные атрибуты	Аудит Мандатная метка	Подпись
Элемент	Обычный	По ум	олчанию
🗹 Пользователи 🗹 Гр	уппы 🗹 Остальные		Добавить элемент аудита
			Да Отмена

В открывшемся окне перейти во вкладку «Аудит» (см. рисунок В.29.).

Рисунок В.29. – Аудит папки

Для добавления аудита на объект необходимо нажать на кнопку «Добавить элемент аудита». После, в открывшемся окне выбрать субъект, для которого будут настраивать права доступа: конкретного пользователя, группу, или остальных пользователей (см. рисунок В.30.).

войства		_
tmp Общие Ярлык Дискреь	Выберите элемент аудита >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	х Подпись
Элемент	Выберите объект	тчанию
✓ Пользователи ✓ Группы	Debian-exim nm-openvpn hplip logcheck avahi administrator systemd-coredump user_1 Да Отмена	Добавить элемент аудита
		Да Отмена

Рисунок В.30. – Добавление аудита

В примере (см. рисунок В.31.) были установлены права для субъектов user\_1, root, и остальные:

войства						>
tmp						
Общие Ярлык	Дискреционн	ые атрибуты	Аудит	Мандатная	метка Подпись	
Элемент		Обычный			По умолчанию	
🖁 user_1	Удалить	s: {oxudnarı f: {oxudnarı	mcy} mcy}	Удалить	s: {oxudnarmcy] f: {oxudnarmcy]	Удалить
🖁 root	Удалить	s: {oxudnarr f: {oxudnarr	mcy} ncy}	Удалить	s: {oxudnarmcy} f: {oxudnarmcy}	Удалить
😂 остальные	Удалить	s: {oxudnarı f: {oxudnarı	mcy} mcy}	Удалить	s: {oxudnarmcy] f: {oxudnarmcy]	Удалить
🗹 Пользователи	🖌 Группы 🔽 С	стальные			Добав	ить элемент аудита
						Да Отмена

Рисунок В.31. – Настройка аудита

Свойства tmp Общие Ярлык Дискреционные атрибуты Аудит Мандатная метка Подпись Элемент Обычный По умолчанию s: {oxudnarmcy} ~ Успешно: o x u d n a Удалить root ×. f: {oxudnarmcy} ✓ d n a r m c v Неудачно: s: {oxudnarmcy} 2 user\_1 Удалить 1: {oxuanarmcy} f: {oxudnarmcy} s: {oxudnarmcy} s: {oxudnarmcy} Удалить 2 остальные Удалить Удалить f: {oxudnarmcy} f: {oxudnarmcy} 🗹 Пользователи 🗹 Группы 🔽 Остальные Добавить элемент аудита Дa Отмена

Пример установки прав доступа (см. рисунок В.32.):

Рисунок В.32. – Установка права доступа

# Настройка контроля целостности файловой системы и программноаппаратной среды.

Открыть терминал Fly и выполнить следующую команду: «sudo nano /etc/cron.daily/afick cron» (см. рисунок В.33.).



Рисунок В.33. – Ввод команды в терминал

В результате выполнения команды, в текстовом редакторе «nano» откроется на редактирование файл «afick\_cron» (см. рисунок В.34.).



Рисунок В.34. – Результат выполнения команды

В нем необходимо найти параметры «LOGFILE», «ERRORLOG» и изменить их на (рисунок В.35.):

```
LOGFILE="/dev/null"
```

```
ERRORLOG="/dev/null"
```



Рисунок В.35. – Изменение параметров «LOGFILE», «ERRORLOG»

Также, необходимо изменить команду запуска на (см. рисунок B.36.): nice -n \$NICE \$AFICK -с \$CONFFILE -k > \$LOGFILE 2>\$ERRORLOG



Рисунок В.36. – Изменение команды запуска

Аналогично открыть файл «/etc/afick.conf» командой «sudo nano /etc/afick.conf» (см. рисунок В.37.).



Рисунок В.37. – Открытие файла «/etc/afick.conf»

Результат выполнения команды – на рисуноке В.38..



Рисунок В.38. – Файл «/etc/afick.conf»

Изменить параметры (рисунки В.39. и В.40.):

history := /var/log/afick/afick.log

#archive := /var/lib/afick/archive

/boot md5

/lib/modules md5

/etc/security md5

/etc/pam.d md5

/lib/x86\_64-linux-gnu/security md5

/lib/security md5

/sbin md5

/etc/fstab md5

/usr/sbin md5

```
# database : name with full path to database file
database:=/var/lib/afick/afick
# history : name with full path to history file
history := /var/lib/afick/afick.log
# archive : name with full path to directory for archived results
#archive := /var/lib/afick/archive
# report_url : where to send the result : stdout/stderr/null
```

Рисунок В.39. – Изменение параметров «history» и «archive»



Рисунок В.40. – Изменение остальных параметров

После создать файл «affick.sh» и настроить на него права командами (см.

рисунок 41):

```
sudo touch /etc/init.d/afick.sh
```

```
sudo chmod 755 /etc/init.d/afick.sh
```

🛌 ~ : bash — Терминал Fly
Файл Правка Настройка Справка
🔷 🎱 📋 📋 🔍 Is 🗸 🖉
administrator@astra:~\$ sudo touch /etc/init.d/afick.sh administrator@astra:~\$ sudo chmod 755 /etc/init.d/afick.sh administrator@astra:~\$ ls -l /etc/init.d/afick.sh -rwxr-xr-x 1 root root 0 anp 6 23:29 /etc/init.d/afick.sh administrator@astra:~\$

Рисунок В.41. - Создание и настройка прав файла «affick.sh»

Открыть созданный файл командой «sudo nano /etc/init.d/afick.sh» и вписать (см. рисунки В.42. и В.43.):

#!/bin/sh

### BEGIN INIT INFO

# Provides: afick

# Required-Start: \$local fs

# Required-Stop: \$local fs

# Default-Start: 2 3 4 5

# Default-Stop: 0 1 6

# Short-Description: Контроль целостности при старте системы

# Description: Контроль целостности при старте системы

### END INIT INFO

PATH=/sbin:/bin:/usr/sbin:/usr/bin

. /lib/lsb/init-functions

```
case $1 in
start)
log_daemon_msg "Starting integrity check" "afick"
log_end_msg 0
/usr/bin/afick -c /etc/afick.conf -k 2>&1 > /dev/null
status=$?
log_daemon_msg "Integrity check_results" "afick"
```

есho "Для использования данного скрипта необходимо запустить его с параметром start. Например: afick.sh start"

;;

esac



Рисунок В.42. – Первая часть созданного файла



Рисунок В.43. – Вторая часть созданного файла

И выполнить команды «sudo afick -i» и «sudo update-rc.d afick.sh defaults» (см. рисунок B.44.):



Рисунок В.44. – Выполнение команд

Аналогичного результата можно добиться, используя графическую утилиту afick.

Запустить ее из меню быстрого доступа (см. рисунок В.45.):





Откроется утилита как на рисунке В.46.:

🙉 afic	k-gui 2.11-1							- 0	×
_ меню									_
<u>Ф</u> айл	Действия	а <u>н</u> ализ	<u>н</u> астройка	/etc/afick.conf	<u>о</u> пции а	архив	Помощь		
– Разде	л изменений	ă ————							
– Разде	л предупре	кдений —							
– Секци	я хода выпо	лнения –							
				🔳 Отображ	ать ход вн	ыполне	ения		_
									_
проше	дшее время		оставше	еся время				ļ	

## Рисунок В.46. – Утилита affick

Выбрав пункт «действия»-«инициализация базы» провести первичную настройку утилиты (см. рисунок В.47.):



Рисунок В.47. – Инициализация БД affick

Для ручной настройки контроля целостности отдельных файлов их нужно прописать в конфигурационном файле утилиты. Доступ к нему можно получить как «настройка»-«редактирование» (см. рисунки В.48. и В.49.):



Рисунок В.48. – Выбор в меню

# ! /var/www/html/snortsnarf
/boot md5
/lib/modules md5
/etc/security md5
/etc/pam.d md5
/lib/x86_64-linux-gnu/security md5
/lib/security md5
/sbin md5
/etc/fstab md5
/usr/sbin md5
****

Рисунок В.49. – конфигурационный файл

В данный файл необходимо прописать путь до контролируемых папок и используемый алгоритм для вычисления контрольной суммы (см. рисунок В.50.)

# ! /var/www/html/snortsnarf
/boot md5
/lib/modules md5
/etc/security md5
/etc/pam.d md5
/lib/x86_64-linux-gnu/security md5
/lib/security md5
/sbin md5
/etc/fstab md5
/usr/sbin md5
/home/administrator/Desktop/test.file md5
/home/administrator/Desktop/TestFolder md5
·
#######################################
If the signature constraints and share the transmission

Рисунок В.50. – Настройка контроля целостности для файла и папки

После настройки необходимо обновить базу данных в пункте «действия» (см. рисунок В.51.):



Рисунок В.51. – Обновление базы

В качестве проверки отредактируем проверяемый файл, а также скопируем его в проверяемую папку (см. рисунки В.52. и В.53.):

🍪 t	est.	file –	- Kate		
Фа	йл	Пр	авка	Вид	Проекты
HTB	8	2			
/Meł	hoi	me >	admini	strator	> Desktops
ok	1	so	mete	xt	
đ	2				
1					
-					

Рисунок В.52. – Редактирование файла



В результате, при проверке, целостности файлов они будут отображены в утилите (см. рисунок В.54.):



Рисунок В.54. – Проверка контроля целостности

Необходимо обратить внимание, что в конфигурационном файле указываются расширения файлов, которые будут игнорироваться (см. рисунок B.55. – exclude\_suffix):



Рисунок В.55. – Игнорирование расширений

Также существует возможность настройки мандатного контроля целостности.

Включите подсистему мандатного контроля целостности в ОС. Включите защиту ФС при загрузке (см. рисунок В.56.):



Рисунок В.56. – Включение защиты ФС

Проверьте статус систем подсистем при помощи консольных утилит (см. рисунки В.57. и В.58.):



Рисунок В.57. – Проверка статуса системы astra-mic-control



Рисунок В.58. – Проверка статуса системы set-fs-ilev

Также можно проверить статус в графической утилите монитора безопасности (см. рисунок В.59.):

Мон	нитор безопасности		
	Подсистема	Статус	Сообщение
1	Блокировка системных команд (df, chattr, arp, ip, и т.д.)	×	
2	Блокировка консоли для пользователей	×	
3	Блокировка интерпретаторов	×	
4	Блокировка интерпретатора bash	×	
5	Блокировка макросов	×	
6	Режим Мандатного Контроля Целостности	1	
7	Мандатный Контроль Целостности на файловой системе	1	
8	Запрет установки бита исполнения	×	
9	Блокировка трассировки ptrace	×	
10	Блокировка одновременной работы с разными уровнями sumac	×	
11	Блокировка клавиш SysRq	1	
12	Межсетевой экран UFW	×	
13	Системные ограничения ulimits	×	

Рисунок В.59. – проверка статус в графической утилите

Создайте каталог в ОС и назначьте ему требуемый уровень целостности (см. рисунок В.60.):

войства		· · · · · · · · · · · · · · · · · · ·
user_1		
Общие Ярлык Дискреци	онные атрибуты Аудит Мандатная метка Подпи	Ю
Уровень конфиденциальности:	Уровень_0	~
Уровень целостности:	Низкий	~
Категории:	Низкий	
	Высокий	
Спец. атрибуты:	Ccnr	
		Да Отмена

Рисунок В.60. – Создание каталога с требуемым уровнем целостности

Назначьте пользователю требуемый уровень целостности (см. рисунок В.61.):

Пользователь: use	er_1					
🔔 Общие 🛛 🎝 В	Блокировка	🏡 Аудит	🙇 Привилегии 🚺 МРД 🚍 Ср	ок д	ействия ន Графический киоск Fly 🛛 Боты	
			Уровни			
К	(онфиденциа	льность			Целостность	
Минимальный:	😑 0:Уровень	_0		$\sim$	- 0:Низкий	$\sim$
Максимальный:	😑 1:Уровень	_1		$\sim$	🗢 0:Низкий	$\sim$
			Категори	1	⊇ 0:Низкий	Di
Разряд ∨ На	аименование	Мин.	Макс.		🐱 63:Высокий	
📔 1 — Ка	атегория_2					
🖬 о Ка	атегория_1					

Рисунок В.61. – Настройка уровня целостности пользователя

Перейдите в системные параметры (см. рисунок В.62.):



Рисунок В.62. – Путь к системным параметрам

Настройте монитор безопасности на регистрацию событий, связанных с блокировкой трассировки ptrace, запрет монтирования носителей для непривилегированных пользователей, запрета установки бита исполнения. (см. рисунки В.63. и В.64.):

Системные параметры
Включить режим работы файловой системы ОС - 'только чтение'
🗹 Блокировка клавиш SysRq для всех пользователей, включая администраторов
🗹 Запрет монтирования носителей непривилегированным пользователям
Включить межсетевой экран
Настройка правил
Блокировка системных команд для пользователей
Блокировка выключения/перезагрузки ПК для пользователей
Настройка блокировки при входе в систему
Включение системных ограничений ulimits
🗌 Блокировка одновременной работы с разными уровнями в пределах одной сессии
🗹 Блокировка трассировки ptrace для всех пользователей, включая администраторов
Блокировка макросов
🗹 Запрет установки бита исполнения для всех пользователей, включая администраторов

# Рисунок В.63. – Настройка монитора безопасности

Монитор безопасности  Подсистема Статус Сообщение  Блокировка системных команд (df, chattr, arp, ip, и т.д.) К Блокировка консоли для пользователей Блокировка интерпретаторов К Блокировка интерпретатора bash Блокировка интерпретатора bash Блокировка макросов Режим Мандатного Контроля Целостности Маназтиний Контроля Целостности			
Подсистема	Статус	Сообщение	
Блокировка системных команд (df, chattr, arp, ip, и т.д.)	×		
Блокировка консоли для пользователей	×		
Блокировка интерпретаторов	×		
Блокировка интерпретатора bash	×		
Блокировка макросов	×		
Режим Мандатного Контроля Целостности	1		
Мандатный Контроль Целостности на файловой системе	1	ниже:8 выше:0 норма:228188	
Запрет установки бита исполнения	1		
Блокировка трассировки ptrace	1		
Блокировка одновременной работы с разными уровнями sumac	×		
Блокировка клавиш SysRq	1		
Межсетевой экран UFW	×		
Системные ограничения ulimits	×		
Блокировка выключения/перезагрузки ПК для пользователей	×		
Запрет монтирования носителей непривилегированным пользователям	1		
Режим ЗПС (замкнутой программной среды) в исполняемых файлах	×		
Режим ЗПС (замкнутой программной среды) в расширенных атрибутах	×		
	Подсистема Блокировка системных команд (df, chattr, arp, ip, и т.д.) Блокировка консоли для пользователей Блокировка интерпретаторов Блокировка интерпретатора bash Блокировка интерпретатора bash Блокировка макросов Режим Мандатного Контроля Целостности Мандатный Контроль Целостности на файловой системе Запрет установки бита исполнения Блокировка трассировки ptrace Блокировка клавиш SysRq Межсетевой экран UFW Системные ограничения ulimits Блокировка выключения/перезагрузки ПК для пользователей Запрет монтирования носителей непривилегированным пользователям Режим ЗПС (замкнутой программной среды) в исполняемых файлах	Подсистема Статус Глокировка системных команд (df, chattr, arp, ip, и т.д.) Х Блокировка системных команд (df, chattr, arp, ip, и т.д.) Х Блокировка консоли для пользователей Х Блокировка интерпретаторов Х Блокировка интерпретатора bash Х Блокировка интерпретатора bash Х Блокировка интерпретатора bash Х Режим Мандатного Контроля Целостности Мандатный Контроль Целостности на файловой системе Запрет установки бита исполнения Блокировка одновременной работы с разными уровнями sumac Клокировка клавиш SysRq Межсетевой экран UFW Системные ограничения ulimits Блокировка выключения/перезагрузки ПК для пользователей Запрет монтирования носителей непривилегированным пользователям Режим ЗПС (замкнутой программной среды) в исполняемых файлах Ка	

Рисунок В.64. – Результат настройки монитора безопасности

# Настройка прав разграничения доступа для внешних носителей информации

Открыть управление политикой безопасности и перейти: «Устройства и правила» - «Устройства» (см. рисунок В.65.).

🤠 Управление политикой безопасности - Огр	аничения на размещение устройств 🛛 🗖	×
Файл Правка Настройки Помощь		
ⓒ ⊙ ⊘ ⊙    + -   ゔ	C O Bce V	
∽- 📮 astra	Ограничения на размещение и правила учета устройств	
>- 🛒 Аудит	🖉 Устройства 📋 Правила	
>- 🏛 Группы		-
>- 🚰 Замкнутая программная среда	Наименовани V Пользователь Группа Права доступа Включено	
— 🚇 Мандатное управление доступ		
>- 🕡 Мандатные атрибуты		
>- 🕅 Мандатный контроль целостно		
— 🎦 Монитор безопасности		
>- 🚹 Настройки безопасности		
>- 🐴 Политики учетной записи		
>- 🏯 Пользователи		
>- 🚋 Привилегии		
>- 💽 Управление квотами		
Устройства и правила		
>- 🔝 Правила		
>-@ Устройства		
	Подстановка 🗸 Фильтр	

Рисунок В.65. – Окно ограничение на размещения и правила учета устройств

Подключить устройство, для которого планируется настройка (см. рисунок В.66.):



Рисунок В.66. – Подключение устройства



Нажать «Создать новый элемент» (см. рисунок В.67.).

Рисунок В.67. – Список устройств

Выбрать устройство для настройки из списка устройств (см. рисунок В.68.)



Рисунок В.68. – Выбор необходимого устройства из списка

Настроить разграничения прав доступа к устройству. После – нажать применять, для фиксации настроек в системе (см. рисунок В.69.).

