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 данных», «Защита компьютерных сетей 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 IM-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 файл-дисках;

- 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 исходным (установка параметров по умолчанию), что 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 представлен пример настройки СЗИ. 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 OT-инфраструктуры с минимальными усилиями со стороны обслуживающего персонала.

Центр мониторинга Кода Безопасности.

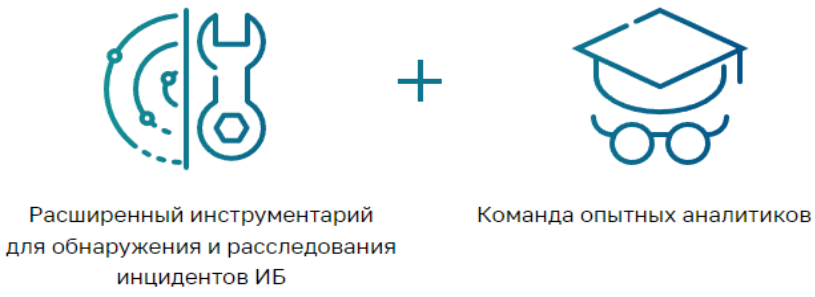

Рисунок 1 – Центр мониторинга Кода Безопасности

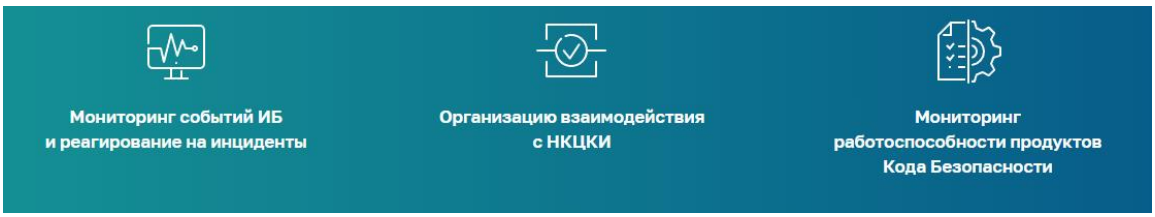

Рисунок 2 – Код Безопасности обеспечивает

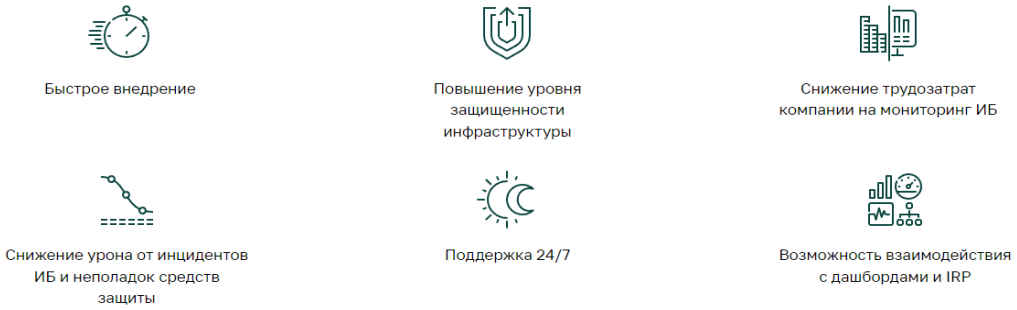

Рисунок 3 – Преимущества

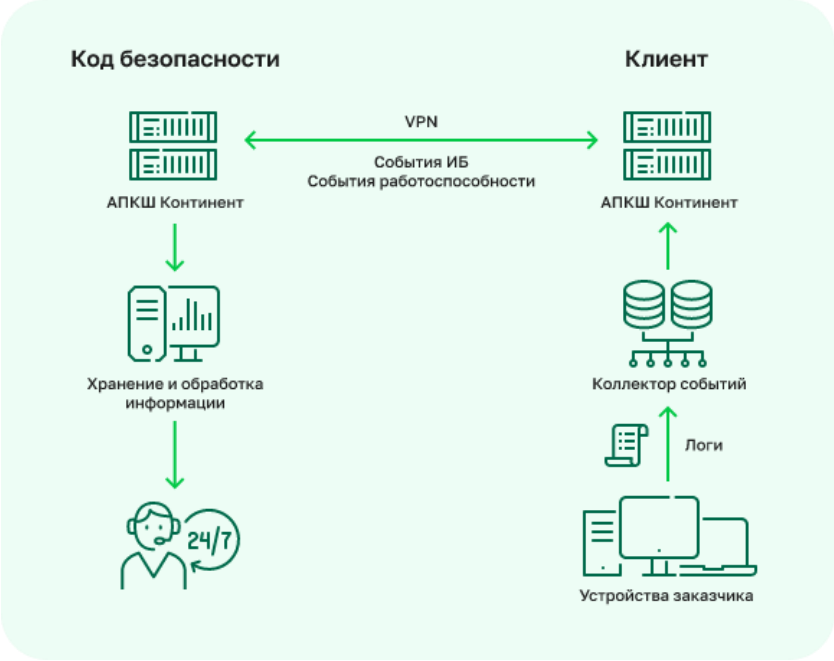

Рисунок 4 – Сбор информации на площадке заказчика и ее обработка в Коде Безопасности

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.

Иерархия подчинённости серверов безопасности. 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 в нём рекомендуется включать не более 15 000 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 или секретной 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 бизнес-процессы, 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 %.

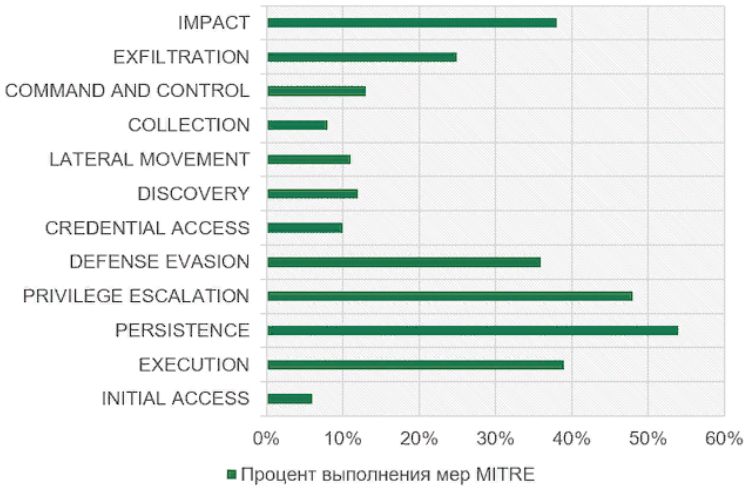

Рисунок 5 – Обнаружение техник злоумышленников на разных стадиях кибератак с помощью Secret Net Studio

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 управление и мониторинг событий. 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 компонентов инфраструктуры и оповещения о подозрительных 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.

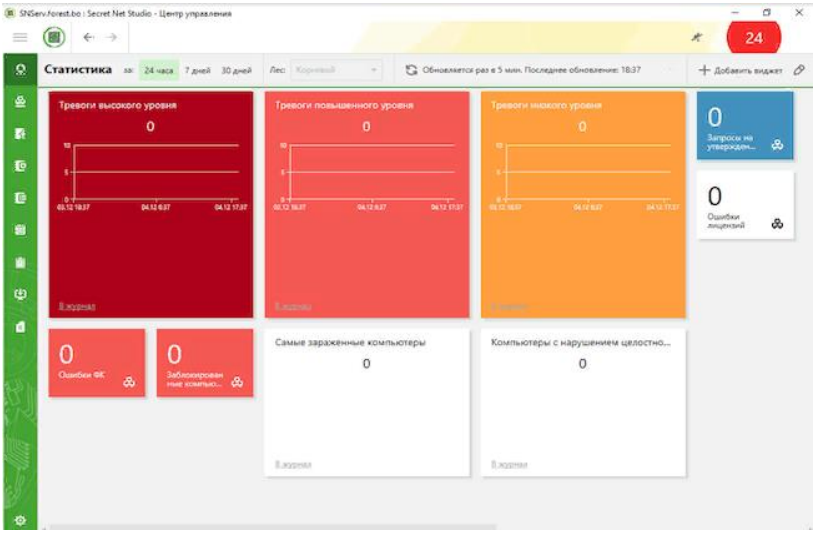

Рисунок 6 – Страница «Статистика» центра управления «Secret Net Studio»

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).

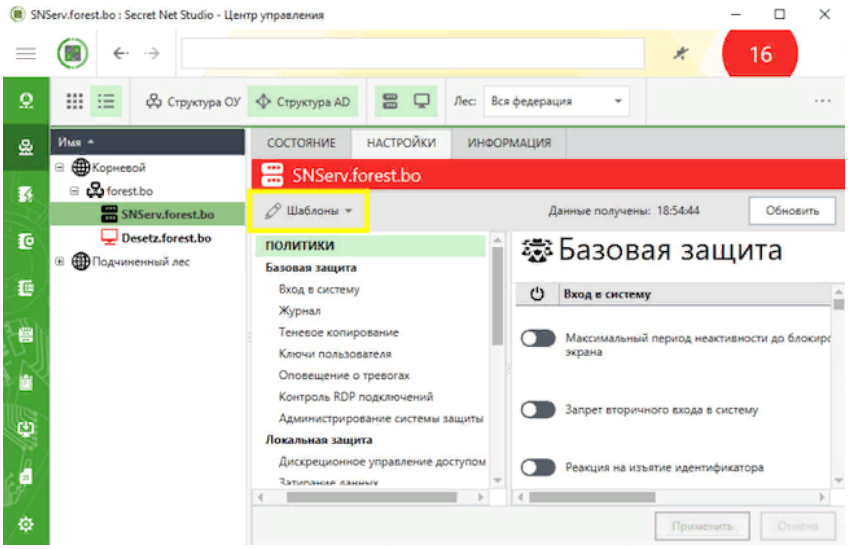

Рисунок 7 – Меню «Шаблоны» центра управления Secret Net Studio

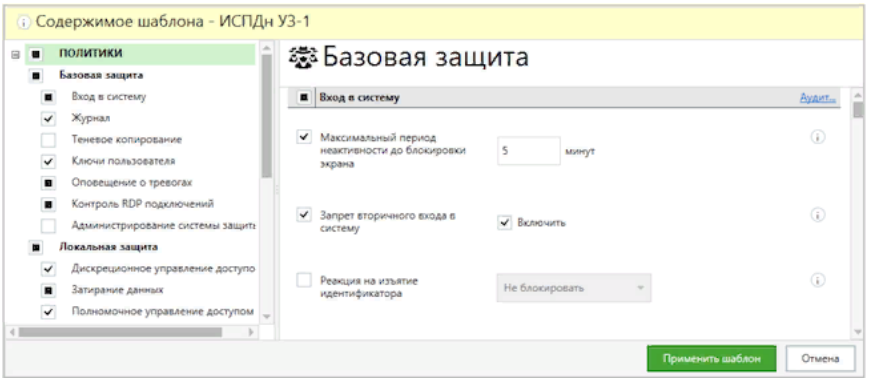

Рисунок 8 – Предустановленный шаблон для ИСПДн 1 УЗ (центр управления Secret Net Studio)

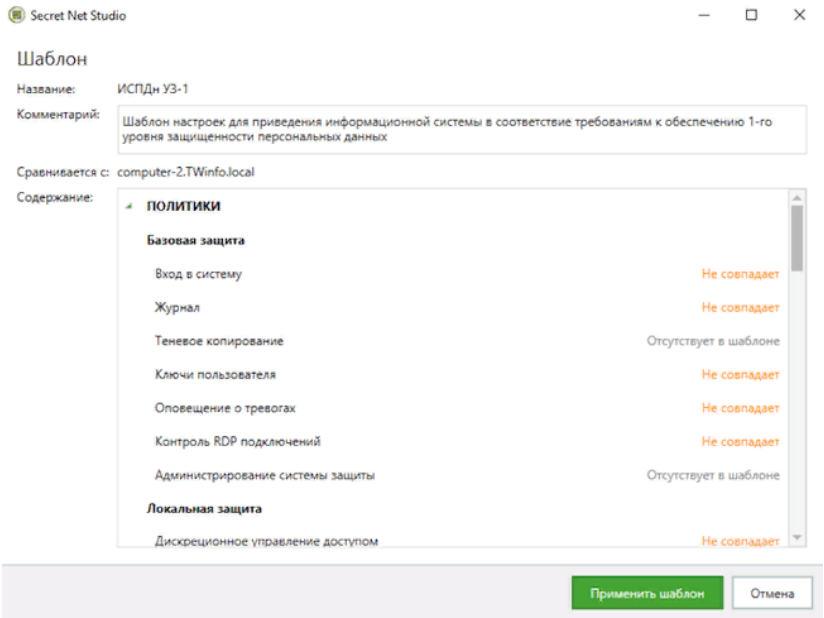

Рисунок 9 – Сравнение созданного шаблона с предустановленным для ИСПДн 1 УЗ (центр управления Secret Net Studio)

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 особенностью версии Secret Net Studio 8.8 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 того, кто шифрует и где хранится информация для возможности 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 АК3, 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 ОС 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 ОС она декомпозируется на следующие основные классы задач:

Идентификация и аутентификация пользователей. Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании механизма PAM, 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 PAM. 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 доступа. В ОС механизм дискреционного разграничения доступа обеспечивает проверку дискреционных ПРД, формируемых в виде базовых ПРД ОС семейства Linux, формируемых в виде идентификаторов субъектов (идентификатор 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 ≥ L1 и C0 ≥ C1;

- операция исполнения разрешена, если L0 ≥ L1 и C0 ≥ 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 другого процесса, так как непривилегированный 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 cron) 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 ОС 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 ОС digsig_verif и может функционировать в одном из следующих режимов:

1) 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 Small Office Security», «Kaspersky Endpoint Security Cloud». Для среднего бизнеса: «Kaspersky Endpoint Security Cloud», «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 веб-ресурсов, 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, у 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 проверк***а. 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.).

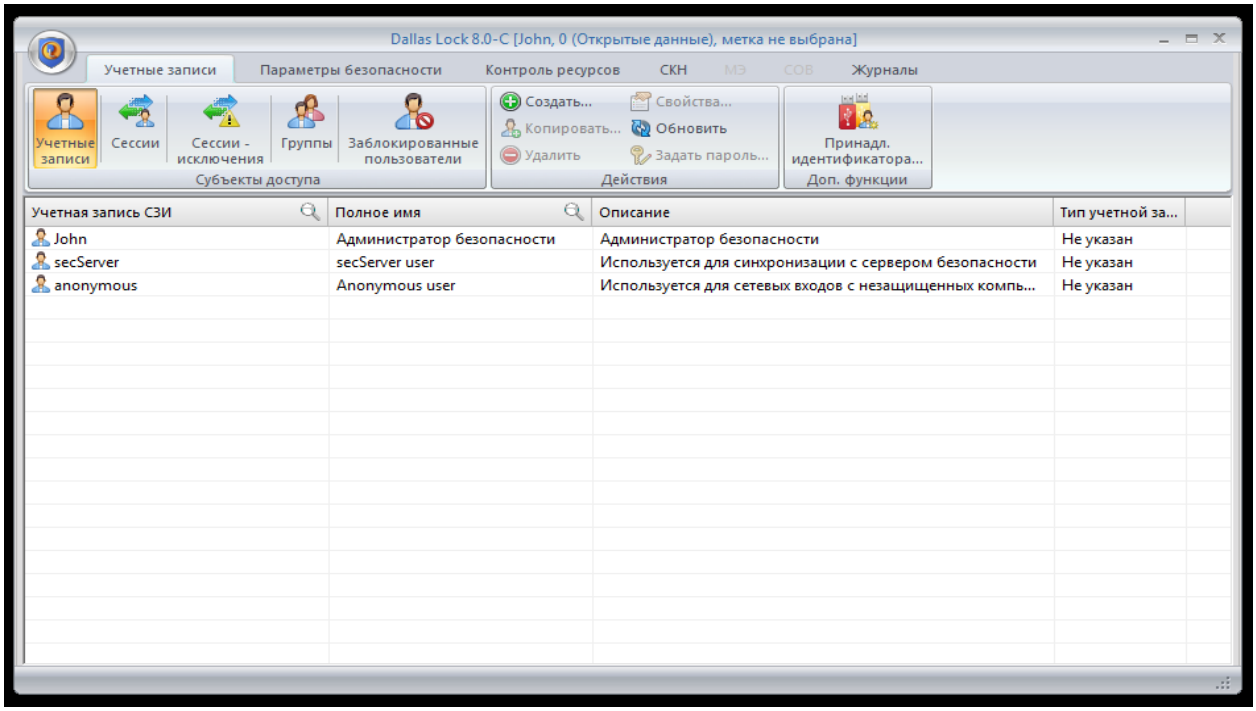

Рисунок А.1. – Окно оболочки администратора системы защиты

Нажать кнопку создать в категории действия, или в контекстном меню, открывающимся по нажатию на правую кнопку мыши (см. рисунок А.2.).

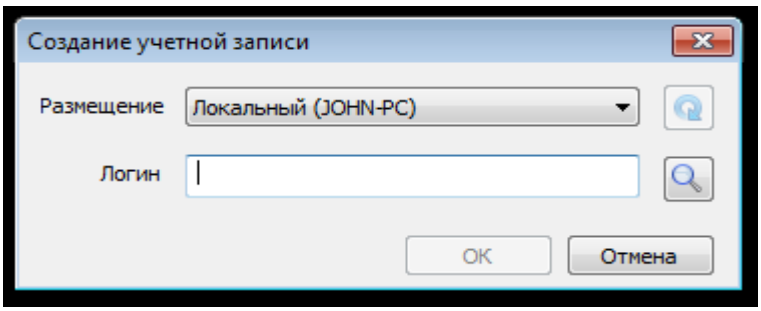

Рисунок А.2. – Окно создания учетной записи

В открывшемся окне в поле размещения выбрать локальный и указать логин регистрируемого пользователя (см. рисунок А.3.).

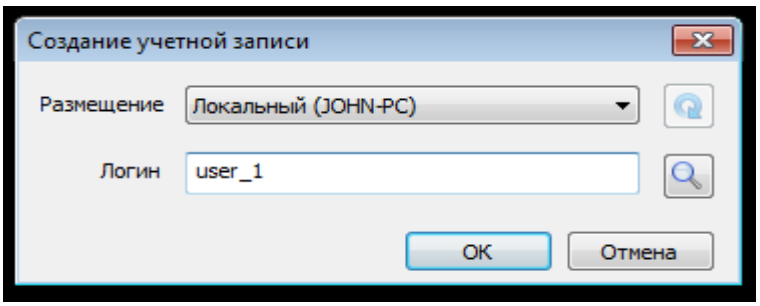

Рисунок А.3. – Заполненной окно создания учетной записи

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: " / \ [ ] : | < > + = ; , ? @ *); 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.).

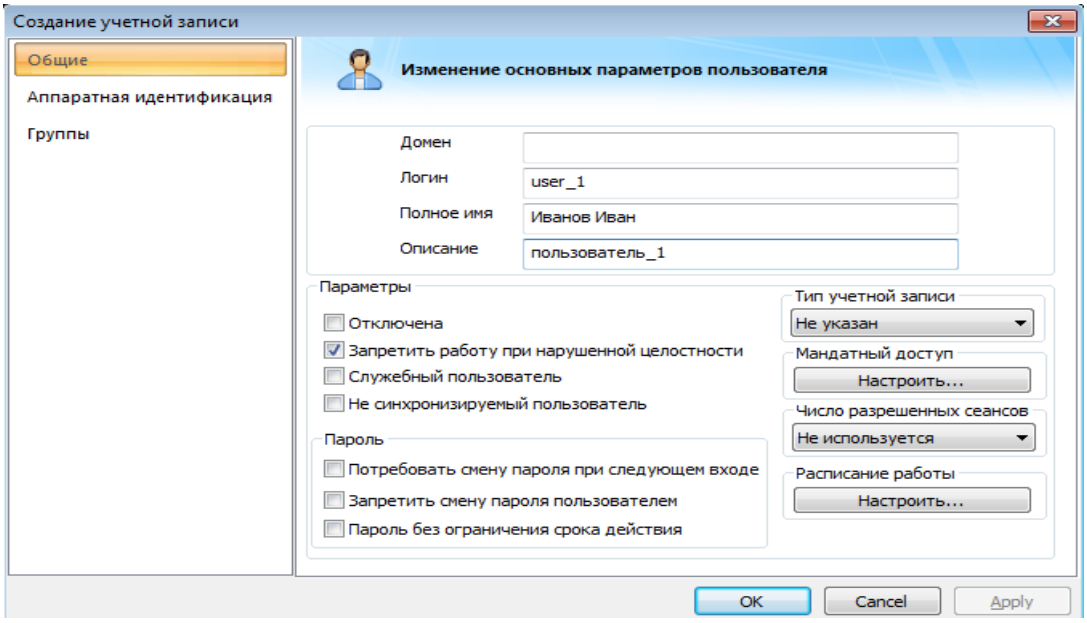

Рисунок А.4. – Окно редактирования параметров учетной записи

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

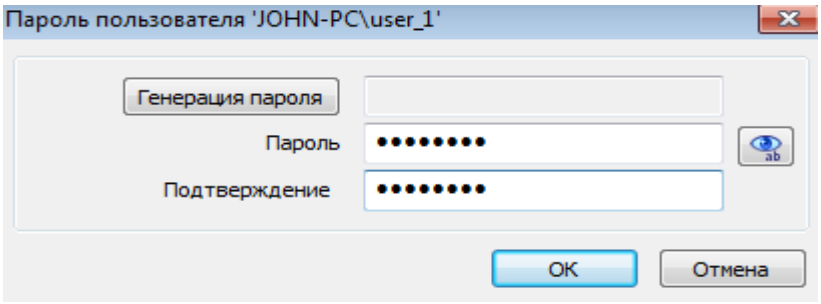

Рисунок А.5. – Окно создания пароля пользователя

Либо воспользоваться функцией генерации пароля (см. рисунок А.6.):

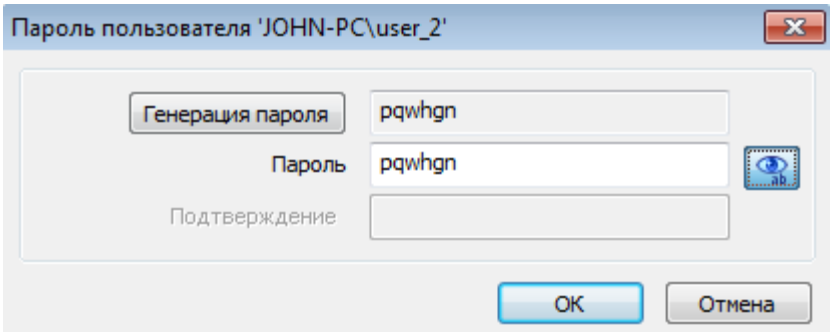

Рисунок А.6. – Пример создания пароля при помощи генерации

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

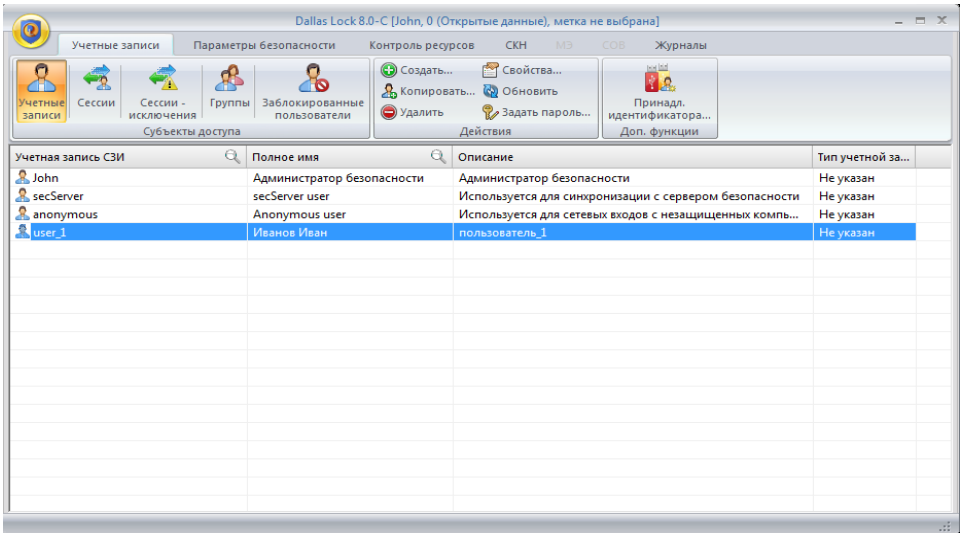

Рисунок А.7. – Окно учетной записи с новым пользователем

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.).