🦁 Управление политикой безопасности - Ограничения на размещение устройства: test 💷 🔍						
<ul> <li>✓ ■ astra</li> <li>&gt; # Аудит</li> <li>&gt; □ Группы</li> </ul>	Наименование: test Включено					
<ul> <li>Замкнугах программная среда</li> <li>Мандатное управление доступ</li> <li>Мандатные атрибуты</li> <li>Мандатный контроль целостно</li> <li>Монитор безопасности</li> <li>Настройки безопасности</li> </ul>	Пользователь Рооt Чтение Запись Выполнение Пользователь Стальные Остальные Остальные Чтение Запись Выполнение Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Остальные Ост					
>- 🏩 Пользователи	Свойства					
<ul> <li>Привилегии</li> <li>Управление квотами</li> <li>Упройства и правила</li> </ul>	1     ENV     ID_SERIAL     ==     "Kingston					
>- 🚹 Правила - 🕜 Устройства - 🕽 test	Описание					

Рисунок В.69. – Результат настройки устройства

## ПРИЛОЖЕНИЕ Г

## Пример настройки CAB3 «Kaspersky Endpoint Security»

### Шаг 1. Выполнить настройку модуля «Обновление»

Необходимо выполнить следующие действия:

Для настройки параметров установки обновлений баз вирусных сигнатур (далее – БВС) необходимо определить к какой группе относится средство ВТ.

- 1. Автономное средство ВТ.
- 2. Средство ВТ, входящее в состав самостоятельного АП сети Интернет.
- 3. Средство BT, управляемое «Kaspersky Security Center».

#### Автономное средство ВТ

1) Создать в корневом каталоге системного диска директорию для обновлений баз вирусных сигнатур (далее – БВС) с названием Updates (например: D:\Updates\).

Произвести настройку прав доступа к данной директории, для этого:

– отключить общий доступ к файлам (Панель управления → «Вид»
 «Параметры» → «Изменить параметры папок и пользователей» → вкладка
 «Вид» → убрать флаг «Использовать мастер общего доступа»
 (рекомендуется)) (см. рисунок Г.1.);

Параметры папок	$\times$
Общие Вид Поиск	
Представление папок	
Вы можете применить этот вид (например, "Таблица" или "Значки") ко всем папкам такого типа.	
Применить к папкам Сброс вида папок	
Дополнительные параметры:	
Выводить полный путь в заголовке окна 🔺	1
Запускать окна с папками в отдельном процессе	
Использовать мастер общего доступа (рекомендует	
Использовать флажки для выбора элементов	
Отображать буквы дисков	
Отображать значки файлов на эскизах	
Отображать обработчики просмотра в панели просм	
Отображать описание для папок и элементов рабоче	
Отображать сведения о размере файлов в подсказк	
Отображать сжатые или зашифрованные файлы NTI	
🔲 Показать уведомления поставщика синхронизации 义	
< >>	
Восстановить значения по умолчанию	
ОК Отмена Примени	тъ

Рисунок Г.1. – Флаг «Использовать мастер общего доступа (рекомендуется)»

– произвести настройку прав доступа к данной директории (Нажать правой кнопкой «мыши» по директории «С:\Updates\» → Свойства → вкладка Безопасность. Ниже поля «Группы или пользователи» выбрать «Изменить». Настроить доступ для пользователей, при необходимости добавить отсутствующих в списке пользователей или групп, нажав «Добавить» и введя имя пользователя или название группы. В поле «Разрешения для …» выбрать разрешить «Полный доступ») (см. рисунок Г.2.).
and a sublement							Предырные	e eepowe	Had	22
Indexes a	Uniperte gotomore a Getileurony -	· Unan dictyn *. H	Ter.	E * Cl. 1	M		Officient	"Дретул	0450	HECH
fotpaneor		where a product in last	-	- Lover			Имя объекта	Chlpdates		
Загружи	Perflogs	14.07.0009.501	Charles I Bellinesas				Брутты или пользо	CONTRACT OF		
Proposed rate	g. Program Fred	1100.000 (4.20	Planes & doctores				А. Процидание то	composy		
Carlo and Creek	Oreparts		Origes a disherent				А. окстема			
Lat.nerres	Barnin Ongusta e recent	1008 C	Planes + makhener				Advencedance	SH (WIN-HKBL7	FUDVJAVAgene	wet the
Brate	Poperpers as to	ADION NO.					ild, Flam-sceareru	WIN-HKSL7FU	DVJA/Rome some	aten.
- Diventation		100					Чтобы изменить ра	A SPECIFICAL SPECIFICAL		
Molporene	Concern generation	· · · · ·					нажните кнопку "И	foreners"		-
Mytund	Andrews a factor	and a second second				-	Estpewerers gits rp	synne .	Passan	1
-		and a second					Concentrative record	EN()	1000000	
Koschworsp	Orquiers						Полных доступ			
Care	Bupearte						Attended a strange	and the second second	5	
	Korupoerre						Список селетион	HOTO NAME	20	
	Column april						Vinerant		1	
	YAANNA						Janaco		1	
	Oppression						Чтобы зваать особ	бые разрешения	inter filers	CO-POT
	Carlos and						"Дополнительно"	cue ro-doard)	100008	-
	Land Land Land						Gupoli-es of year	CONTRACTOR	H # DESCRIPTION	N. 1
Updates - Terror c galas	(Jara announced 06.09.2003 17.38							OK	Отитна	1
Updates Terror pallo	Arra and 0100,203 2738			_	0 2	D	Paspeueries gas a	OK	Otwene es"	
ирания Попос с файла ибор: "Поль	ала водо 200 200 2738	nnы"			8 ×	Г	Разрешение для л Безопескость	OK	Disvenia es"	1
ирания Почила файли ибор: "Поль	озователи" или "Гру	ппы"			8 ×	ſ	Pappeseries gas a Bestration of the Heal of being	OK rpyritsu "Updat	Oronena es <sup>4</sup>	10
ирания Пенас факе ибор: "Поль Выберите ти	ала анимини водо 203 2738 взователи" или "Гру п объекта:	ппы"			8 ×	ſ	Разрешения для л Бязотасность Ини объекта Брута или пользо	OK rpyritsu "Updat C. Updates watesk	Oronena es <sup>4</sup>	10
ирания Пенесськи ибор: "Поль Выберите ти	ала аниение 6032031738 взователи" или "Гру п объекта: еди" "Прупры" или "Г	ппы"	artu fasonar		2 X	ſ	Разрешение для л Бязопасность Иня объеста Дорты или польбо Дорождане тр Польжане	OK rpyriteu "Updat C "Updates earens reactors	Oroma es <sup>c</sup>	(ne
ибор: "Поль Выберите ти "Пользоват	озователи" или "Гру п объекта: ели", "Группы" или "	ппы" Встроенные субъ	екты безопас	нк <u>Т</u> илы об	ව X		Papewerkes are a Besonancers Mex of sector Dynte was republic Rooussame rp Rooussame rp	OK rpymteu "Updat C-Updates earrese: coepe;	Crowna es"	(fe
орани Пенас файн ибор: "Поль Выберите ти "Пользоват	озователи" или "Гру п объекта: ели", "Группы" или "Г	ппы" Встроенные субъ	екты безопас	ни Пильн об	ন্থ <mark>স</mark> ইচektos		Разрешение для п Бязотасность Имя объеста Врутны или гользо В Посидания го В доссника В доссника В доссника В доссника В доссника В доссника В доссника В доссника В доссника	OK rpymtsu "Updat C *Updates eartese peartese peartese pear (WTH HKSL7	Epones es"	
ибор: "Поль Выберите ти "Пользоват В сдедующе	озователи" или "Гру п объекта: ели", "Группы" или " м месте:	ппы" Встроенные субъ	екты безопас	н	२         ×           Зъектов)         •	r	Разрешение для л Бязопасность Ини объекта Вруппы или полько Ф. посилания гр Ф. посилания гр	OK rpynthu "Updat C-Updates samenx peepx; thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus thus	Converse es*	
ирали Режес райо ибор: "Поль Выберите ти "Пользоват В сдедующе WIN-HK9L7I	алалинины 90.01.203.1738 взователи" или "Гру п объекта: ели", "Группы" или "Г м месте: FUDVJA	ппы" Встроенные субъ	екты безопас	нк <u>Т</u> ипы об <u>Р</u> азме	? Х 5ъектов		Разрешение для п Бязотасность Имя объеста Врутик или пользо Вр. Пользователи В. Состана В. Состана	OK rpyntw "Updat C *Update earear gw (Mitheks), TPU (Mitheks), TPU	Crewse es"	про
ирания Пенес фейн ибор: "Поль Выберите ти "Пользоват В сдедующе WIN-HK9L7I Вледите цене	озователи" или "Гру п объекта: ели", "Группы" или "Г м месте: FUDVJA	ппы" Встроенные субъ истов (помосль):	екты безопас	н <u>Т</u> ипы об <u>Р</u> азме	?         X           5ъектов		Разрешение для п Бязопасность Имя объеста Врутик или полько По Полькования по По Полькования по По По Полькования по По	OK rayethu "Update C-Updates earnest coeepe; WMH-HKC, TU (WMH-HKC, TU	es"	Стр. востры утельн Уда
ирани Пенес фак ибор: "Поль Выберите ти "Пользоват В сдедующе WIN-HK9L7/ Введите уме	ала анимана 60.03.203.1738 взователи" или "Гру п объекта: ели", "Группы" или "Г м места: FUDVJA зна выбираемых объе	ппы" Встроенные субъ жтов ( <u>примеры</u> ):	екты безопас	н <u>Т</u> ипы об <u>Р</u> азме	? Х 5ъектов		Разрешение для л Безопасность Ини объеста Вропы ини польбо Ф. Польдане тра В. Пользователя В. Пользователя В. Пользователя В пользователя Азминистропо"	OK rpyrmu "Updat C "Updates eaness" coeeper With Hells With	Creese es <sup>-</sup> FUDUA Apere DUA Apere DUA Apere DUA Apere DUA Apere DUA Apere	онстра атели Уда
ирания Полос село ибор: "Поль Выберите ти "Пользоват В с <u>р</u> едующе WIN-HK9L7I Введите уме Администра	ала анимани 0.03.203.1738 взователи " или "Гру п объекта: ели", "Группы" или "Г м месте: FUDVJA зна выбираемых объе ятор	ппы" Встроенные субъ жтов ( <u>примеры</u> ):	екты безопас	н <u>Типы об</u> <u>Вазме</u>	З Х Бъектов шение		Разрешение для л Бязопасность Ина объяста Бруты или польбо Ф. Польдант пр Ф. Дольдант пр Ф. Дола Пор Ф. Дола П	OK rpyntis 'Updat C'Update eanese: coeepx; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twoseex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; twosex; two	Enverse es <sup>-</sup> UVUIA Agrow DVIA Agrow DVIA Agrow DVIA Agrow DVIA Agrow Pageware Pageware	Спо острани Ула Заг
орания Пенес файн ибор: "Поль Выберите ти "Пользоват В сдедующе WIN-HK9L7/ Введите уме Администра	ала анимани 0.03.203.1738 взователи " или "Гру п объекта: ели", "Группы" или " м месте: FUDVJA эна выбираемых объе этор	ппы" Встроенные субъ жтов ( <u>примеры</u> ):	екты безопас	нк <u>Типы об</u> <u>Р</u> азме	2 × 5ъектов съектов съектов съектов съектов съектов	r 	Разрешения для т Бязопалость Иня объястя. Врутны иля пользо М. Польеданя гр В. постная А. Доненая А. Доненая В. Доненая А. Доненая Варонцения для тр Даниенстрато Пользователи Пользователи Пользователи	OK rayithu "Update C-Update eartest coepey" (W10+HKC) TU (W10+HKC) TU	Creees es" PUDU/A Apren DUA fanssee DUA fanssee DUA fanssee Popears Popears	Zaa Stela
ибор: "Поль выберите ти "Пользоват В сдедующе WIN-HK9L7/ Введите уме Администра	ала анимани 90.00.2003/200 воователи" или "Гру п объекта: ели", "Группы" или "Г м места: FUDVJA на выбираемых объе втор	ппы" Встроенные субъ эктов ( <u>примеры</u> ):	екты безопас	нк <u>Т</u> ипы об <u>Р</u> азме	? Х 5ъектов шение тъ имена		Разрешение для л Базопасность Ини объекта Вруппы или полько Ф. Польданет у Пользователи Восращения для гр Даниестирато" Пользователи Пользователи Пользователи Накова досут Накова досут Накова досут Накова досут Накова досут	OK rpyrmu "Updat C "Updates earrest" compony W/MILHER, THE pyrmu earrest	Crewess as FUDVLA Japan FUDVLA Japan DVLA Flatson Pageaun Pageaun Pageaun	Za Za
орани Полосфай «Бор: "Поль Выберите ти "Пользоват В сдедующе WIN-HK9L7I Введите уме Администра	ала анимани 00032031738 взователи" или "Гру п объекта: ели", "Группы" или "Г м месте: FUDVJA зна выбираемых объе атор	ппы" Встроенные субъ эктов ( <u>примеры</u> ):	екты безопас	нк <u>Т</u> ипы об <u>Р</u> азме Провери	У Х Бъектов съектов съектов съектов съектов съектов съектов съектов съектов съектов		Разрешение для л Безопасность Ина объекта Булты или польбо Ф. Посьеданто и Ф. Досьеданто Ф. Досьеда	OK rpyntis 'Updat C 'Update sancs coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; coecpx; c	Crewess es <sup>-</sup> COVID Adverse COVID Adverse C	Zan Zan Zan
орани Попос файн Корр: "Поль Зыберите ти "Пользоват 3 сдедующе WIN-HK9L7/ Зведите заме Администра	алалинный 000.2001/14 взователи" или "Гру п объекта: ели", "Группы" или "Г м месте: FUDVJA на выбираемых объе втор	ппы" Встроенные субъ эктов ( <u>примеры</u> ):	екты безопас	нк <u>Типы об</u> <u>Разме</u> Провери	2 Х Съектов съектов съектов тъ имена		Разрешение для л Бязопасность Иня объестя Пруты или польбо М. Польдания тр В. система А. Авинесскато М. Авинесскато Аленнестрото Пальная аступ Наменестрото Пальная систи Наменестрото Пальная систи Наменестрото	OK rayithu "Update C-Updates earnesi coecepic) tour (MIN-HEEL rosepic) tour (MIN-HEEL rosepic) tour (MIN-HEEL rosepic) tour (MIN-HEEL rosepic)	Crewess es" PUDULA Aprove DULA flans see DULA flans see Pospetaris Pospetaris	Vaa Jar
орани Полософан Сора: "Поль Заборите ти "Пользоват 3 сдедующе WIN-HK9L7/ Введите уме Администра	ала анимани 90.00.2003/200 воователи" или "Гру п объекта: ели", "Группы" или "Г м места: FUDVJA зна выбираемых объе втор	ппы" Встроенные субъ эктов ( <u>примеры</u> ):	екты безопас	нк <u>Т</u> ипы об <u>Р</u> азме	? Х 5ъектов щение пъ имена	-	Разрешение для л Бязопасность Ини объекта Вруппы или полько Ф. Польданит у Данности и Данности и Польдователи Польдователи Нокок с одарже Чтонке и вытали Польба и ли	OK rpyrmu "Updat C *Updates earners: coeeper; www.exect. symme earners: coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeeper; coeper; coeeper; coeeper	Crewess as PUDVLA Agrees PUDVLA Agrees DVLA Postson Postson Postson P	Van Stelat

Рисунок Г.2. – Настройка прав доступа к директории

2) Разархивировать архив с актуальным полным комплектом БВС, загруженный ранее и скопировать содержимое каталога «Updates», полученного при разархивировании, в директорию D:\Updates\.

3) Для настройки задачи обновления необходимо в «Kaspersky Endpoint Security»:

– на вкладке «Обновления» в разделе «Обновление баз и модулей приложения» выбрать пункт «Настройки» (см. рисунок Г.3.);

Kas Endp	persky point Security	Обновление	? _		;
	Мониторинг	Обновление баз и модулей приложения Загружено: 76,58 МБ		¢	
Ô	Безопасность	Обновить Остановить обновление			
$\mathbb{C}$	Обновление				
Ę	Задачи	Откат к предыдущей версии баз		6	
ନ୍ମ	Лицензия				
		Откатить			

Рисунок Г.3. – Настройка компонента «Обновления»

– нажать на вкладку «Расписание обновления баз», в открывшемся окне
в пункте «Запускать обновления» указать «Вручную» и нажать «ОК» (см. рисунки Г.4. и рисунок Г.5.);

			1 C	-	<u>ц</u>
Kas	persky	< Обновление			
Endp	point Security	Настройки обновления			
ᇜ	Мониторинг				
Ô	Безопасность	Обновление Настройки обновления баз и модулей приложения.			
$\mathbb{C}$	Обновление	Режим запуска и источник обновлений			
Ģ	Задачи	Расписание обновления баз Автоматически (рекомендовано)			
0	Лиценция	Настроить источники обновлений			
н		Серверы обновлений "Лаборатории Касперского"			
		Запускать обновление баз с правами			
		Запускать обновление баз с правами техущего пользователя			
		Загрузка и установка обновлений модулей приложения			
		Загружать обновления модулей приложения			
		Устанавливать критические и одобренные обновления			
		Устанавливать только одобренные обновления			
Берсик 11.9.0.3	51	Копирование обновлений			

Рисунок Г.4. – Настройка обновлений



Рисунок Г.5. – Выбор режима запуска обновления

 – в поле «Загрузка и установка обновлений модулей приложения» убрать галочку напротив пункта «Загружать обновления модулей приложения» (см. рисунок Г.6.);



Рисунок Г.6. – Настройка обновлений

– в «Прокси-сервер для обновлений» нажать кнопку «Настроить». В открывшемся окне «Прокси-сервер» поставить галочку напротив пункта «Не использовать прокси-сервер». Нажать кнопку «ОК» (см. рисунки Г.7. и Г.8.);



# Рисунок Г.7. – Настройка обновлений

🖲 Не использовать прокси-се	рвер	
Автоматически определять	настройки прокси-сервера	
🔘 Использовать указанные н	астройки прокси-сервера	
Адрес:	Порт:	
	80 🗘	
Имя пользователя:	Пароль:	
	Пароль	
🗑 Не использовать прокси-се	Пароль рвер для локальных адресо	ē

Рисунок Г.8. – Настройка параметров обновлений

– в окне настроек обновления выбрать «Настроить источники обновлений». В открывшемся окне «Источники обновлений» поставить статус «Выключено» напротив пунктов «Kaspersky Security Center» и «Серверы обновлений «Лаборатории Касперского»«. Нажать кнопку «Добавить» и

указать путь к папке Updates, содержащую актуальные обновления и нажать кнопку «Выбрать». Нажать кнопку «ОК»(см. рисунок Г.9.);



Рисунок Г.9. – Выбор источника обновлений

 в окне «Настройки обновлений» нажать кнопку «Сохранить»(см. рисунок Г.10.);



Рисунок Г.10. – Сохранение обновлений

– для запуска задачи обновления БВС необходимо в окне «Обновление баз» нажать на кнопку «Обновить» (см. рисунок Г.11.);

Kas Endp	oersky oint Security	Обновление	0	
nn ©	Мониторинг Безопасность	Обновление баз и модулей приложения Последнее обновление: 41 минуту назад Расписание: Вручную Обновить	¢ @	]
$\mathbb{C}$	Обновление			
F	Задачи	Откат к предыдущей версии баз Последний откат: Не запускалось	G	]
ð	Лицензия			
		Откатить		

Рисунок Г.11. – Запуск обновлений БВС в ручном режиме

– в дальнейшем для обновления БВС необходимо периодически обновлять файлы в каталоге «C:\Updates\» путем разархивирования актуального архива с БВС с заменой файлов и запускать задачу обновления БВС. Для обновления KES 11 применяется архив типа «KES11\_YYYYMMDD.rar», где YYYY – год, MM – месяц, DD – день создания БВС.

# Средство ВТ, входящее в состав самостоятельного АП сети Интернет

1) В главном окне САВЗ выбрать меню «Обновление». Далее необходимо открыть параметры задачи «Обновление баз и модулей приложения», нажав на значок шестеренки. В поле «Прокси-сервер для обновлений» нажать на кнопку «Настроить». В появившемся окне указать параметры, исходя из условий эксплуатации средства ВТ, например, поставить галочку напротив пункта «Автоматически определять настройки прокси-сервера» и нажать кнопку «ОК» (см. рисунок Г.12.).

Не использовать прокси-о	ервер	
Автоматически определят	ь настройки прокси-сервера	
🔘 Использовать указанные н	астройки прокси-сервера	
Адрес:	Порт:	
	80 🗘	
🔘 Использовать аутентиф	рикацию на прокси-сервере	
Имя пользователя:	Пароль:	
	Пароль	
Не использовать прокси-со	ервер для локальных адресо	8
• пе использовать прокси-о	ервер для локальных адресо	0
		20190 / Marca

Рисунок Г.12. – Настройка параметров прокси-сервера

2) В разделе «Режим запуска и источник обновления» выбрать пункт «Расписание обновления баз». В открывшемся окне в пункте «Запускать обновление:» выбрать параметр «По часам», далее выбрать пункт «Выполнять каждые:» ввести значение «2» и нажать кнопку «ОК» (см. рисунки Г.13. и Г.14.).



Рисунок Г.13. – Настройка задачи обновления самостоятельного АП сети Интернет

сам	•
🗘 часа	
7 🗘	
🗘 минут	
	٦
	ОК Отмена

Рисунок Г.14. – Настройка задачи обновления самостоятельного АП сети Интернет

3) В разделе «Режим запуска и источник обновления» выбрать пункт «Настроить источники обновления» и в появившемся окне поставить статус «Включено» напротив «Серверы обновлений «Лаборатории Касперского», далее нажать на кнопку «ОК» (см. рисунок Г.15.).

		? – 🗆 🗙
Kaspersky	< Настройки обновления	
Endpoint Security	Источники обновлений	
Мониторинг	<b>+ Добавить</b> 🖉 Изменить 💼 Удалить 1 Вверх	↓ Вниз
Безопасность	Ф. Поиск	
С Обновление	О Источник	Статус
<b>До</b> Задачи	Серверы обновлений "Лаборатории Касперского"	Включено
🛱 Лицензия	Kaspersky Security Center	Выключено
Под упровлением: 10.196.2.132 Серене подслочны: 2 минуты назад		
Версия: 11.9.0.351		
¢ ¢	ОКОтмена	

Рисунок Г.15. – Настройка источника обновлений

4) В окне «Настройки обновлений» нажать кнопку «Сохранить» (см. рисунок Г.16.).



Рисунок Г.16. – Сохранение обновлений

## Средство ВТ, управляемое «Kaspersky Security Center»

Выполнить подключение к «Kaspersky Security Center» для получения всех необходимых настроек. После успешной настройки подключения обновление БВС будет производиться в порядке и с периодичностью, заданными на сервере администрирования. Порядок подключения описан далее.

Для успешного взаимодействия САВЗ, установленного на средстве ВТ, с сервером администрирования, необходимо специальное программное обеспечение – агент администрирования сервера Kaspersky Security Center (далее - Network Agent). Примечание: При подключении средства ВТ к серверу администрирования Kaspersky Security Center настройки KES 11 выполняются на сервере и все параметры настроек задаются в соответствии с настоящей инструкцией. Для установки Агента администрирования Kaspersky Security Center необходимо:

– загрузить инсталляционный пакет Network Agent с сетевых ресурсов СПД или с МНИ с дистрибутивами САВЗ (необходимо чтобы версия Network

Agent была не ниже версии Kaspersky Security Center, к которому осуществляется подключение);

- запустить исполняемый файл «setup.exe»;

– в поле «Адрес сервера:» ввести DNS-имя или IP-адрес Kaspersky Security Center, к которому необходимо подключиться и нажать далее (см. рисунок Γ.17.).

🛃 Агент администрирования Ка		Х				
Сервер администрирования Выберите Сервер администрирования.						
Укажите устройство, на которон установлен Сервер администрирования. Введите номер порта Сервера администрирования. Значение должно быть в интервале от 1 до 65535.						
Порт:	14000					
SSL-nopt:	13000					
Использовать SSL для со	единения (	с Серверон а,	дминистрир	ования		
Разрешить Агенту администрирования открыть UDP-порт						
UDP-nopt:	15000		1			
		< Назад	Далее	:>	Отмен	a

Рисунок Г.17. – Выбор сервера администрирования

В дальнейшем следует до завершения установки нажимать кнопку «Далее», оставляя все параметры по умолчанию.

После установки CAB3 и агента администрирования необходимо проверить соединение с сервером «Kaspersky Security Center» следующим образом:

1) открыть меню управления САВЗ, выбрать раздел «Настройка»;

2) в открывшемся меню под словом «Настройка» должна быть запись, подтверждающая, что средство ВТ работает под политикой, а также запись о текущем сервере (см. рисунок Г.18.).



Рисунок Г.18. – Проверка подключения к серверу «Kaspersky Security Center»

Если через 10 минут запись не появилась, целесообразно провести проверку соединения с сервером «Kaspersky Security Center». Для этого необходимо:

 перейти в каталог «C:\Program Files (x86)\Kaspersky Lab\NetworkAgent» (если операционная система не 64-разрядная, то «C:\Program Files\Kaspersky Lab\NetworkAgent»);

2) запустить утилиту «klcsngtgui.exe». Примечание: для корректной работы утилиты необходимы права локального администратора (см. рисунок Г.19.);

Image: Section in the supervise for any interview in the section is interview intervi	ощи Главная Педелиться Ви	Средства работы с примоз	NetworkAgent		- 0	×
<ul> <li>A statement gener (C) + Program Film (ddb) + Karpenrky Lab + NetworkAgent</li> <li>Parasepa</li> <li>Phanae C dealwaten</li> <li>Parasepa</li> <li>Phanae C dealwaten</li> <li>Data</li> <li>Da</li></ul>	* Соперенти на панесе Коперенти Соперенти Бактрого достуга Вуфтр обенне	Bogiesans Comepoants nyts Distasura temas	реместить в • 🗙 Хданить • пировать в • =] Перенненовать Творядачить	Hosan narea Cottante Cottante	<ul> <li>Выделять все</li> <li>Снять выделян</li> <li>Обратить выделян</li> <li>Обратить выделянь</li> </ul>	ни ление
Planese         Altra strateveneste         Ten         Panarpa          dumps         15:07.2022 15:08         Harna c dialination         Harna c dialination           Bases         15:07.2022 15:08         Harna c dialination         Data           Data         15:07.2022 15:08         Harna c dialination         Harna c dialination           Data         15:07.2022 15:08         Harna c dialination         Harna c dialination           Pattor         15:07.2022 15:08         Harna c dialination         Harna c dialination           Pattor         15:07.2022 15:08         Harna c dialination         Harna c dialination           Pattor         15:07.2022 15:08         Harna c dialination         Harna c dialination           Pattor         15:07.2022 15:08         Harna c dialination         Harna c dialination           Hara stratevents         15:07.2022 15:08         Harna c dialination         Harna c dialination           Hara stratevents         11:05:201 14:63         Approxement         529 KE           K gettystemisto.exe         17:03:2021 23:48         Pipertoxement         218 KE           R kingelitice         17:03:2021 23:48         Pipertoxement         508 KE           K kingeritice         17:03:2021 23:51         Pipertoxement         508 KE      <	🔶 👘 – 🕂 📒 н. Локальный диск (С	2) + Program Files (x86) + Ka	spersky Lab 🔹 NetworkAgent	4 Đ	Flower: NetworkAgent	P
dumps       15.07.2022 15:00       Пагна с файлами         Bases       15.07.2022 15:00       Пагна с файлами         Data       15.07.2022 15:00       Пагна с файлами         Data       15.07.2022 15:00       Пагна с файлами         Interna c forman       15.07.2022 15:00       Пагна с файлами         Interna c forman       15.07.2022 15:00       Пагна с forman         Interna c forman       10.5200 114:32       Докрамит         Integrity_manifestami       11.05202 12:340       Приложение       529 K5         K spetsysteminfo.axe       17.03.2021 23:40       Приложение       218 K5         Integrity_manifestami       17.03.2021 23:40       Приложение       218 K5         Integrity_mainfo.axe       17.03.2021 23:40       Приложение       150 K5         Integrity_mainfestami       17.03.2021 23:40       Приложение       150 K5         Integrity_mainfestami       17.03.2021 23:51       Приложение       150 K5         Integrity_mainfestami       17.03.2021 23:51       Приложение       150 K5	^	Manusar	Даты извленения	Ten	Размира	1
Bases       15.07.2022 15:88       Палка с файлами         Data       15.07.2022 15:21       Палка с файлами         Protocrap       15.07.2022 15:09       Палка с файлами         Interna c forma       15.07.2022 15:09       Палка с forma         Interna c forma       15.07.2022 15:09       Палка с forma         Interna c forma       15.07.2022 15:09       Палка с forma         Interna c forma       15.02.07.14:23       Anxyonerr.20.44       T8.45         Integrity_manifestami       11.05.2071 14:23       Anxyonerr.20.44       T8.45         Integrity_check_toolexe       17.03.2021 23:49       Приножение       218.745         Integrity_check_toolexe       17.03.2021 23:49       Приножение       123.45         Integrity_check       17.03.2021 23:41       Приножение       123		-dummi	15:07.2822 15:00	Папка с файлами		
Oda       15/07.2022 15/21       Tarvia c фolkname         protecomp       15/07.2022 15/09       Herna c фolkname         trbac       15/07.2022 15/09       Harna c фolkname         trbac       17/07.2022 15/09       Harna c фolkname         trbac       17/07.2022 15/49       Honconcense       218/7         trbac       17/07.2021 25/49       Honconcense       218/7         trback.eve       17/07.2021 25/49       Honconcense       1218/5         trback.eve       17/07.2021 25/49       Honconcense       1218/5         trback.eve       17/07.2021 25/49       Honconcense       1218/5         trback.eve       17/07.2021 25/51       Honconcense       1218/5         trback.eve       17/07.2021 25/51       Honconcense       1218/5         trback.eve       17/07.2021 25/51       Honconcense       1218/5     <		Bases	15.07.2022 15:08	Папиа с файлания		
protocomp       15.07.2022 15:09       Hernis c файлами         Hac       15.07.2022 15:08       Hanca c файлами         Hac       15.07.2022 15:08       Hanca c файлами         Hac       11.05.2021 15:08       Hanca c файлами         Hac       17.03.2021 23:48       Приложение       529 85         As getsysteminfo.coc       17.03.2021 23:48       Приложение       239 85         Integrity_inteck_toolese       17.03.2021 23:49       Приложение       2 167 85         Histpuld.coe       17.03.2021 23:49       Приложение       4 204 85         Histople.coe       17.03.2021 23:49       Приложение       420 85         Histople.coe       17.03.2021 23:49       Приложение       508 85         Histople.coe       17.03.2021 23:51       Приложение       508 85         Histople.coe       17.03.2021 23:51       Приложение       508 85         Histople.coe       17.03.2021 23:51       <		Data	15.87.2022 15/21	Папка с байлами		
that       15.07.2023 15:08       Hanca C dealmasse         Highlandstamil       11.05.2021 14:33       Aproposent XML       18.45         APDTAgt.cm       17.03.2021 32:46       Opencostnee       529.45         Apditation       17.03.2021 32:48       Opencostnee       529.45         Apditation       17.03.2021 32:49       Opencostnee       3314.45         Histogity_check_toolese       17.03.2021 33:49       Opencostnee       2187.45         Histogity_check_toolese       17.03.2021 33:49       Opencostnee       4204.45         Histogity_check_toolese       17.03.2021 33:49       Opencostnee       580.45         Histogity_check       17.03.2021 33:49       Opencostnee       580.45         Histogity_chece       17.03.2021 33:51       Opencostnee       147.45         Histogits.cos       17.03.2021 33:51       Opencostnee       247.45         Histogits.cos       17.03.2021 33:51       Opencostnee       247.45         Histogits.cos       17.03.2021 3		proteomp	15.07.2022 15:09	Петна с файлами		
W. file_integrity_manifestami       11.05.2021 14:32       Документ XML       15.85         K. APDDTAgt.exe       17.03.2021 23:48       Приложение       529 K5         M. gettysteminfo.cxe       17.03.2021 23:49       Приложение       3 314 K5         M. Magarity_check_toolese       17.03.2021 23:49       Приложение       2 187 K5         M. Magarity_check_toolese       17.03.2021 23:49       Приложение       2 187 K5         M. Magarity_check_toolese       17.03.2021 23:49       Приложение       2 187 K5         M. Magarity_check       17.03.2021 23:49       Приложение       2 187 K5         M. Maddal ene       17.03.2021 23:49       Приложение       2 187 K5         M. Maddal ene       17.03.2021 23:40       Приложение       180 K5         K. Beangtgui.exe       17.03.2021 23:41       Приложение       180 K5         K. Beangtgui.exe       17.03.2021 23:41       Приложение       180 K5         K. Beangtgui.exe       17.03.2021 23:51       Приложение       180 K5         M. Manageri.exe       17.03.2021 23:51       Приложение       180 K5         M. Manageri.exe       17.03.2021 23:51       Приложение       180 K5         M. Manageri.exe       17.03.2021 23:51       Приложение       266 K5         M.		rhac	15.07.2022 15:08	flames c dedinases		
K       AVPDTAgt.ses       17.03.2021 23:48       Пристоявание       529.85         Xs. getsysteminfo.exe       17.03.2021 23:49       Пристоявание       3.314.85         III Integrity_check_tool.exe       17.03.2021 23:49       Пристоявание       2.167.85         III Integrity_check_tool.exe       17.03.2021 23:49       Пристоявание       4.204.45         III Integrity_case       17.03.2021 23:49       Пристоявание       4.204.45         III Integrity_case       17.03.2021 23:49       Пристоявание       4.204.45         III Integrity_case       17.03.2021 23:51       Пристоявание       4.204.45         III Integrity_case       17.03.2021 23:51       Пристоявание       4.474.45         III Integrity_case       17.03.2021 23:51       Пристоявание       4.407.45         III Integrity_case       17.03.2021 23:51       Пристоявание       4.407.45         III Integrity_case		it file integrity manifest	aml 11.05.2021 14:32	Документ XML	18 \$5	
Septysteminfo.cse         17.03.2021 23:48         Приложение         3.314.85           Extragrity_check_toolese         17.03.2021 23:48         Приложение         2.167.85           Extragrity_check_toolese         17.03.2021 23:48         Приложение         4.204.45           Extragrity_check_toolese         17.03.2021 23:48         Приложение         4.204.45           Extragrity_check_toolese         17.03.2021 23:48         Приложение         4.204.45           Extragrity_check         17.03.2021 23:48         Приложение         4.204.45           Extragrity_check         17.03.2021 23:40         Приложение         4.204.45           Extragrity_check         17.03.2021 23:40         Приложение         580.45           Extragrity_check         17.03.2021 23:51         Приложение         580.45           Extragrity_check         17.03.2021 23:51         Приложение         518.05           Extragrity_check         17.03.2021 23:51         Приложение         546.85           Extragrit_exte <t< td=""><td></td><td>AVPDTAgt.exe</td><td>17.83.2021 23:40</td><td>Приложение</td><td>529 85</td><td></td></t<>		AVPDTAgt.exe	17.83.2021 23:40	Приложение	529 85	
Imintegrity_check_toolese       17.03.2021 23-49       Приложение       2 187.45         Imintegrity_check_toolese       17.03.2021 23-49       Приложение       4 204.45         Imintegrity_check_toolese       17.03.2021 23-49       Приложение       4 204.45         Imintegrity_check_toolese       17.03.2021 23-49       Приложение       4 204.45         Imintegrity_check_toolese       17.03.2021 23-49       Приложение       586.45         Imintegrity_check       17.03.2021 23-49       Приложение       586.45         Imintegrity_check       17.03.2021 23-51       Приложение       4 220.45         Imintegrity_chece       17.03.2021 23-51       Приложение       147.45         Imintegrity_chece       17.03.2021 23-51       Приложение       147.45         Imintegrity_chece       17.03.2021 23-51       Приложение       148.45         Imintegrity_chece       17.03.2021 23-51       Приложение       147.45         Imintegrity_chece       17.03.2021 23-51       Приложение       148.45         Imintegrity_chece       17.03.2021 23-51       Приложение       266.45         Imintegrity_chece       17.03.2021 23-51       Приложение       246.45         Imintegrity_chece       17.03.2021 23-51       Приложение       144.45		a getsysteminfo.exe	17.03.2621 23:49	Приложение	3 3 14 855	
It bicpuld.coe         17.03.2021 23-49         Приложение         4 204 85           It biolidition         13.03.1031 33-45         Приложение         121 85           It biolidition         17.08.2021 23-49         Приложение         121 85           It biolidition         17.08.2021 23-49         Приложение         121 85           It bicspy.com         17.08.2021 23-49         Приложение         150 455           It bicspy.com         17.03.2021 23-49         Приложение         150 455           It bicspy.com         17.03.2021 23-51         Приложение         4220 45           It binagent.com         17.03.2021 23-51         Приложение         147 85           It binagent.com         17.03.2021 23-51         Приложение         318 65           It binagent.com         17.03.2021 23-51         Приложение         246 45           It binagent.com         17.03.2021 23-51         Приложение         147 85           It binagent.com         17.03.2021 23-51         Приложение         1		integrity check tool.exe	17.03.2021 23:49	Приложение	2 187 85	
Till Maddel ave         17.03.2021 23.40         Damage Mark         1728 25           K         BioingRiguities         17.03.2021 23.40         Dipartocenses         S80 KE           K         BioingRiguities         17.03.2021 23.51         Dipartocenses         S80 KE           K         BioingRiguities         17.03.2021 23.51         Dipartocenses         S80 KE           K         BioingRift.exe         17.03.2021 23.51         Dipartocenses         266 KE           K         BioingRift.exe         17.03.2021 23.51         Dipartocenses         246 KE           K         Hongowit.exe         17.03.2021 23.51         Dipartocenses         246 KE           K         Hongowit.exe         17.03.2021 23.51         Dipartocenses         246 KE           K         Hongowit.exe         17.03.2021 23.51         Dipartocenses         245 KE     <		(III) kicpuld.eve	17.03.2021 23-49	Приложение	4 204 45	
K         Houngtguiteen         17.03.2021 23-00         Приложение         580 KB           K         Houpydaat         17.03.2021 23-01         Приложение         4220 AB           K         Houpydaat         17.03.2021 23-01         Приложение         147 KB           K         Houpydaat         17.03.2021 23-01         Приложение         318 KB           K         Houpydaatae         17.03.2021 23-01         Приложение         318 KB           K         Houpydaatae         17.03.2021 23-01         Приложение         318 KB           K         Houpydaatae         17.03.2021 23-01         Приложение         344 KB           K         Houpydaatae		IT Heridel eve.	100.000.000	Ones	177.45	
K         Bicspryasiz         1/2032021         23.49         Приложение         504 Kb           Midumper.exe         17.03.2021         23.61         Приложение         4.220 K5           Minover.exe         17.03.2021         23.61         Приложение         147 K5           Minover.exe         17.03.2021         23.61         Приложение         147 K5           Minogeri.exe         17.03.2021         23.61         Приложение         318 65           Minageri.exe         17.03.2021         23.61         Приложение         318 65           Minageri.exe         17.03.2021         23.61         Приложение         318 65           Minageri.exe         17.03.2021         23.61         Приложение         4407 K5           Minageri.exe         17.03.2021         23.61         Приложение         4407 K5           Minageri.exe         17.03.2021         23.61         Приложение         124 45           Minageri.exe         17.03.2021         23.61         Приложение         124 45           Minageri.exe         17.03.2021         23.62         Приложение         124 45		K Hesngtguiese	17.83.2021 23-49	Притокание	585 KB	
Midumper.exe         17.03.2021 23:51         Приложение         4 220 X5           It Minover.exe         17.03.2021 23:51         Приложение         147 X5           It Minover.exe         17.03.2021 23:51         Приложение         147 X5           It Minover.exe         17.03.2021 23:51         Приложение         518 K5           It Minover.exe         17.03.2021 23:51         Приложение         518 K5           It Minover.exe         17.03.2021 23:51         Приложение         4407 K5           It Minover.exe         17.03.2021 23:51         Приложение         124 K5           It Minover.exe         17.03.2021 23:51         Приложение         124 K5		K Beipsylese	17.03.2021 2394	Приложение	204 85	
Importance         17.03.2021 23:51         Приложение         147.35           ImageName         17.03.2021 23:51         Приложение         318.45           ImageName         17.03.2021 23:51         Приложение         318.45           ImageName         17.03.2021 23:51         Приложение         266.45           ImageName         17.03.2021 23:51         Приложение         24.47 K5           ImageName         17.03.2021 23:51         Приложение         4.407 K5           ImageName         17.03.2021 23:51         Приложение         124.45           ImageName         17.03.2021 23:02         Приложение         124.45		No kidumper.exe	17.03.2021 23:51	Приложение	4 220 86	
Imagentace         17.03.2021 23:51         Приложение         \$18.65           Imagentace         37.03.2021 23:51         Приложение         266.65           Imagentace         17.03.2021 23:51         Приложение         246.75           Imagentace         17.03.2021 23:51         Приложение         4407.85           Imagentace         17.03.2021 23:51         Приложение         4457.85           Imagentace         17.03.2021 23:51         Приложение         584.85           Imagentace         17.03.2021 23:52         Помполетиче         4451.85		ill kimover, eve	17.03.2021 23:51	Приложение	147 85	
Imagentiase         17.03.2021 23:51         Приложение         266 K5           Minagentiase         17.03.2021 23:51         Приложение         4 407 K5           Imagentiase         17.03.2021 23:52         Приложение         4 451 K5		kinagchik.exe	17.03.2021 23:51	Приложение	318 65	
Idensities         17.03.2021 23:51         Приможение         4.407 KE           Til Minageeds.exe         17.03.2021 23:51         Приможение         124 KE           Til Mospees.exe         17.03.2021 23:52         Приможение         124 KE		i kinagent.exe	17.03.2021 23:51	Приложение	266 KG	
Image:ds.com         17/03.2021 23:51         Приложение         124.65           Image:ds.com         17/03.2021 23:52         Приложение         4.451 K5		kinagnti.exe	17.03.2021 23:51	Приложения	4 497 85	
Mospres.eve 17.03.2021 23.52 Trownowsnike 4.451 K5		📧 kinagwids.exe	17.03.2021 23:51	Приложение	124.85	
	v	(II) Mospreplexe	17.03,2021 23:52	Приложение	4.451.85	100