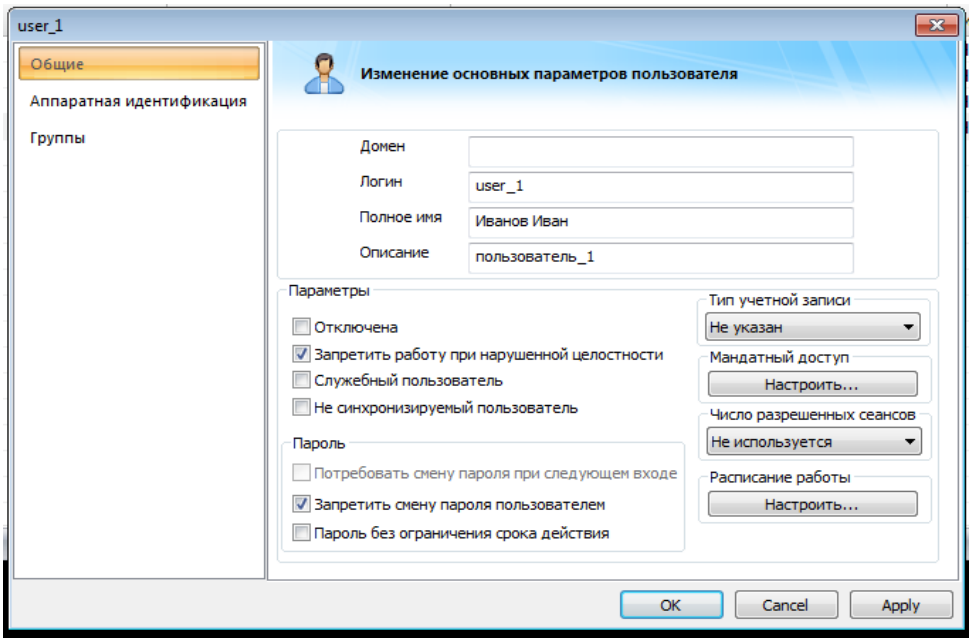

Рисунок А.8. – Окно редактирования основных параметров пользователя

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

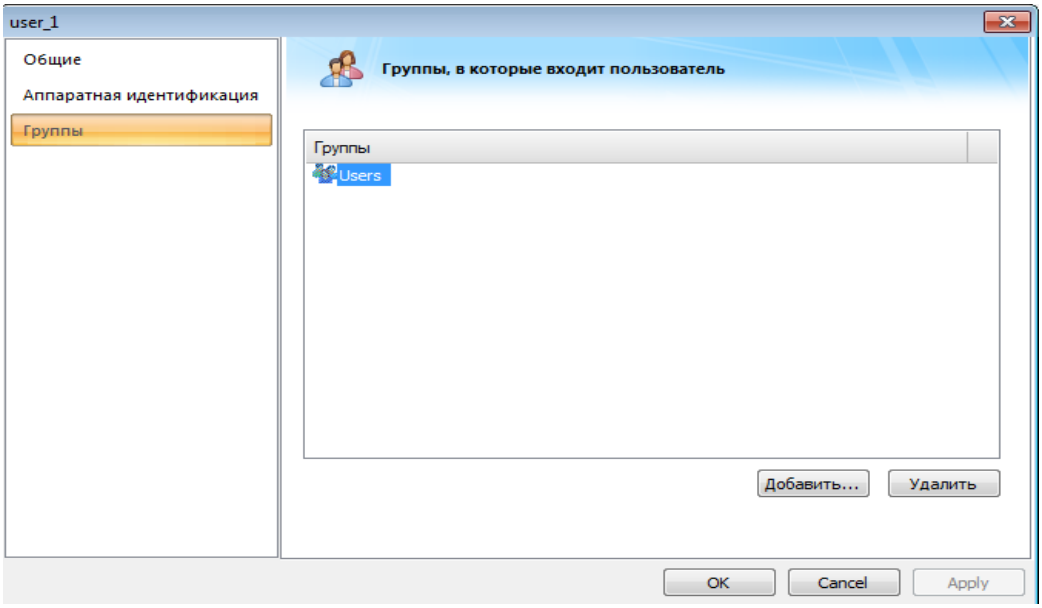

Рисунок А.9. – Окно редактирования групп пользователя

Настройка идентификации и аутентификации

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

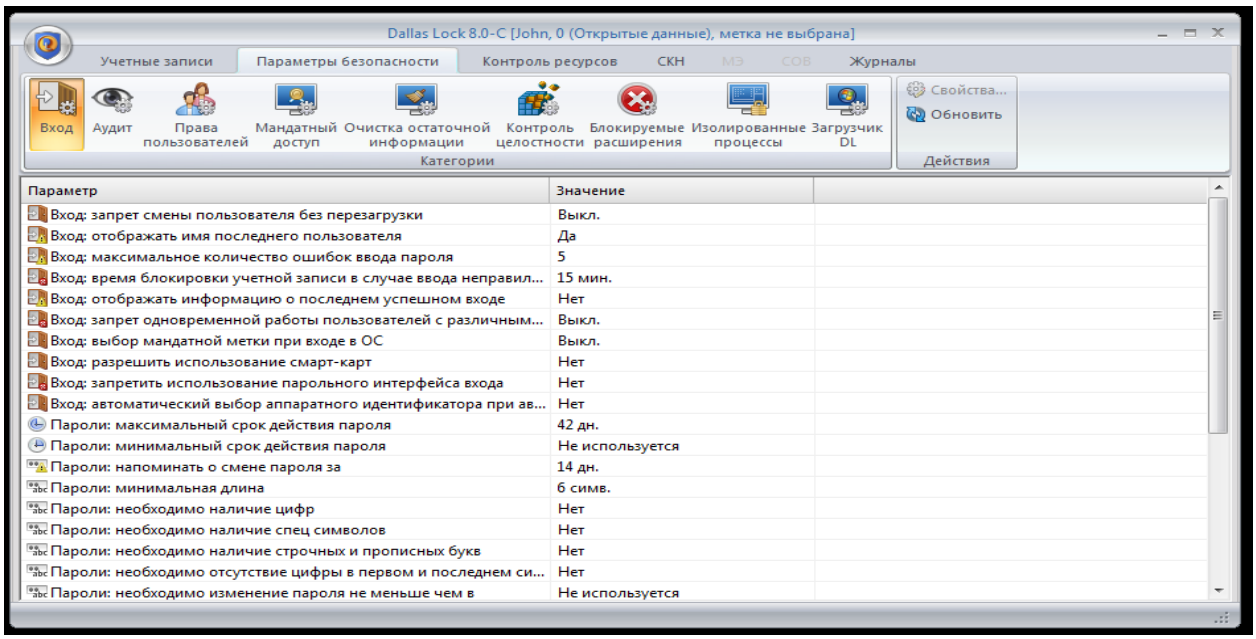

Рисунок А.10. – Список параметров входа

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

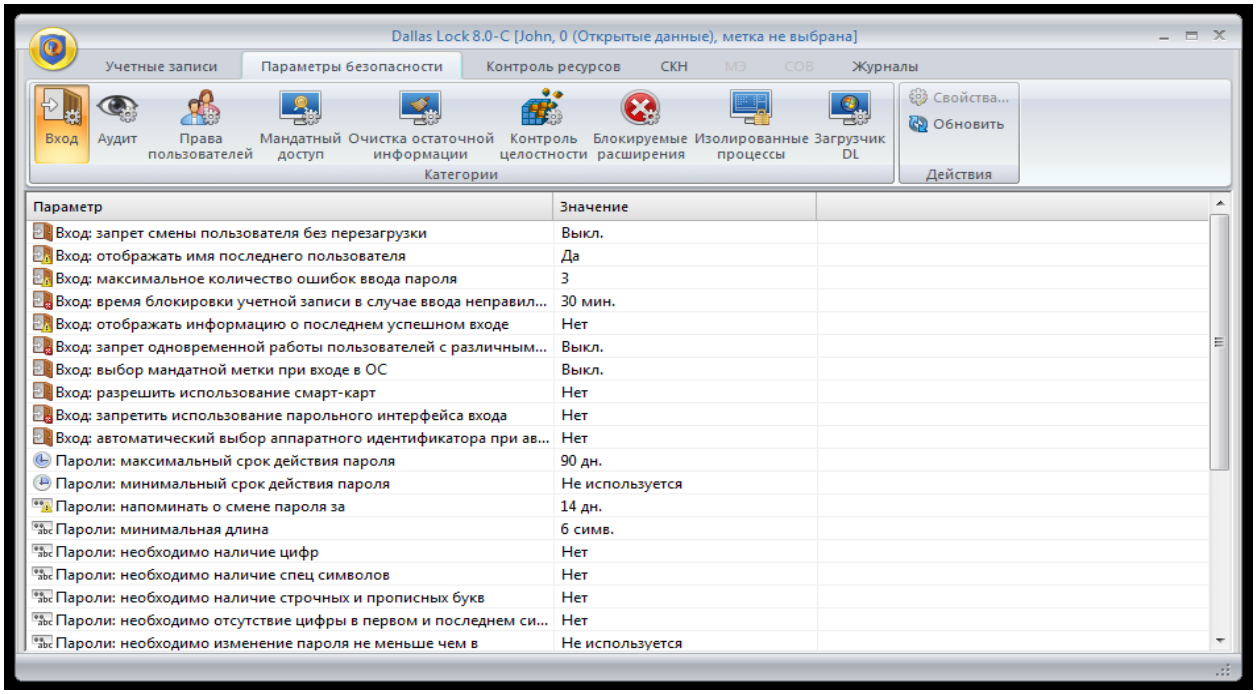

Рисунок А.11. – Пример настройки списка параметров входа

Установка прав разграничения доступа

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

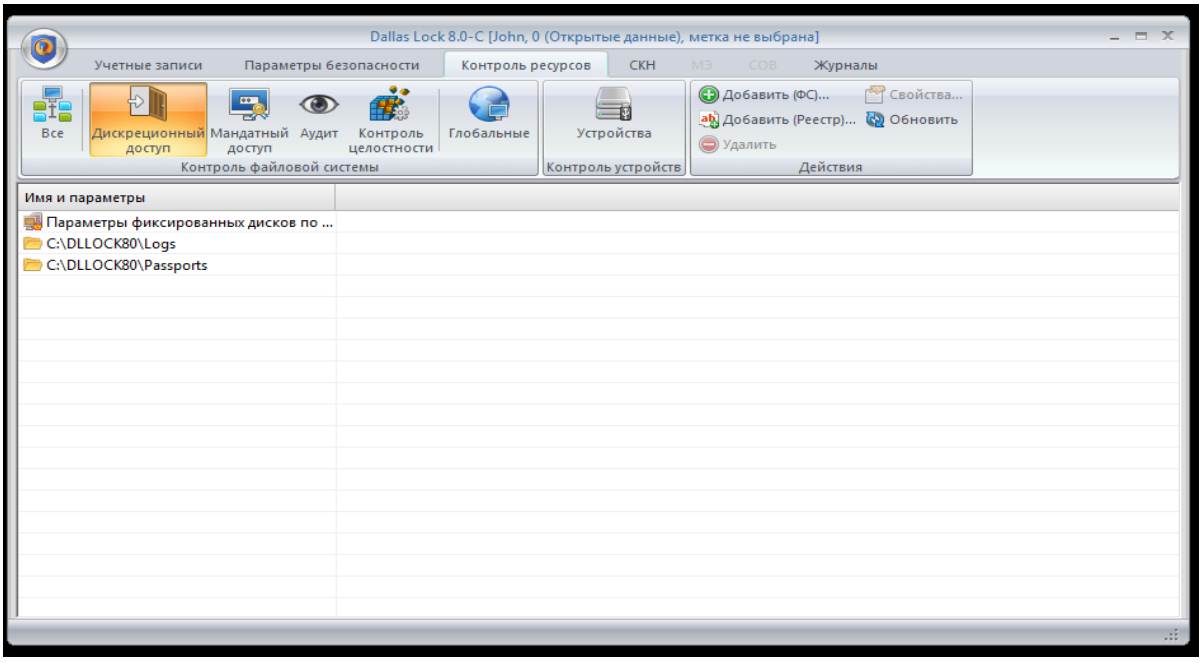

Рисунок А.12. – Окно дискреционного доступа

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

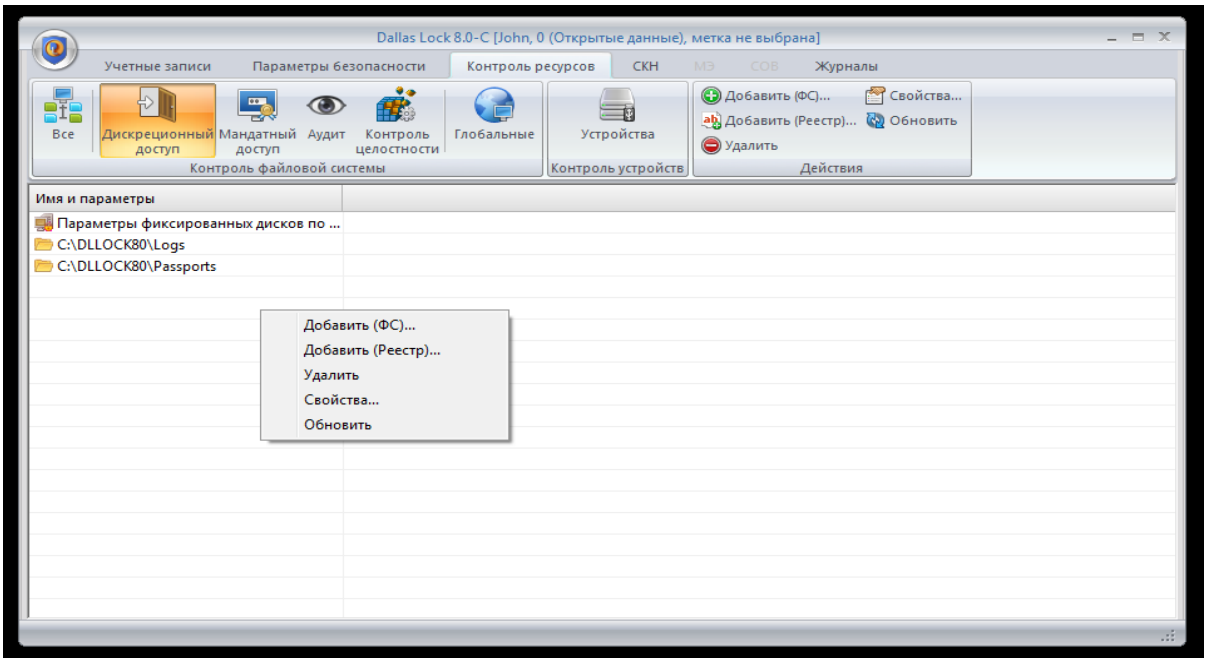

Рисунок А.13. – Пример вызова контекстного меню

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

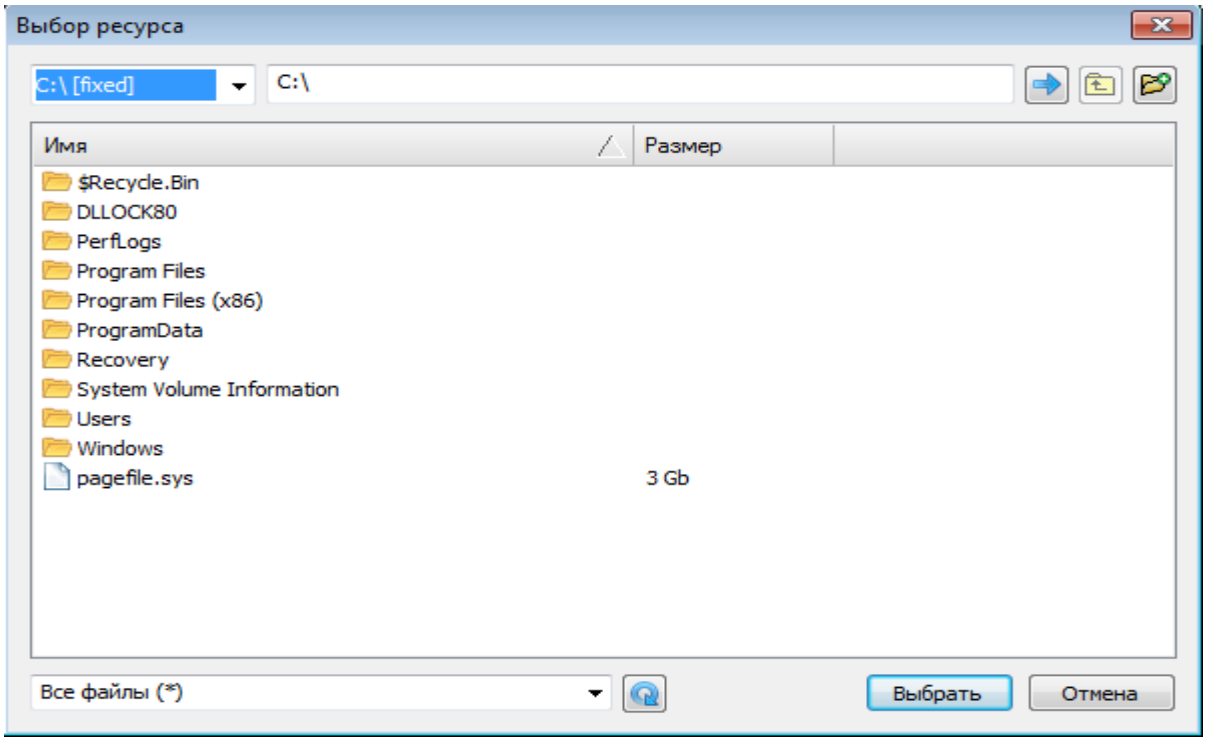

Рисунок А.14. – Меню выбора ресурса

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

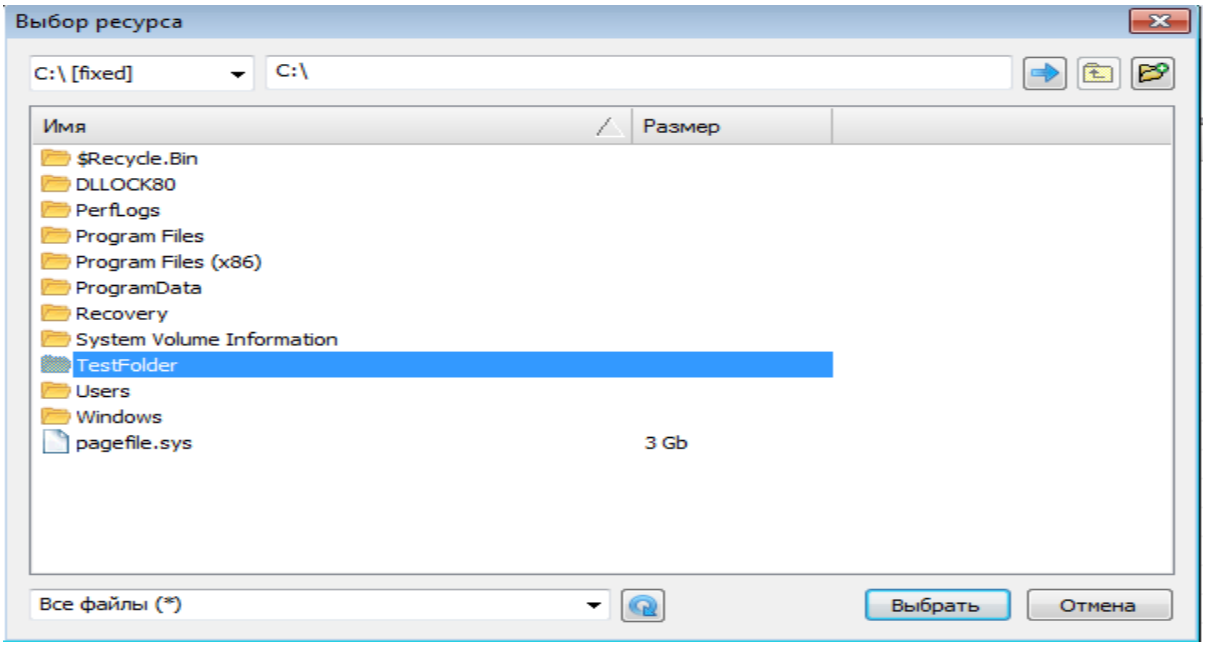

Рисунок А.15. – Пример выбора ресурса

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

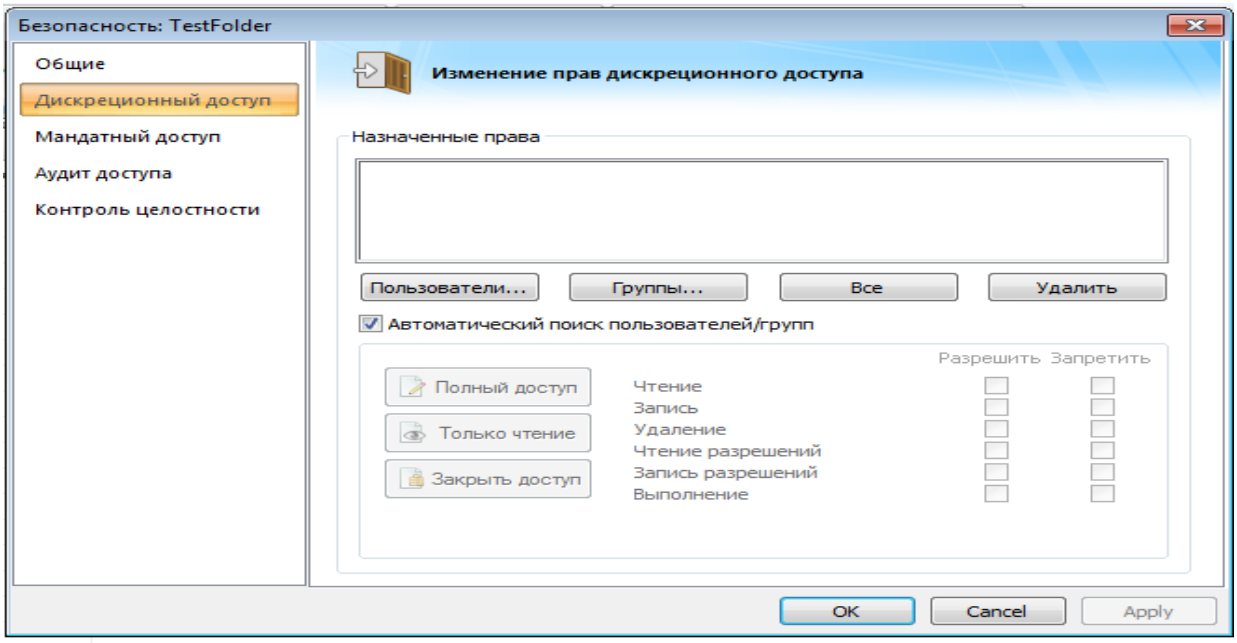

Рисунок А.16. – Окно настройки дискреционного доступа

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

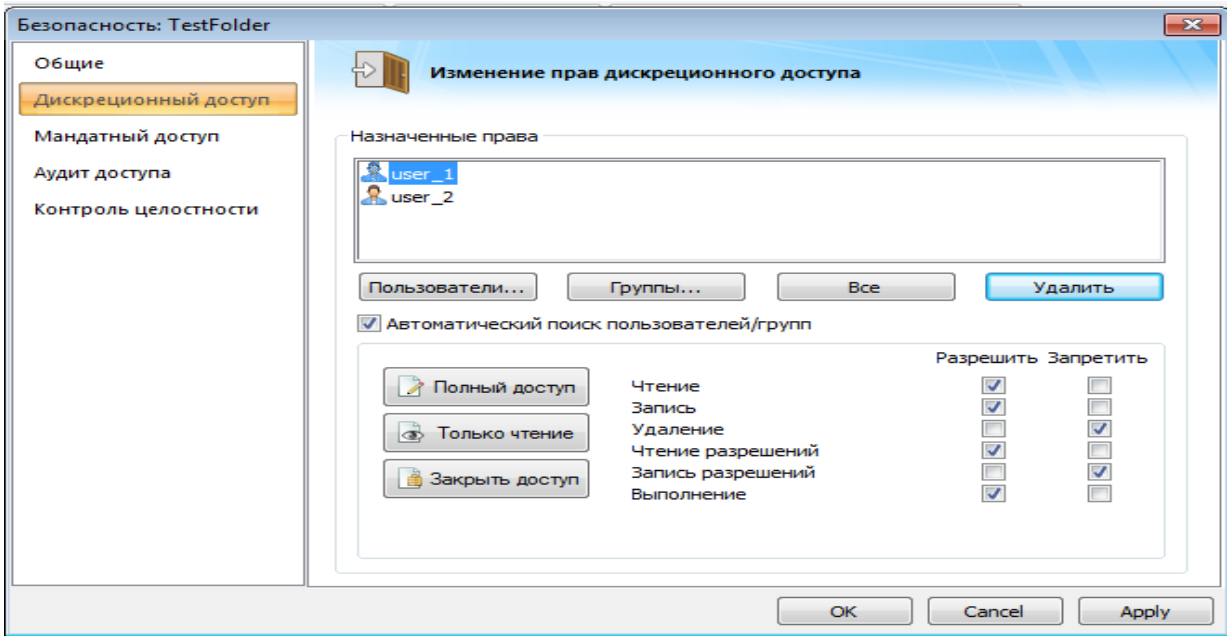

Рисунок А.17. – Пример настройки дискреционного доступа

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

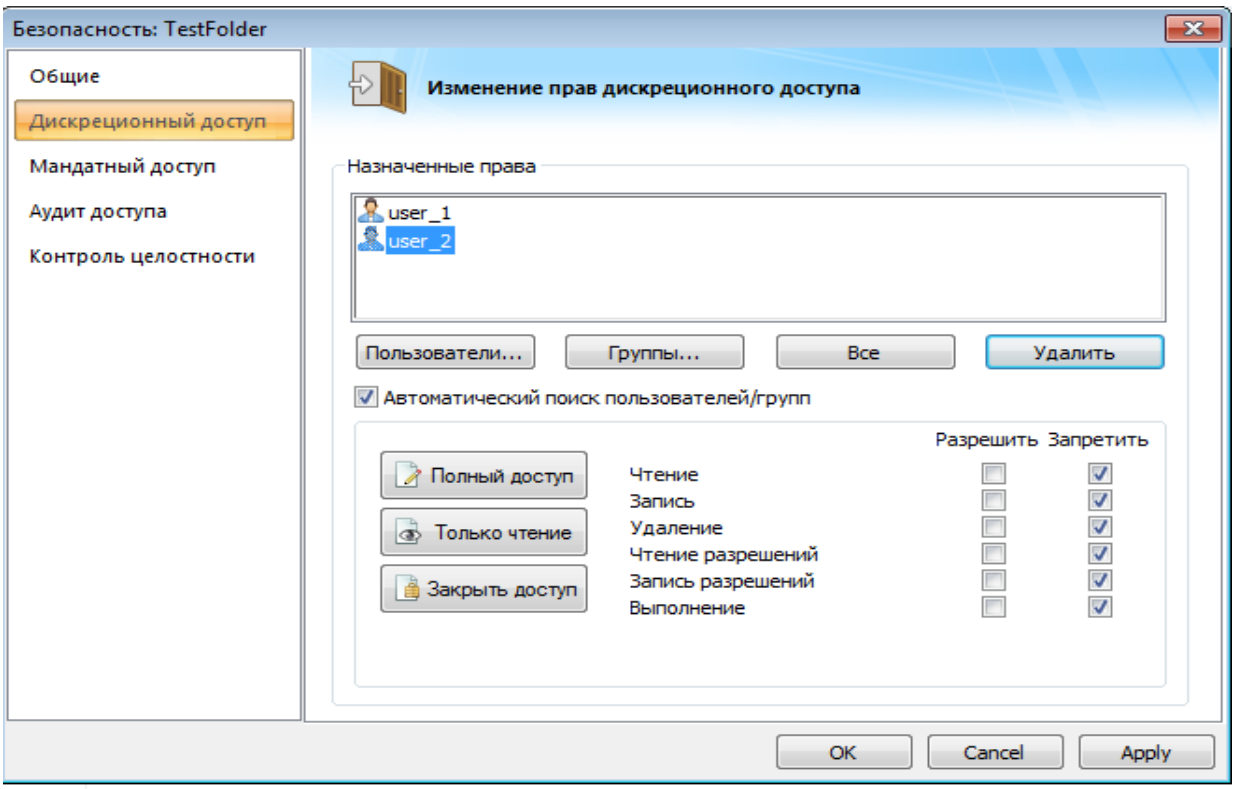

Рисунок А.18. – Пример настройки набора разрешений

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.).

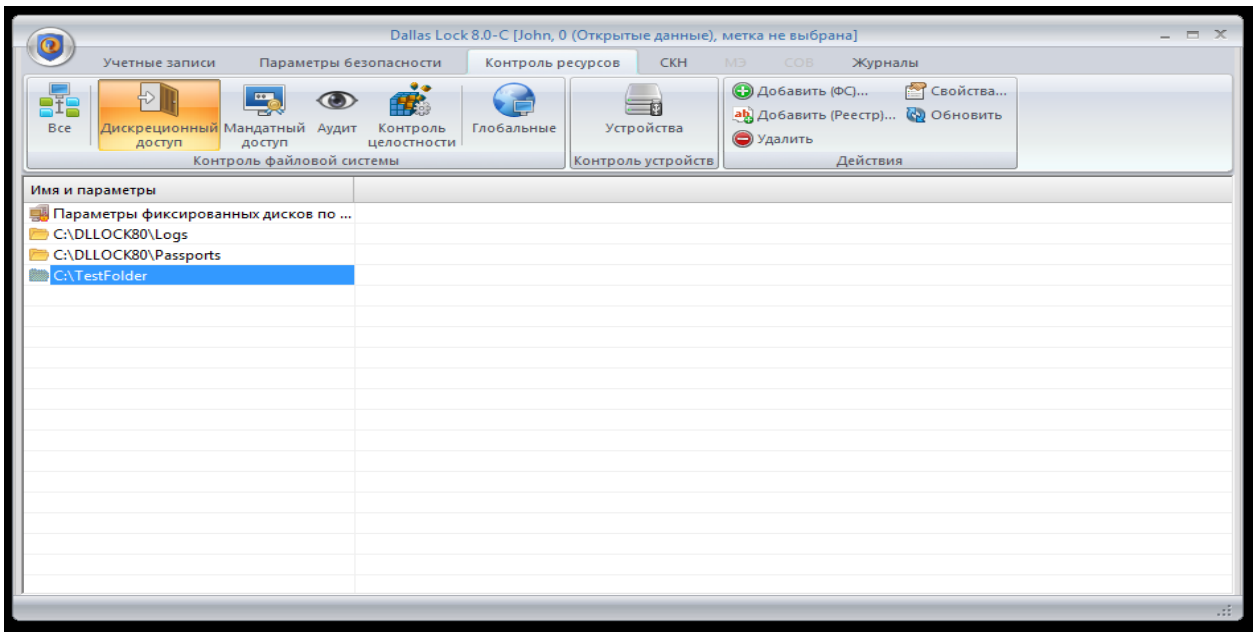

Рисунок А.19. – Результат создания настройки дискреционного доступа

Настройка очистки остаточной информации

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

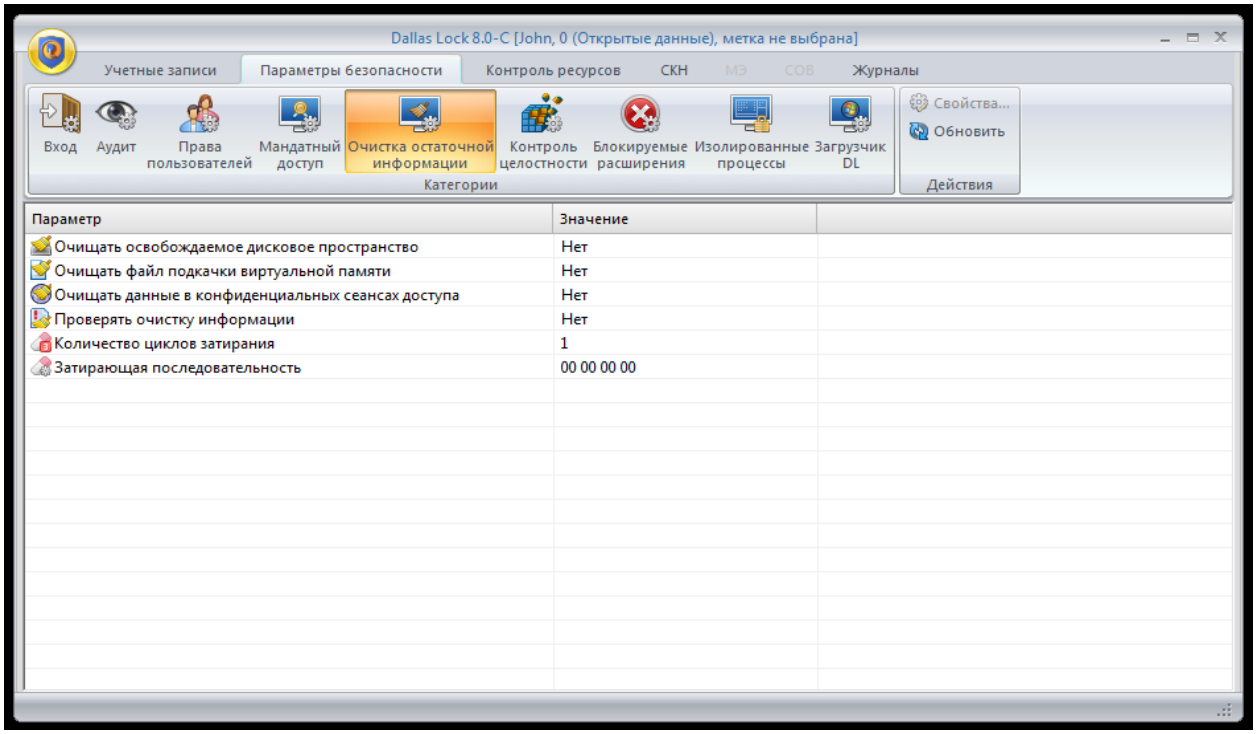

Рисунок А.20. – Окно очистки остаточной информации

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.).

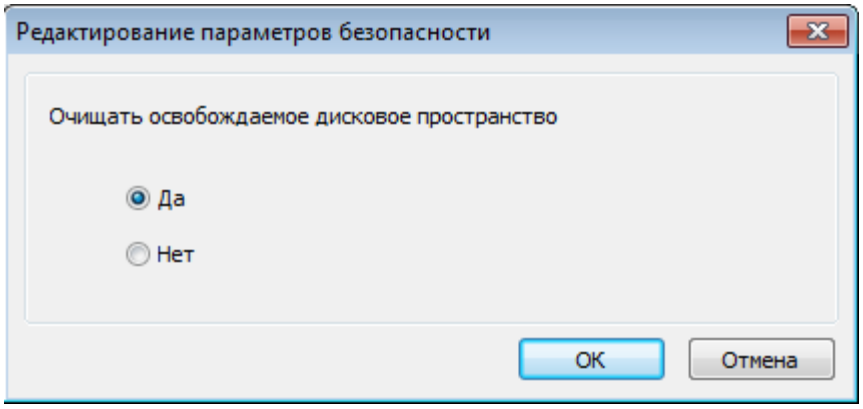

Рисунок А.21. – Окно настройки очистки дискового пространства

Количество циклов затирание установить в соответствии с требованиями политики безопасности (см. рисунок А.22.).

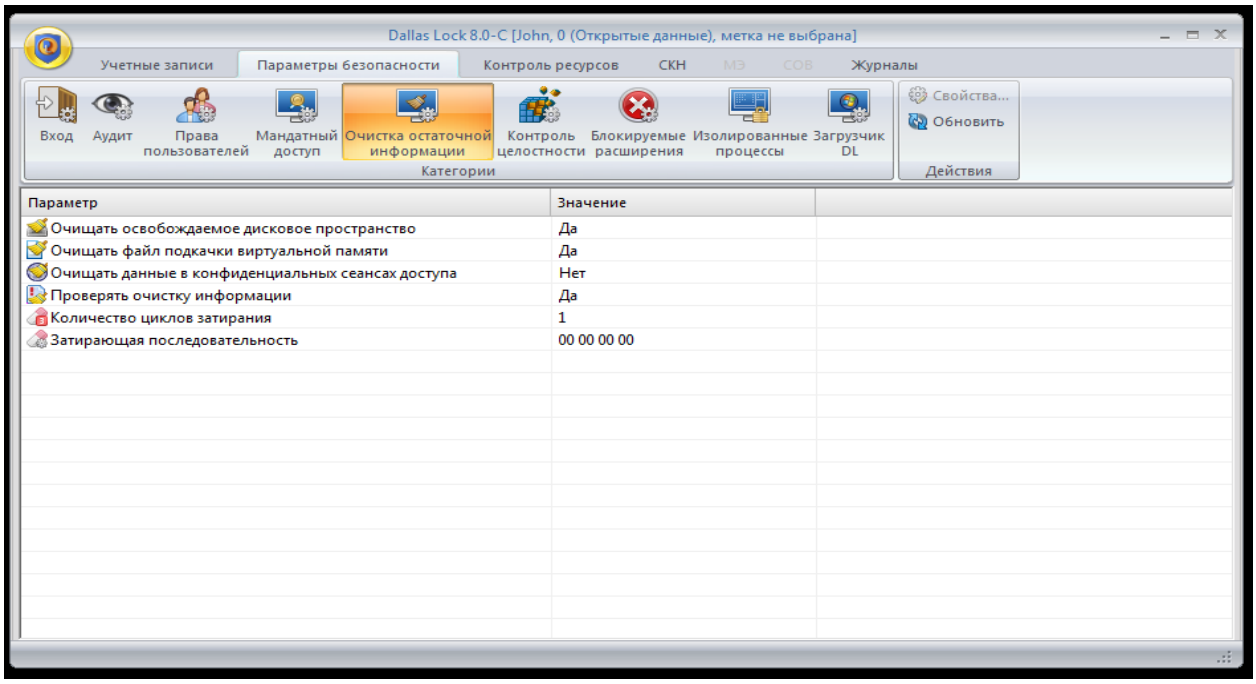

Рисунок А.22. – Пример настройки очистки остаточной информации

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.).

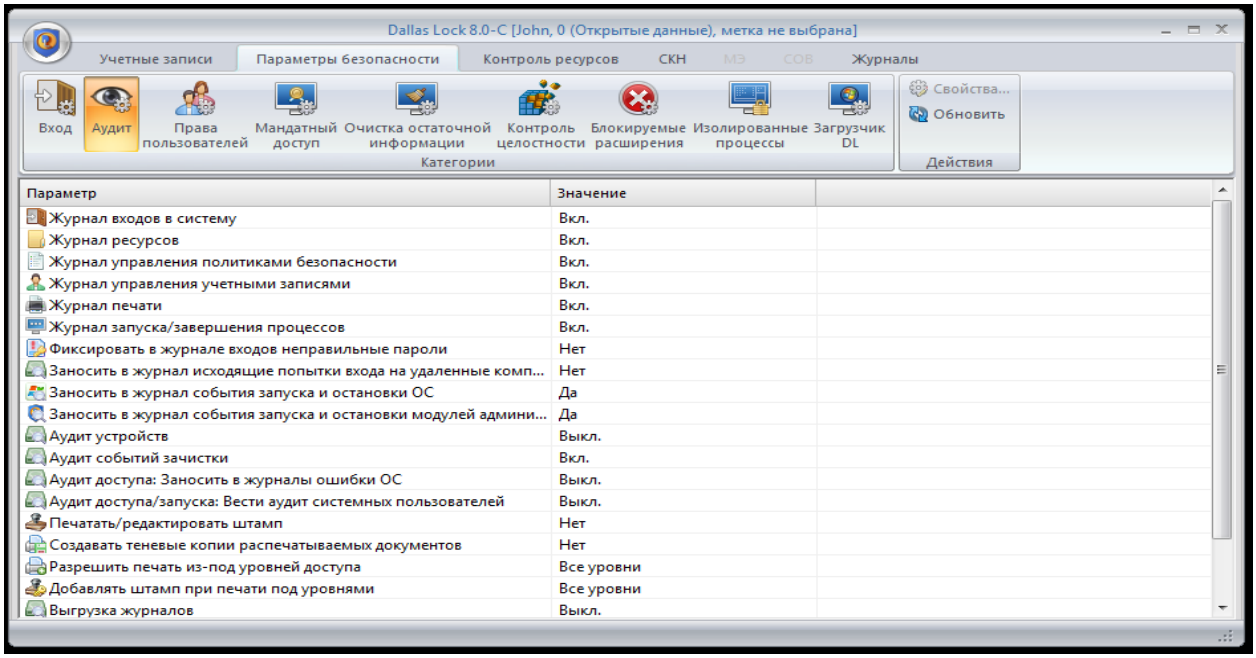

Рисунок А.23. – Окно настройки аудита

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

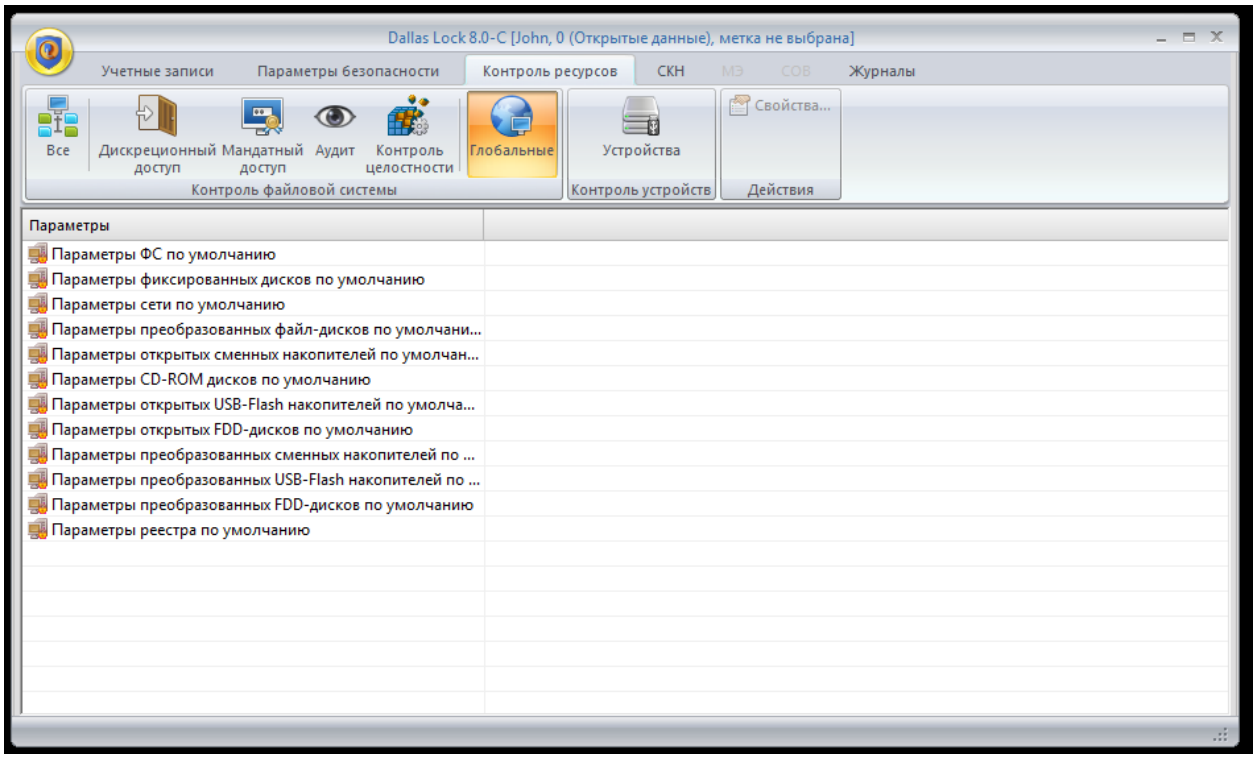

Рисунок А.24. – Глобальные параметры

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

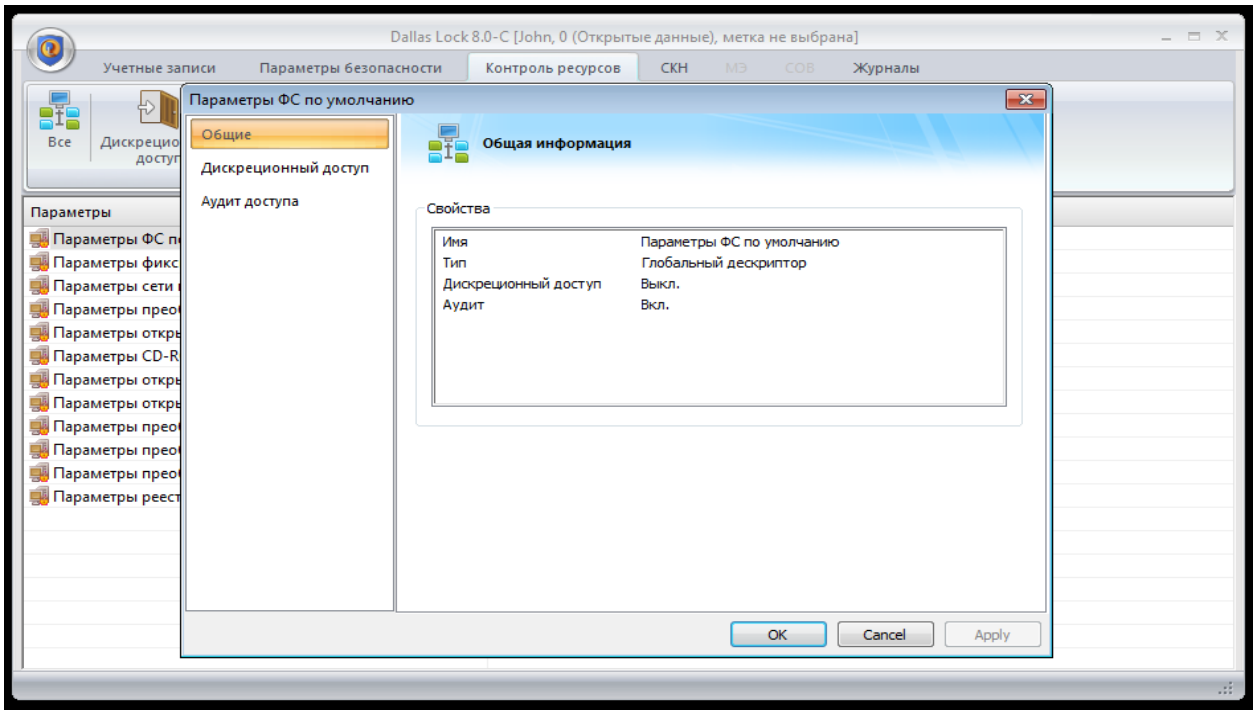

Рисунок А.25. – Свойства глобального параметра

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

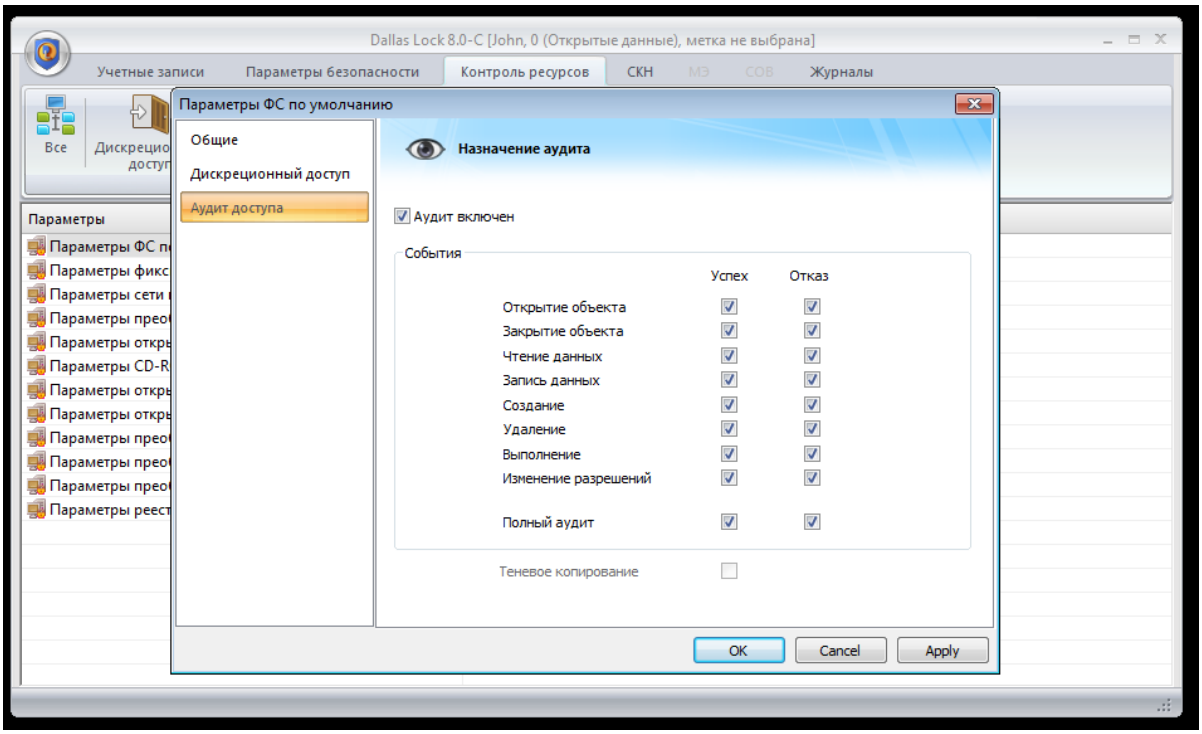

Рисунок А.26.– Настройка аудита доступа глобального параметра

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

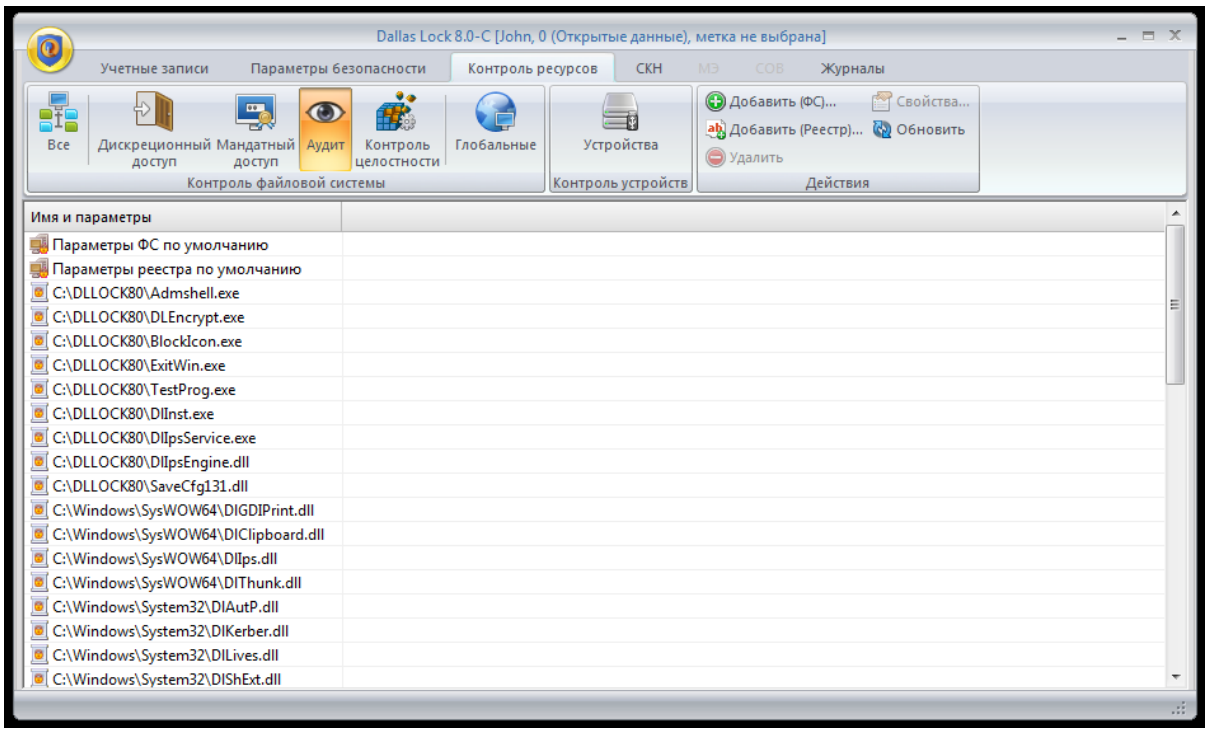

Рисунок А.27. – Настройка аудита для локальных объектов ФС

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

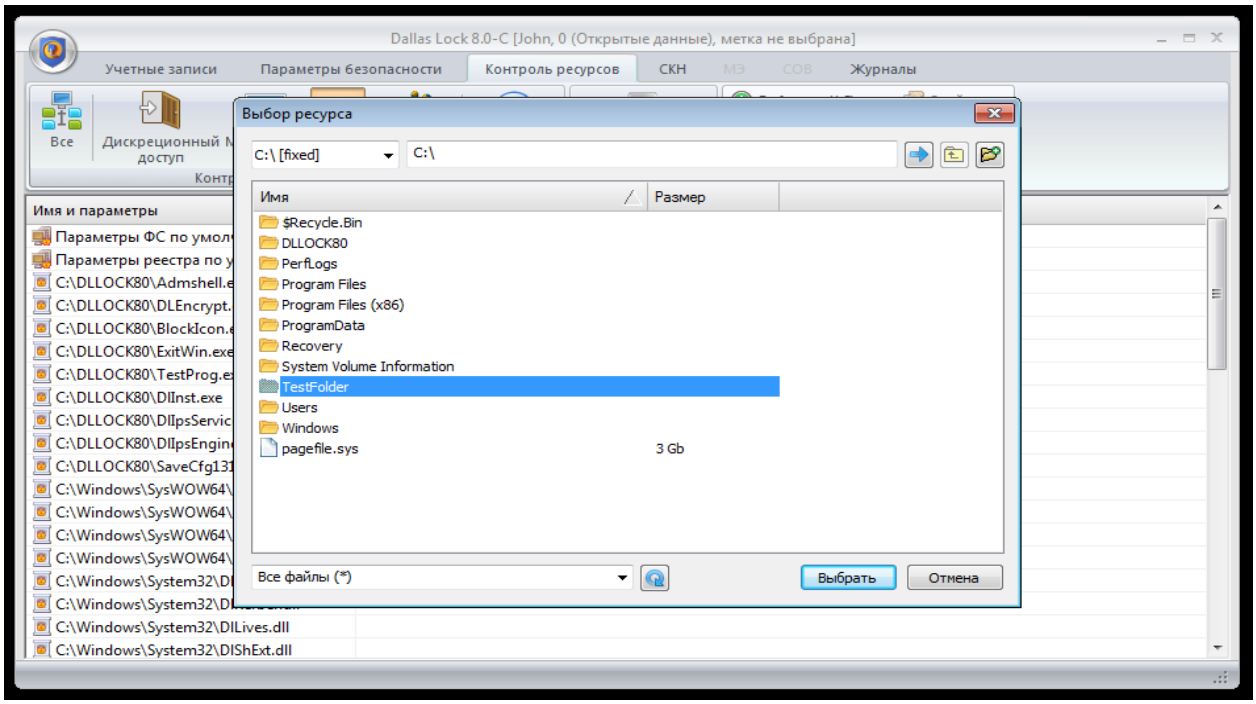

Рисунок А.28. – Выбор ресурса для назначения аудита

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.).

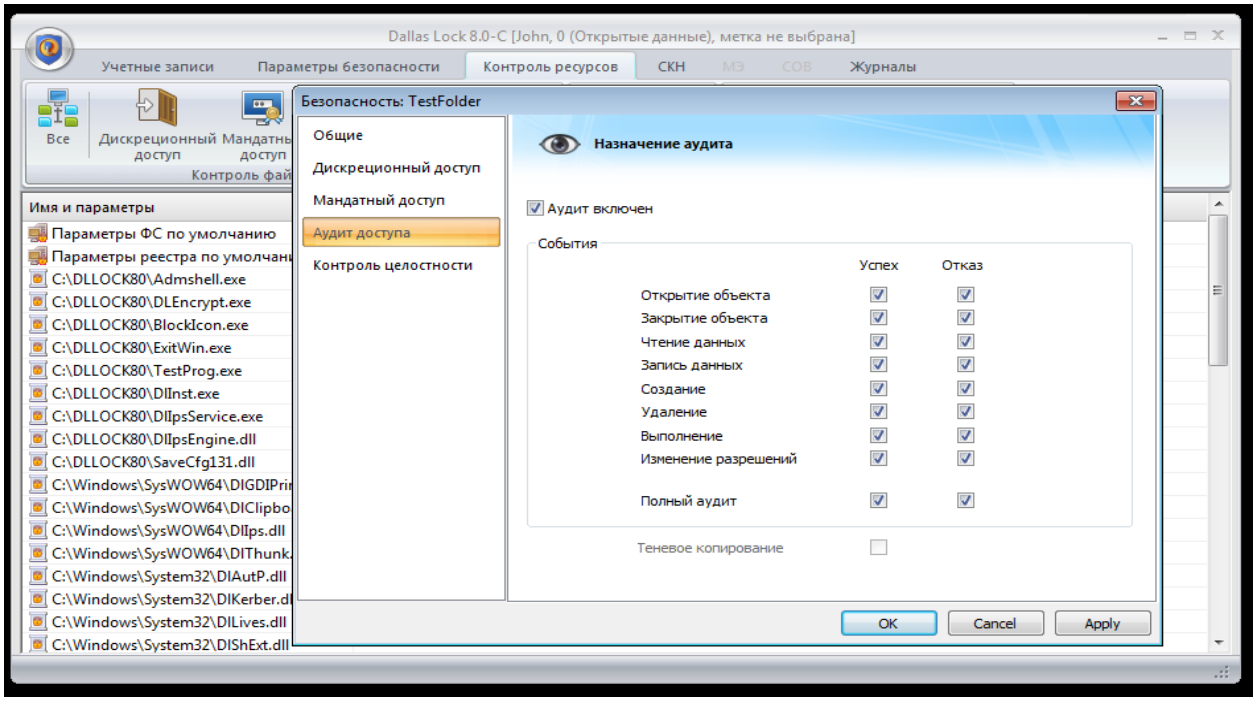

Рисунок А.29. – Настройка аудита доступа для ресурса ФС

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

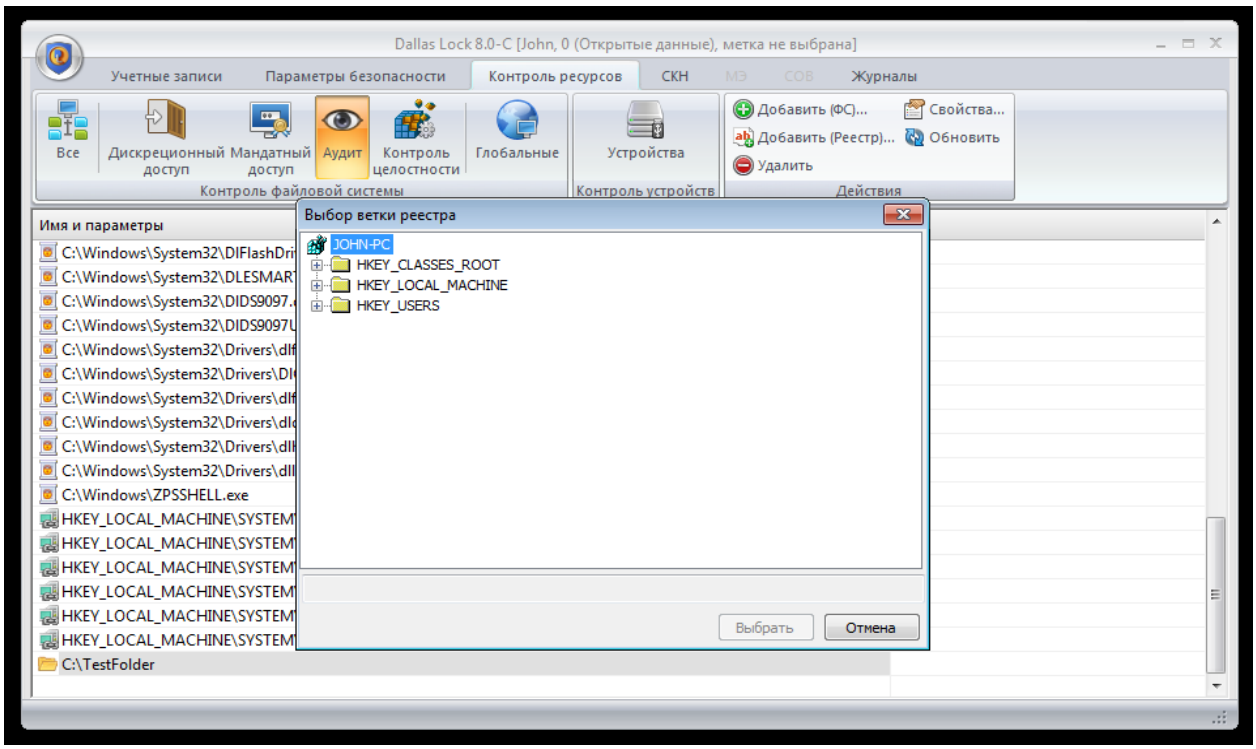

Рисунок А.30. – Выбор ветки реестра

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

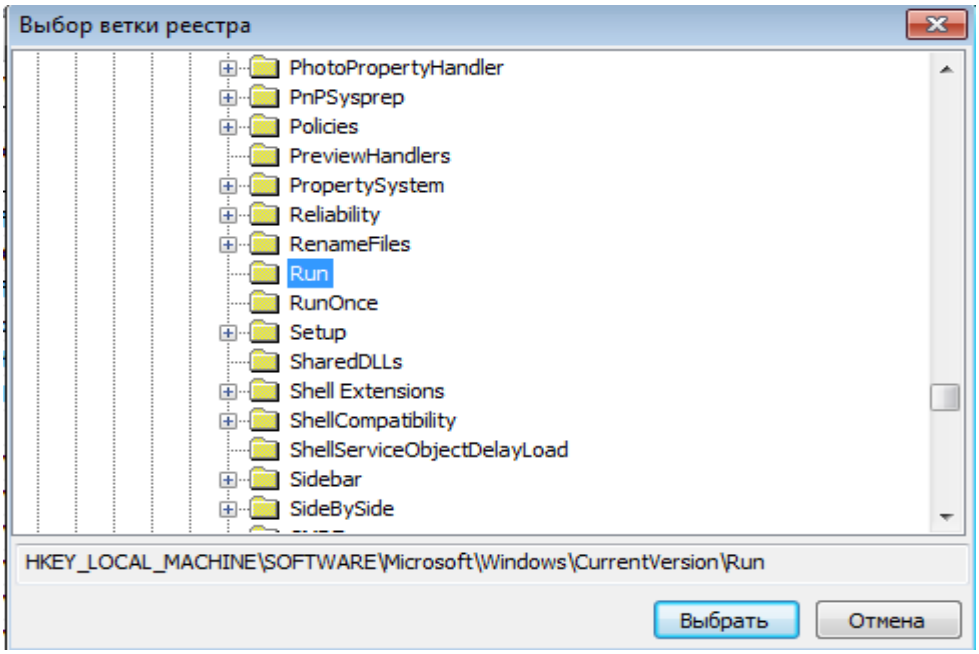

Рисунок А.31. – Выбор реестра

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

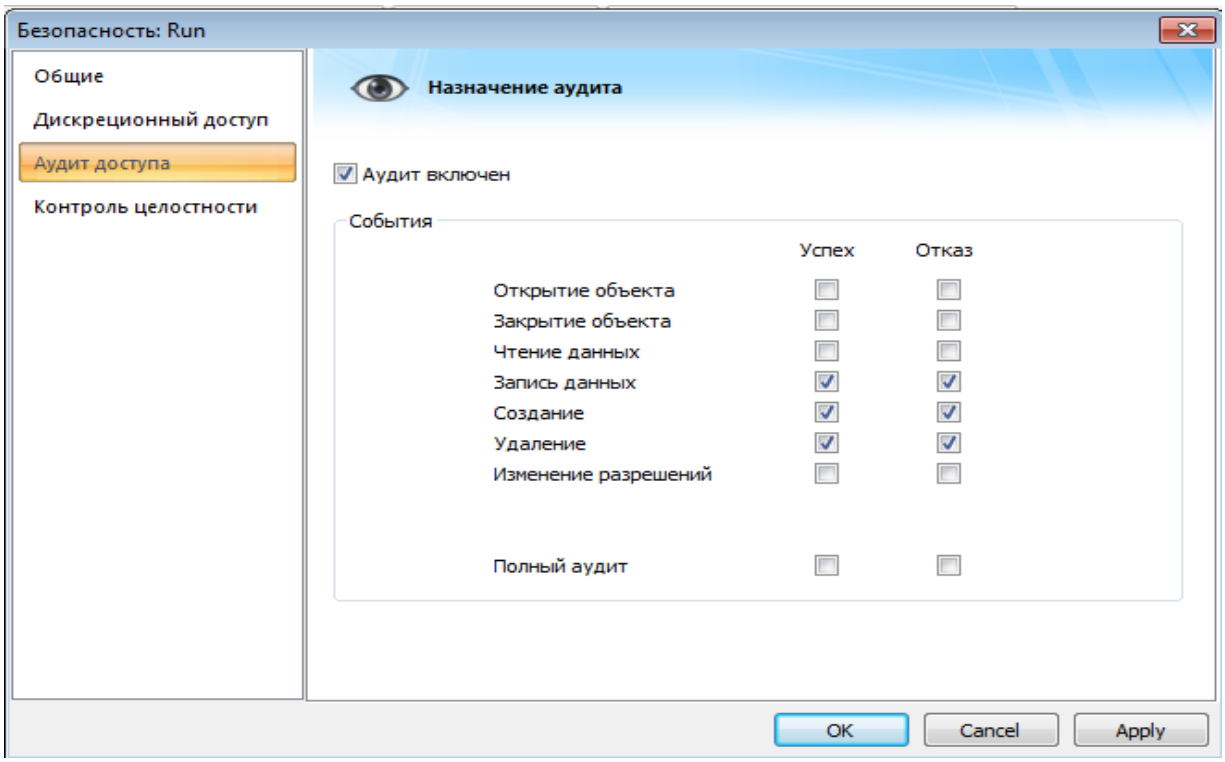

Рисунок А.32. – Назначение аудита доступа для выбранного реестра

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

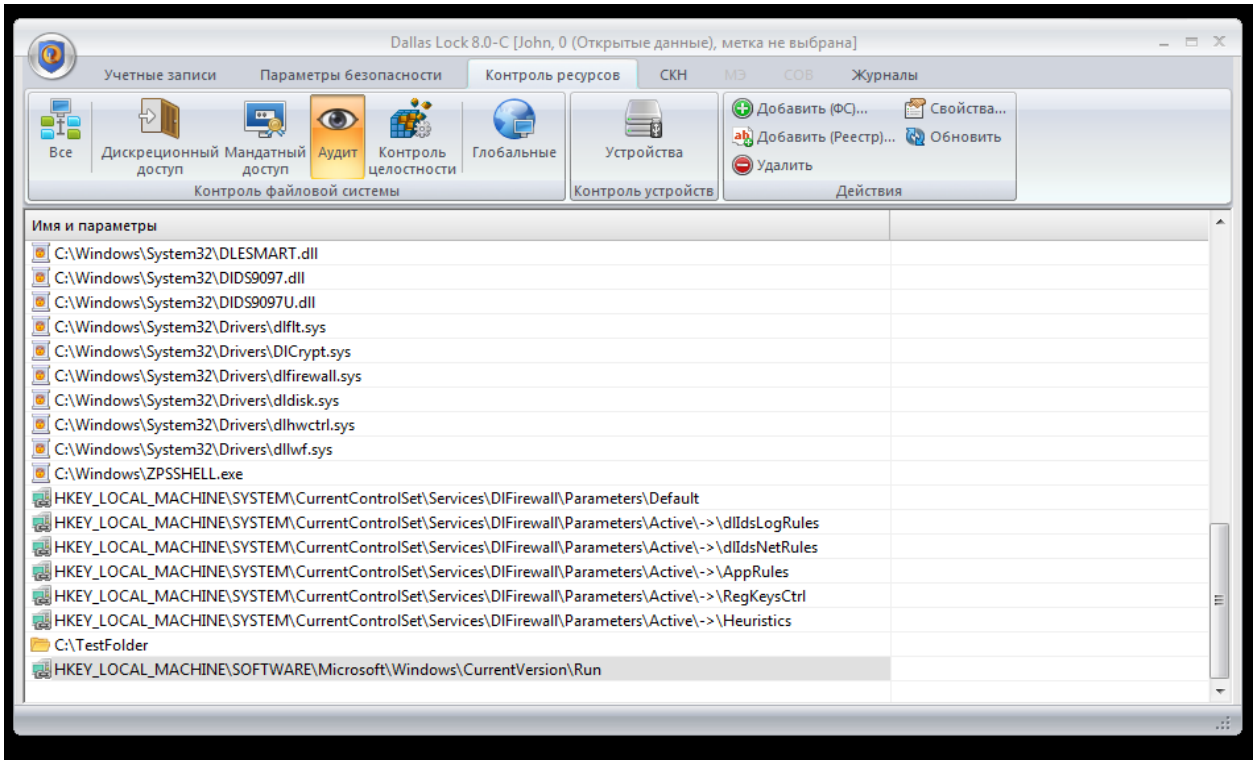

Рисунок А.33. – Результат добавления элементов аудита

Настройка контроля целостности файловой системы и программно-аппаратной среды

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

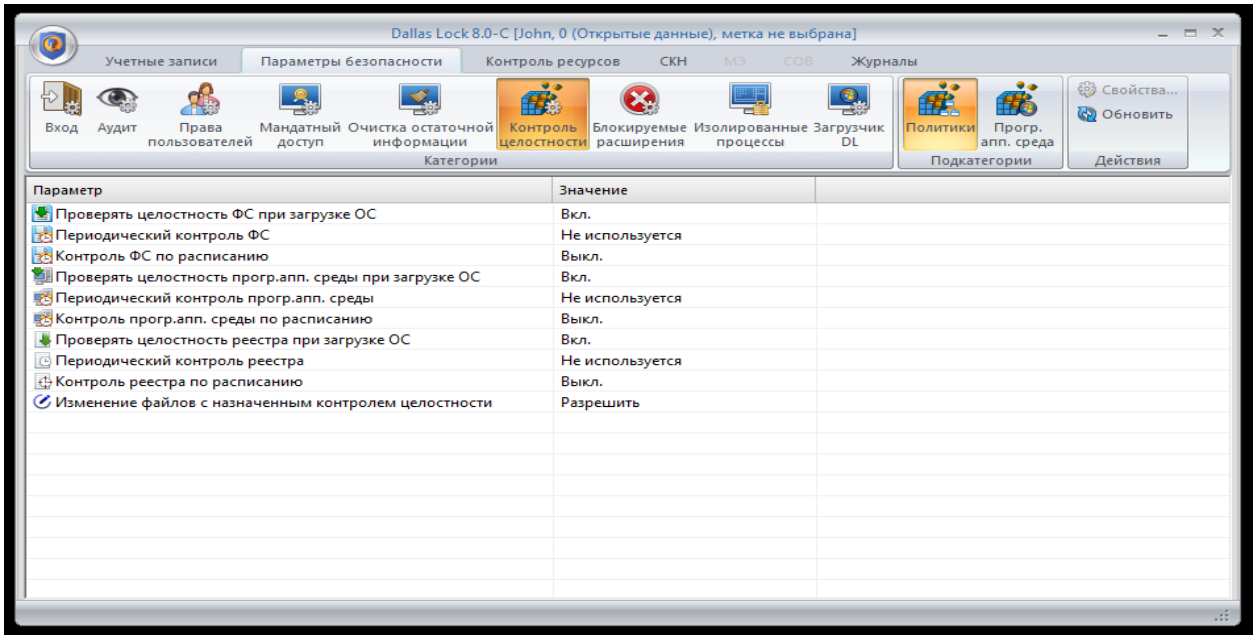

Рисунок А.34. – Настройка общих параметров среды

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

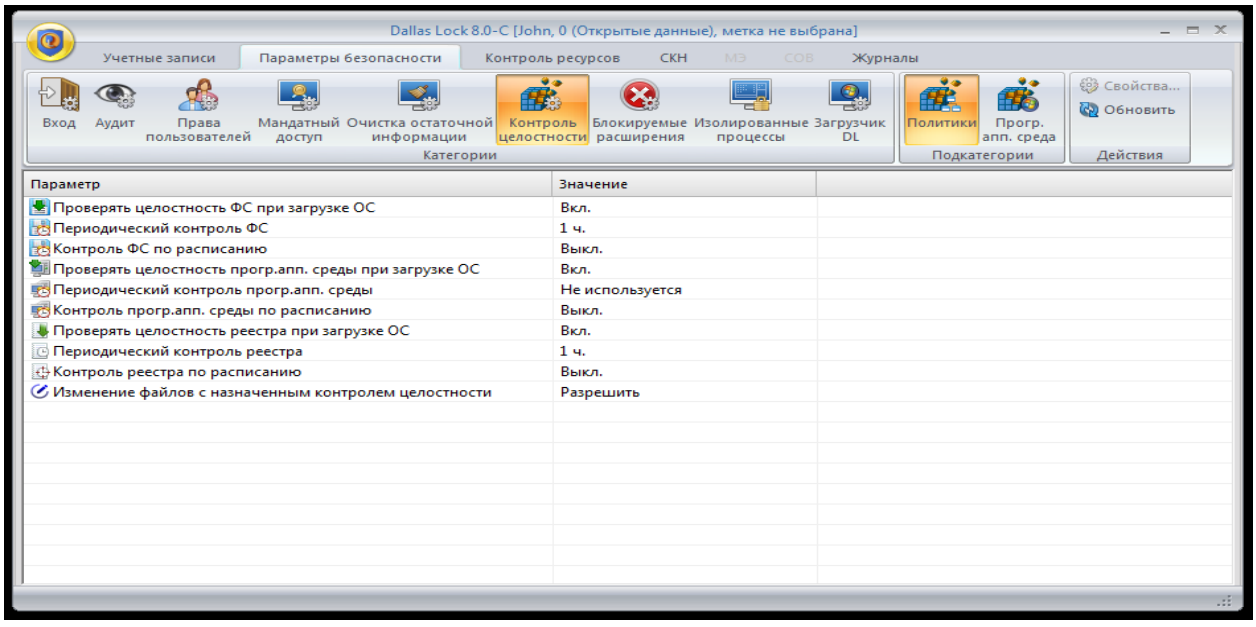

Рисунок А.35. – Результат изменения параметра

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

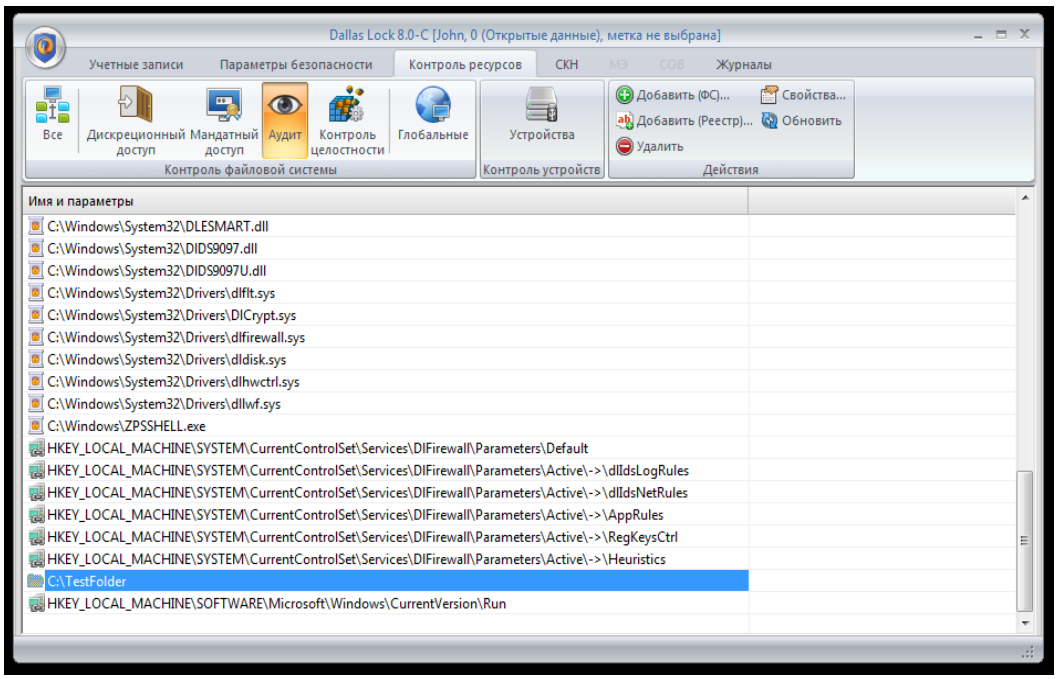

Рисунок А.36. – Выбор объекта для настройки контроля целостности

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.).