Рисунок Г.19. – Запуск утилиты «klcsngtgui.exe»

3) в открывшемся окне выбрать «Запустить утилиту klnagchk» (см. рисунок Г.20.).

Агент администриро	вания		×		
Отправить пакет пульс	Текущий сервер	10.196.2.132	^		
Запустить утилиту	Текущий профиль				
<u>kinagchk</u>	kinagchk Последнее подключение 15.07.2022 15:28:15				
	Версия Агента администрирования 13.0.0.11247 (openssl)				
	Защита	Выполняется			
	Антивирусная база	15.07.2022 13:02:00			
Поспелная полная поверка					

Рисунок Г.20. – Запуск утилиты «klnagchk»

В результате появится командная строка, в которой отображается различная диагностическая информация о взаимодействии с Kaspersky Security Center. Параметры, требующие внимания, выделены красным прямоугольником (см. рисунок Г.21.).



Рисунок Г.21. – Вывод утилиты «klnagchk.exe»

## Шаг 2. Выполнить настройку модуля «Базовая защита»

Настройка модуля «Базовая защита» заключается в настройке компонентов «Защита от файловых угроз», «Защита от веб-угроз», «Защита от почтовых угроз», «Защита от сетевых угроз», «Сетевой экран», «Защита от атак BadUSB», «AMSI-защита» (см. рисунок Г.22.).



Рисунок Г.22. – Общий вид раздела настроек «Базовая защита»

## Компонент «Защита от файловых угроз»

Компонент «Защита от файловых угроз» предназначен для проверки на наличие ВПО открытых и запускаемых файлов в локальной файловой системе, а также на смонтированных (присоединенных) дисках. Компонент постоянно находится в оперативной памяти средства ВТ.

Для настройки данного компонента необходимо:

1) в разделе «Базовая защита» перейти в меню «Защита от файловых угроз» (см. рисунки Г.22. и Г.23.);

2) в появившемся окне активировать «Защита от файловых угроз» (см. рисунок Г.23.);

 далее в поле «Действие при обнаружении угрозы» выбрать пункт необходимый пункт и нажать кнопку «Расширенная настройка» (см. рисунок Г.23.);



Рисунок Г.23. – Настройка компонента «Защита от файловых угроз»

4) в раскрывающемся меню в поле «Типы файлов» выбрать необходимое условие, в поле «Изменить область защиты» выбрать пункты «Все внешние устройства» и «Все жесткие диски» (см. рисунки Г.24. и Г.25.). Нажать «ОК»;



Рисунок Г.24. – Настройка компонента «Защита от файловых угроз»

	? – 🗆 ×			? – 🗆 🗙
Kaspersky	< Настройка	Kaspersky	< Настройки Защиты от файловых угроз	
Endpoint Security	Настройки Защиты от файловых	Endpoint Security	Область Защиты от файловых угроз	
	угроз		+ Добавить 🗇 Удалить	
Безопасность	Типы файлов	Безопасность	Область проверки	Статус
С Обновление	<ul> <li>Все файлы</li> <li>Файлы, проверземые по формату</li> </ul>	С Обновление	Все внешние устройства	Включена
🕎 Задачия	О Файлы, проверяемые по расширению	Задачия	📄 Все жесткие диски	Включена
— Д Лицензия	Изменить область защиты Методы проверки	— Ор Лицензия	Все сетевые диски	Выключена
Педераличност 19.1962.20 Саран правологи 1.60097 якада 1.6009 1.192.351	In the second s	Годи управляется ТС 1962-132 Та 1962-132 Та аналуу накад Баронор 11.68.331		
	Сехранить Отмена		ОК Отмена	

Рисунок Г.25. – Настройка области защиты

5) далее в поле «Методы проверки» включить «Эвристический анализ», в поле «Оптимизация поверки» выбрать пункт «Проверять только новые и измененные файлы», в поле «Проверка составных файлов» выбрать пункты «Проверять архивы», «Проверять дистрибутивы», «Проверять файлы офисных форматов (см. рисунок Г.26.);



Рисунок Г.26. - Настройка компонента «Защита от файловых угроз»

6) выбрать пункт «Не распаковывать составные файлы большого размера», определить максимальный размер файла, выбрать пункт «Распаковывать составные файлы фоновом режиме», В определить минимальный размер файла, активировать «Технология iSwift» и «Технология «iChecker» в разделе «Технологии проверки» и нажать «Сохранить» (см. рисунок Г.27.);



Рисунок Г.27. – Настройка проверки составных файлов

## Компонент «Защита от почтовых угроз»

Компонент «Защита от почтовых угроз» предназначен для проверки входящих и исходящих сообщений на наличие в них опасных объектов. Он запускается при старте операционной системы, постоянно находится в оперативной памяти средства ВТ и проверяет все почтовые сообщения по протоколам POP3, SMTP, IMAP и NNTP. Примечание: настройка данного компонента необходима только для самостоятельных абонентских пунктов (далее – АП) сети Интернет. Для автономных средств ВТ, а также средств ВТ, входящих в состав самостоятельной ЛВС, допускается данный компонент отключить.

Для настройки данного компонента необходимо:

1) в разделе «Настройки базовой защиты» перейти в меню «Защита от почтовых угроз» (см. рисунки Г.22. и Г.28.);

2) в появившемся окне активировать «Защиту от почтовых угроз» (см. рисунок Г.28.);

3) в поле «Действие при обнаружении угрозы» установить выбор необходимом в пункте и в меню «Расширенные настройки» в разделе «Эвристический анализ» установить выбор в «Использовать эвристический анализ» и переместить ползунок вверх на «Глубокий». Далее нажать на кнопку «Сохранить» (см. рисунок Г.28.);



Рисунок Г.28. – Настройка компонента «Защита от почтовых угроз»

## Компонент «Защита от веб-угроз»

Компонент «Защита от веб-угроз» предназначен для защиты информации, поступающей на средство ВТ по НТТР-протоколу, а также для предотвращения запуска на средстве ВТ опасных скриптов, полученных через браузер.

Защита от веб-угроз предусматривает контроль НТТР-трафика, проходящего только через порты, указанные в списке контролируемых портов САВЗ.

Примечание: настройка данного компонента необходима только для самостоятельных АП сети Интернет. Для автономных средств ВТ, а также средств ВТ, входящих в состав самостоятельной локальной вычислительной сети (далее – ЛВС), допускается данный компонент отключить.

Для настройки данного компонента необходимо:

1) в разделе «Настройки базовой защиты» перейти в меню «Защита от веб-угроз» (см. рисунки Г.22. и Г.29.);

 в появившемся окне активировать «Защиту от веб-угроз» (см. рисунок Г.29.);

 в поле «Действие при обнаружении угрозы» выбрать пункт «Запрещать загрузку» и нажать на кнопку «Расширенная настройка» (см. рисунок Г.29.);

	? – 🗆 ×
Kaspersky	< Настройка
Endpoint Security	Настройки Защиты от веб-угроз
Мониторинг	
D Безопасность	Вкл Ващита от веб-угроз Проверяет входящий веб-трафик и предотвращает запуск опасных скриптов.
С Обновление	Узнать больше
<b>Б</b> о Задачи	Уровень безопасности Значения настроек текущего уровня безопасности отличаются от значений по умолчанию.
<b>ਊ</b> Лицензия	Восстановить рекомендуемый уровень безопасности
	Действие при обнаружении угрозы
	<ul> <li>Запрещать загрузку</li> <li>н. н. н</li></ul>
	О информировать
Под управлением: 10.196.2.132	Расширенная настройка ч
Сервер подключенс 2 миняуты назад Версик 11.9.0.351	измесния с расшарелные настрояки приложения, если вы опытный пользователь компьютера, пеправильная настроика приложения может снизить вашу защиту.
¢ 0	Сохранить Отмена

Рисунок Г.29. – Настройка компонента «Защита от веб-угроз»

4) в появившемся окне в поле «Методы проверки» установить выбор в пунктах «Проверять веб-адрес по базе вредоносных веб-адресов», «Использовать эвристический анализ для обнаружения вирусов», в поле «Анти-фишинг» установить выбор в пунктах «Проверять веб-адрес по базе фишинговых веб-адресов» и «Использовать эвристический анализ». Далее нажать кнопку «Сохранить» (см. рисунок Г.30.). Примечание: раздел «Доверенные веб-адреса» компонента «Защита от веб-угроз» необходимо веб-угроз» необходимо оставить без изменений.



Рисунок Г.30. – Настройка компонента «Защита от веб-угроз»

## Компонент «AMSI-защита»

Компонент «AMSI-защита» предназначен для поддержки интерфейса Antimalware Scan Interface от Microsoft и позволяет обнаруживать угрозу и уведомлять о ней стороннее приложение, например Microsoft Office. После получения уведомления сторонняя программа не дает выполнить вредоносные действия.

Для настройки данного компонента необходимо:

1) в разделе «Настройки базовой защиты» перейти в меню «AMSIзащита» (см. рисунки Г.22. и Г.31.);

2) в открывшемся меню активировать «AMSI-защита». В пункте «Проверка составных файлов» отметить только «Проверять файлы офисных форматов» « (см. рисунок Г.31.);

3) в пункте «Ограничение по размеру» активировать «Не распаковывать составные файлы большого размера» и пункте «Максимальный размер» установить параметр, исходя из технических возможностей средства ВТ, и нажать «Сохранить» « (см. рисунок Г.31.).

	? – 🗆	×
Kaspersky	< Настройка	
Endpoint Security	Настройки AMSI-защиты	
Мониторинг		
Безопасность	AMSI-защита Позволяет другим приложениямы и службам проверять объекты через интерфейс AMSI с помощью Kaspersky Endpoint Security.	
С Обновление		
💭 Задачи	Проверять архивы	
<b>О</b> Лицензия	<ul> <li>Проверять дистрибутивы</li> <li>Проверять файлы офисных форматов</li> </ul>	
	Ограничение по размеру	
	Не распаковывать составные файлы большого размера	
	На проверку файлов, извлекаемых из архивов, эта настройка не распространяется.	
	Максимальный размер файла	
10.196.2.132	4 🗘 M5 (or 1 до 9999)	
Сарвер подскочан. 2 минуты назад		
11.9.0.351		
¢ Q	Сохранить	

Рисунок Г.31. – Настройка компонента «AMSI-защита»

## Компонент «Сетевой экран»

Компонент «Сетевой экран» предназначен для обеспечения защиты данных, хранящихся на средстве ВТ пользователя, путем блокировки всех возможных для операционной системы угроз во время подключения средства ВТ к сети Интернет или к локальной сети. Примечание: применение СВТ возможно в трех режимах: автономное СВТ, СВТ, входящее в состав самостоятельной ЛВС, самостоятельный АП. Настройка, приведенная в настоящей инструкции применима для автономных СВТ. Для СВТ, входящих в состав самостоятельной ЛВС данный компонент допускается отключить, Для самостоятельного АП необходимо включить компонент и настроить параметры, исходя из условий эксплуатации.