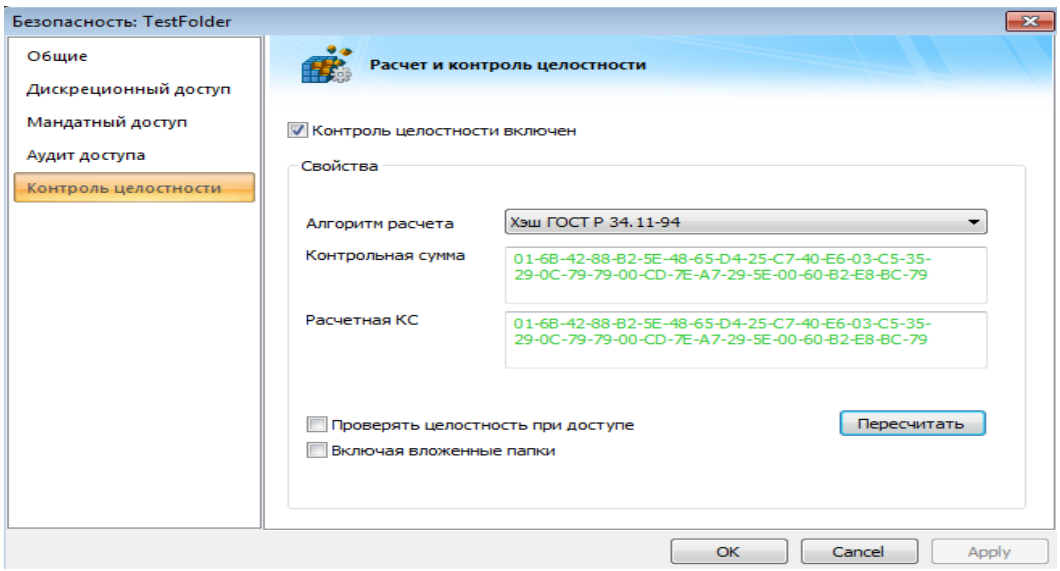

Рисунок А.37. – Настройка контроля целостности для директории

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

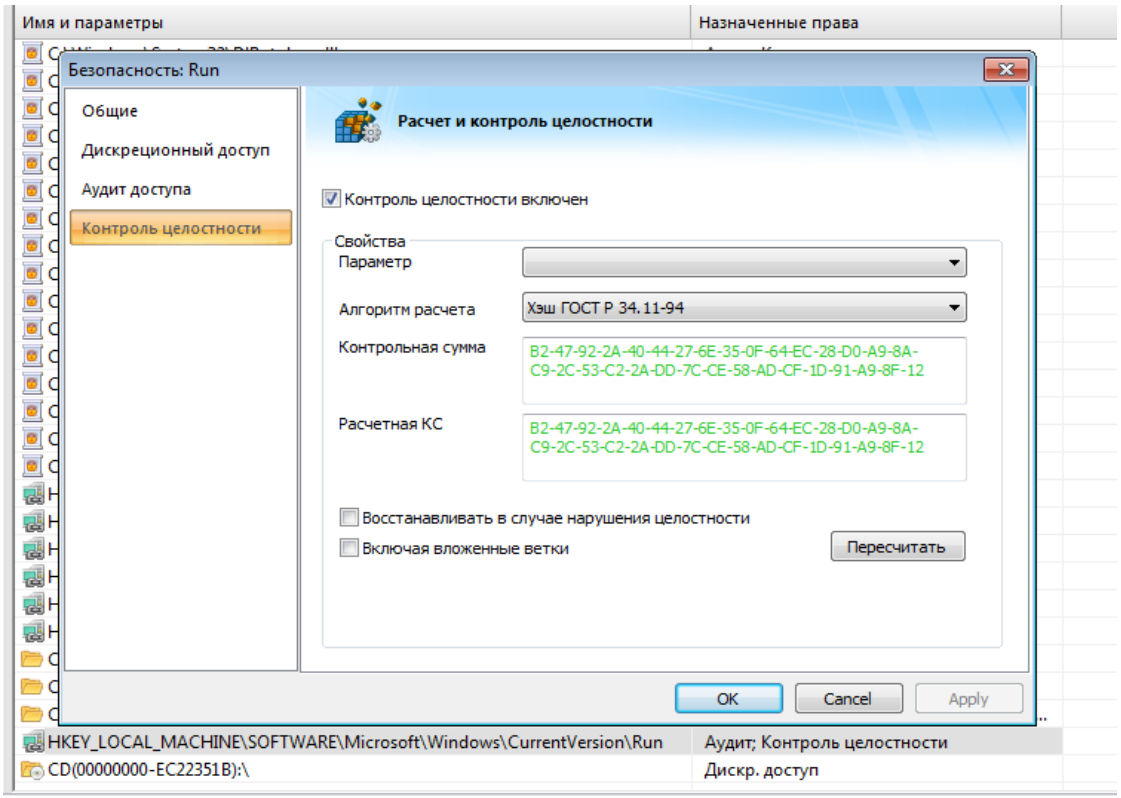

Рисунок А.38. – Настройка контроля целостности для регистра

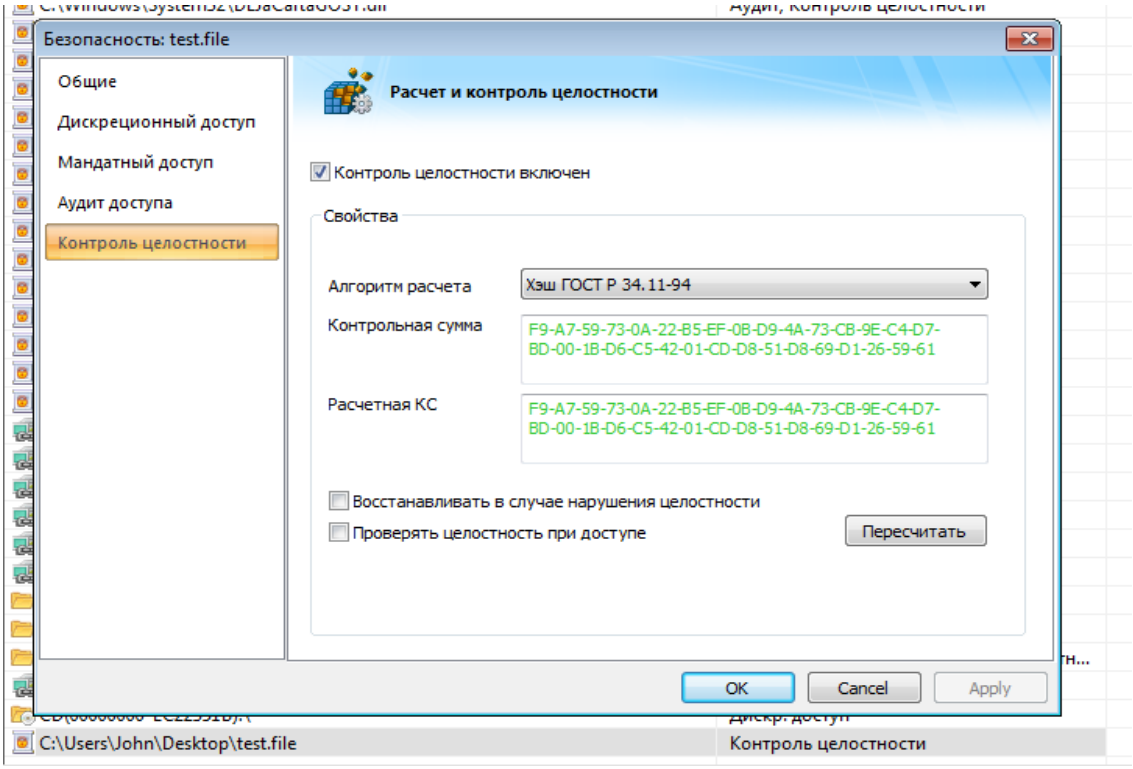

Рисунок А.39. – Настройка контроля целостности для файла

Настройка прав разграничения доступа для внешних носителей информации

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

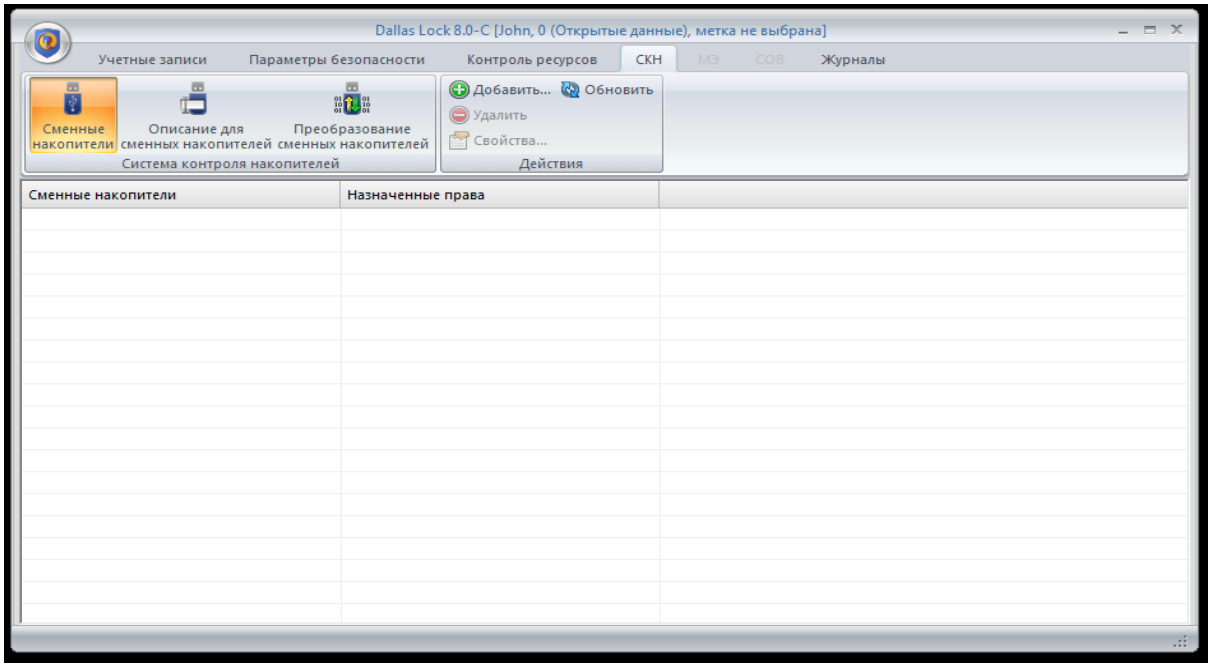

Рисунок А.40. – Окно настроек сменных накопителей

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

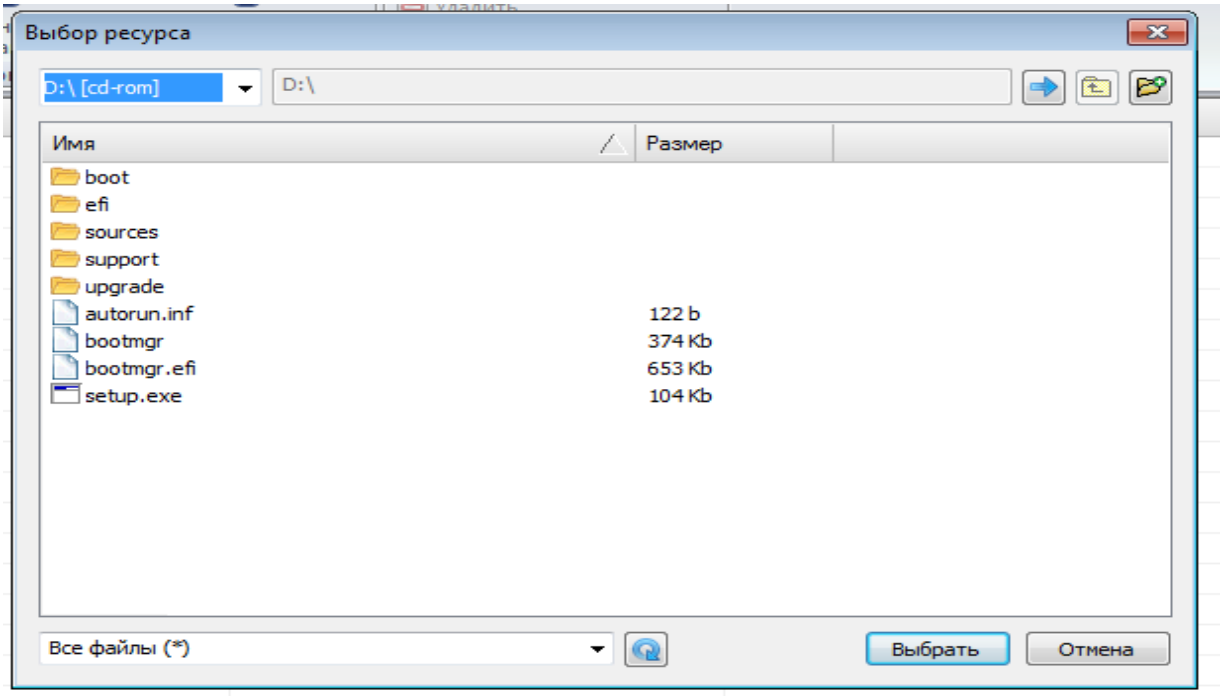

Рисунок А.41. – Выбор внешнего носителя

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

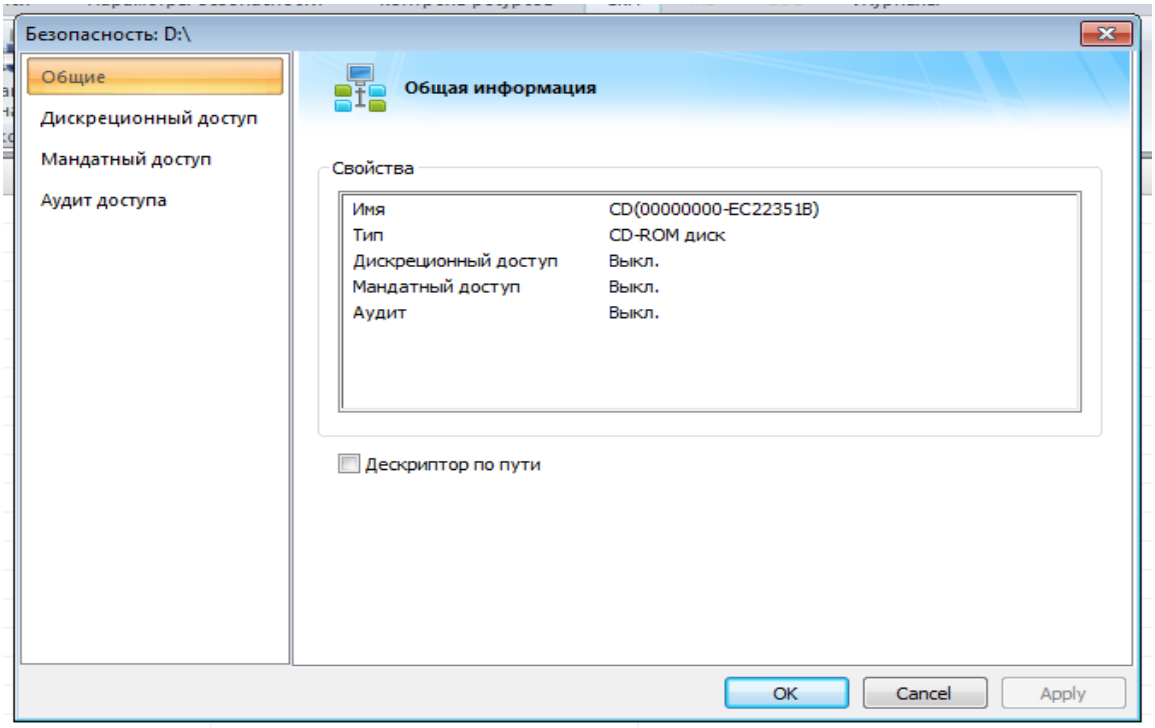

Рисунок А.42. – Окно настройки безопасности внешнего носителя

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

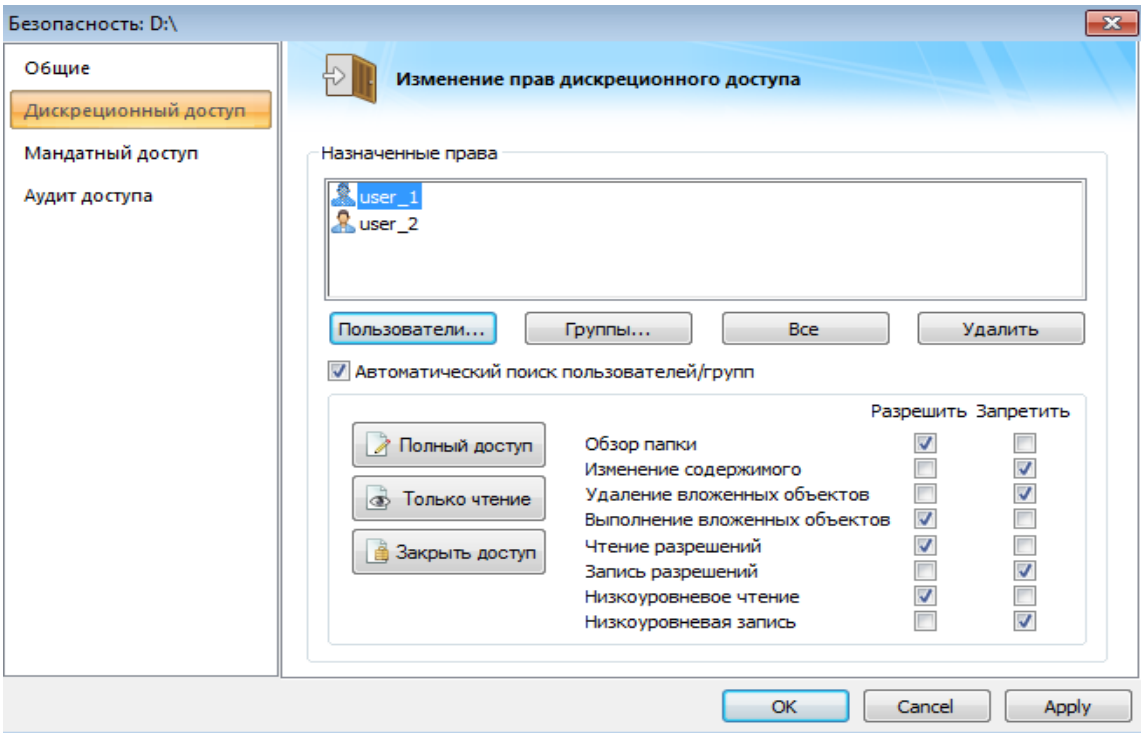

Рисунок А.43. – Настройка для пользователя «user_1»

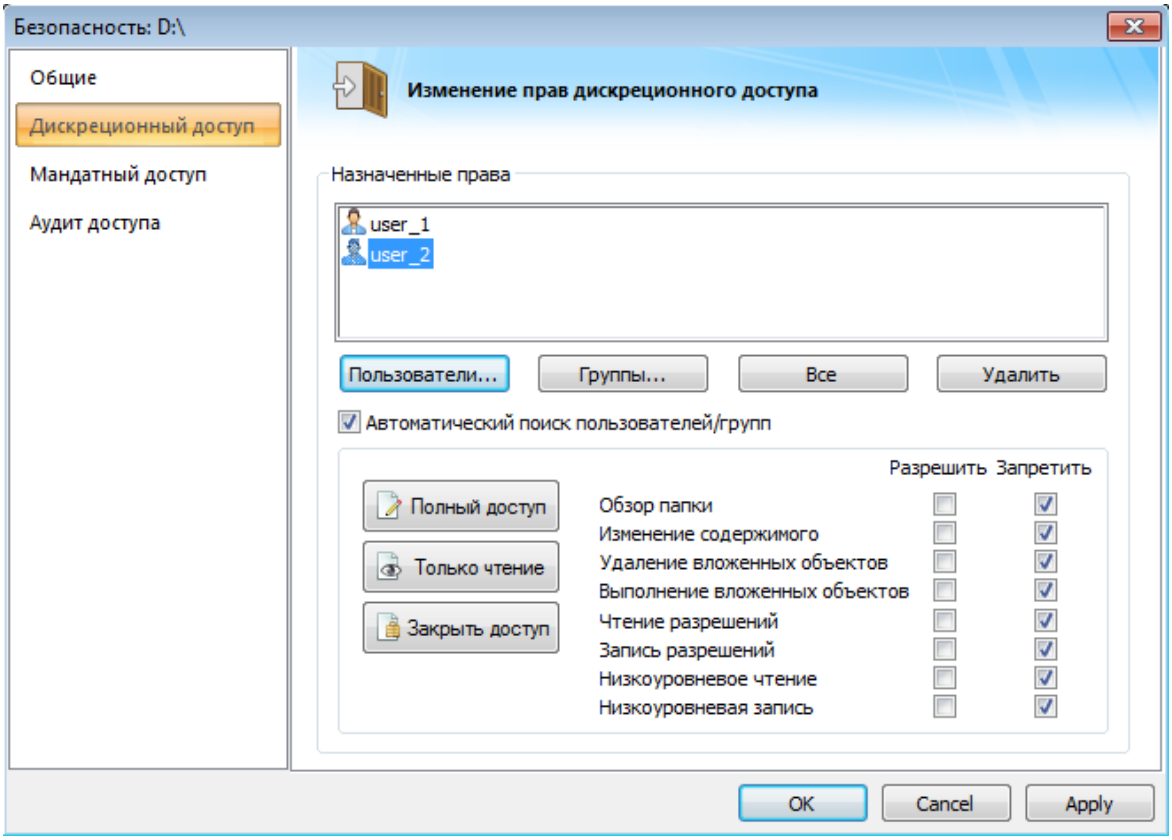

Рисунок А.43. – Настройка для пользователя «user_2»

Результат добавление дискреционного доступа для сменного накопителя (см. рисунок А.44.).

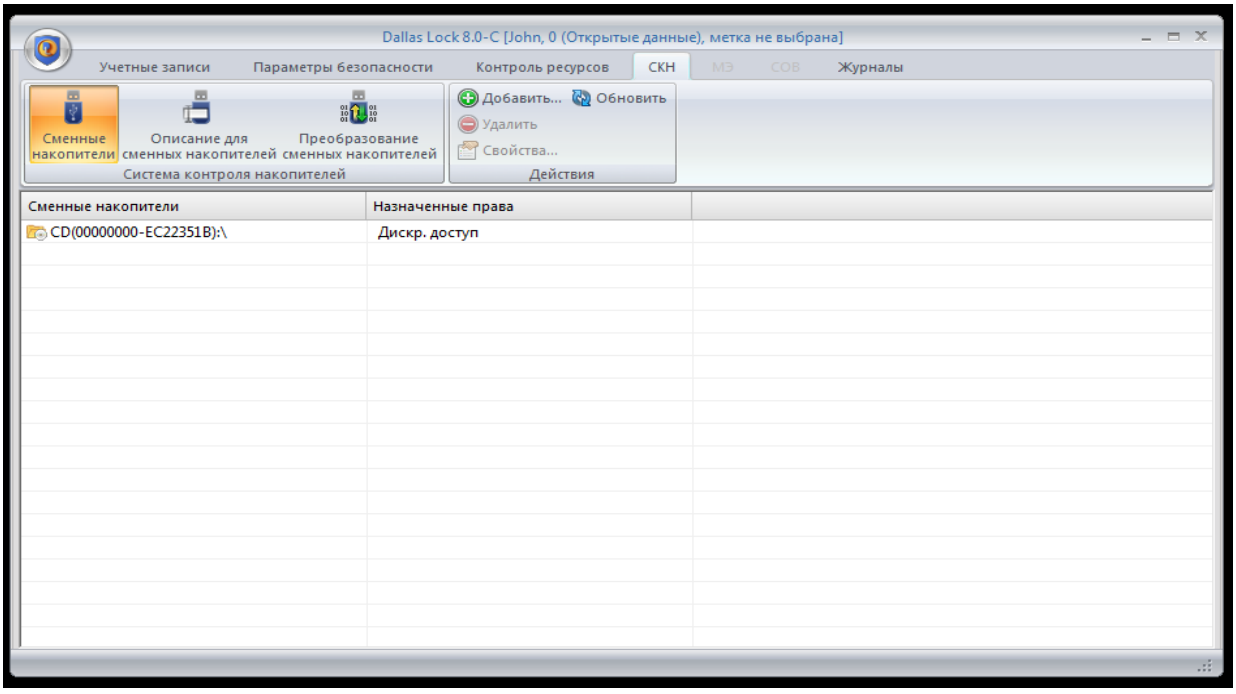

Рисунок А.44. – Результат добавления настройки

Проверка настроек

Зашли в user_1 (см. рисунок А.45.).:

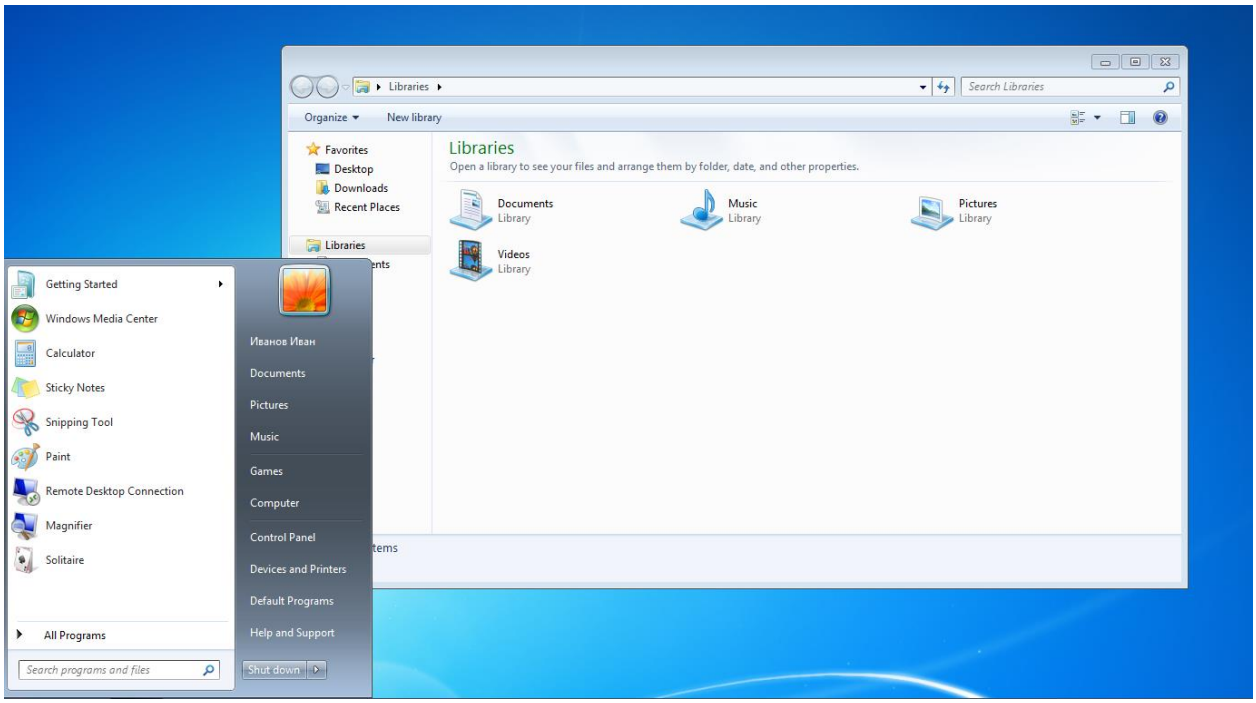

Рисунок А.45. – Вход в систему от лица «user_1»

Попытка записи в защищенную папку «TestFolder» (см. рисунок А.46.).

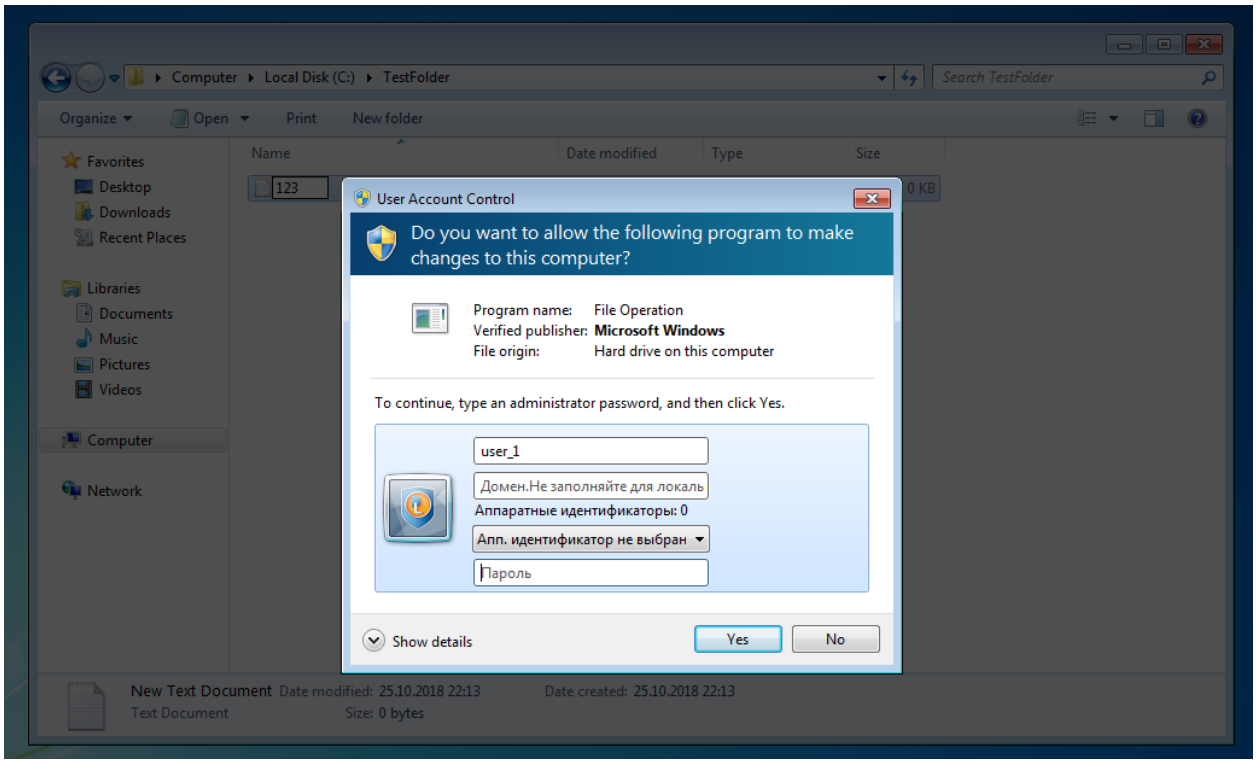

Рисунок А.46. – Попытка записи

Результат выполнения операции – ошибка записи (см. рисунок А.47.).

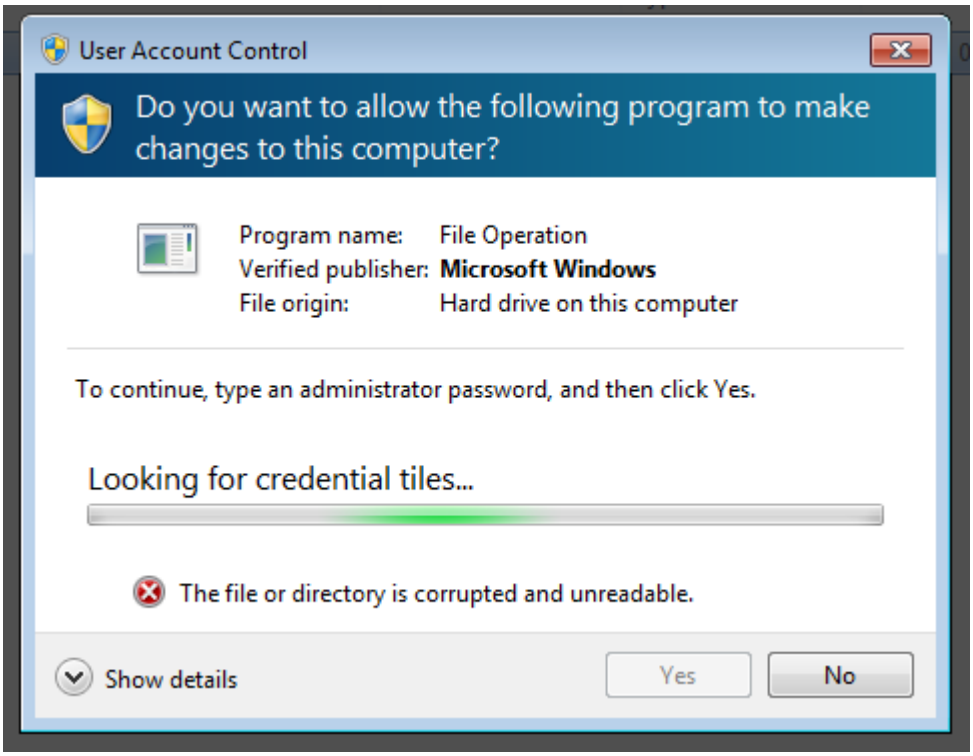

Рисунок А.47. – Результат выполнения операции

Аналогичная попытка записи, с использованием учетной записи администратора безопасности (см. рисунок А.48.).

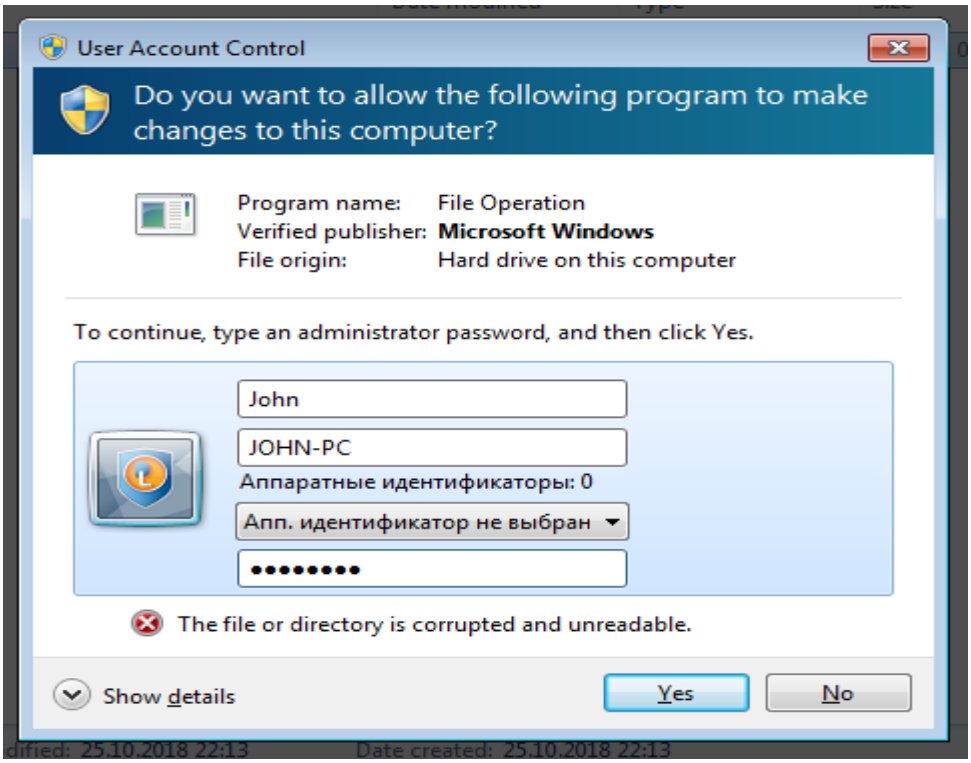

Рисунок А.48. – Повторная попытка с использованием прав администратора безопасности

Получилось создать файл (см. рисунок А.49.).

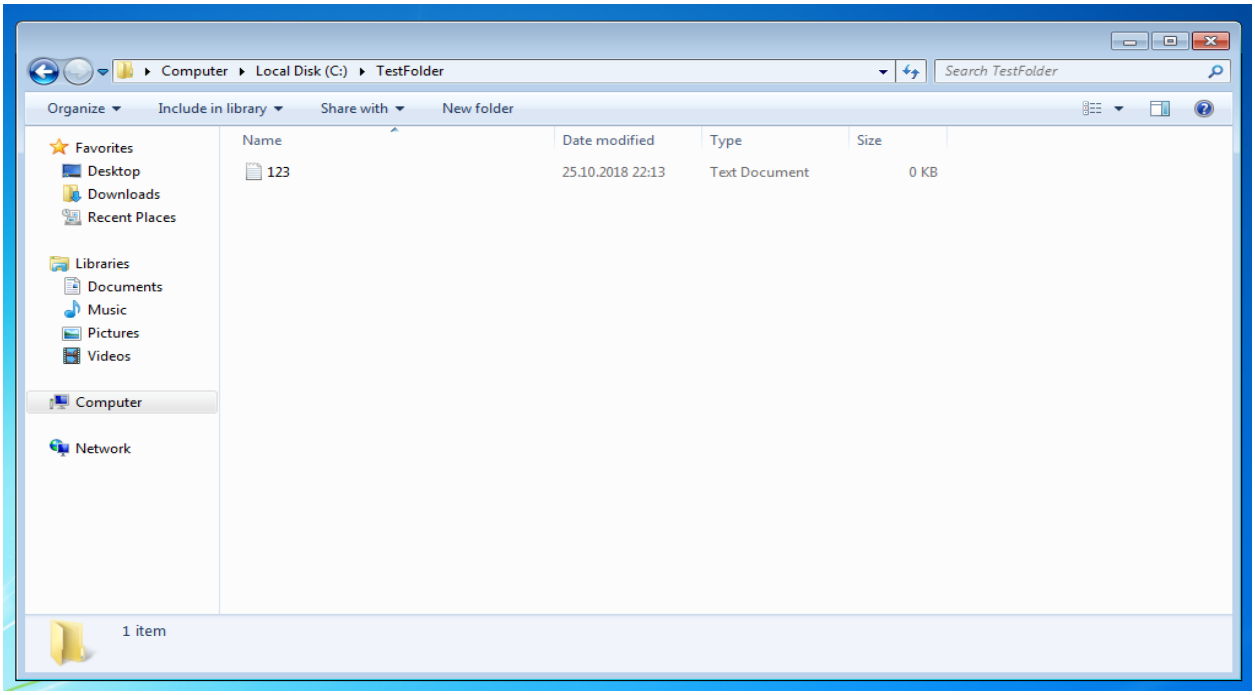

Рисунок А.49. – Созданный файл

Уведомления об нарушение целостности контролируемого ресурса (см. рисунок А.50.).

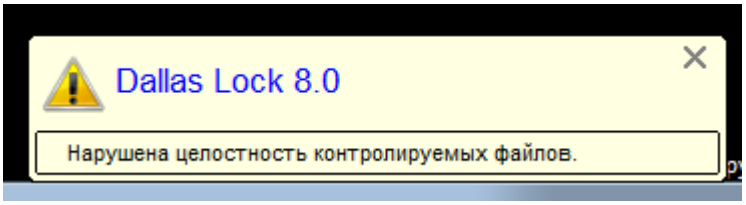

Рисунок А.50. – Уведомление о нарушение целостности папки

Запись в журнале о попытке нарушения целостности отслеживаемого объекта (см. рисунок А.51.)

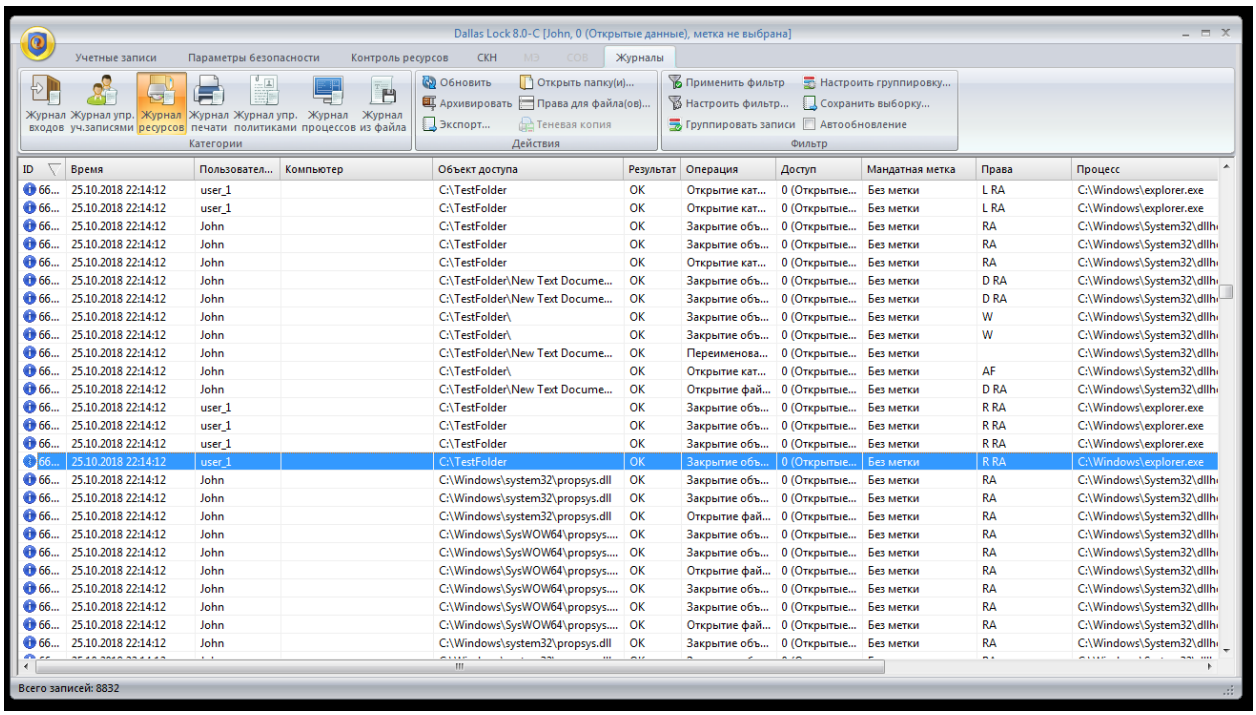

Рисунок А.51. – Журнал ресурсов

Запись в журнале входов о нарушении целостности (см. рисунок А.52.).

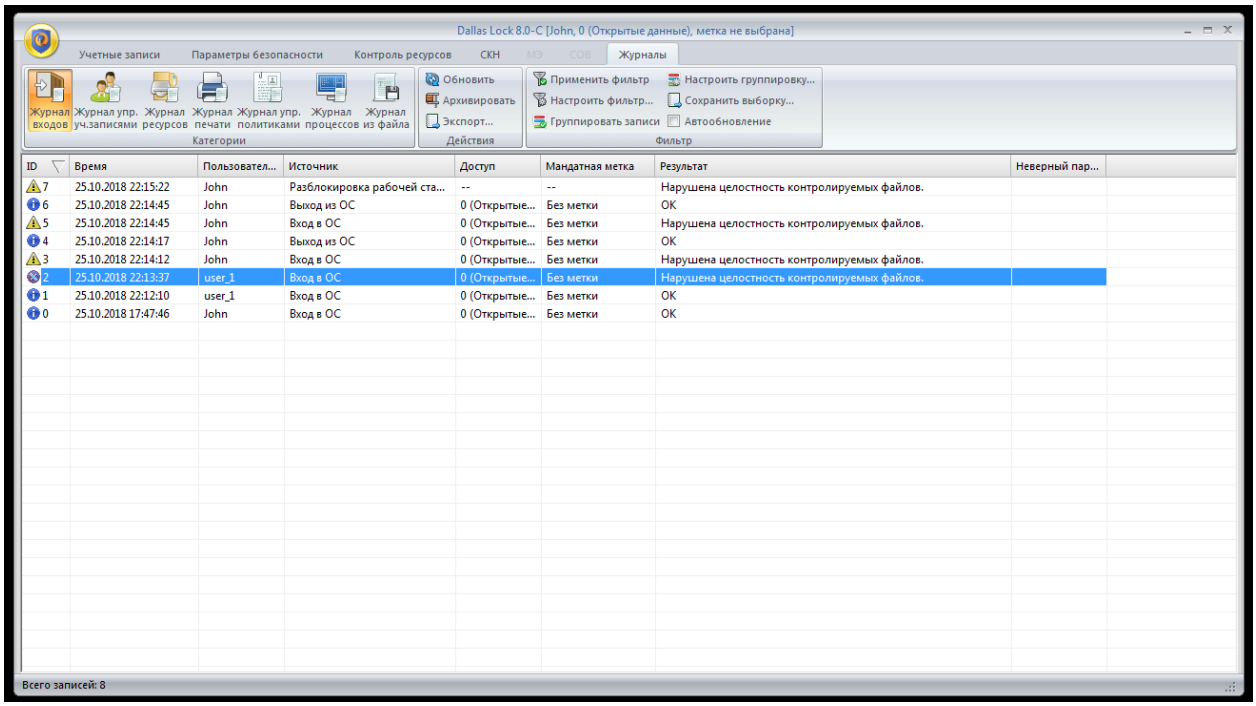

Рисунок А.52. – Журнал входов

Блокирование пользователя «user_2» (см. рисунок А.53.)

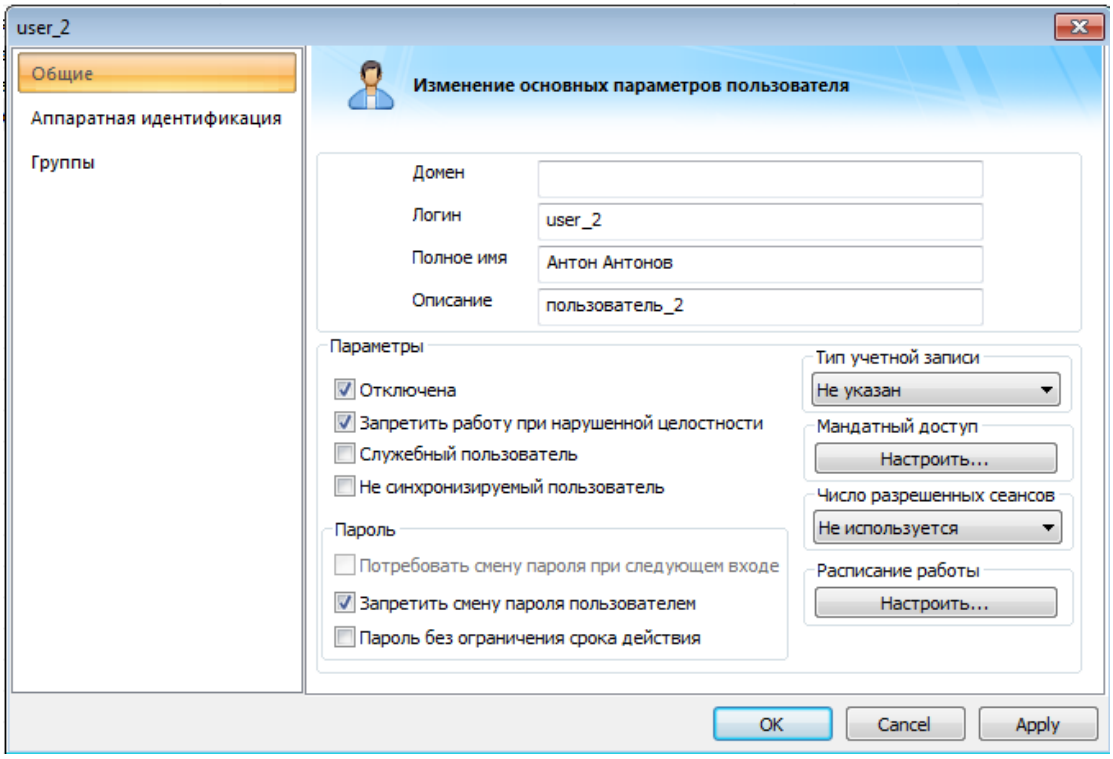

Рисунок А.53. – Блокировка учетной записи «user_2»

Попытка входа от лица заблокированной учетной записи (см. рисунок А.54.).

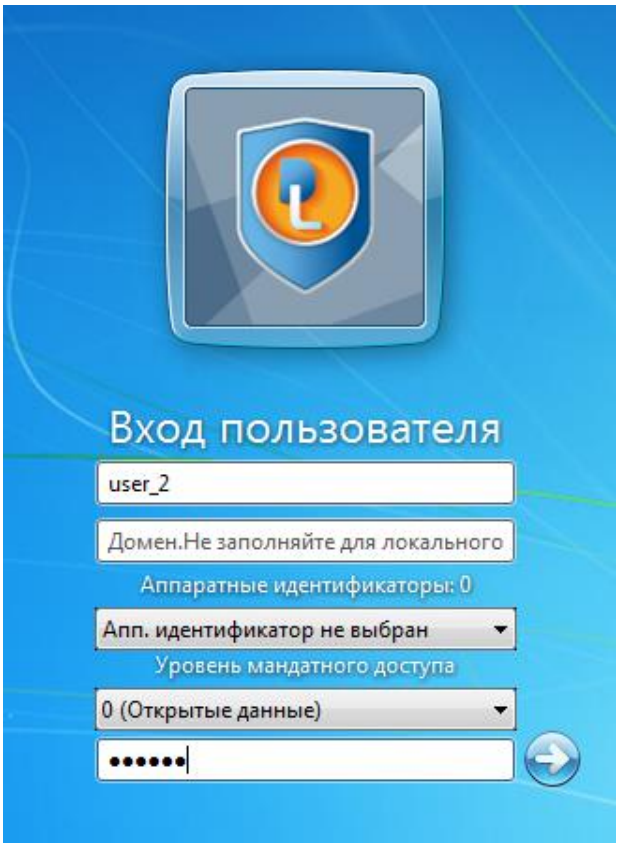

Рисунок А.54. – Попытка входа от лица заблокированной записи

Результат попытки (см. рисунок А.55.).

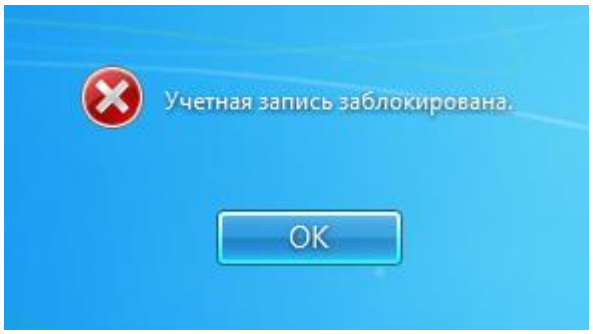

Рисунок А.55. – Результат входа с заблокированной записи

Многократные попытки входа в учетную запись с использованием неверного пароля (см. рисунок А.56.).

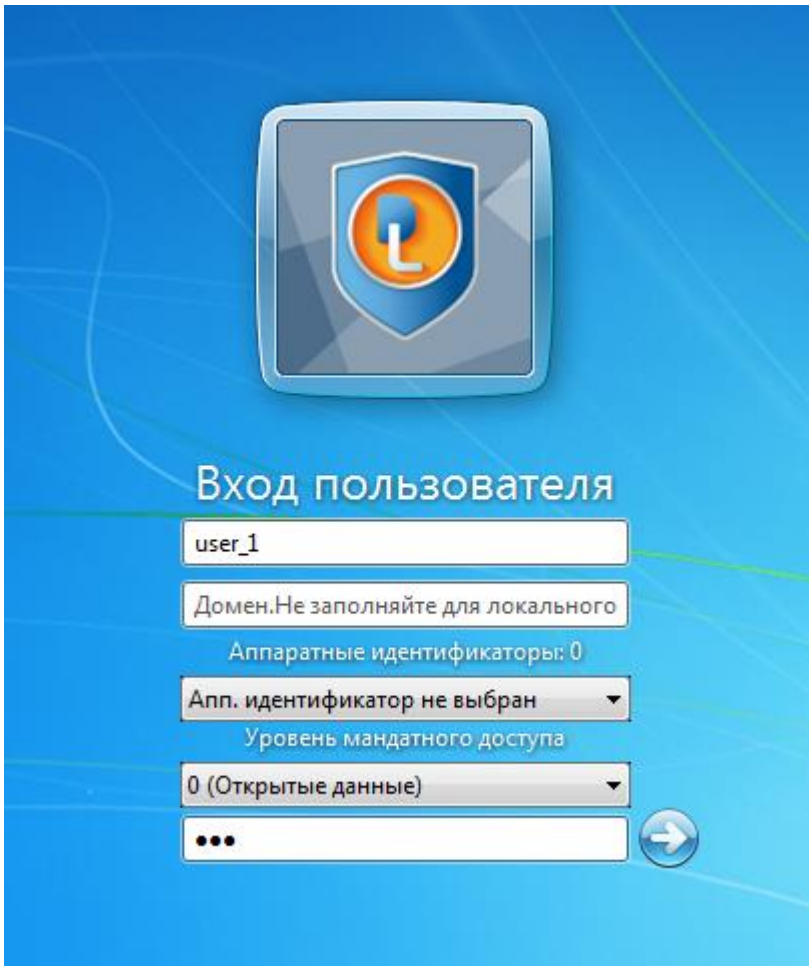

Рисунок А.56. – Вход в учетную запись «user_1» с неправильным паролем

Результат – учетная запись заблокирована из-за превышения допустимого количества попыток (см. рисунок А.57.).

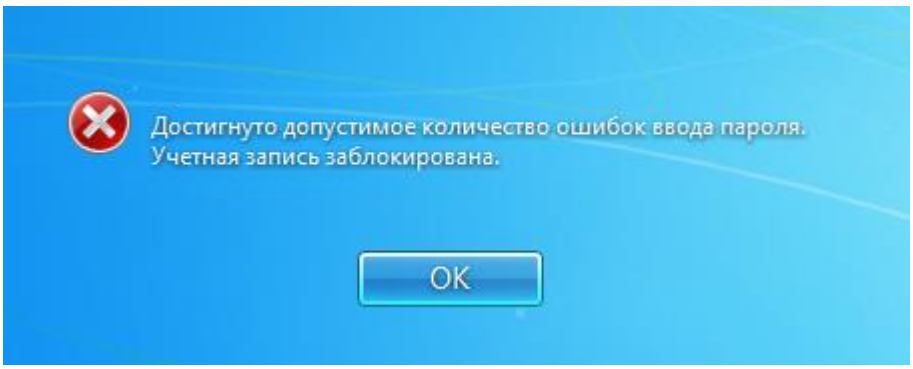

Рисунок А.57. – Блокировка записи

Записи о вышеперечисленных попытках входа отражены в журнале (см. рисунок А.58.).

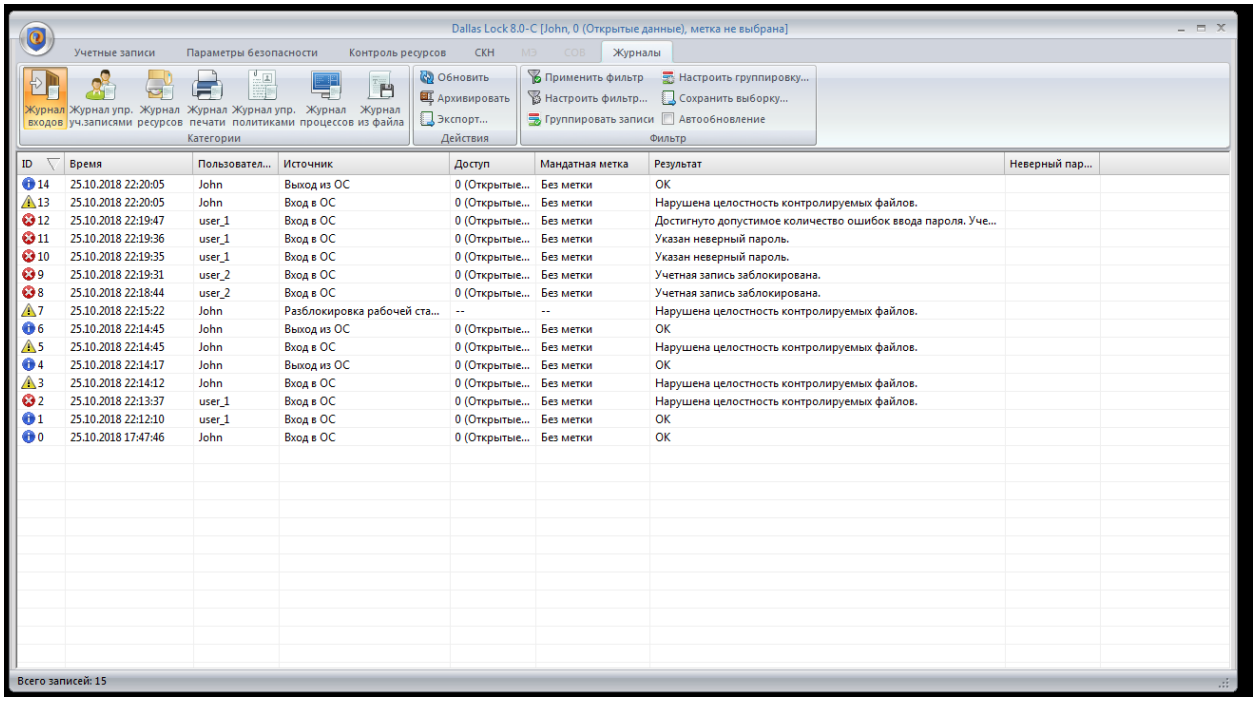

Рисунок А.58. – Записи в журнале входов

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 ПО 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. и Б.2.. СЗИ «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».

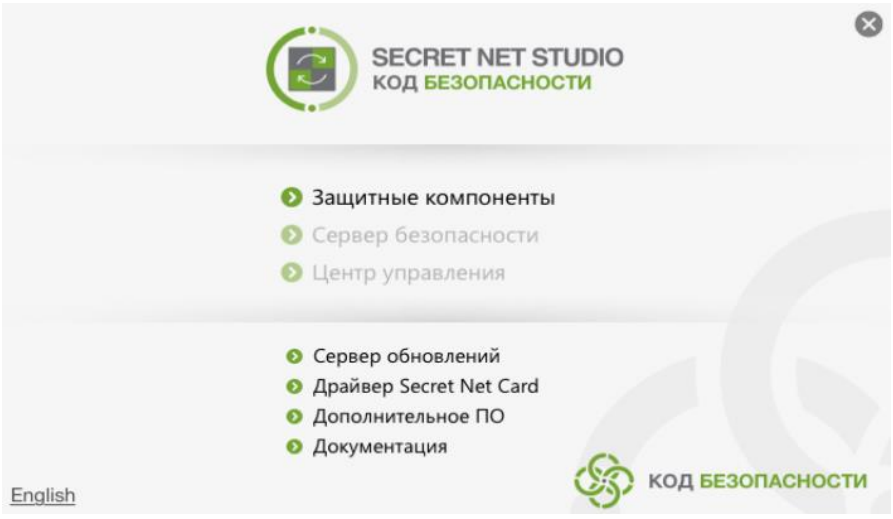

Рисунок Б.1. – Запуск «Secret Net Studio»

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

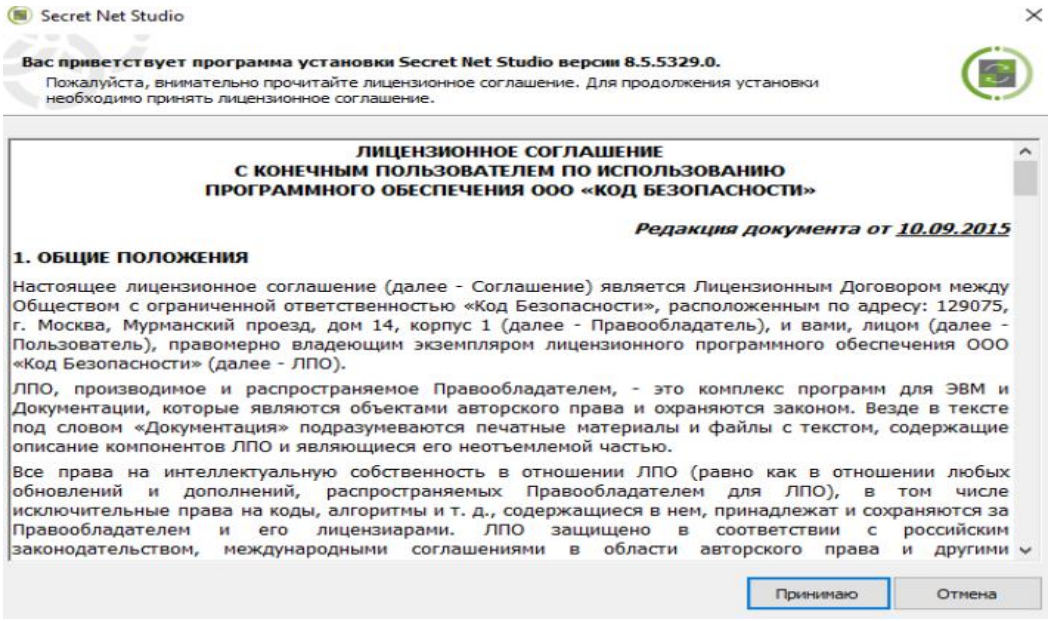

Рисунок Б.2. – Лицензионное соглашение

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.