Для настройки данного компонента необходимо:

1) в разделе «Настройки базовой защиты» перейти в меню «Сетевой экран» (см. рисунки Г.22. и Г.32.);

2) далее активировать «Сетевой экран» и нажать кнопку «Пакетные правила» (см. рисунок Г.32.):

								?		$\times$
Kasper	sky	< Настро	ойка							
Endpoin	t Security	Настр	ойки (	Сетево	ого экр	ана				
Mo Mo	ниторинг									
<b>О</b> Без	опасность	盟	Сетевой экр Фильтрует о локальную	ран сетевую акти сеть и интер	вность и обе нет.	спечивает без	опасный досту	/n e	Вкл	
C 06	новление		Узнать бол	њше						
<b>До</b> Зад	ачи	Правила прі Настройка сет	оиложений гевых правил пр	риложений в о	перационной о	истеме.				
<b>ਊ</b> Лиц	цензия	Пакетные пр Настройка пра	авила авил для сетевь	ых пакетов и по	токов данных.					
		Доступные о Настройка сете	сети гевых соединен	เหตี.						
Под управления 10.196.2.132 Сервер подилю 3 минуты наз Версик 11.9.0.351	ем: Чаяс а <b>д</b>									
¢	G	Сохрани	ип	Отмена	]					

Рисунок Г.32. – Настройка компонента «Сетевой экран»

3) в появившемся окне «Пакетные правила» выделить любое пакетное правило (нажать левой кнопкой мыши на него). Выделить все пакетные правила, нажав комбинацию клавиш Ctrl+A. В верхней панели действия (над

сетевыми пакетными правилами) нажать на кнопку «Удалить» для удаления всех выделенных пакетных правил (см. рисунки Г.32. и Г.33.);

k Пакетные правила		?	– o ×
Пакетные правила			
+ Добавить 🖉 Изменить 🛅 Удалить 🕇 Вверх 🗍 Вниз	С. Поиск		
🕑 Название	Разрешение	Статус	Адрес
TOR		Неактивно	
DNS over TCP	8	С Активно	
Запросы к серверу DNS по протоколу UDP	8	🚺 Активно	
Sending E-Mails	8	С Активно	
Любая сетевая активность (Доверенная сеть)		С Активно	Доверенная с
Любая сетевая активность (Локальная сеть)	8	С Активно	Локальная сеть
Remote Desktop		🔵 Активно	
Local Services (TCP)		С Активно	
Local Services (UDP)		С Активно	
Входящая активность по протоколу ТСР		С Активно	

Рисунок Г.33. – Удаление пакетных правил

4) создать правило, запрещающее любую сетевую активность на средстве ВТ. Для этого во вкладке «Пакетные правила» нажать кнопку «Добавить». В появившемся окне выбрать статус правила «Активно», в поле «Действие» выбрать «Запрещать». В поле «Название» добавить название. Убедиться, что в поле «Направление» выбрано «Входящее/Исходящее», а в полях «Удаленные адреса» и «Локальные адреса» установлены значения «Любой адрес» и нажать «Сохранить» (см. рисунок Г.34.);

Пакетные правила        Caryc       Добавление пакетного правила       Шабоос сетесого правила
Addamens Transmens Transme
Image: Papeusewe Cray:     Agec       Image: Papeusewe Cray:     Agec       Image: Papeusewe Cray:     Agec       Image: Papeusewe Cray:     Cray:       Image: Papeusewe Cray:     Cray:       Image: Papeusewe Cray:     Cray:       Image: Papeusewe Cray:     Transmo       Image: Papeusewe Cray:
Handaner:     Ceretore правило NH       Дебствие:     Запрецать       @ Направление:     Владящее / Исодящее       @ Протовол:     Все
Abberuwe: Barpenann * C Harpansenne: Brogstuge / Mongature * C Tiporonan: Bro *
C         Harpaneever         Brogenue         *           C         Pportosis.         Box         *
C Tepresa. to ·
Churcher mert. Churcher Angec *
Accasult age:     Accosult age:     Accosult age:
О Записывать события
Настройки ниже рекомендуется менять только опытикии пользователям
Сохранит. Отмени

Рисунок Г.34. – Настройка сетевых пакетных правил

5) в новом окне проверить наличие правила и нажать «Закрыть» (см. рисунок Г.35.).



Рисунок Г.35.– Результат создания правила, запрещающего любую сетевую

#### Компонент «Защита от сетевых угроз»

Компонент «Защита от сетевых угроз» предназначен для проверки входящего сетевого трафика на наличие активности, характерной для сетевых атак. Обнаружив попытку сетевой атаки на средство ВТ пользователя, САВЗ блокирует сетевую активность атакующего средства ВТ. После этого на экран выводится уведомление о том, что была попытка сетевой атаки с указанием информации об атакующем средстве ВТ.

Примечание: на автономных средствах ВТ допускается данный компонент не включать.

Для включения/отключения данного компонента необходимо:

1) в разделе «Настройки базовой защиты» перейти в меню «Защита от сетевых угроз» (см. рисунки Г.22. и Г.36.);

2) в появившемся окне активировать «Защиту от сетевых угроз» и «Защиту от МАС-спуфинга», выбрать пункт «Только уведомлять» в разделе «При обнаружении атаки МАС-спуфинг» и нажать кнопку «Сохранить» (см. рисунок Г.36.).



Рисунок Г.36. – Настройка компонента «Защита от сетевых угроз»

## Компонент «Защита от атак BadUSB»

Компонент «Защита от атак BadUSB» предназначен для предотвращения подключения к компьютеру зараженных USB-устройств, имитирующих клавиатуру.

Для настройки данного компонента необходимо:

1) в разделе «Настройки базовой защиты» перейти в меню «Защита от атак BadUSB» (см. рисунки Г.22. и Г.37.);

2) в открывшемся меню активировать «Защита от атак BadUSB» и «Запретить использование экранной клавиатуры для авторизации USBустройств» в разделе «Авторизация USB-устройств при подключении» (см. рисунок Г.37.);

3) в поле «Максимальное количество попыток авторизации USBустройства» указать необходимое значение, и в поле «Таймаут при достижении максимального количества попыток» указать требуемое значение (см. рисунок Г.37.).

	?		
Kaspersky	< Настройка		
Endpoint Security	Настройки Защиты от атак BadUSB		
На Мониторинг			
D Безопасность	<ul> <li>Защита от атак BadUSB</li> <li>Предотвращает использование USB-устройств, имитирующих поведение клавиатур.</li> </ul>	Вкл	
С Обновление	Узнать больше		
<b>Бо</b> Задачи	Авторизация USB-устройств при подключении		
<b>Q</b> Лиценаия	Запретить использование экранной клавиатуры для авторизации USB-устройств		
	Авторизация USB-устройств Максимальное количество попыток авторизации USB-устройства: 5 0 раз (от 1 до 10)		
Под угравлениес 10.1962.132 Север подологие:	Таймаут при достижении максимального количества попыток:		
Меньше минуты назад Версик 11.9.0.351			
0 O	Сохранить Отмена		

Рисунок Г.37. – Настройка компонента «Защита от атак BadUSB»

## Шаг 3. Выполнить настройку модуля «Продвинутая защита»

Настройка модуля «Продвинутая защита» заключается в настройке компонентов «Kaspersky Security Network», «Анализ поведения», «Защита от эксплойтов», «Предотвращение вторжений», «Откат вредоносных действий».

## Компонент «Kaspersky Security Network»

Компонент «Kaspersky Security Network» предназначен для высокой скорости реакции САВЗ на новые виды угроз, повышения эффективности работы некоторых компонентов защиты, а также снижения вероятности ложных срабатываний.

Примечание: данный компонент функционирует только на средствах ВТ имеющих подключение к сети передачи данных МО РФ (далее – СПД). Для автономных средств ВТ необходимо данный компонент отключить.

Для включения/отключения компонента необходимо в главном окне САВЗ нажать значок «Настройки» и в разделе «Продвинутая защита» перейти в меню «Kaspersky Security Network» и перевести кнопку в положение «Включить» (см. рисунки Г.38., Г.39. и Г.40.).



Рисунок Г.38. – Главное окно «Kaspersky Endpoint Security 11 для Windows»

Kas Endp	<b>persky</b> point Security	г — Настройка меренау гларонт зесилту.		
	Мониторинг	Продвинутая защита 🤿		
0		Kaspersky Security Network Облачная база знаний о репутяции файлов, интернет-ресурсов и програмыного обеспечения.		
C F	Обновление Задачи	Анализ поведения Анализирует поведение приложеный и обнаруживает сложные утроты, такие как приложения-вымосатели.	•	
õ	Лицензия	Защита от эксплойтов блосирует действия кредоносных приложений, которые используют улзвимости в програмыном обеспечении.		
		Откат вредоносных действий Опсатывает действия, произведянные вредоносными приложениями.		
Под упра	Marrowski 1.132	Предотвращение вторжений Предотвращает выпознение прихожнимы опасных для системы действий и контролирует доступ к ресурсам системы.		
Серенр п 1 минут Версик	назад	Контроль безопасности л		
11.9.0.3		Контроль приложений Контроленрует запуск приложений пользователеми.		
¢	ø	Контроль устройств	•	

Рисунок Г.39. – Общий вид раздела настроек «Продвинутая защита»



Рисунок Г.40. – Компонент «Kaspersky Security Network»

#### Компонент «Анализ поведения»

Компонент «Анализ поведения» предназначен для сбора информации о действиях программ на средствах ВТ и предоставления ее другим компонентам защиты в целях повышения эффективности их работы. Данный компонент использует шаблоны опасного поведения программ, которые состоят из последовательностей действий, классифицируемых САВЗ как опасные.

В случае, если активность программы совпадает с одним из шаблонов опасного поведения, САВЗ выполняет выбранное ответное действие. Функциональность САВЗ, основанная на шаблонах опасного поведения, обеспечивает проактивную защиту средства ВТ.

Для настройки данного компонента необходимо:

1) в разделе «Продвинутая защита» перейти в меню «Анализ поведения» (см. рисунки Г.39. и Г.41.);

2) в появившемся окне выбрать пункт «Включить Анализ поведения» (см. рисунок Г.41.);

3) далее в поле «При обнаружении вредоносной активности программы» выбрать необходимый пункт (предпочтительно удалить) и нажать кнопку «Сохранить». Остальные параметры оставить без изменений (см. рисунок Г.41.).



Рисунок Г.41. – Настройка компонента «Анализ поведения»

## Компонент «Защита от эксплойтов»

Компонент «Защита от эксплойтов» предназначен для контроля исполняемых файлов, запускаемых уязвимыми программами. При попытке запуска исполняемых файлов из уязвимой программы пользователя происходит блокировка данного файла. Информация о запрете запуска исполняемого файла сохраняется в отчете о работе компонента «Защита от эксплойтов».

Для настройки данного компонента необходимо:

1) в разделе «Продвинутая защита» перейти в меню «Защита от эксплойтов» (см. рисунки Г.39. и Г.42.);

2) в появившемся окне выбрать пункт «Включить Защиту от эксплойтов» (см. рисунок Г.42.);

3) в поле «При обнаружении эксплойта» выбрать необходимый пункт (предпочтительно «Блокировать операцию»). Активировать функцию «Включить защиту памяти системных процессов» и нажать кнопку «Сохранить» (см. рисунок Г.42.).

			×
Kaspersky	< Настройка		
Endpoint Security	Настройки Защиты от эксплойтов		
Мониторинг			
Безопасность	Защита от жетлойтов Блокирует действия вредоносных приложений, которые используют укваимости в программном обеспечении.	Bica	
С Обновление	Узнать больше		J
<b>Бо</b> заталин	При обнаружении эксплойта:		
	<ul> <li>Блокировать операцию</li> <li>Информировать</li> </ul>		
	Включить защиту памяти системных процессов		
Под управление 10.196.2.132 Спртер перелялителя. 1 минуту назад Вероле 11.9.0.351			
¢ 0	Спуранить Отмена		

Рисунок Г.42. – Настройка компонента «Защита от эксплойтов»

#### Компонент «Предотвращение вторжений»

Компонент «Предотвращение вторжений» предназначен для предотвращения выполнения программами опасных для системы действий, а также обеспечения контроля доступа к ресурсам операционной системы и персональным данным.

Компонент контролирует работу программ, в том числе доступ программ к защищаемым ресурсам (например, к файлам и папкам, ключам реестра), с помощью правил контроля программ. Правила контроля активности программ представляют собой набор ограничений для различных действий программ в операционной системе и прав доступа к ресурсам компьютера.

Для настройки данного компонента необходимо:

1) в разделе «Продвинутая защита» перейти в меню «Предотвращение вторжений» (см. рисунки Г.39. и Г.43.);

2) в появившемся окне активировать «Предотвращение вторжений» (см. рисунок Г.43.);

3) в поле «Правила обработки приложений» выбрать пункты «Обновлять правила контроля ранее неизвестных программ из базы KSN», «Доверять программам, имеющим цифровую подпись», «Удалять правила контроля программ, не запускавшихся более 60 дней» и нажать кнопку «Сохранить» (см. рисунок Г.43.).



Рисунок Г.43. – Настройка компонента «Предотвращение вторжений»

## Компонент «Откат вредоносных действий»

Компонент «Откат вредоносных действий» предназначен для отката действий, произведенных ВПО в операционной системе.

Для настройки данного компонента необходимо:

1) в разделе «Продвинутая защита» перейти в меню «Откат вредоносных действий» (см. рисунки Г.39. и Г.44.);

2) в появившемся окне активировать «Откат вредоносных действий» и нажать кнопку «Сохранить» (см. рисунок Г.44.).



Рисунок Г.44. – Настройка компонента «Откат вредоносных воздействий»

#### Шаг 4. Выполнить настройку модуля «Контроль безопасности»

Настройка модуля «Контроль безопасности» заключается в настройке компонентов «Веб-Контроль», «Контроль устройств», «Адаптивный контроль аномалий», «Контроль приложений» (см. рисунок Г.45.).



Рисунок Г.45. – Меню настроек «Контроль безопасности»

#### Компонент «Контроль приложений»

Компонент «Контроль приложений» предназначен для контроля запуска программ пользователями и запуска программ с применением правил контроля запуска программ.

Для настройки данного компонента необходимо:

1) в разделе настроек «Контроль безопасности» выбрать меню «Контроль приложений» (см. рисунки Г.45. и Г.46.);

2) в появившемся окне активировать «Контроль приложений» и нажать кнопку «Сохранить» (см. рисунок Г.46.).

Примечание: допускается более детальная настройка данного компонента должностным лицом, производящим настройку САВЗ, исходя из используемого программного обеспечения. Режим контроля программ устанавливается параметром «Белый список» (запрещено все, что явно не разрешено), либо «Чёрный список» (разрешено все, что явно не запрещено).



Рисунок Г.46. – Настройка компонента «Контроль приложений»

#### Компонент «Контроль устройств»

Компонент «Контроль устройств» предназначен для обеспечения безопасности конфиденциальной информации путем ограничения доступа

пользователей к устройствам, установленным или подключенным к средству ВТ.

Для настройки данного компонента необходимо:

1) в разделе настроек «Контроль безопасности» выбрать меню «Контроль устройств» (см. рисунки Г.45. и Г.46.);

2) в появившемся окне активировать «Контроль устройств» и нажать кнопку «Сохранить» (см. рисунок Г.47.). Примечание: если на средстве ВТ установлено и настроено средство защиты информации «Secret Net», то допускается данный компонент активировать, но не настраивать;

		? – 🗆 🗙
Kas	persky	< Настройка
Endp	oint Security	Настройки Контроля устройств
品		
0		<ul> <li>Вол </li> <li>Вол </li> <li>Вол </li> <li>Вол </li> <li>Вол </li> <li>Вол </li> </ul>
C	Обновление	Настройка доступа
Ş	Задачи	Устройства и сети Wi-Fi Правила доступа для устройств и сетей Wi-Fi.
ନ୍ମ	Лицензия	Шины подключения
		Правила доступа к шинам подключения.
		Доверенные устройства
		Успройства, доступ к которым всегда разрешён.
		Анти-Бриджинг
		Компоният не поввояет одновременно установить несколько селевых сонданений для компьютира. Это поввояет защитить корпоративную сеть от апак через незащищеньке, несанкционированные сети.
Подупра 10.1962	1.132	Шаблоны сообщений
Сереер п 3 нимерт	logichid-kiki: Na MESAA	Сообщение о блокировке
Берсия 11.9.0.3		Шеблон сообщения, которов появляется у пользователя при обращения с заблокированному устройству или при попытки совершить запрещенения операцию с содерживым устройства.
		Casting and a second se
	o	Сокранить Отмена

Рисунок Г.47. – Настройка компонента «Контроль устройств»

3) во вкладке «Устройства и сети Wi-Fi» запретить доступ к запоминающим устройствам: «Съемные диски» (по соответствующему устройству, нажать левой кнопкой мыши, в выпадающем меню выбрать пункт «Запрещать»). Запретить доступ к внешним устройствам (в зависимости от требований, предпочтительно «Модемы», «Bluetooth»), выбрав около соответствующего устройства доступ «Запрещать» (см. рисунки Г.48. и Г.49.). Далее последовательно нажать «ОК»;

K Kaspersky Endpoint Security	? – 🗆 X	K Kaspensky Endpoint Security ? - D
Типы устройств		← Настройки Контроля устройств
Доступ к запоминающим устройствам		Правила доступа к устройствам Запись событий в хорная
Имя	Доступ	Доступ
Жестине диски	Зависит от шины подключения	<ul> <li>Разрешать</li> <li>Вапренцать</li> </ul>
Стемпие диски	Разрешать	Эзвикит от шины подключения
Дискеты	Зависит от шины подключения	Ограничивать правилами
СD/0VD-приводы	Зависит от шины подключения	Права пользователей
Портативные устройства (МТР)	Зависит от шины подключения	🕂 Добавить 🖉 Изменить 🗎 Удамить
Доступ к внешним устройствам		Пользователь Приоря Расписание доступа Состояние Чтение Зались
Имя	Доступ	🗌 Все 🛛 🗘 По умслчанию 🌑 Включено 😰 😢
Принтеры	Зависит от шины подключения 🗸 🗸	
Модемы	Разрешать 🗸	
	ОК Отмена	ОК Отмен

Рисунок Г.48. – Запрет использования устройств

Kaspersky Endpoint Security	? - 🗆
Типы устройств	
Изая	Доступ
Принтеры	Зависит от шины подключения 🗸 🗸
Модемы	Зависит от шины подключения 🗸 🗸
Стримеры	Зависит от шины подключения 🗸 🗸
Многофункциональные устройства	Зависит от шины подключения 🗸 🗸
Устройства чтения смарт-карт	Зависит от шины подключения 🗸 🗸
Windows CE USB ActiveSync ycrpoйcrea	Зависит от шины подключение 🗸 🗸
Внешние селевые адаптеры	Зависит от шины подключения 🗸 🗸
Bluetooth	3anpeujatu 🔨
Камеры и оканеры	Разрешать
	✓ Запрещать
locтул к сетям Wi-Fi	Зависит от шины подключения

Рисунок Г.49. – Запрет использования устройств

4) перейти во вкладку «Шины подключения», в появившемся окне необходимо запретить доступ к шинам (в зависимости от требований, предпочтительно «Инфракрасный порт» и «FireWire»). Нажать кнопку «Сохранить» (см. рисунок Г.50.);
| Kaspersky<br>Endpoint Security                                                                         | < Настройки Контроля устройств<br>Шины подключения                                                                | ? – ¤ ×                                                                              |
|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Мониторинг<br>Бесопасность<br>СОбновление<br>Задания<br>Ликценския                                     | Шины подслючения устройств<br>Инфракрасный порт<br>Последовательный порт<br>Параллельный порт<br>USB<br>FireWitro | Доступ<br>Запрещать<br>Разрещать<br>Разрещать<br>Разрещать<br>Разрещать<br>Запрещать |
| Под управляющих<br>16.196.2.132<br>Серева подахочнос<br>1 <b>павоуту назада</b><br>Бироок<br>11.90.331 | PCMCIA                                                                                                            | Разрешать                                                                            |
| 0 0                                                                                                    | ОК Отмена                                                                                                         |                                                                                      |

Рисунок Г.50. – Запрет использования шин «Инфракрасный порт» и «FireWire»

5) создать разрешения для используемых съёмных дисков. Для этого подключить планируемый к использованию съемный диск к средству ВТ. Выбрать вкладку «Доверенные устройства» и нажать кнопку «Выбрать». В открывшемся окне «Выбор доверенных устройств» в пункте «Отображать подключенные устройства:» выбрать пункт «в данный момент». Далее в столбце «Устройства» в группе «Съемные диски» выбрать подключенный съемный диск. Нажать последовательно кнопки «ОК» и «ОК» (см. рисунок Г.51.).