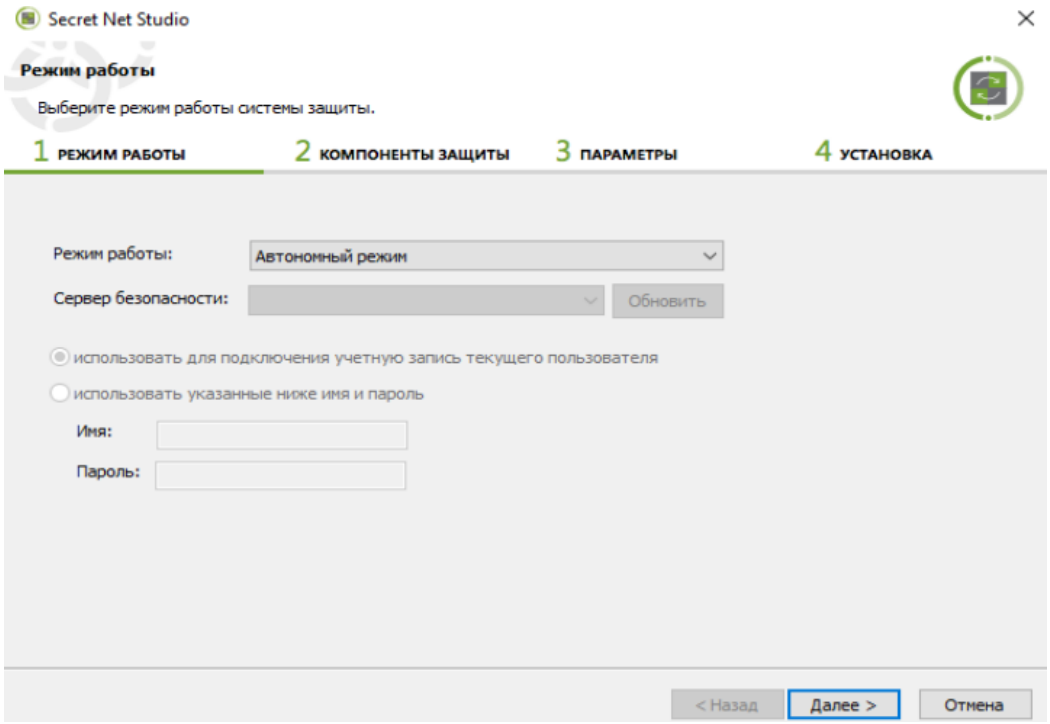

Рисунок Б.3. – Выбор режима работы

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

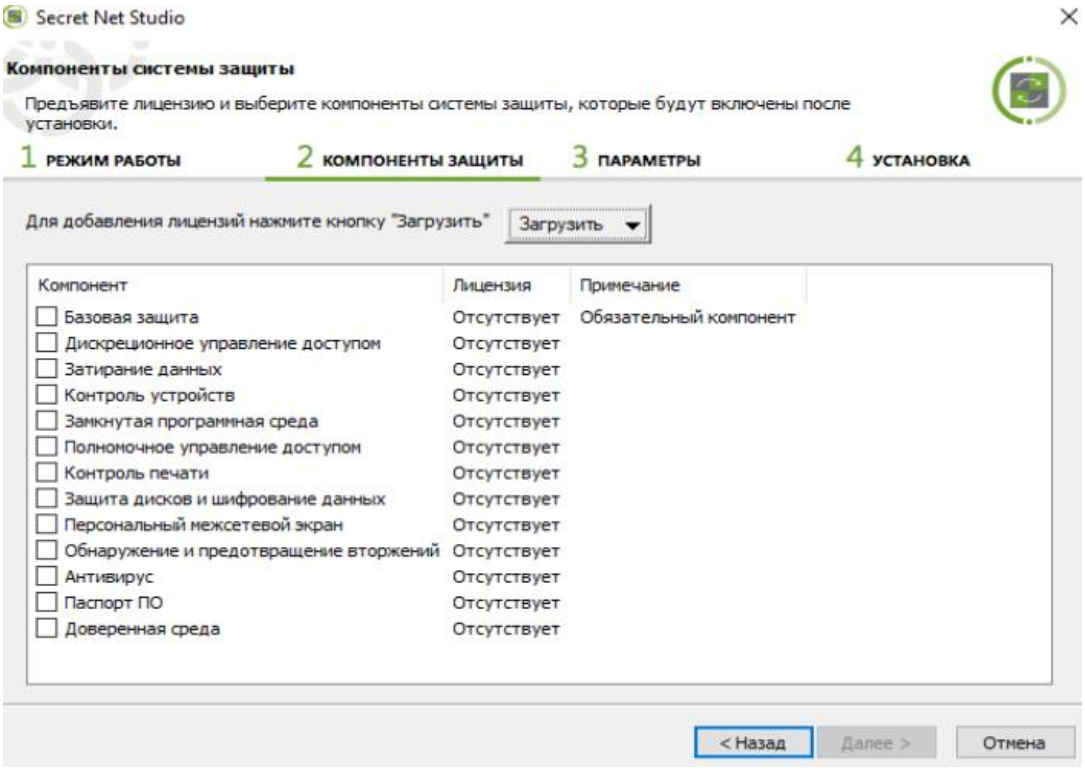

Рисунок Б.4. – Окно выбора компонентов защиты

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

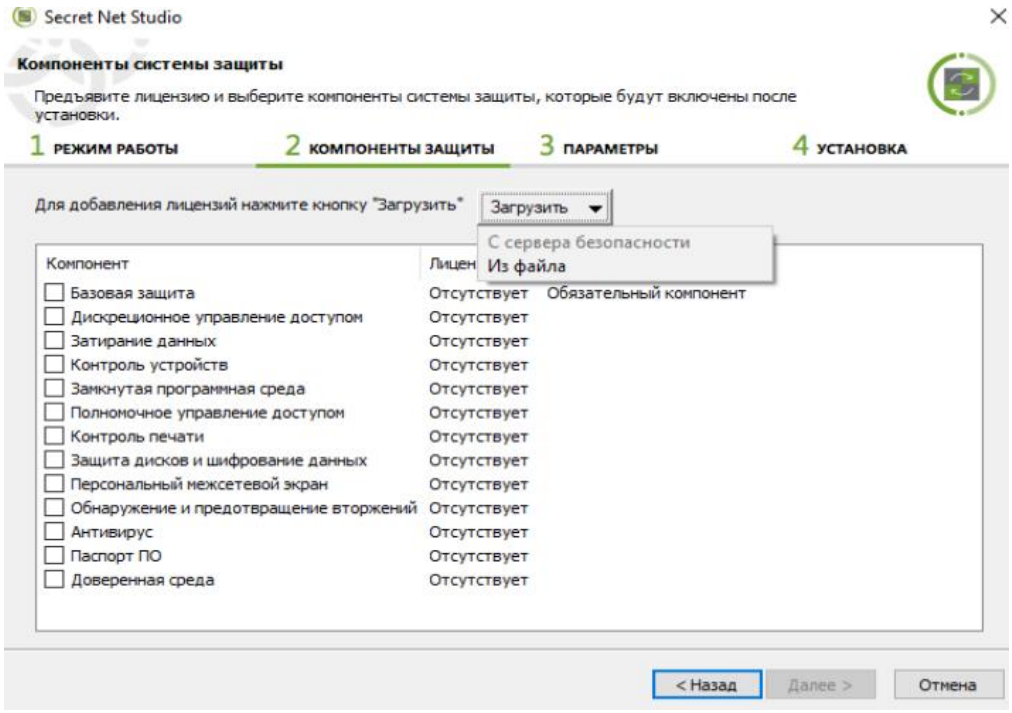

Рисунок Б.5. – Загрузка ключа (лицензии)

Выберите нужный файл в появившемся диалоге.

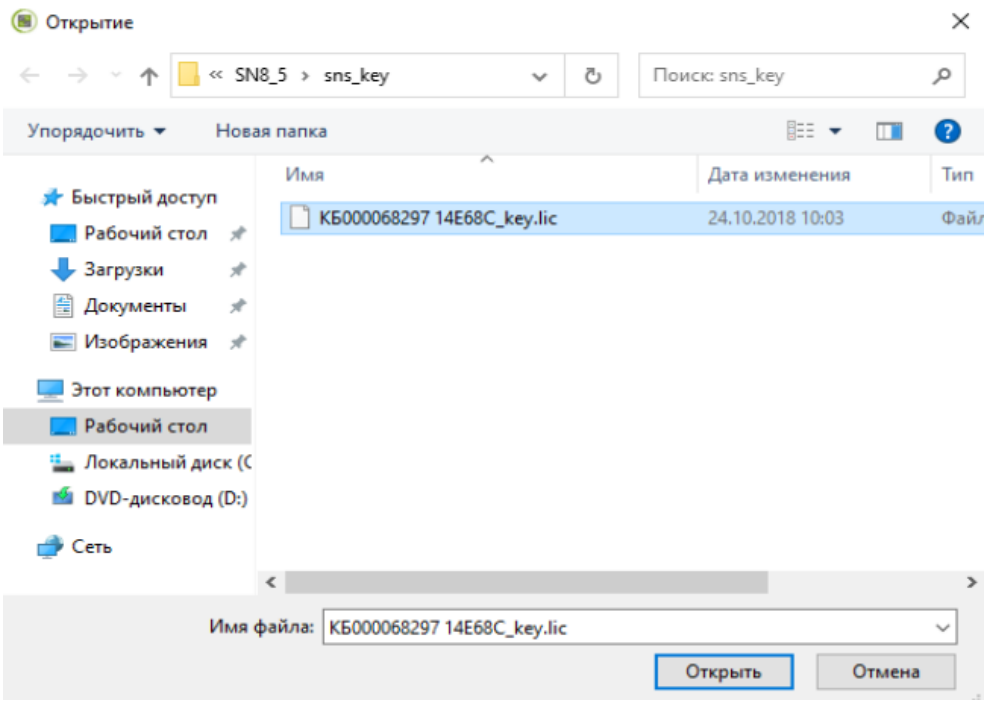

Рисунок Б.6. – Выбор файла для загрузки ключа

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.

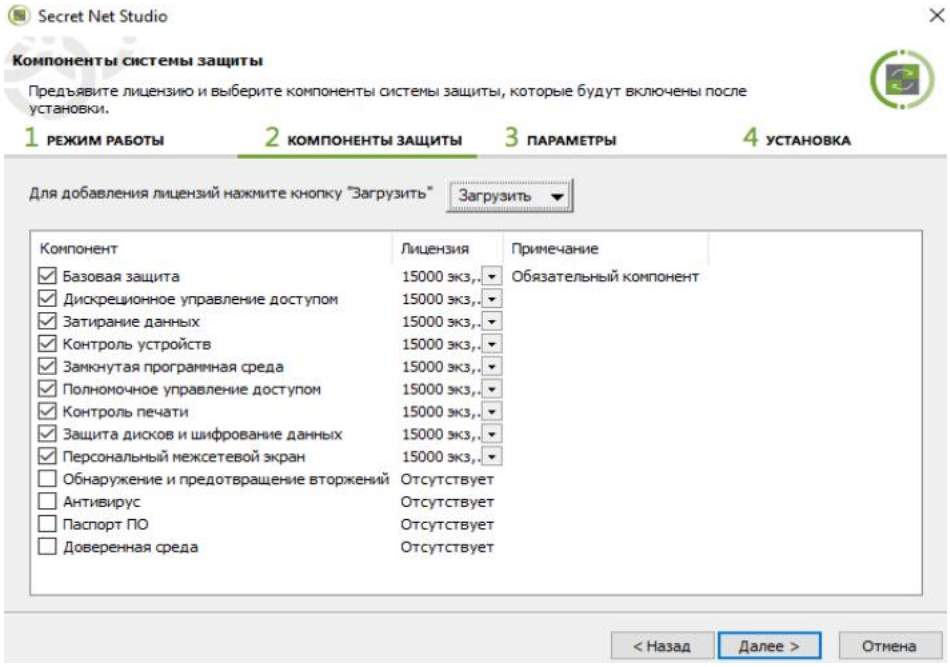

Рисунок Б.7. – Выбор компонентов защиты

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).

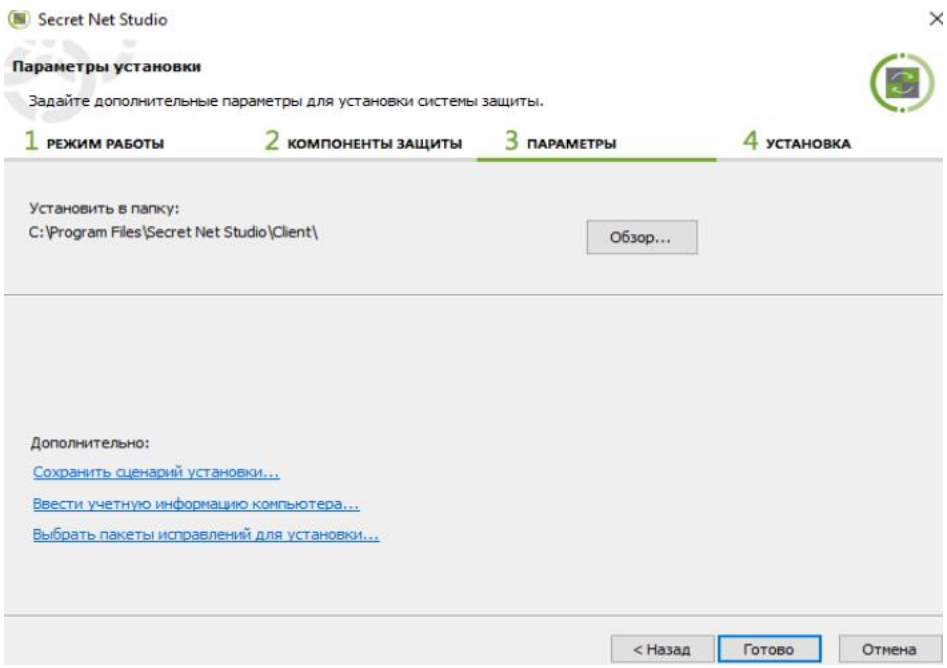

Рисунок Б.8. – Окно параметров установки

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

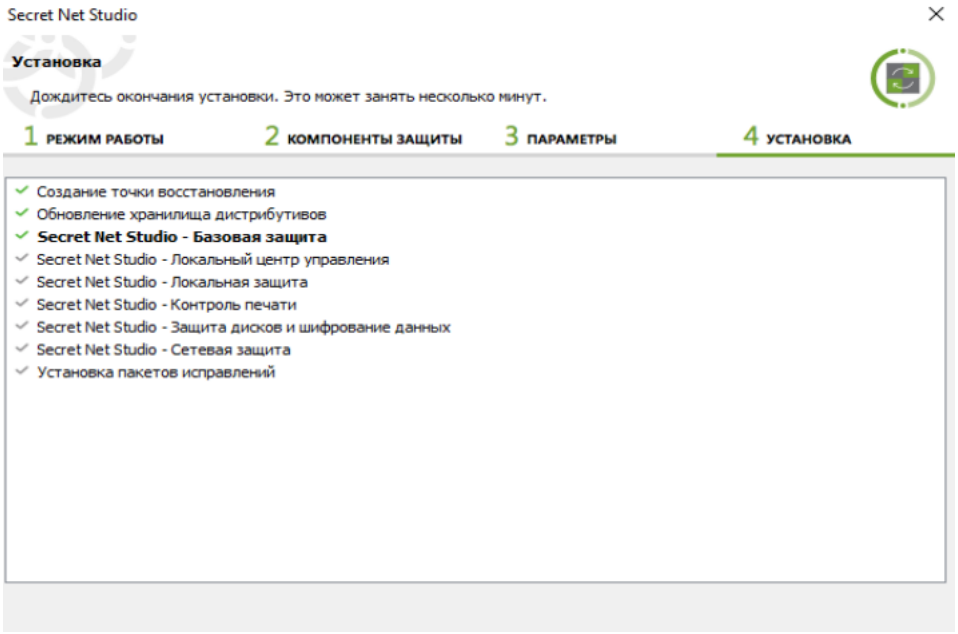

Рисунок Б.9. – Процесс установки

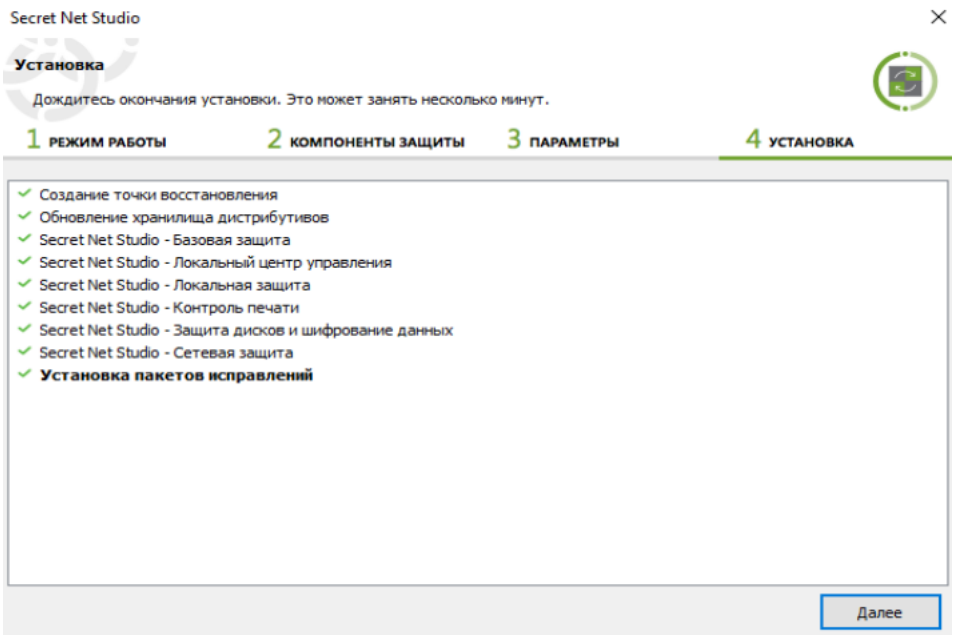

Рисунок Б.10. – Завершение процесса установки

На экране появится завершающий диалог со сведениями о выполненных операциях и предложением перезагрузить компьютер.

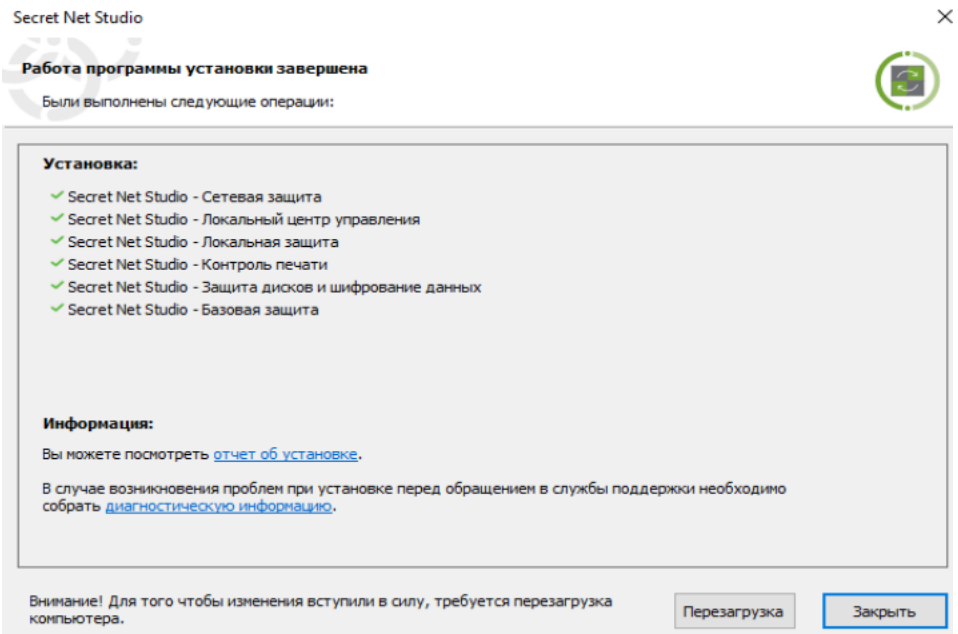

Рисунок Б.11. – Окно завершения установки

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.

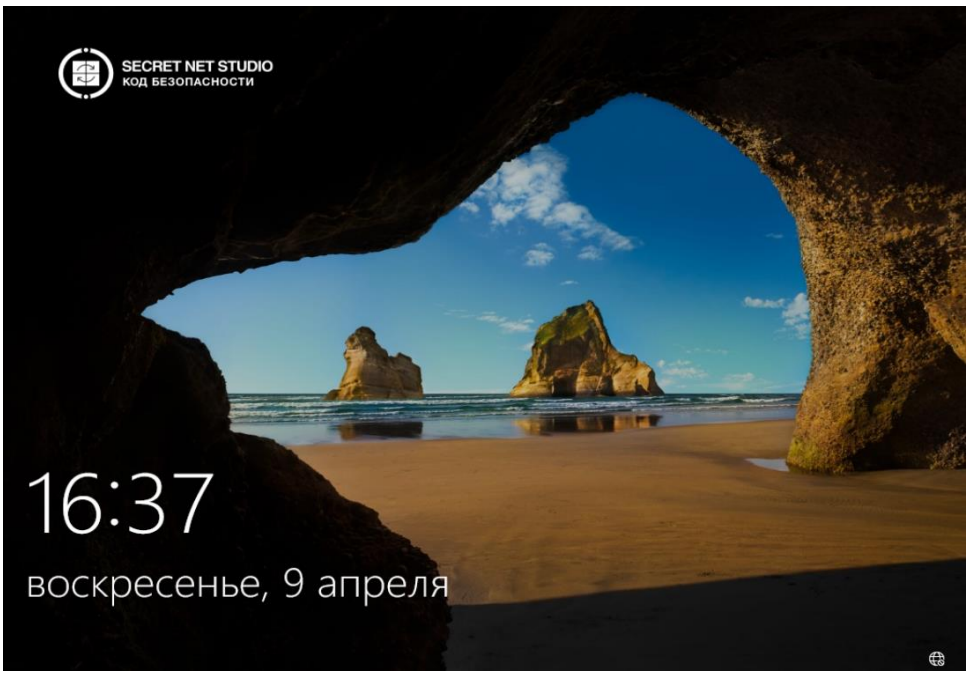

Рисунок Б.12. – Экран блокировки после установки «Secret Net»

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.

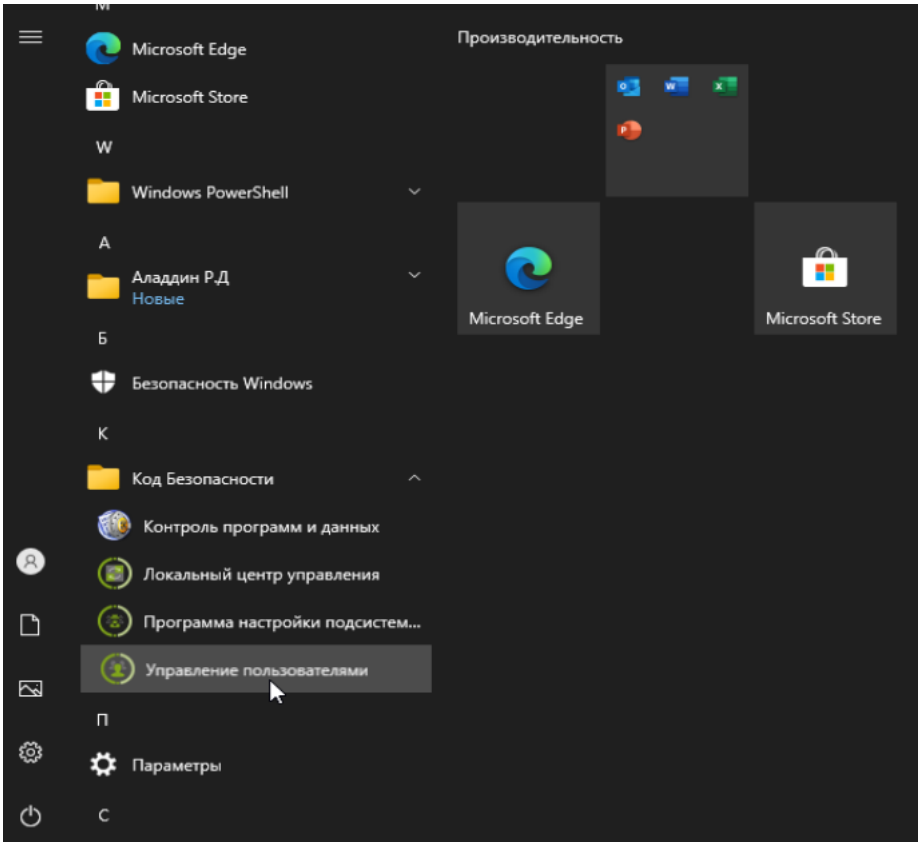

Рисунок Б.13. – Меню «Пуск», управление пользователями

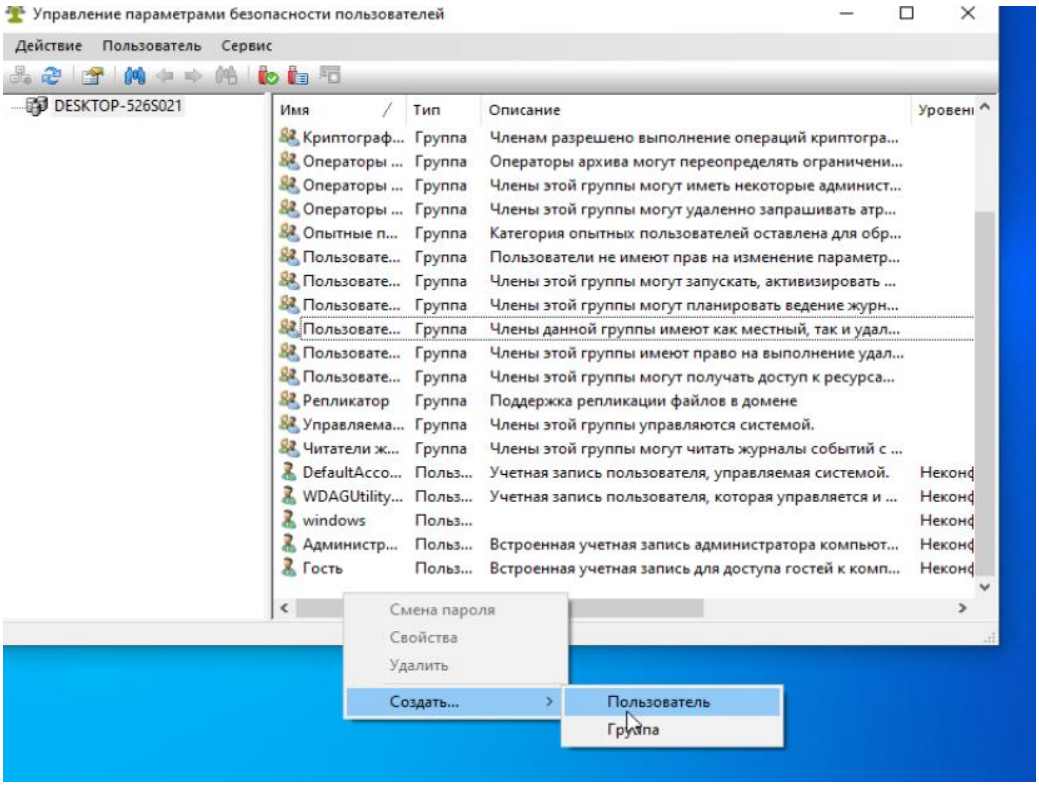

Рисунок Б.14. – Окно управления параметрами безопасности пользователей

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.

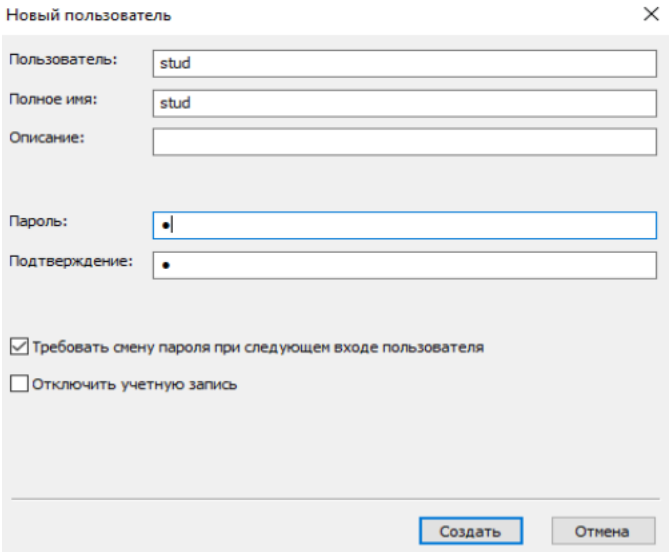

Рисунок Б.15. – Окно добавления пользователя

Для добавленного пользователя произвести смену пароля.

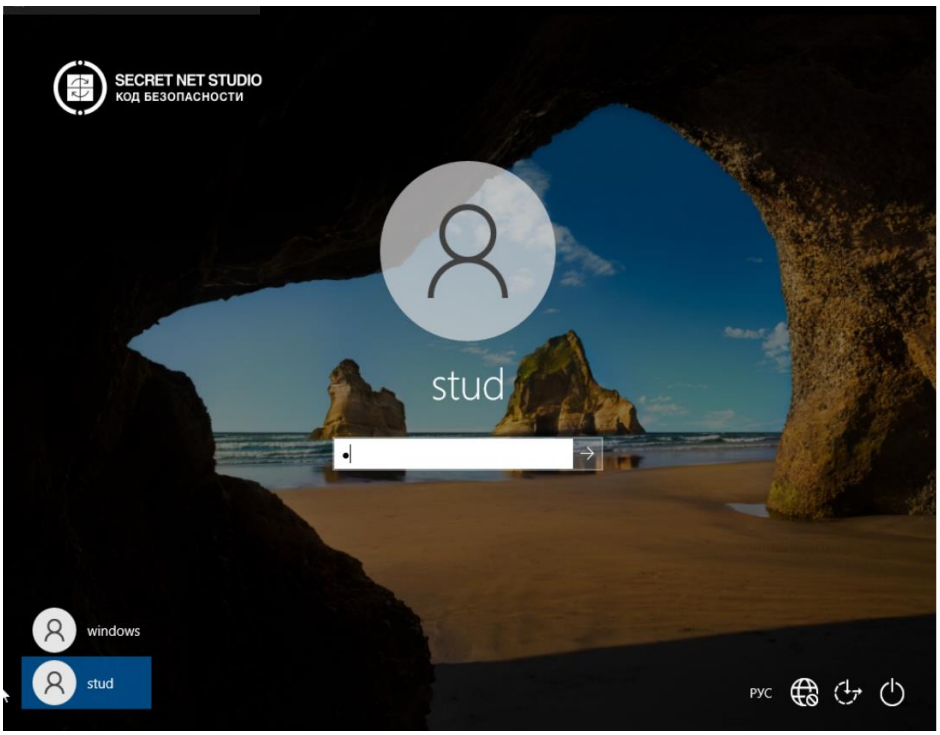

Рисунок Б.16. – Вход от лица добавленного пользователя

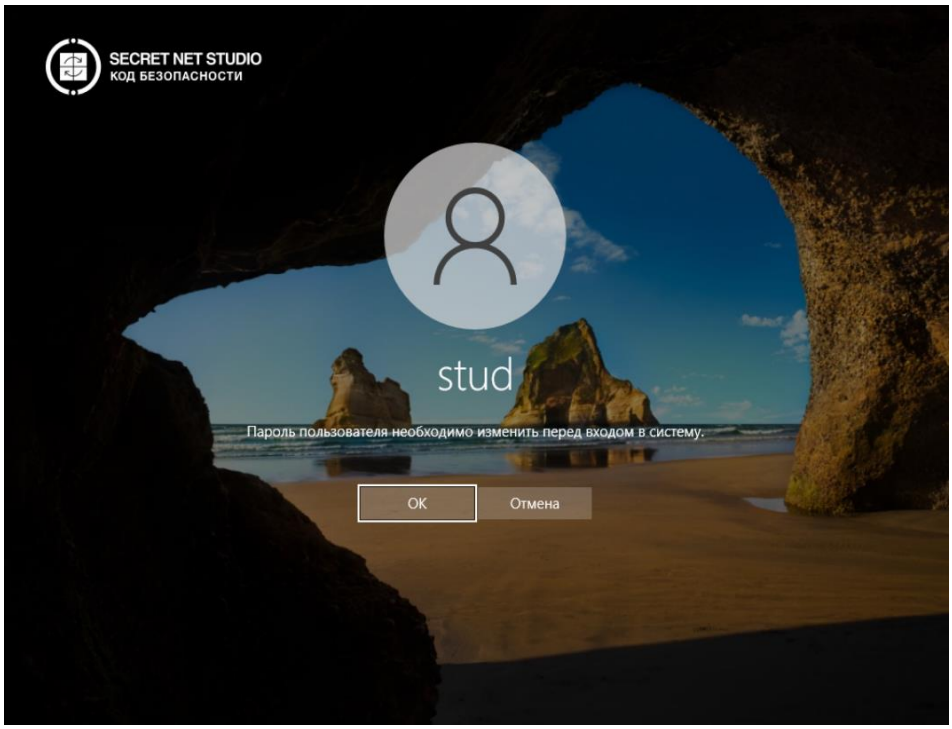

Рисунок Б.17. – Сообщение о требовании изменения пароля

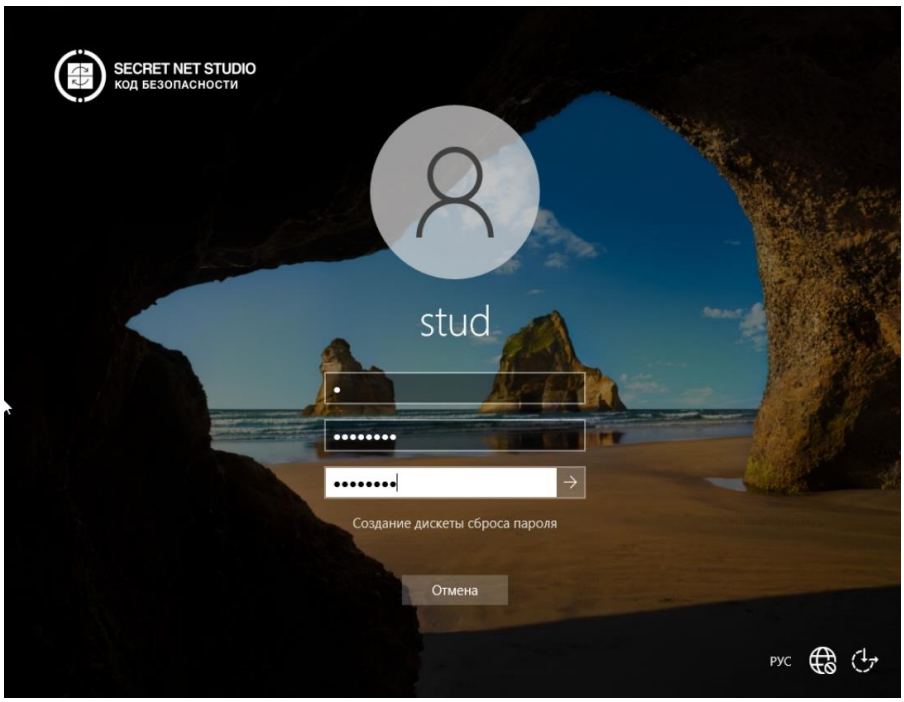

Рисунок Б.18. – Изменение пароля

Настройка Политик безопасности

1) Загрузите ОС 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.)

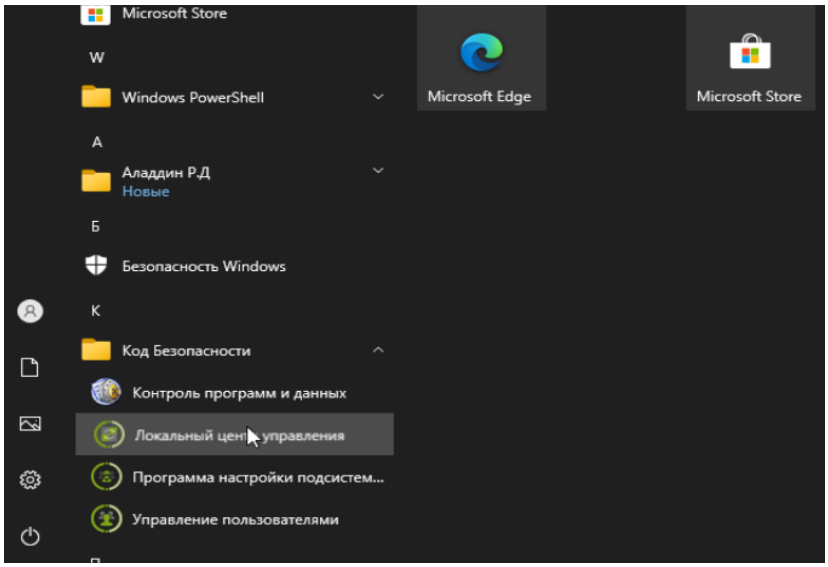

Рисунок Б.19. – Меню «Пуск», локальный центр управления

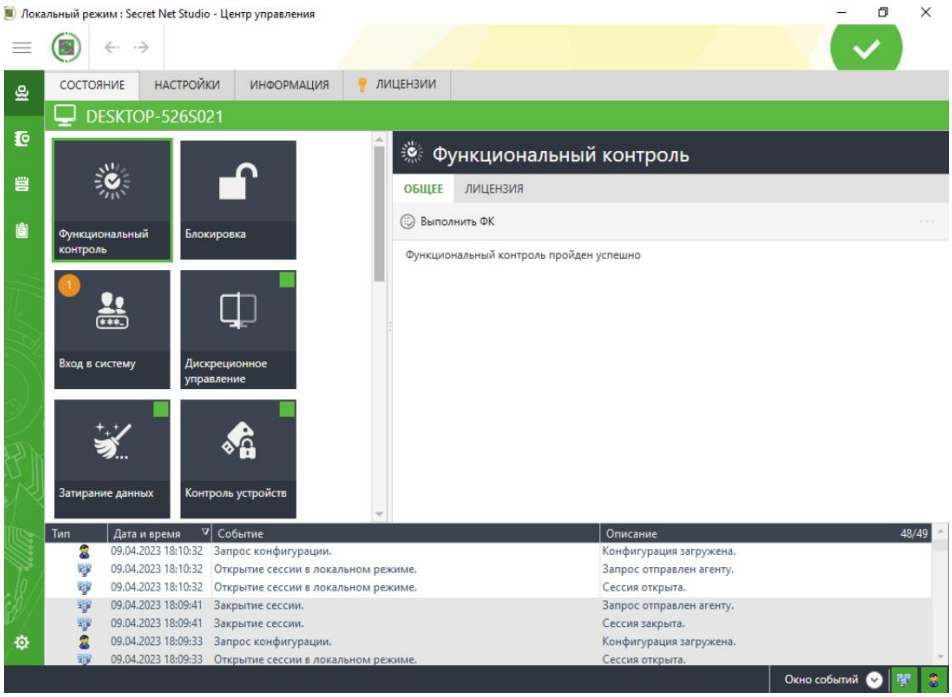

Рисунок Б.20. – Окно центра управления «Secret Net Studio»

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.).

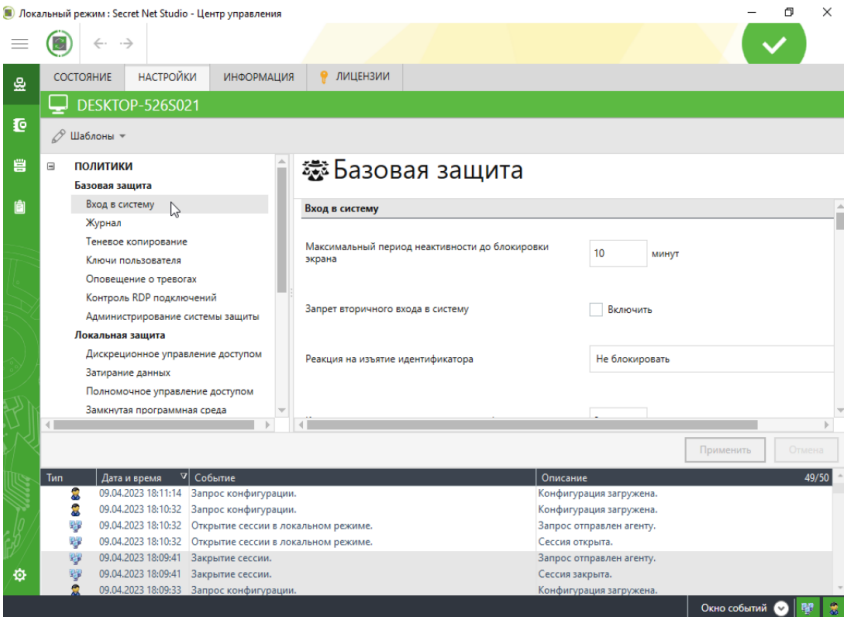

Рисунок Б.21. – Окно настройки

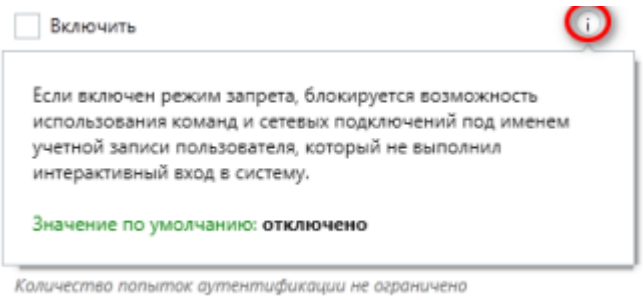

Рисунок Б.22. – Кнопка информация («i») в окне приложения

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», «Ключи пользователя», «Оповещение о тревогах», «Контроль RDP подключений», «Администрирование системы защиты») — объединяет параметры функционирования механизмов базовой защиты клиента. Перейдите в группу «Базовая защита» и выполните настройки в соответствии с заданием. Последовательная настройка модуля «Базовая 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

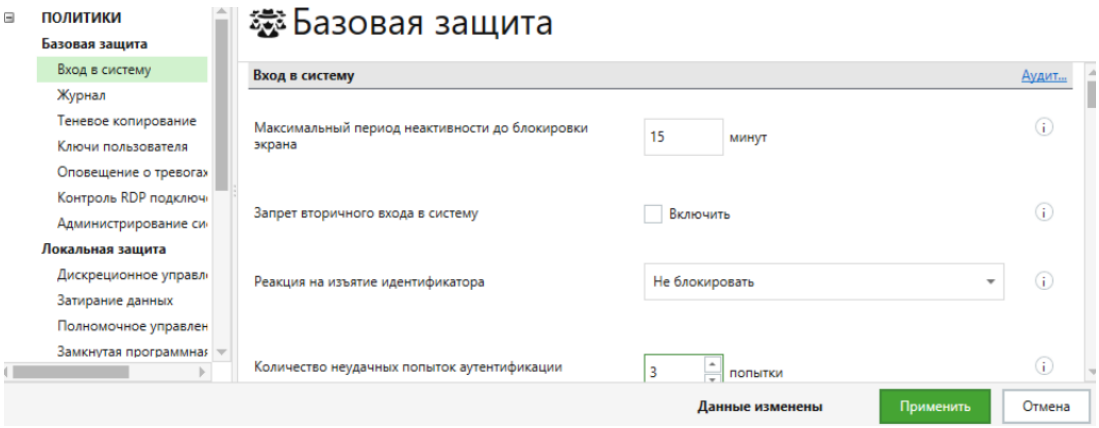

Рисунок Б.23. – Настройка входа в систему

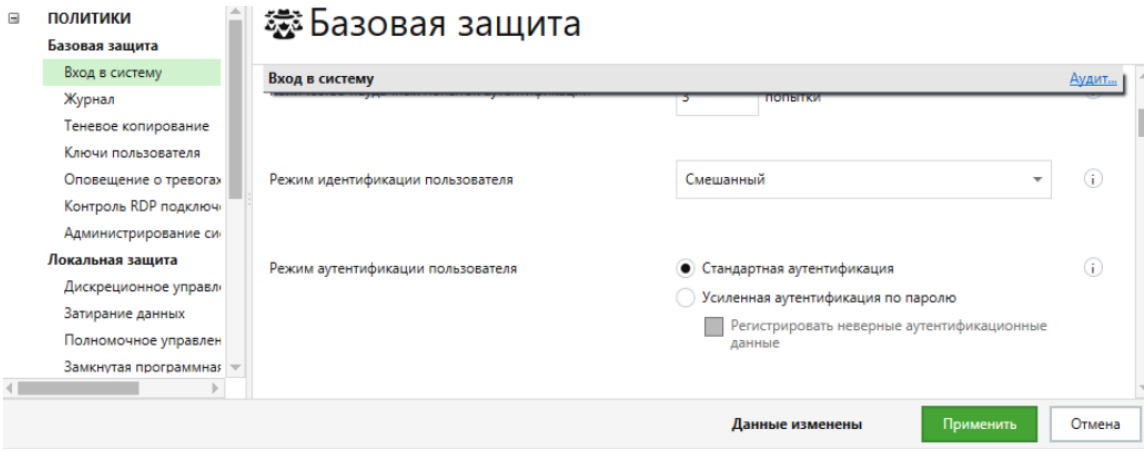

Рисунок Б.24. – Настройка входа в систему: режим идентификации и аутентификации пользователя

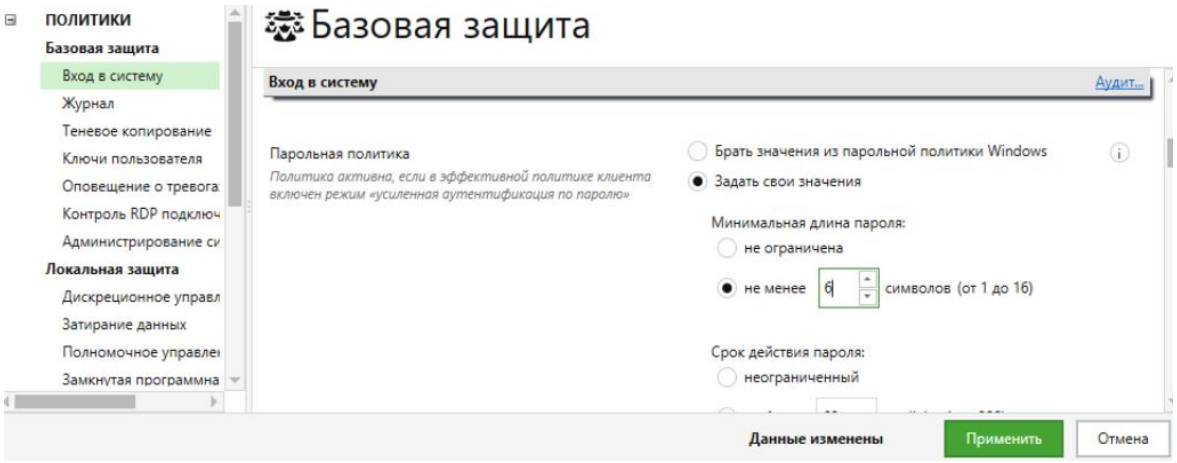

Рисунок Б.25. – Настройка входа в системы: парольная политика

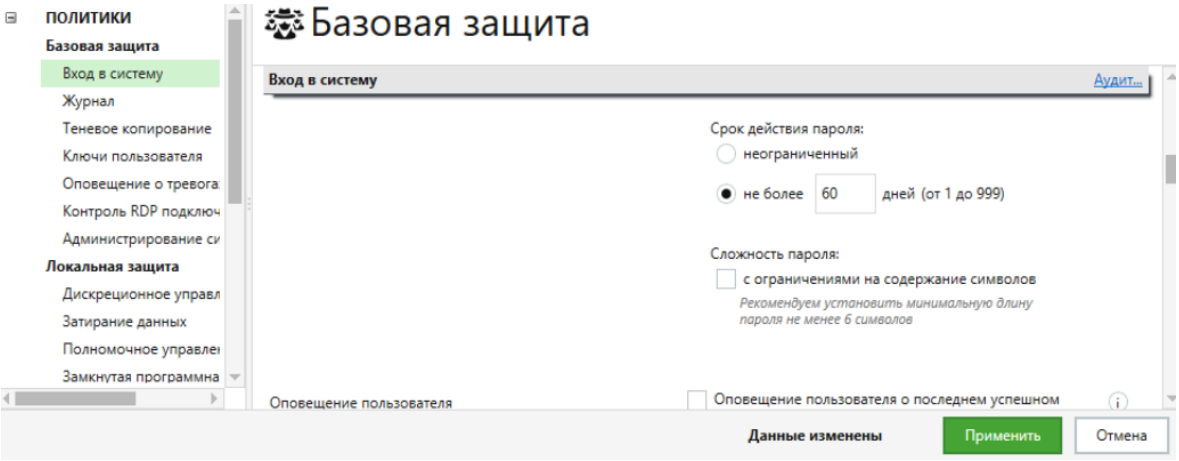

Рисунок Б.26. – Настройка входа в системы: парольная политика, продолжение

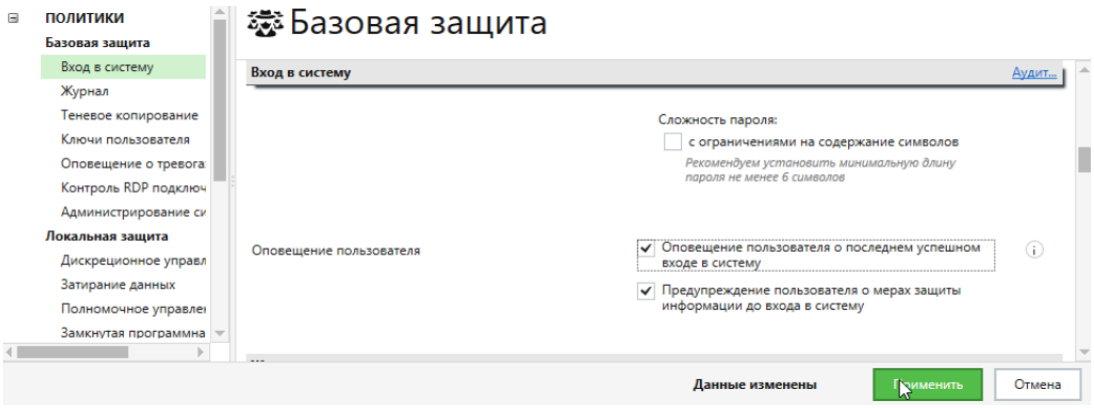

Рисунок Б.27. – Настройка входа в системы: оповещение пользователя

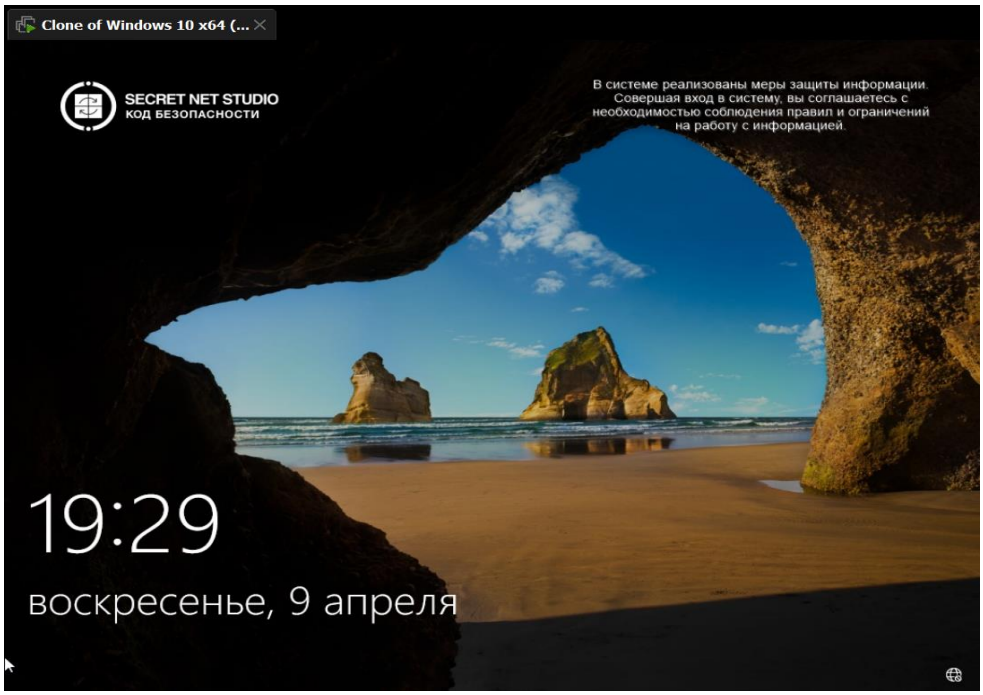

Рисунок Б.28. – Уведомление о принятых мерах защиты на экране блокировки

Настройка журнала

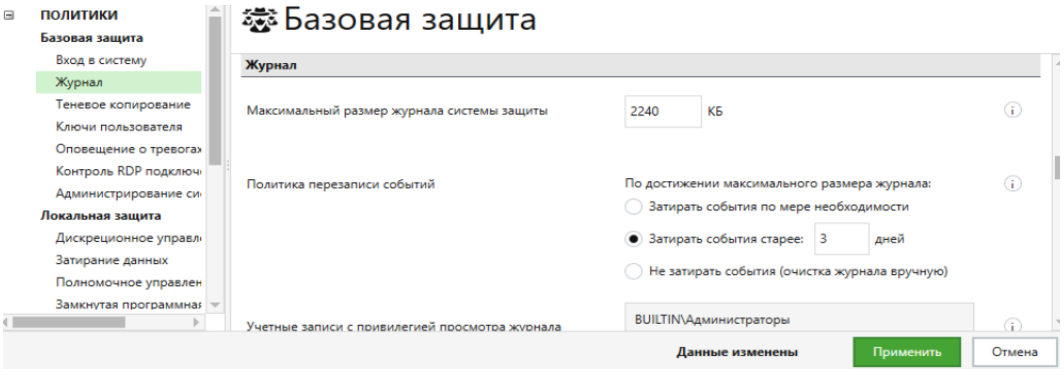

Рисунок Б.29. – Настройка журнала: максимальный размер журнала системы защиты, политика перезаписи событий

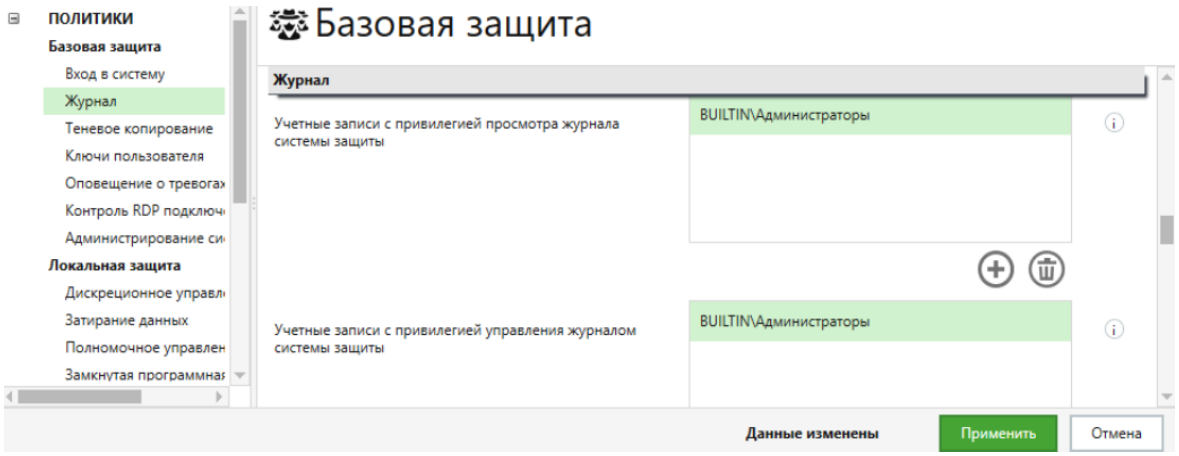

Рисунок Б.30. – Настройка журнала: учётные записи с привилегией просмотра и управления журнала системы защиты

Настройка теневого копирования

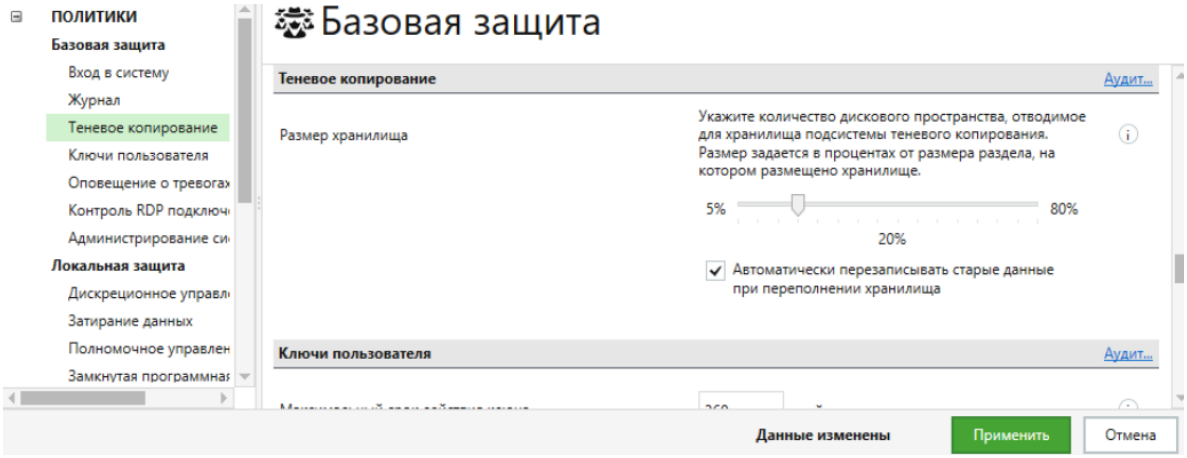

Рисунок Б.31. – Настройка теневого копирования

Настройка ключей пользователя

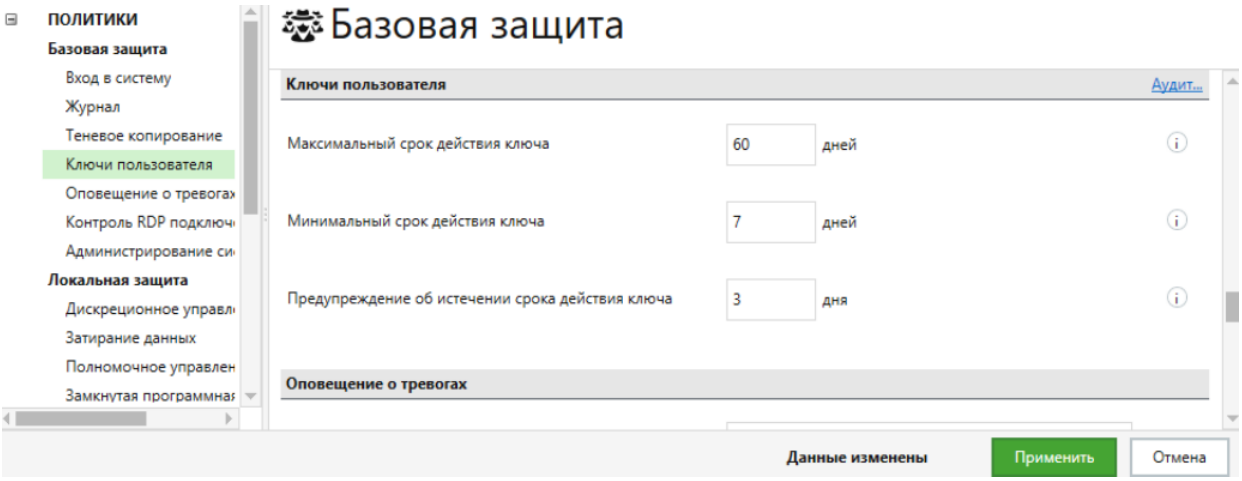

Рисунок Б.32. – Настройка ключей пользователя

Настройка оповещения о тревогах

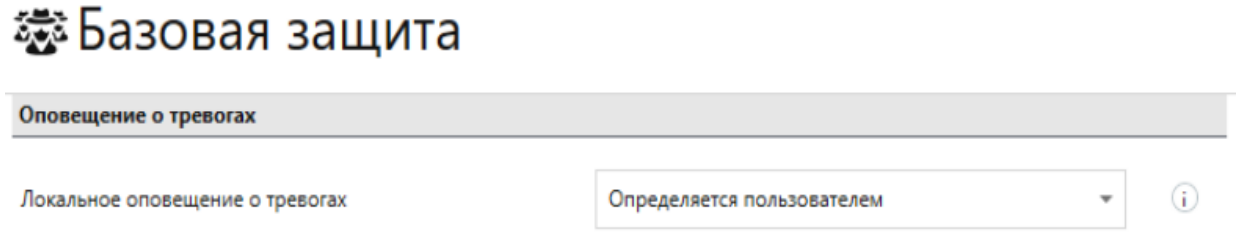

Рисунок Б.33. – Настройка оповещения о тревогах

Настройка контроля RDP подключений

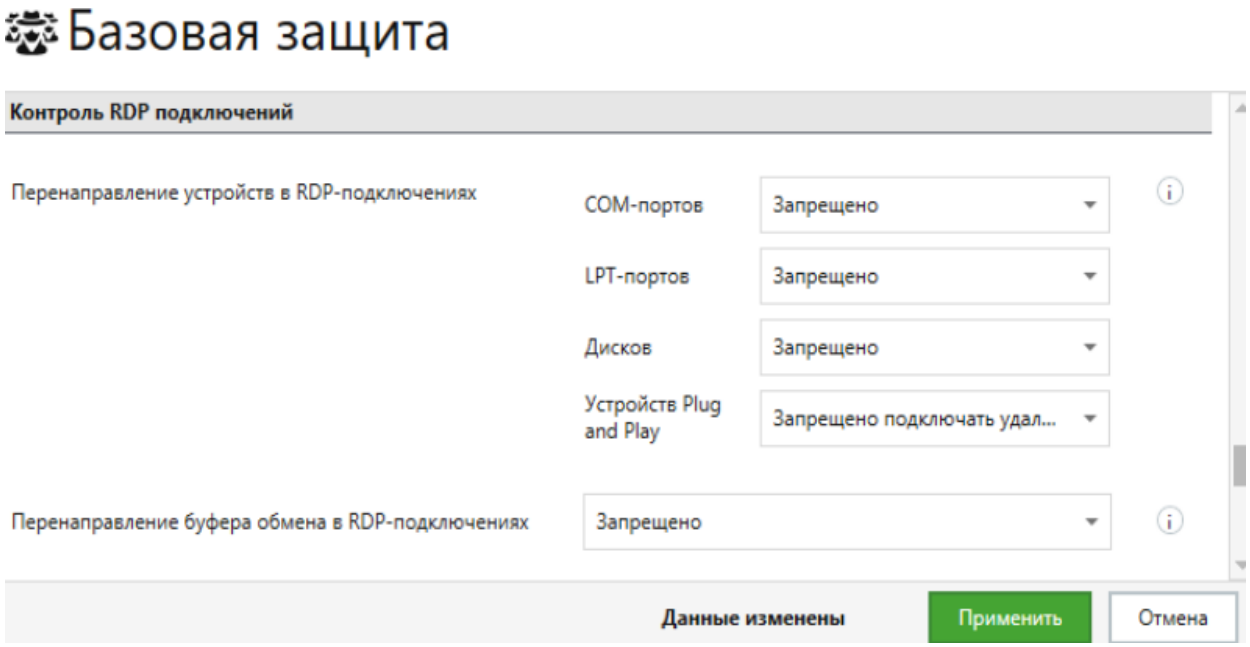

Рисунок Б.34. – Настройка контроля RDP подключений

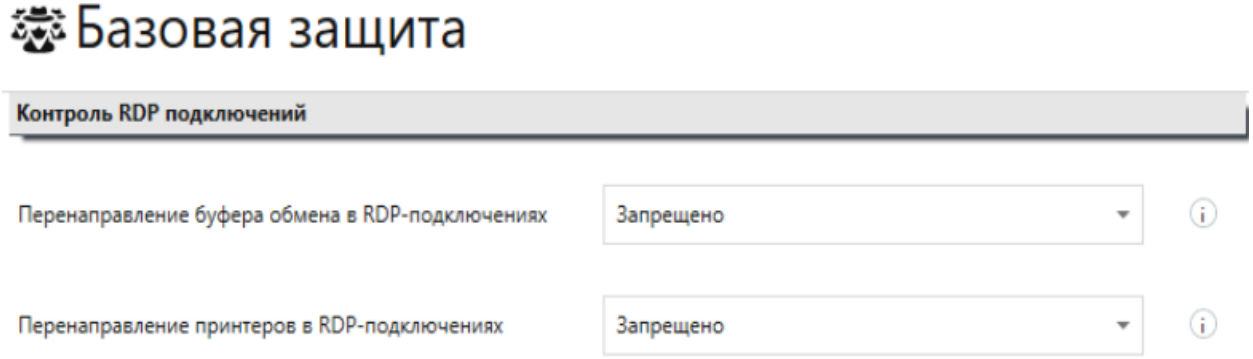

Рисунок Б.35. – Настройка контроля RDP подключений, продолжение

Настройка администрирования системы защиты

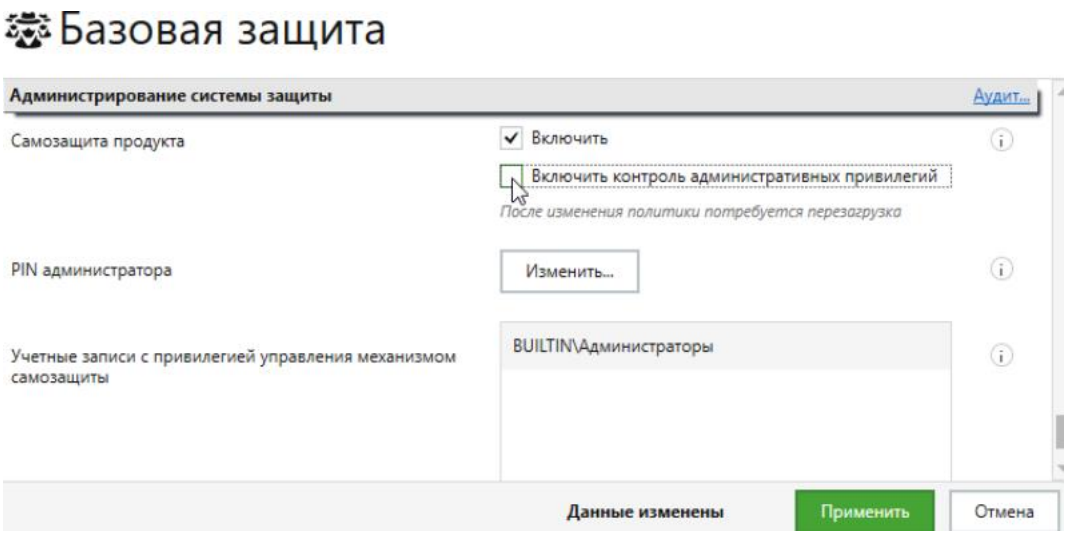

Рисунок Б.36. – Настройка администрирования системы защиты

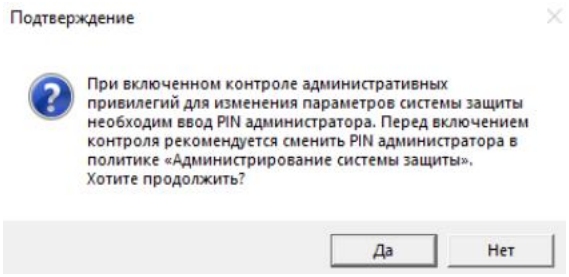

Рисунок Б.37. – Настройка администрирования системы защиты: предупреждение о необходимости PIN

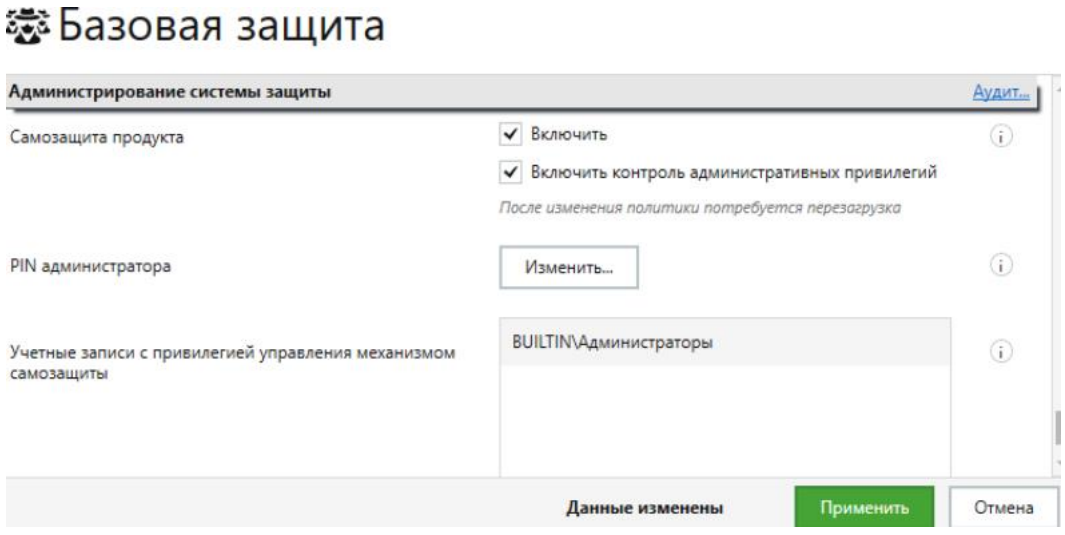

Рисунок Б.38. – Настройка администрирования системы защиты, продолжение

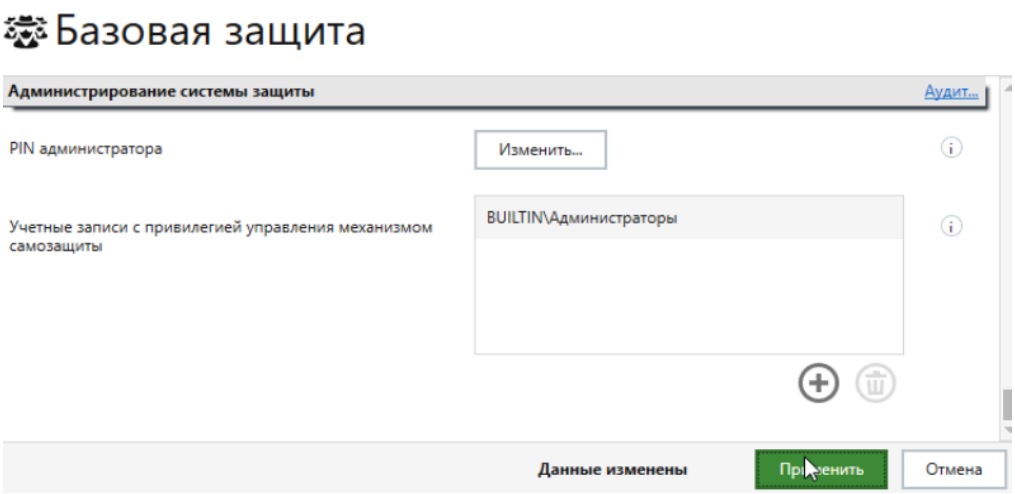

Рисунок Б.39. – Настройка администрирования системы защиты, завершение

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.