Примечание: при необходимости в поле «Разрешать пользователям и/или группам пользователей:» можно перечислить учетные записи, для которых выбранное устройство будет доверенным.

Kaspersky Endpoint Security	<ul> <li>Настройки Контроля устройств</li> <li>Ловеренные устройства</li> </ul>	× Kaspersky Endpoint Security	7 – п × « Доверенные устройства Выбор доверенных устройств
Mountpare beconsoire	Sudgan         // Hassons         It /gabons         Q Boitz           Humopr         []: Sumopr         []: Sumopr	Monuropuer O Seminations	Виберина устройствоја) для добавления в список доверонных устройств. Отображать падилоченные устройства: Иданный измент + Q. Пенск
Chicateune Jacone Q Jacquester	🗋 Наквания — Тип устройства — Модель / Ид., — Пользовател., — Кончингарий:	С Облаванные С Задание О Ликриския	Утронства         Состояния           • Хаспон диски         -           • 519320325AS         -           \$SSID0560470, @PROD_519320325AS4819615/1988/05600000         Подаление
Пар у раничение 14 Мад. 20 20 1 Бануу салад 1 Бануу салад 1 Бануу 1 1 Бануу 1 1 Бануу 1	Снисек пуст.	Pag.processore Na 160.2.13 Santaga and Santaga and Santaga and Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na Na N	<ul> <li>СОКУЮ-прияван</li> <li>Канеры и сканеры</li> <li>Коммонтарий:</li> <li>Пользователи и / или трупны пользователей</li> <li>+ добаать.</li> <li>С ланить.</li> </ul>
0 0	OK. Omena		Отмена

Рисунок Г.51. – Выбор доверенных устройств

## Компонент «Веб-контроль»

Компонент «Веб-контроль» предназначен для контроля действия пользователей в локальной сети организации, ограничения или запрета доступа к веб-ресурсам.

Примечание: Настройка данного компонента необходима только для самостоятельных АП сети Интернет. Для автономных средств ВТ, а также средств ВТ, входящих в состав самостоятельной ЛВС, допускается данный компонент не настраивать.

Для настройки данного компонента необходимо:

1) в разделе настроек «Контроль безопасности» выбрать меню «Вебконтроль» (см. рисунки Г.45. и Г.52.);

2) в появившемся окне активировать «Веб-Контроль» и нажать кнопку «Сохранить» (см рисунок Г.52.).



Рисунок Г.52. – Настройка компонента «Веб-контроль»

При необходимости настройки блокировки веб-ресурсов выполняются следующие шаги:

1) в разделе настроек «Контроль безопасности» выбрать меню «Вебконтроль» (см. рисунки Г.45. и Г.52.);

2) перейти в меню «Правила доступа к веб-ресурсам» (см. рисунок Г.53.);



Рисунок Г.53. – Настройка правил доступа к веб-ресурсам

3) в открывшемся меню добавить новое правило, для этого нажать на кнопку «Добавить» (см. рисунок Г.54.);

< Настройки Веб-Контроля					
Правила доступа к веб-р	есурсам				
+ Добавить 🖉 Изменить 🗇 Удалит	ы ↑ Вверх ↓ Вниз	С. Поиск			
П Название правила: Состояние	Действие	Условия			
	Не задано ни одного правила				

Рисунок Г.54. – Добавление нового правила доступа к веб-ресурсам

4) в разделе «Правило доступа к веб-ресурсам» необходимо присвоить название новому правилу, в меню «Состояние» выбрать «Активно», в меню «Действие» выбрать «Запрещать», в разделе «Содержимое фильтра» активировать «По категориям содержания» и нажать «Настроить» (см. рисунок Г.55.);

Коравила доступа к веб-ресурсам
Добавление правила
Правило доступа к веб-ресурсам
Название правила
Новое правило
Состояние
. Активно
Не активно
Действие
О Разрешать
💿 Запрещать
О Предупреждать
Содержимое фильтра
По категориям содержания Настроить
Потипам данных
Настроить
ОК Отмена

Рисунок Г.55. – Настройка правил доступа к веб-ресурсам

5) в категориях содержания выбрать необходимые пункты, а также развернуть пункт «Запрещено региональным законодательством» и выбрать

пункт «Запрещено законодательством Российской Федерации» и нажать «ОК» (см. рисунок Г.56.).



Рисунок Г.56. – Настройка категорий содержания

Вместе с тем есть возможность ограничивать доступ к конкретным адресам сайтов. Для этого необходимо выбрать «К отдельным адресам» в разделе «Адреса» и добавить адрес сайта. Для сохранения настроек нажать «ОК» (см. рисунок Г.57.).

К Правила доступа к веб-ресурание	рсам	
Добавление прави	ла	
Адреса		
💿 Ко всем адресам		
🔘 К отдельным адресам		
+ Добавить 🖉 Изменить	🛱 Удалить [ Импорт 🗍 Экспорт	
🗌 Адрес	Количество адресов	Состояние
	Адреса не указаны	
Пользователи		
Ко всем пользователям		
🔘 К отдельным пользователям и / или	и группам	
+ Добавить 🗇 Удалить		
Пользователь или группа		
ОК Отмена		

Рисунок Г.57. – Настройка категорий содержания

### Компонент «Адаптивный контроль аномалий»

Компонент «Адаптивный контроль аномалий» отслеживает и блокирует действия, нехарактерные для компьютеров сети организации. Для отслеживания нехарактерных действий Адаптивный контроль аномалий использует набор правил (например, правило Запуск Windows PowerShell из офисного приложения). Правила созданы специалистами «Лаборатории Касперского» на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил и, например, разрешить запуск PowerShell-скриптов для автоматизации решения корпоративных задач.

Для настройки данного компонента необходимо:

1) в разделе настроек «Контроль безопасности» выбрать меню «Адаптивный контроль аномалий» (см. рисунки Г.45. и Г.58.);

2) в появившемся окне активировать «Адаптивный контроль аномалий» и нажать кнопку «Сохранить» (см. рисунок Г.58.);

Kas	persky	< Безопасность	
Endp	oint Security	Настройки Адаптивного контроля	
	Мониторинг	аномалий	
0	Безопасность	Гарана Адаптияный контроль аномалий Вил 🌔	
S	Обновление	Контролирует действик, некарактерные для компьютеров сети, на основе типичных сценкариев вредоносной активности. Узнать больше	J
Ş	Задачи		
~		Правила	
님	Лицензия	Изменить правила	
		Шаблоны	
		Сообщение о блокировке	
		Шаблон сообщения, появляющегося при беокеровки запуска приложения.	
		Сообщение администратору	
		Шаблон свобщения администратору. Испольтуется в случае, если запусс приложники, по мнение пользоватиля, забловирован свамбочно.	
берсия 11.9.0.3	51		
ø	о <i>ф</i>	Сохранить Активация Wi	ndc ть W

Рисунок Г.58. – Настройка компонента «Веб-контроль»

В разделе «Настройки Адаптивного контроля аномалий» нажать изменить правила. Установить чекбоксы около существующих правил, нажать «ОК»(см. рисунки Г.59. и Г.60.).



Рисунок Г.59. – Изменение правил адаптивного контроля аномалий

		?	- 0	×
< Ha	стройки Адаптивного контроля аномалий			
Пра	вила			
	зменить – Подтвердить обновления – С Импорт – В Экспорт			
8	Правило Состояние Действие		Исклю	
> 🖸	Астивность офионых программ			
> 🛛	Использование инструментария управления Windows			
› 🛛	Активность интерпретаторов скриптовых языков			
> 🛛	Нетипичная активность программ			
		A	тивация \	Wind
			обы активир здед "Парам	

Рисунок Г.60. – Установка правил адаптивного контроля

## Шаг 5. Выполнить настройку модуля «Общие настройки»

Настройка модуля «Общие настройки» заключается в настройке компонентов «Настройки приложения», «Настройки сети», «Угрозы и

исключения», «Отчеты и хранилище», «Интерфейс», «Управление настройками» (см. рисунок Г.61.).



Рисунок Г.61. – Меню настроек «Общие настройки»

## Компонент «Настройки приложения»

Для настройки компонента «Настройки приложения» необходимо:

1) в разделе настроек «Общие настройки» выбрать «Настройки приложения» (см. рисунок Г.61.);

2) в открывшемся разделе должны быть выбраны все пункты, кроме «Применять технологию лечения активного заражения» в разделе «Режим работы» и «Включить возможность внешнего управления системными службами» в разделе «Самозащита» (см. рисунок Г.62.);



Рисунок Г.62. – Настройка компонента «Настройки приложения»

 в поле «Отладочная информация» выключить «Запись дампов» и «Защита файлов дампов и файлов трассировки». Нажать кнопку «Сохранить» (см. рисунок Г.63.).

	<ul> <li>включить возможность внешнего управления системными служоами</li> </ul>
	Отладочная информация
	Включить запись дампов
	Включить защиту файлов дампов и файлов трассировки
4	Сохранить Отмена

Рисунок Г.63. – Настройка компонента «Настройки приложения»

## Компонент «Настройки сети»

Для настройки компонента «Настройка сети» необходимо:

1) в разделе настроек «Общие настройки» выбрать «Настройки сети» (см. рисунок Г.61.);

2) в открывшемся разделе выбрать пункты «Ограничивать трафик при лимитном подключении» в разделе «Учет стоимости подключения», выбрать

способ контроля портов в разделе «Контролируемые порты», выбрать способ контроля соединений «Проверка защищенных соединений», «Использовать выбранное хранилище сертификатов для проверки защищенных соединений в приложениях Mozilla» и «Использовать хранилище сертификатов Windows» и нажать «Сохранить» (см. рисунок Г.64.).

Примечание: при необходимости возможно добавление доверенных адресов или приложений путем добавления их в соответствующие пункты настроек «Доверенные адреса» и «Доверенные приложения».



Рисунок Г.64. – Настройка компонента «Настройка сети»

## Компонент «Угрозы и исключения»

Компонент «Угрозы и исключения» позволяет настраивать типы обнажаемых объектов и исключать из проверки различные файлы и делать исполняемые файлы доверенными.

Для настройки компонента «Угрозы и исключения» необходимо:

1) в разделе настроек «Общие настройки» выбрать «Угрозы и исключения» (см. рисунок Г.61.);

2) в появившемся окне в разделе «Исключения из проверки и доверенная зона» выбрать пункт «Настроить исключения» (см. рисунок Г.65.). В открывшемся окне можно добавить файлы, каталоги или программы которые исключаются из проверки выбранным компонентом. Для добавления необходимо нажать кнопку «Добавить», в новом окне в поле «Файл или папка» указать путь к файлу или папке, и в «Компонентах защиты» выбрать, для каких компонентов добавляется исключение (см. рисунок Г.66.).



Рисунок Г.65. – Настройка компонента «Угрозы и исключения»

К Настройом угроз и исслючений		? – 🗆
< Исключения		
Добавление нового исключе	ния	
чала или папка		
00	op	
Имя или маска имени файла или тапки.		
Объект		
Имя или маска имени объекта по классификации Вирус-	ой энциклопедии (например, EICAR-Test-File).	
Хеш файла		
Paco	man.	
Если указан хаза файла, то в исключения на попадат изм	ноный файл.	
Компоненты защиты		
🔘 Все компоненты		
💿 Только выбранные		
🗌 Проверка		
🗌 Защита от файловых угроз		
🗌 Защита от почтовых угроз	•	Активация Чтобы активии
Защита от веб-угроз		раздел "Парам

Рисунок Г.66. – Добавление исключения

Примечание: настройка исключений производится исходя из конкретных условий эксплуатации средства ВТ. Возможно добавление доверенных программ типа «Secret Net», «JaCarta SF-ГОСТ» и др..

## Компонент «Отчеты и хранилище»

Для настройки компонента «Отчеты и хранилище» необходимо:

1) в разделе настроек «Общие настройки» выбрать «Отчеты и хранилище» (см. рисунок Г.61.);

2) в подразделе отчеты в поле «Хранить не более» указать количество дней и в поле «Ограничить размер файла отчетов до» ограничение размера файла (см. рисунок Г.67.);

3) в подразделе резервное хранилище в поле «Хранить отчеты не более» указать количество дней и нажать кнопку «Сохранить» (см. рисунок Г.67.).



Рисунок Г.67. – Настройка компонента «Отчеты и хранения»

## Компонент «Интерфейс»

Для настройки компонента «Интерфейс» необходимо:

1) в разделе настроек «Общие настройки» выбрать «Интерфейс» (см. рисунок Г.61.);

2) в подразделе «Уведомления о состоянии локальных антивирусных баз» установить необходимые значение в зависимости от типа средства ВТ (предпочтительно, на автономном средстве ВТ»15» дней для уведомления «Базы устарели» и «22» дня для уведомления «Базы сильно устарели» (см. рисунок Г.68.). на средстве ВТ, входящем в состав ЛВС «8» дней для уведомления «Базы устарели» и «15» дней для уведомления «Базы сильно устарели») (см. рисунок Г.68.);



Рисунок Г.68. – Настройка компонента «Интерфейс»

3) в поле «Уведомления» нажать кнопку «Настройка уведомлений» (см. рисунок Г.68.);

4) настроить параметры уведомлений для категории «Аудит системы» в соответствии с рисунками Г.69. и Г.70.;

Kaepersky Endpoint Security					- 0 ×
О	Caduryes	Сохранять в локальном отчете	Сохранять в журнале событий Windows	Увадомлять на экране	Уведомлять по почте
	< Критические события	٥	0	0	•
	Нарушено Лицензионное соглашение	٥	٥	•	•
Анализ псекдения	Срок действия лицензии почти истек		0	8	•
Защита от эксплойтов	Базы поврождены или отсутствуют			8	•
Предотвращение вторжений	Базы сильно устарели			8	•
О базовая экерта	Автозапуск приложения выключен	٥	•	0	•
Защита от файловых угроз	Ошебка актепации	٥	0	0	•
Защита от веб-утроз	Обнаружена активная упроза. Требуется запуск процедуры лечения активного заражения			8	•
·····	Серверы KSN надоступны	٥	0	0	•
защита от почтовых угроз	Недосталочно места в хранилице карантина	٥	٥	•	•
Сетевой жран	Объект не восстановлен из карантина	٥	٥	0	•
Защита от сетевых упроз	Объект не удален из карантина	٥	0	•	•
AMSI-защита	Установлено союдинение с доменом с недоверенным сертификатом	٥	0	0	•
С Контроль безопасности	Возникла ощибка проверки защифрованного свединения. Домен добавлен в список изолечений	٥	•	•	•
Адаттивный контроль аномалий	<ul> <li>Отказы функционирования</li> </ul>	٥	0	0	•
Former and second	Не удалось выполнить задачу	٥	0	0	•
контроль приложении	<ul> <li>Продпреждения</li> </ul>	٥	•	•	•
Контроль устройств	Обнаружено некорректное завершение предыдущей сесони работы приложения	٥	٥	0	•
Веб-Контроль	Срок действия лицензии скоро истеквет	٥	0	•	•
2 Jagree	Базы устарели	Ū	0	8	•
Обновление баз	Автоналическое обновление выклачено	٥	•	0	0
Проверка	Самозацита приложения выключена	0	•	•	•
Трумую *				OK	Отмена

Рисунок Г.69. – Настройка уведомлений для категории «Аудит системы»

Kaspensky Endpoint Security					- 0 ×
•	Caduma	Сохранять в локальном отчете	Сохранять в журнале событий	Уведомлять на экране	Уведомлять по почте
Аудит системы			Windows		0
Продликутал заканта	Для завершения обновления необходимо перезапустить прихожение	•		•	•
Аналия повединия	Необходима перезагрузка компьютера			0	•
	Установлены не все компоненты приложения, которые позволяет использовать лициканя	٥	0	0	0
Защита от эксплойтов	Запущена процедура лемения активного заражения	٥	0	•	•
Предотвращение вторжений	Процедура лемания активного заражания завершена	٥	0	0	0
🔿 Bascese seepra	Некорректный резервный ключ	٥	0	•	•
Защита от файловых угроз	Подписка скоро истекает	۵	٥	0	•
Защита от веб-уграз	Невозмохоно восстановить объект на резиряного хранилища	٥	0	•	0
	Обнаружена подгорительная оптевая активность			8	•
Защита от почтовых угроз	Задищинное сондининие разореано	٥	٢	0	•
Сетевой экран	Yvacrine a KSN aukonoveno	٥	0	0	0
Защита от сетевых угроз	Обработка прихожнием некоторых функций ОС отключена.	۵	٥	•	•
AMSI-защита	В хранилище карантина скоро закончится место	۵	٥	•	0
С Контроль безопалности	Соединение заблокировано	۵	0	•	•
Адаттивный контроль аномалий	<ul> <li>Информационние</li> </ul>	٥	0	0	•
	Приложение запущено	۵	٢	•	•
Контроль приложений	Приложение остановлено	٥	٢	0	0
Контроль устройств	Дайствия с рекурсания приложения заблокировано самозацитой	۵	0	0	0
веб-Контроль	Отчет снижден		0	0	0
- 3upres	Групповая политика деактивирована	۵		0	0
Обновление баз	Изменены настройог приложения	٥	٢	•	0
Проверка	Задано запущено	۵	0	•	0
Врумую •				OK	Отмена

# Рисунок Г.70.– Настройка уведомлений для категории «Аудит системы»

5) настроить параметры уведомлений для категории «Анализ поведения» в соответствии с рисунком Г.71.;

Kaspensky Endpoint Security					- • ×
О	Codures	Сохранять в локальном отчете	Сохранять в журнале событий Windows	Уведомлять на экране	Уведомлять по почте
В Продеменутал защита	Критические события	٥	٥	٥	0
	Обнаружен вредонооный объект		۵	۲	0
	Невозможно удалить	0	٥	٥	0
Защита от эксплойтов	Процесс завершен	8	٥	8	•
Предотвращение вторжений	Невозможно завершить процесс	0	٥	٥	•
) базовая знарта ———	<ul> <li>Прьдипреждения</li> </ul>	0	•	•	•
Защита от файловых угроз	Откат выполнен	٥	۵	٥	0
Защита от веб-уграз	Заприщию	٥	٥	٥	•
Secure of postories stress	Объект удален	٥	٥	۲	0
Setting of Internation Arthop	Объект будет удален при перезагрузке	•	0	۲	•
Сетевой экран	Невозможно создать резервную копию объекта	٥	0	0	•
Защита от сетевых угроз	Обнаружено легальное приложение, которое может быть использовано элоумышленниками для нанесения вреда компьютеру или данным пользоват	٢	•	0	•
AMSI-защита	< Информационные	٥	0	0	•
🕻 Контроль безопасности	Файл восстановлен	•	۵	0	•
Адаптияный контроль аномалий	Создана резервная копия объекта	•	•	0	0
Course on the second	Значение реестра восстановлено	0	٥	0	0
	Зкачание реестра удалено	0	٥	0	0
Контроль устройств	Объект переименован	ū	۵		•
Веб-Контроль					
Jagaren					
Обновление баз					

# Рисунок Г.71. – Настройка уведомлений для категории «Анализ поведения»

6) настроить параметры уведомлений для категории «Защита от эксплойтов» в соответствии с рисунком Г.72.;



Рисунок Г.72. – Настройка уведомлений для категории «Защита от эксплойтов»

7) настроить параметры уведомлений для категории «Предотвращение вторжений» в соответствии с рисунками Г.73. и Г.74.;

Kaspersky Endpoint Security					- 0 ×
o	Collumn	Сохранять в ложальном отчете	Сохранять в журнале событий	Уведоналеть на зеране	Уведомлять по почте
Ayyar orcieda	< Критические события	0	Windows	0	•
Проденнутая знарта		-	-	-	-
Анализ поведения		-	-	•	0
Защита от зерплойтов	Лечение навозможно	8	-	-	0
	Невозможно удалить	8	8	•	•
Предотвращение вторжений	Ошибка обработки	٢	•	0	•
О Баховка закрета	Процесс завершен	٥		•	•
Защита от файловых угроз	Невсомского завершить процесс	٥	0	•	•
Защита от воб-утроз	<ul> <li>Придпреждения</li> </ul>	٥	0	•	•
	Невсаможно создать резервную колно объекта	۲	•	0	•
Защита от почловых утроз	Объект не обработан	٢		•	•
Сетевой экран	Объект закинфрован	0	0	0	•
Защита от сетевых угроз	Объект поврежден	۵	•	•	•
AMSI-salayna	Объект будет удален при перезагрузке	۵	8	8	•
С Контроль безопалности	Объект будет вылечен при перезагрузке	•	٢	•	•
Адалтивный контроль аномалий	Обнаружено легальное приложении, которое может быть использовано акоумышленниками для нанесения вреда компьютеру или данным пользоват	0	•	•	•
	Невозможно воостановить объект из резервного хранилища	٥		•	•
контроль приложении	Объект удален	۵	۵	•	•
Контроль устройств	Объект вылечен	۵	•	•	•
веб-Кантроль	<ul> <li>Информационные</li> </ul>	•		•	•
Jageree	Объект обработан	•		•	•
Обновление баз	Создана резервная копин объекта	٢	•	•	•
Промерка	Объект пропукаен			•	•
Ерумую *				OK	Отмена

Рисунок Г.73. – Настройка уведомлений для категории «Предотвращение вторжений»

Kaspersky Endpoint Security					
	Column	Сокранить в локальном отчете	Сокранить в журнале событий Місліпия	Увадомлять на экране	Уведомлять по почте
		•		0	0
Проденнутая защита	Column Taxangponan		<u> </u>	0	0
1	Объект поврежден	•	•	•	•
Avants reegover	Объект будят удален при перехагрузке	٥	8	٥	0
Защита от эксплойтов	Объект будет вылечен при перезагрузке	٥	٢	٥	0
Предотерациние вторжений	Обнаружено легальное приложение, которое может быть использовано звоумышленныками для нанесения вреда компьютеру или данным пользоват	٥	0	•	0
O Gescese seapro	Невозможно восстановить объект на резираного хранилица	٥	0	•	0
Защита от файловых угроз	Объект удален	٥	0	٥	0
Защита от веб-угроз	Объект вылечин	٥	0	٥	•
	< Информационные	•	0	•	•
and the output of the second second second	Объект обработан		•	0	•
Сетевой экран	Создана резирвная копин объекта	٥	0	•	0
Защита от сетевых угроз	Объект пропущен		•		0
AMSI-защита	Обнаружен аркив		0	•	0
C. Kompers feronsorers	Обнаружин улакованный объект	D	•	•	•
Адаттивный контроль аномалий	Объект перезалисан выянченной ранее колмей	٥	•	•	•
F	Информация об обнаруженном объекте	0	•	•	•
котроль приложении	Обнаружен зацищенный паролем архив	٥	•	•	0
Контроль устройств	Объект восстановлен на резервного хранилища	۵	8	•	•
Веб-Контроль	Приложение помещено в группу доверенных приложений	٥	•	•	•
2 Jappen	Приложные помещено в группу с ограничениеми	۵		•	•
Обновление баз	Сработая компонент Предотвращение вторжений	٢	•	•	•
Провержа	Объект наездится в списке разрединные в Локальном KSN	•	•	•	•
Прумую *				CK	Отмена

Рисунок Г.74. – Настройка уведомлений для категории «Предотвращение вторжений»

8) настроить параметры уведомлений для категории «Сетевой экран» в соответствии с рисунком Г.75.;



Рисунок Г.75. – Настройка уведомлений для категории «Сетевой экран»

9) настроить параметры уведомлений для категории «Защита от файловых угроз» в соответствии с рисунками Г.76. и Г.77.;

🗶 Kaspensky Endpoint Security					
Аудит системы В Проденнутах защита	События	Сохранять в локальном отчете	Сохранять в журнале событий Windows	Уведснаять на зеране	Уведомлять по почте
Аналио поекдения	<ul> <li>Гритические события</li> </ul>	٥	0	0	0
Защита от желлойтов	Обнаружен вредоносный объект	٥	٥	•	0
Предотвращение вторжений	Лечение невозмажно	٥	0	•	0
C foreign starts	Невозможно удалить	٥	٥	•	0
	Ошебка обработое	٥	0	0	0
Защита от фийловых угроз	Процесс заверыен	٥	•	0	0
Защита от виб-утраз	Невезиконо завершить процесс	٥	0	0	0
Защита от почтовых угроз	<ul> <li>Продпреждения</li> </ul>	٥	•	0	0
Сетевскі зеран	Невезможно соддять резервную колико объекта	۵	0	0	0
Защита от сетевых угроз	Объект не обработан	٥	•	0	0
AMSI Jawarta	Объет зашифрован	٥	•	0	0
	Объект поврежден	٥	•	•	0
С Контроль бекопасности	Объект будет удален при перезагрузке	٥	٥	۲	•
Адаттивный контроль аномалий	Объект будег вылечен при перезагрузов	۵	۵	8	0
Контроль приложений	Обнаружено легальное приложение, которое может быть использовано звоумышленимами для нанесения вреда компьютеру или данным пользоват	٥	•	0	0
Контроль устройств	Невозможно восстановить объект на резервного хранилища	۵	•	•	•
Beő-Kompon.	Объект удален	٥	٥	۰	•
C June .	Объект зылячен	۵	۵	8	•
	Онкаг выязонном	٥	0	0	•
Othersterize das	~ Информационные	•	•	0	0
Проверка	Объект обработан		•	0	0
Проверка целостности	Создана резервная колия объекта	٢	•	0	0
Еруную •				CK	Отмена

Рисунок Г.76. – Настройка уведомлений для категории «Защита от файловых угроз»

Kaspensky Endpoint Security					- 0 ×
Аудит системы В Продентутия медита	Column	Сохранять в локальном	Сокранить в журнале	Уведомлять на экране	Уведомлять по почте
Анализ поекдения	Невсамскою садать резервную копию объекта	0	0	0	0
Јацита от желиойтов	Объект не обработан	٥	0	0	0
Предотвращение вторжений	Объект зашифрован	٥	0	0	0
	Объект поярежден	0	0	0	•
	Объект будет удален при перехагрузка	٥	٥	•	0
Защита от файловых угроз	Объект будет вылечен при пирезагрупке	٢	٢	•	0
Защита от виб-утроз	Обнаружено легальное приложение, которое может быть использовано звоумышленниками для нанесения вреда компьютеру или данным пользоват	0	0	0	0
Защита от почтовых угроз	Невозможно восстановить объект на резнряното хранклица	٥	0	0	0
Сетевой жран	Объет удален	٢	٢	•	0
Защита от сетезьк угроз	Сбъект вылечен	٥	٥	۲	0
	Откат выполния	٥	0	0	0
	< Информационные	0	0	0	0
Сочтронь безопасности —	Объект обработан	0	0	0	0
Адаттивный контроль аномалий	Создана резервная колия объекта	۲	0	0	0
Контроль приложений	Объект пропущен	•	•	•	•
Контроль устройств	Обнаружон архия	0	0	0	0
Beő-Kampons	Обнаружен упакованный объект	•	0	•	0
2 June	Объект перезалисан кълеченной раное колией	٢	0	•	•
	Обнаружен зацищенный парелен арния	٢	0	0	•
Обновление баз	Информация об обнаружение объекто	۲	0	•	0
Проверка	Объект восстановлен из резервного хранилица		۲	0	0
Проверка целостности	Объект наявдится в списке разреджных в Локальном KSN	0	0	0	0
Ерумую *				CK	Отмена

Рисунок Г.77.– Настройка уведомлений для категории «Защита от файловых угроз»

10) настроить параметры уведомлений для категории «Защита от веб-

угроз» в соответствии с рисунком Г.78.;

🗶 Kaspensky Endpoint Security					- 0 ×
Аудит системы © Продененутия экцито	Column	Сокранить в локальном отчете	Сокранить в журнале событий	Уведсналять на экране	Уведомлять по почте
Анализ поведения	У Критические события	0	Windows	0	0
Защита от застлойтов	Обнаружен кредоносный объект	0	0	•	•
Предотвращение вторжений	Забложирована опасная социка	٢	٢	•	0
0.1	Оперыта относная ссыяка	٥	٥	•	•
	Обнаружна ранее открытак опасная ссыяка	٥	8	0	0
Защита от файловых угроз	Ощибка обработки	0	8	•	•
Защита от виб-угроз	<ul> <li>Прядупреждения</li> </ul>	٥	0	0	0
Защита от почловых угреа	Обнаружено легальное приложение, которое может быть использовано засумышленниками для нанесения вреда компьютеру или данным пользоват	٢	0	•	0
Сетевсії жран	Запрящию	٥	0	0	0
Защита от сетевых угроз	Загружа объеста запрещена	٥	٥	•	•
44470	Объект покрежден	0	0	0	0
Portsi cangitta	< Информационные	0	0	0	•
С Контроль безопасности ———	Объект обработан	0	0	0	0
Адаттивный контроль аномалий	Ссылка обработана	0	0	0	•
Контроль приложений	Информация об обнаружение объекте	٢	0	0	•
Контроль устройств	Обнаружин улакованный объект	0	0	0	•
Be6-Kompons	Обнаружен архне	0	0	0	•
<b>0</b> )	Обнаружин зацищинный паролен архив	۲	0	•	•
() A() ()	Объект находится в стихке разреденных в Локальном КSN	٢	٥	0	•
Обновление баз	Ссылка находилот в списое разрешенных в Локальном КSN	۲	٢	•	•
Проверка					
Проверка целостности					
Врумую *				OK	Отмена

Рисунок 1 – Настройка уведомлений для категории от веб-угроз»

«Защита

11) настроить параметры уведомлений для категории «Защита от сетевых угроз» в соответствии с рисунком Г.79;



# Рисунок Г.79 – Настройка уведомлений для категории «Защита от сетевых угроз»

12) настроить параметры уведомлений для категории «Защита от почтовых угроз» в соответствии с рисунком Г.80.;

Kaepersky Endpoint Security					
Аудаг сактемы В Проденнутая защита	Column	Сохранять в локальном отчете	Сохранять в журнале событий Windows	Уведсниять на экране	Увадомлять по почте
Анализ поведения	<ul> <li>Критические события</li> </ul>	0	0	0	•
Защита от зелтнойтов	Обнаружен кредоносный объект	٥	٢	•	•
Предотвращение вторжений	Ленения находысано	0	0	0	0
G factors assets	Ошибна обработки	٥	٥	٥	•
	<ul> <li>Предупреждения</li> </ul>	0	0	0	•
Защита от фийловых угроз	Объект не обработан	٥	0	•	•
Защита от виб-утроз	Обнаружено легальное приложение, которое может быть истользовано звоумышленниками для нанесения вреда компьютеру или данным пользоват	۲	0	0	•
Защита от почтовых угроз	Объект попрежден	٢	0	0	•
Сетевскі зиран	Невсомского восстановить объект на резервного кранилица	0	0	0	•
Защита от сетезых угроз	Объект удален	۲	۲	•	•
AMEL SHOWERS	Объект вылечен	٥	٥	•	0
ninsi salajina	Объект удалин в соответствии с настройками	۲	0	0	•
С Контроль бехотисности ———	» Информационные	0	0	0	0
Адаттивный контроль аномалий	Объект обработан	0	0	0	•
Контроль приложений	Создана резервная колия объекта	٥	0	0	0
Контроль устройств	Обнаружон архия	0	0	0	•
Be6-Kompon,	Обнаружен утакованный объект	0	0	0	0
<b>0</b> January	Объект переименован	۲	0	•	0
	Информация об обнаруженном объекте	٢	0	0	•
Обновление баз	Обнаружон зацящинный парсмен архия	۲	0	•	0
Проверка	Объект восстановлен из резервного хранилеща	٥	۲	•	•
Проверка целостности	Объект нандится в списке разреденных в Локальном KSN	٥	0	•	•
Врумую +				OK	Отмена

Рисунок Г.80. – Настройка уведомлений для категории «Защита от почтовых угроз»

13) настроить параметры уведомлений для категории «AMSI защита» в соответствии с рисунками Г.81. и Г.82.;

Базовая защита		отчете	событий Windows	•	
Защита от файловых угроз	<ul> <li>Критические события</li> </ul>		Ο		
	Обнаружен вредо	- 😌			
Защита от веб-угроз	AMSI-запрос забл		0	0	Ο
Защита от почтовых угроз	Ошибка обработки	<ul><li>☑</li></ul>		0	Ο
Сетевой экран	<ul> <li>Предупреждения</li> </ul>		0	0	Ο
Защита от сетевых угроз	Объект не обраб… —	•			0
AMSI-защита	Объект зашифров		0	0	Ο
С. Контроль безопасности	Объект поврежден		•	0	Ο
	Обнаружено лега		(		0

# Рисунок Г.81. – Настройка уведомлений для категории «AMSI защита»

🗼 Kaspersky Endpoint Security - 🗆 X							
Предотвращение вторжений	События	Сохранять в локальном	Сохранять в журнале	Уведомлять на экране	Уведомлять по почте		
🔿 Базовая защита ————		отчете	событий Windows				
Защита от файловых угроз	Обнаружено лега			<ul><li>✓</li></ul>			
	Результат провер						
защита от вео-угроз	<ul> <li>Информационные</li> </ul>			0			
Защита от почтовых угроз	Объект обработан	0	Ο	0			
Сетевой экран	Объект пропущен 🗕	0			0		
Защита от сетевых угроз	Обнаружен архив		0	0			
AMSI-защита	Обнаружен упако						
С Контроль безопасности ————————————————————————————————————	Обнаружен защи		Ο	0			
	Информация об о		Ο	0			
Адаптивныи контроль аномалий	Объект находится		2	0	Активация Windows		

Рисунок Г.82. – Настройка уведомлений для категории «AMSI защита»

14) настроить параметры уведомлений для категории «Контроль приложений» в соответствии с рисунком Г.83.;



Рисунок Г.83. – Настройка уведомлений для категории «Контроль приложений»

15) настроить параметры уведомлений для категории «Обновление баз» в соответствии с рисунком Г.84.;

Kaspensky Endpoint Security					- 0 ×
Аудит системы	События	Сокранять в	Сокранять в	Уведскалять на	Уведомлять по почте
Проденнутах защита		OTHERE	columei Windows	экране	
Аналио поведения	<ul> <li>Критические события</li> </ul>	٥	•	•	0
Защита от желлойтов	Ошибка обновления компонента	٥	0	0	•
Предотвращение вторжений	Ошибка кольрования обновлений компонента	٥	0	0	0
) faxees segme	Локальная оцинбка обновления	ē.	•	۰	•
	Селевая сшибка обновления	٥	0	٥	•
Защита от фийловых угроз	Невозможен запуск двух задан одновременно	٥	•	•	•
Защита от виб-утроз	Ошибка проверки баз и модулей приложения	۵	0	•	•
Защита от почтовых угроз	Ошибка взаникдействия с Какрепку Security Center	٥	•	•	•
Сетевскі зеран	Обновлены не все компоненты	٥	•	•	•
Защита от сетевых угроз	Обновление завершино успешно, а копирование обновлений завершено с ошибкой	٥	•	•	•
AMS assures	Произоция внутренняя оцибка	Ū	•	۰	•
-	Ошибка установки патча	۵	0	0	•
С Контроль бекотысности	Ошибка опсата патна	٥	0	0	•
Адаттивный контроль аномалий	<ul> <li>Предпрекдения</li> </ul>	٥	0	0	•
Контроль приложений	Операция отменена пользователем	٥	0	0	•
Контроль устройств	< Ниформационные	۵	0	0	•
веб-Кантроль	Выбран источник обновлений	٥	0	0	•
C	Выбран прокон-окреер	۵	•	0	•
	3arpysea quina	٥	•	0	•
Officesterive 6as	Файл загружн	۵	0	0	0
Проверка	Файл установлен	٥	0	0	•
Проверка целостности	ชิมมัก อยังออกอง	٥	0	0	0
Трумую •				OK	Отмена

Рисунок Г.84. – Настройка уведомлений для категории «Обновление баз»

16) настроить параметры уведомлений для категории «Проверка» в соответствии с рисунком Г.85.;

Kaspersky Endpoint Security					- 0 ×
Аудит системы В Проденнутан экцита	Codurms	Сохранить в локальном отчете	Сохранять в журнале событий	Уведомлять на экране	Уведомлять по почте
Анализ поведения	У Тритические события	٥	Windows	0	0
Защита от зекликойтов	Обнаружен вредоносный объект		0	•	•
Предотвращение вторжений	Лечение невозмакано	•	0	•	0
	Невозможно удалить		٥	•	•
	Ощибка обработки	0	0	0	0
Защита от файловых угроз	Процесс завершен	٥	0	0	•
Защита от виб-утроз	Невсомсконо завершить процесс	٢	0	0	0
Защита от почтовых угроз	< Предпреждения	٢	0	0	•
Сетевой жран	Невсомсконо соддать резервную копнос объекта	٢	0	0	0
Защита от сетевых угроз	Объект не обработан	٢	0	0	0
AMEL SHARES	Объект зашифрован	٢	0	0	0
	Объект поярежден	۲	0	0	0
С Контроль безопасности ———	Объект будет удален при перезатрузка	•	٢	٠	0
Адаттиеный контроль эномалий	Объект будет вылечен при пирезагрузке	•	۲	٥	0
Контроль приложений	Обнаружено легальное приложение, которое может быть истользовано звоумышлениками для нанесения вреда компьютеру или данным пользоват	٥	0	•	•
Контроль устройств	Невозможно восстановить объект на резервного хранклица	٢	0	•	•
Be6-Kompons	Объект удален	-	٥	۵	•
() Jacov	Объектанлечин	٥	۲	•	•
	Опсагвыясние	•	٥	۵	•
Concellence Gas	< Информационные		0	•	•
Проверка	Объект обработан		•	•	•
Проверка ценостности	Создана резервная колня объекта	٥	0	•	•
Врумую *				CK	Отмена

Рисунок Г.85. – Настройка уведомлений для категории «Проверка»

17) параметры уведомлений для категорий «Контроль устройств», «Веб-Контроль», «Адаптивный контроль аномалий» и «Проверка целостности» оставить без изменений и нажать кнопку «ОК»;

18) в меню «Настройка интерфейса» включить «Защита паролем» и задать пароль для пользователя «KLAdmin» (см. рисунок Г.86.).

Зстроенная учетная запись адми со всем функциям Kaspersky End	інистратора обладает полн Ipoint Security.	ым доступом
1мя пользователя:		
KLAdmin		
Рекомендуемый: KLAdmin		
Зведите пароль:		
Пароль		
Тодтвердите пароль:		
Повторите пароль		

Рисунок Г.86. – Пароль для пользователя «KLAdmin»

Примечание: учетная запись KLAdmin не имеет отношения к авторизации в операционной системе или специализированному программному обеспечению;

19) настроить права для пользователей. Для этого необходимо выбрать в поле учетных записей «Все» и нажать «Изменить». В открывшемся меню убрать нетребуемые галочки (предпочтительно, все галочки, кроме «Просмотр отчетов» и «Восстановление из резервного хранилища»). Нажать последовательно кнопки «ОК» и «Сохранить» (см. рисунки Г.87. и Г.88.).

Kaspersky		< Настройка	< Настройка				
Endp	point Security	Настройки инте	рфейса				
	Мониторинг	Уведомления о состоянии ло	кальных антиви	русных баз			
¢	Безопасность	Оправлить уведомление "Базы ус 3	тарели", если базы	не обновлялись (дней)			
C	Обновление	Отправлять уведомление "Базы си	льно устарели", ес	ли базы не обноелялись (д	4607)		
Ģ	Задачи	7					
С С	Лиценаня	Защита паролем Защита паролем позволят установить і Капраліку Енфранті Security, снакова вара работу приложения. Россимендуевое зн Изменить пароль	атраночника на управ апность насансциони ачение по умолчанию	ляния всяма или отдельными ф рованного или непреднамарен - для имени пользователя - KLA	зунациями и настройкави ного внесения изменений в dmin.		
		+ Добавить	пь 🕆 Удаля	пъ			
		Имя		Разрешения			
		KLAdmin		Bce	Активация Win		
Sepore 11.9.0.3		Boe		Просмотр отчетов	Чтобы активировать раздел "Параметры		

Рисунок Г.87. – Настройка прав для пользователей



Рисунок Г.88. – Настройка прав для пользователей

## Компонент «Управление настройками»

Для настройки компонента «Управление настройками» необходимо:

1) в разделе настроек «Общие настройки» выбрать «Управление настройками» (см. рисунок Г.61.);

2) нажать на ссылку «Экспортировать», задать имя конфигурационного файла, указать каталог для сохранения и нажать кнопку «Сохранить». В указанном каталоге будет создан файл с расширением «.cfg» (см. рисунок Г.89.);



Рисунок Г.89. – Сохранение настроек конфигурации «Kaspersky Endpoint Security 11»

3) для загрузки конфигурационного файла необходимо нажать на ссылку «Импортировать», выбрать каталог с сохраненным файлом конфигурации и нажать «Открыть» (см. рисунок Г.90.);

	? – D ×	К Открытие						×
Kaspersky	< Настройка	← → - ↑ → 3	тот компьютер > Рабочий стол +	Файл конфигурации		võ R	ыск: Файл конфитурации 🎾	Ē.
Endpoint Security	Управление настройками	Упорядочить - Новая патка				ii.• 🖬 🖡		
Мониторине	Вы можете сохранить текущие настройки работы Kaspensky Endpoint Security в файл и использовать их	^	Имени	Дата изменения	Tan	Размера		
Венльсность	в будущем на другом компьютере или после неправильного изменения настроек. Также вы можете в любой момент вернуться к настройкам по умолчанию.		[] 1.dg	15.07.2022 14:55	<b>Dailn</b> "CFG"	876 KS		
Обновление	Импортировать стрий ранее согрании настройки присокиния							
Баланын	Экспортировать. Указите путь для сокримения файна с терущими настройками приложения.							
Designation Material Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definition Definit	Восстановить Россановите винителя по умлитерии.							
2 Normyria Habia Danner 11.9.0.351		- Vila	e dailna: 1.ctg			~ 5	dg 🗸	
0 0						C	Открыть Отмена	

Рисунок Г.90. – Импорт конфигурации «Kaspersky Endpoint Security 11»

## Шаг 6. Выполнить настройку модуля «Задачи»

Настройка модуля «Задачи» заключается в настройке компонентов «Полная проверка», «Проверка важных областей», «Выборочная проверка», «Проверка съемных дисков», «Проверка из контекстного меню», «Фоновая проверка», «Проверка целостности».

## Компонент «Полная проверка»

Полная проверка – проверка памяти средства ВТ, объектов автозапуска, загрузочных секторов дисков, системного резервного хранилища, всех жестких и сменных дисков, то есть полная проверка средства ВТ, за исключением сетевых дисков.

Для настройки полной проверки необходимо:

1) в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Полная проверка» (см. рисунки Г.З. и Г.91.);



Рисунок Г.91. – Выбор задачи «Полная проверка», «Проверка важных областей», «Выборочная проверка» для настройки

2) в окне «Полная проверка» изменить «Уровень безопасности» на «Высокий» (см. рисунок Г.92.);

3) в поле «Действие при обнаружении угрозы» выбрать необходимый пункт (предпочтительно, «Лечить, удалять, если лечение невозможно») (см. рисунок Г.92.);



Рисунок Г.92. – Настройка задачи «Полная проверка»

4) далее перейти во вкладку «Расписание проверки». В пункте «Запускать проверку:» выбрать требуемый параметр (предпочтительно «Еженедельно»). Указать день недели и время. Поставить галочку в пункте «Запускать пропущенные задачи» (см. рисунок Г.93.);

Примечание: допускается настроить другое расписание, исходя из режима работы пользователей.

			? – 🗆 🗙
Kaspersky	< Задачи		
Endpoint Security			
Мониторинг	Расписание полной	проверки	
—— П Безопасность	Запускать проверку:	Еженедельно 🗸	льное время и замедлять
		понедельник	
С. Обновление		🗌 вторник	
$\sim$		среда	
🗖 Задачи	Дни недели:	четверг	
<b>T</b> 2		💌 пятница	
О Лицензия		суббота	
<b>F</b>		воскресенье	
	Время:	10:00 🗘	
	Отложить запуск	0 🗘 минут	
	после старта приложения на:		
	2.		
Под управлением: 10.105.2.122	<ul> <li>Быполнять только во</li> </ul>	время простоя компьютера	
Сервер подключен:			анилище; Все жесткие диски;
Меньше минуты назад Версия:		ОК Отмена	
11.9.0.351			
0 <b>7</b>	Сохранить	Отмена	

Рисунок Г.93. – Настройка режима запуска обновлений

5) нажать «Расширенная настройка». В зависимости от вычислительной мощности средства ВТ во вкладке «Методы проверки» выбрать уровень эвристического анализа «Средний» или «Глубокий» (см. рисунок Г.94.);



Рисунок Г.94. – Настройка дополнительных параметров задачи «Полная проверка»

6) во вкладке «Проверка составных файлов» выбрать пункты «Проверять все архивы», «Проверять все дистрибутивы», «Проверять все файлы офисных форматов», «Проверять файлы почтовых форматов» (см. рисунок Г.95.);

7) нажать на кнопку «Дополнительно», снять галочку напротив пункта «Не распаковывать составные файлы большого размера» и нажать кнопку «Сохранить» (см. рисунок Г.95.).



Рисунок Г.95. – Настройка области действия компонента «Полная проверка»

## Компонент «Проверка важных областей»

Проверка важных областей — это проверка памяти средства ВТ, объектов автозапуска и загрузочных секторов дисков.

Для настройки проверки важных областей необходимо:

1) в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Проверка важных областей» (см. рисунки Г.3. и Г.91.);

2) далее выбрать пункт «Расписание проверки» (см. рисунок Г.96.);



Рисунок Г.96. – Настройка задачи «Проверка важных областей»

3) во вкладке «Расписание проверки важных областей» в меню «Запускать проверку» выбрать необходимый пункт (предпочтительно «После запуска приложения»). В пункте «Запускать через:» указать необходимое значение и нажать кнопку «ОК» (см. рисунок Г.97.);

	? - 🗆 ×
Kaspersky	< Задачи
Endpoint Security	Настройки проверки важных
Ва Мониторинг	областей
безопасность	Проверка важных областей
С Обновление	и системы объектов и Расписание проверки важных областей
🖵 Задачи	Запускать проверку: После запуска приложения •
Д Лицензия	Запускать черег: 20, 🗘 минут
	<ul> <li>Выполнять только во время простоя компьютера</li> </ul>
	ОК Отмена
Под управлениес 10.196.2.132	О Информировать
Серлер падскочно: 1 минуту нахад Інроня: на в 0.251	Изменить область проверки Системная память: Объекть автозапуска; Загрузочные секторы
11.446351	Расписание проверки
0 0	

Рисунок Г.97.– Настройка режима запуска задачи «Проверка важных областей» 4) нажать кнопку «Расширенная настройка", в поле «Типы файлов» поставить галочку напротив «Все файлы», в поле «Проверка составных файлов» поставить галочки напротив «Проверять все архивы», «Проверять все дистрибутивы», «Проверять все файлы офисных форматов», «Проверять файлы почтовых форматов» (см. рисунок Г.98.);

5) снять галочку напротив пункта «Не распаковывать составные файлы большого размера» и нажать кнопку «Сохранить» (см. рисунок Г.98.);



Рисунок Г.98. – Настройка области действия задачи «Проверка важных областей»

6) в пункте «Метод проверки» в зависимости от вычислительной мощности средства ВТ выбрать уровень эвристического анализа «Средний» или «Глубокий» (см. рисунок Г.99.).



Рисунок Г.99. – Настройка дополнительных параметров компонента «Проверка важных областей»

## Компонент «Выборочная проверка»

Выборочная проверка – задача для проверки файлов по выбору пользователя.

Для настройки выборочной проверки необходимо:

1) в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Выборочная проверка» (см. рисунки Г.3. и Г.91.);

2) настроить Параметры Выборочной проверки аналогично параметрам задачи «Полная проверка», за исключением поля «Режима проверки».

### Компонент «Проверка съемных дисков»

Проверка съемных дисков – задача по проверке, проверяющая все файлы подключаемых съемных дисков.

Для настройки проверки съемных дисков необходимо:

 в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Проверка съемных дисков» (см. рисунки Г.З. и Г.100.);

Kaspersky Endpoint Security		Задачи				
	Мониторинг	Проверка съемных дисков Проверка съемных дисков, например, жестких дисков и USB-флешек, подключенных к компьютер	<sub>уу.</sub>	۵		
Ô	Безопасность					
$\mathbb{C}$	Обновление	D:\ • Запустить проверку				
	Задачи					
ନ୍ମ	Лицензия	Проверка из контекстного меню Проверка отдельного объекта, папки или жесткого диска.	¢	6		
		Проверка запускается из контекстного меню выбранного объекта.				
		Фоновая проверка	тивация	a <b>Q</b> vii		

Рисунок Г.100. – Выбор задачи «Проверка съемных дисков», «Проверка из контекстного меню» для настройки.

2) в появившемся окне в разделе «Задачи» активировать «Проверка съемных дисков» (см. рисунок Г.101.);

3) в открывшемся меню настроить действие при подключении съемного диска, в зависимости от вычислительной мощности средства ВТ выбрать «Быстрая» – для малой мощности или «Подробная» – для средней и высокой (см. рисунок Г.101.);

4) убрать галочку напротив поля «Максимальный размер съемного диска» и нажать кнопку «Сохранить» (см. рисунок Г.101.).



Рисунок Г.101. – Настройка проверки съемных дисков

## Компонент «Проверка из контекстного меню»

Проверка из контекстного меню – специальный вид проверки, позволяющий запустить задачу по проверке выбранных файлов минимальным количеством действий.

Для настройки проверки из контекстного меню необходимо:

 в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Проверка из контекстного меню» (см. рисунки Г.З. и Г.100.);

2) настроить параметры проверки аналогично параметрам выборочной проверки и нажать «Сохранить» (см. рисунок Г.102.).



Рисунок Г.102. – Настройка проверки из контекстного меню

## Компонент «Фоновая проверка»

Фоновая проверка – это режим проверки САВЗ без отображения уведомлений для пользователя. Фоновая проверка требует меньше ресурсов средства ВТ, чем другие виды проверок. В этом режиме САВЗ проверяет объекты автозапуска, памяти ядра и системного раздела.

Настройка данной задачи производится по желанию аналогично предыдущим компонентам.

## Компонент «Проверка целостности»

Задача «Проверка целостности» проверяет модули «Kaspersky Endpoint Security для Windows», находящиеся в папке установки программы, на наличие повреждений или изменений. Если модуль программы имеет некорректную цифровую подпись, то такой модуль считается поврежденным.

Примечание: для увеличения производительности средства ВТ допускается данный компонент не настраивать.

Для настройки данного компонента необходимо:

 в главном окне САВЗ выбрать пункт «Задачи» и нажать на значок шестеренки напротив задачи «Проверка целостности» (см. рисунки Г.3. и Г.103.);



Рисунок Г.103. – Выбор задачи «Проверка целостности» для настройки.

2) в появившемся окне необходимо открыть настройку «Расписание проверки» и в пункте «Запускать проверку:» указать «Еженедельно», день недели и время запуска указать исходя из режима работы пользователя. Последовательно нажать кнопки «ОК» и «Сохранить» (см. рисунок Г.104.).

Kaspersky	< Задачи		? – 🗆
Endpoint Security	Расписание провери	ки целостности	
—- О Безопасность	Запускать проверку:	Еженедельно 👻	ждений или изменений.
С Обновление		понедельник вторник среда	
<b>Бо</b> Задачи	Дни недели:	<ul> <li>четверг</li> <li>пятница</li> </ul>	
<b>Д</b> Лицензия		<ul> <li>суббота</li> <li>воскресенье</li> </ul>	
	Время:	10:00 🗘	
	Отложить запуск после старта приложения на:	0 🗘 минут	
Под управлениемс 10.196.2.132 Сергер подслочен: 2 минуты назад Вирокк 11.9.0.351	Запускать пропущення Выполнять только во п	ые задачи время простоя компьютера ОК Отмена	
¢ 0	Сохранить	Отмена	

Рисунок Г.104. – Настройка расписания запуска контроля целостности