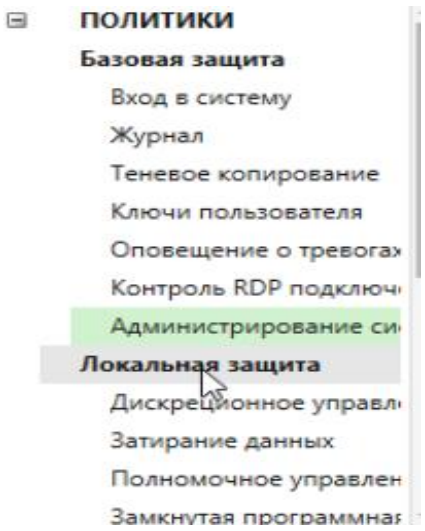

Рисунок Б.40. – Выбор настройки локальной защиты

Настройка дискреционного управления доступом

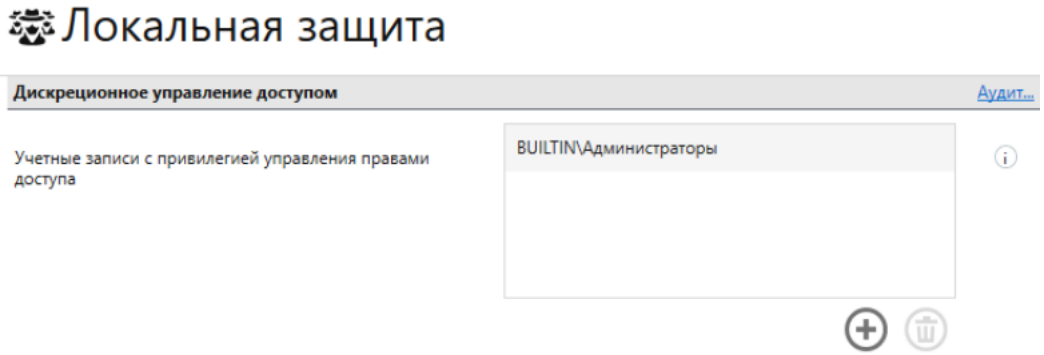

Рисунок Б.41. – Настройка дискреционного управления доступом

Настройка затирания данных

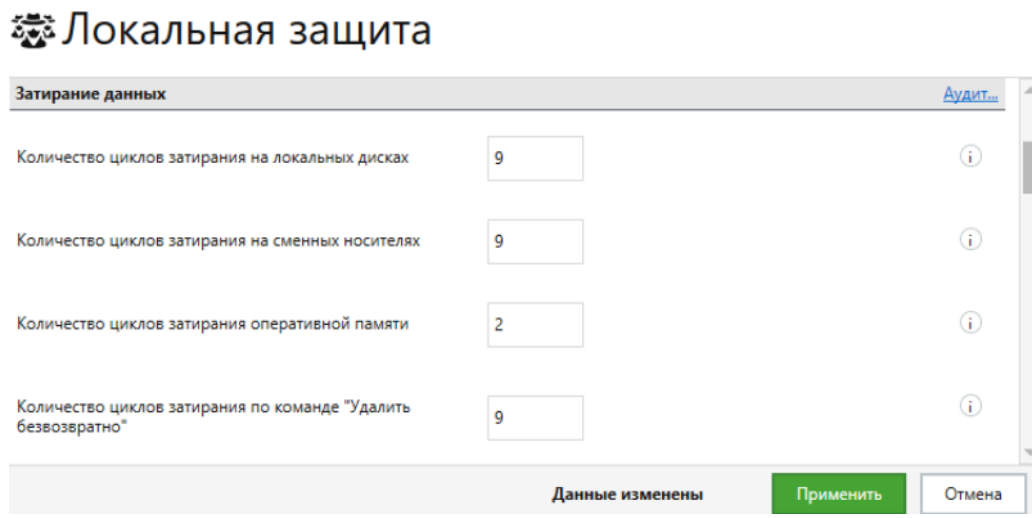

Рисунок Б.42. – Настройка затирания данных

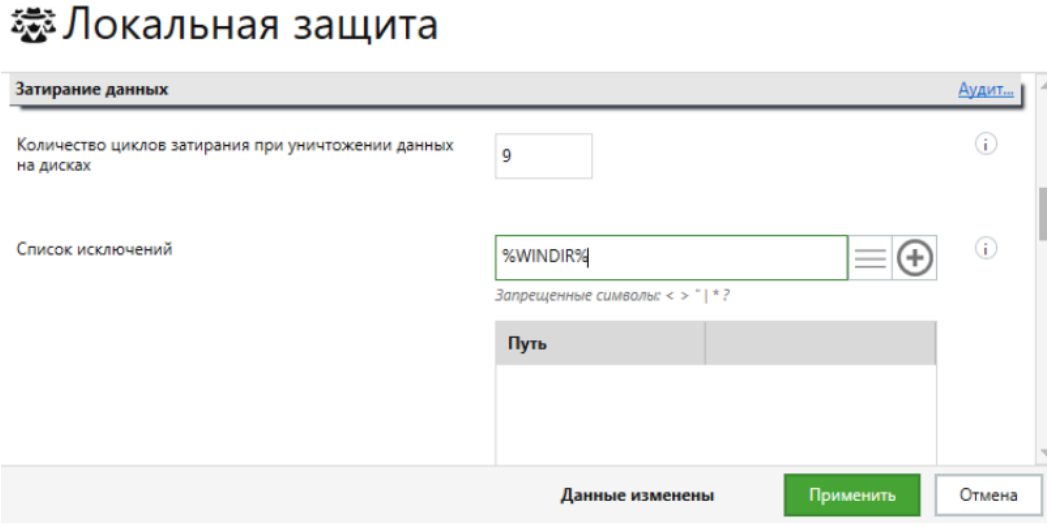

Рисунок Б.43. – Настройка затирания данных, продолжение

Настройка полномочного управления доступом

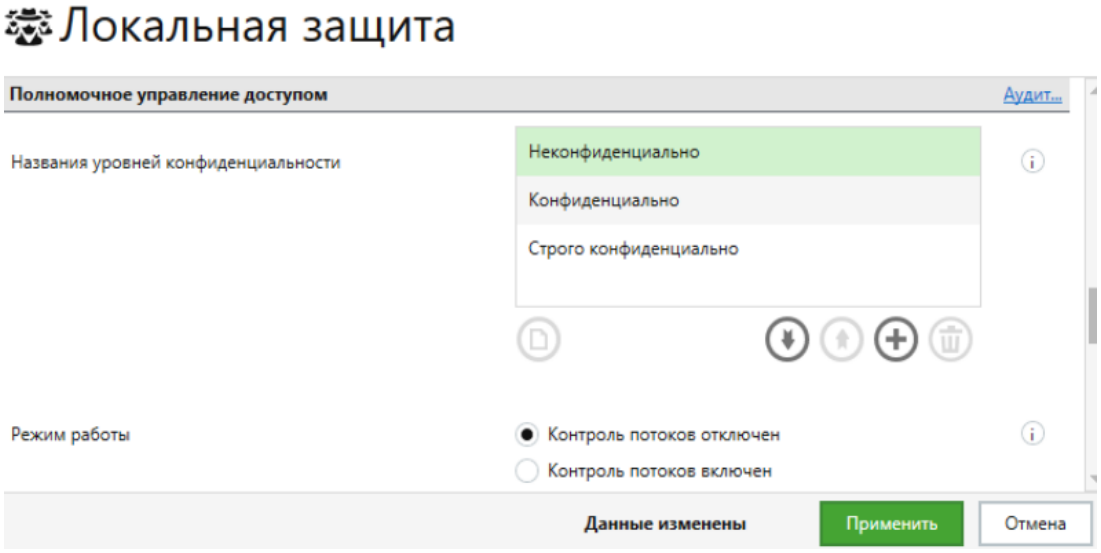

Рисунок Б.44. – Настройка полномочного управления доступом

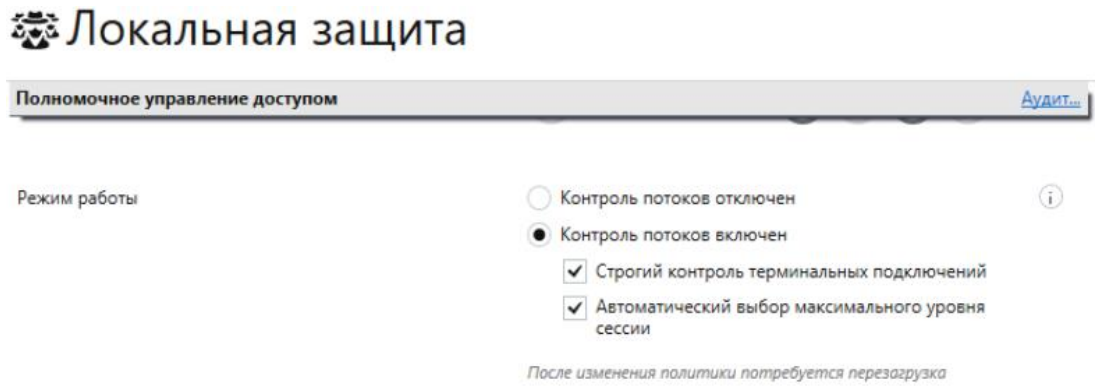

Рисунок Б.45. – Настройка полномочного управления доступом, продолжение

Настройка замкнутой программной среды

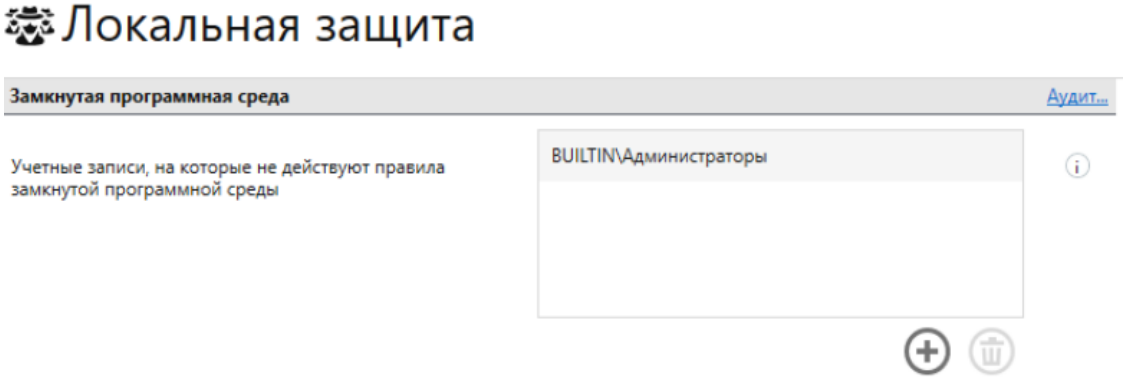

Рисунок Б.46. – Настройка замкнутой программной среды

Настройка защиты диска и шифрования данных

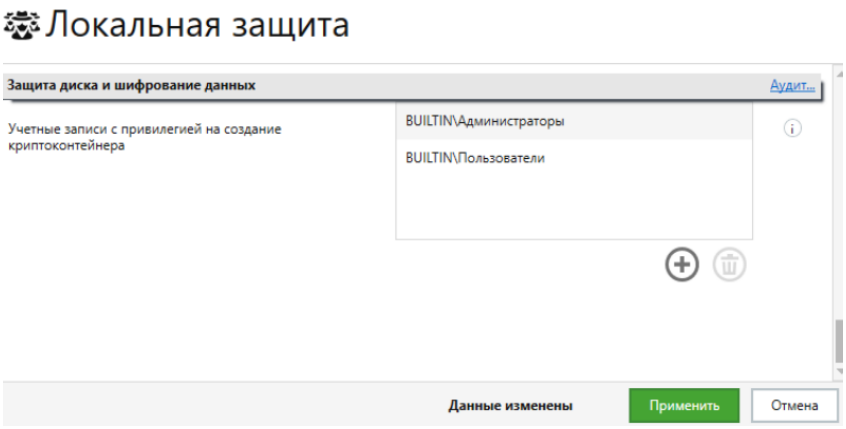

Рисунок Б.47. – Настройка защиты диска и шифрования данных

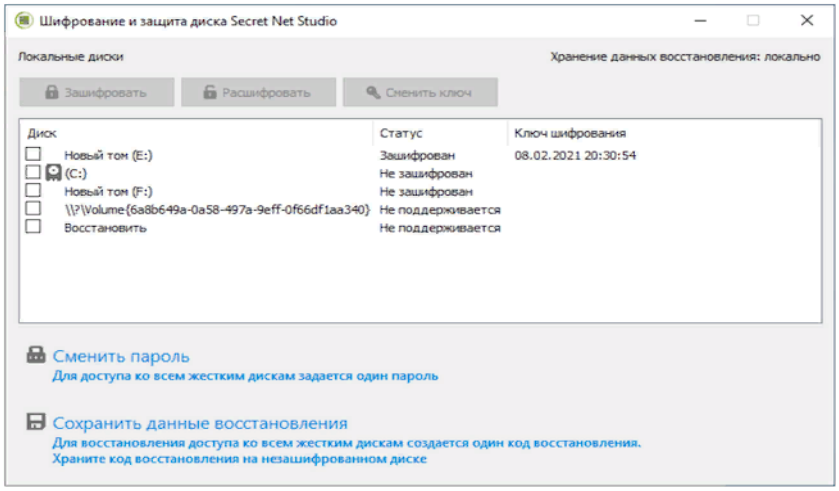

Рисунок Б.48. – Мастер шифрования дисков Secret Net Studio

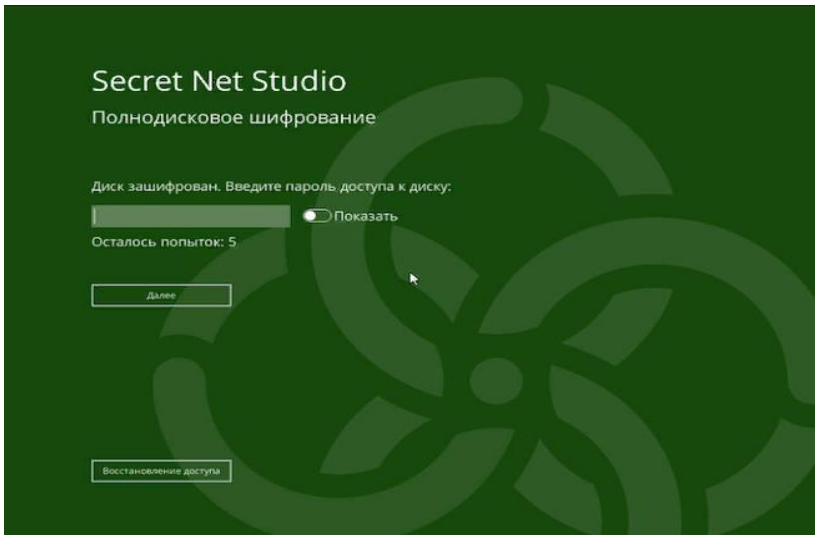

Рисунок Б.49. – Загрузчик Secret Net Studio (запрос пароля для доступа к зашифрованному диску)

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.

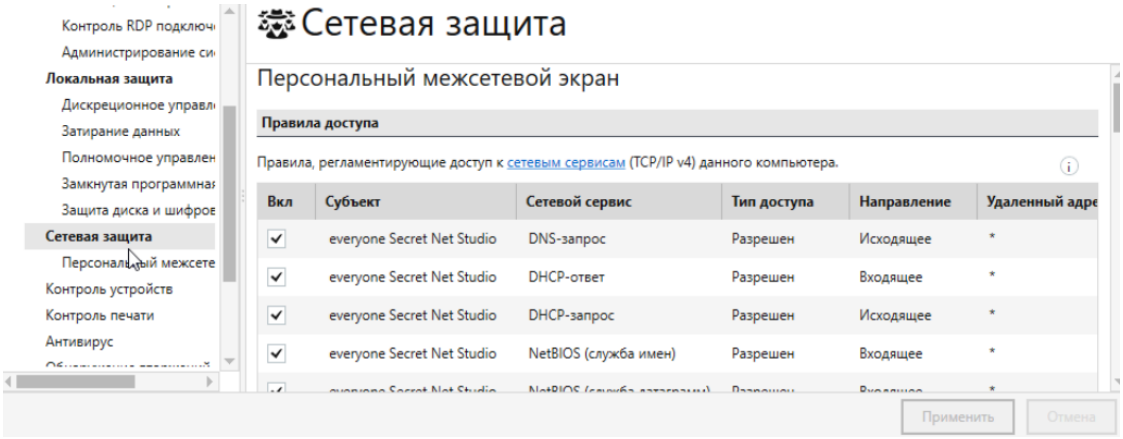

Рисунок Б.50. – Настройка персонального межсетевого экрана: правила доступа

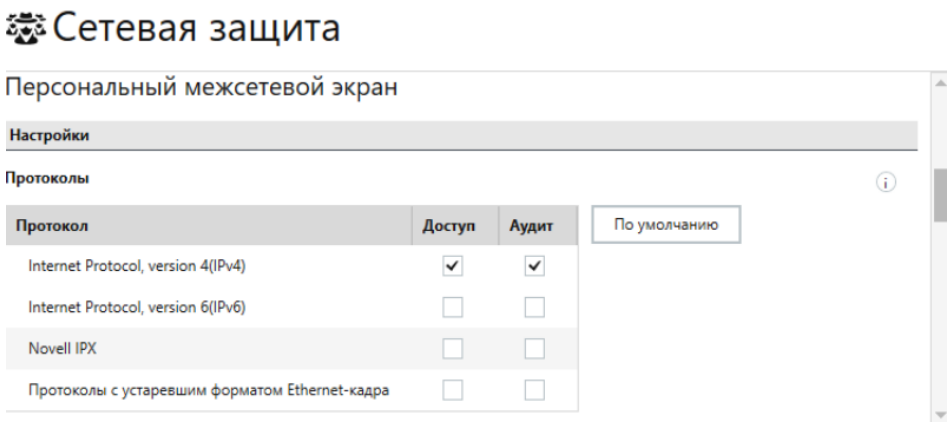

Рисунок Б.51. – Настройка персонального межсетевого экрана: настройка протоколов

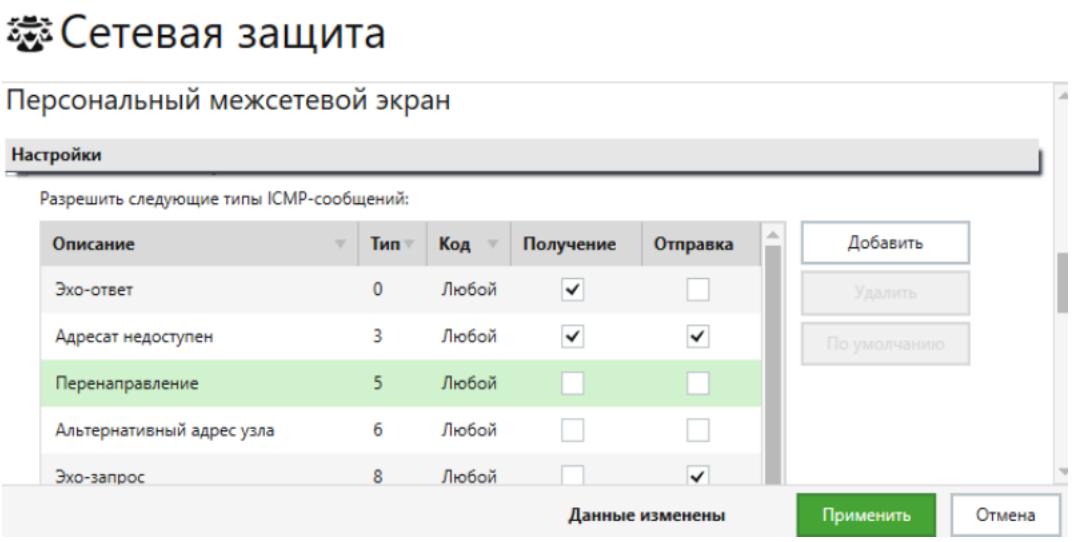

Рисунок Б.52. – Настройка персонального межсетевого экрана: типы ICMP-сообщений

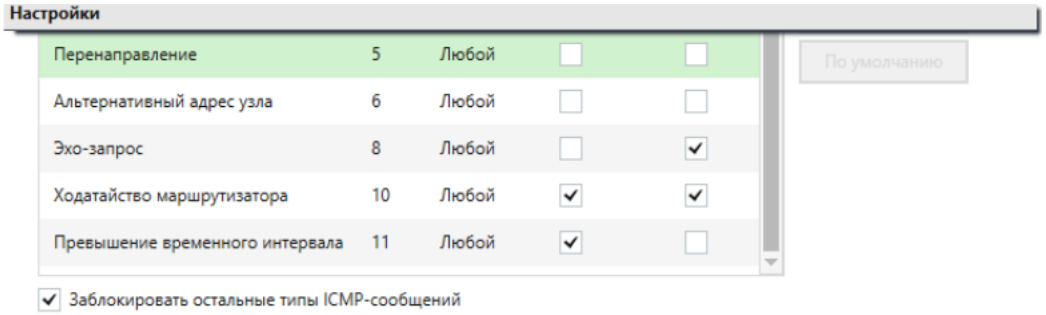

Рисунок Б.53. – Настройка персонального межсетевого экрана: типы ICMP-сообщений, продолжение

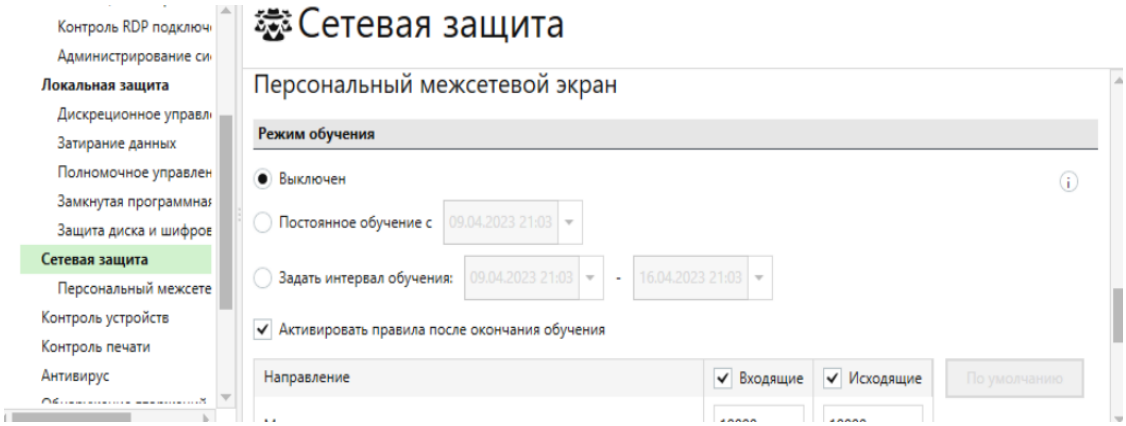

Рисунок Б.54. – Настройка персонального межсетевого экрана: режим обучения

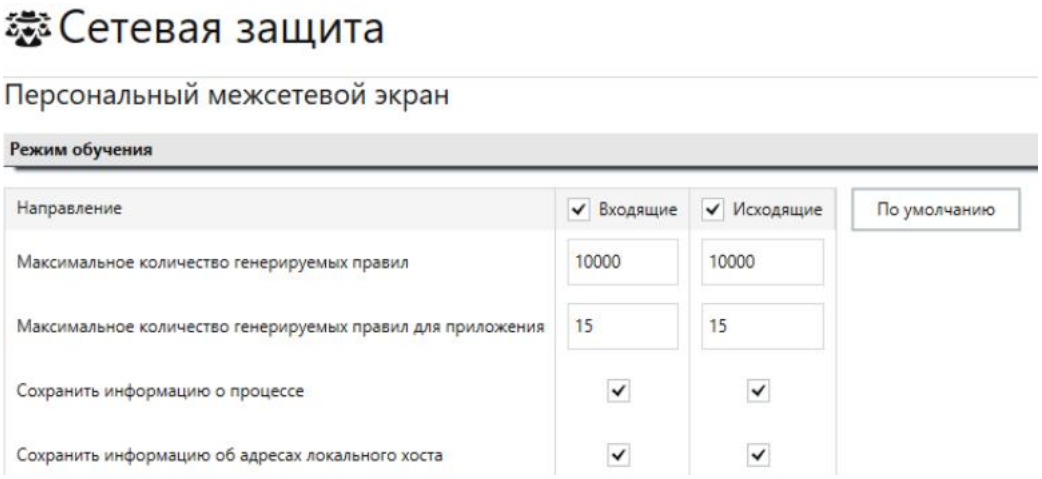

Рисунок Б.55. – Настройка персонального межсетевого экрана: режим обучения, продолжение

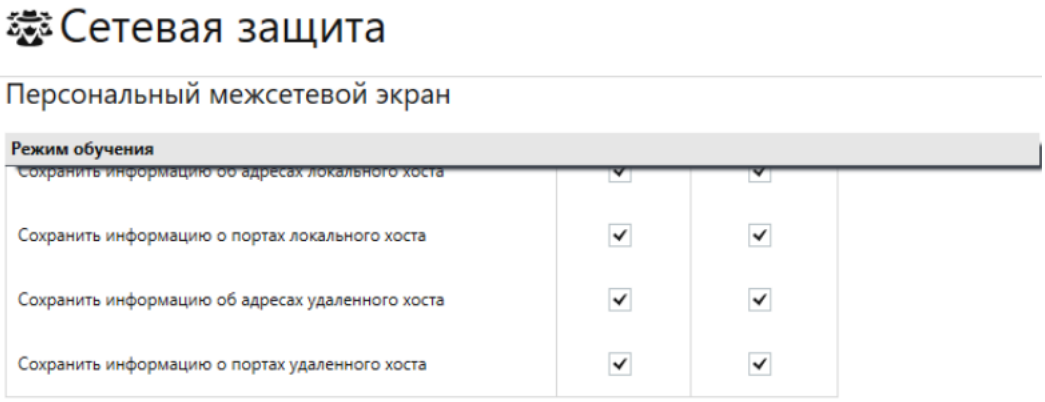

Рисунок Б.56. – Настройка персонального межсетевого экрана: режим обучения, завершение

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» представлена на рисунках Б.57. ÷ Б.63, для фиксации настроек в системе после выбора нажать кнопку «Применить» в правом нижнем углу окна приложения.

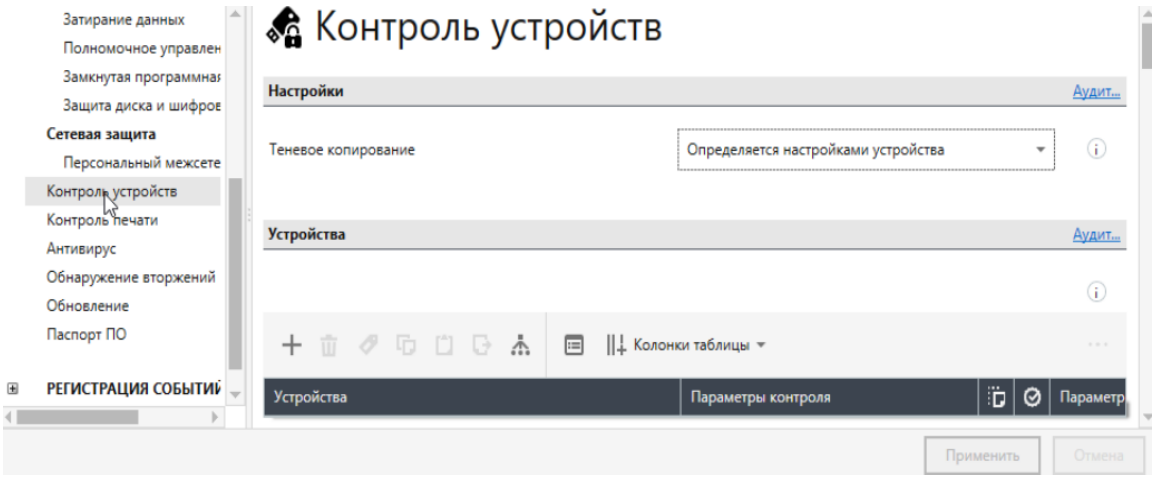

Рисунок Б.57. – Настройка контроля устройств: настройки (теневое копирование)

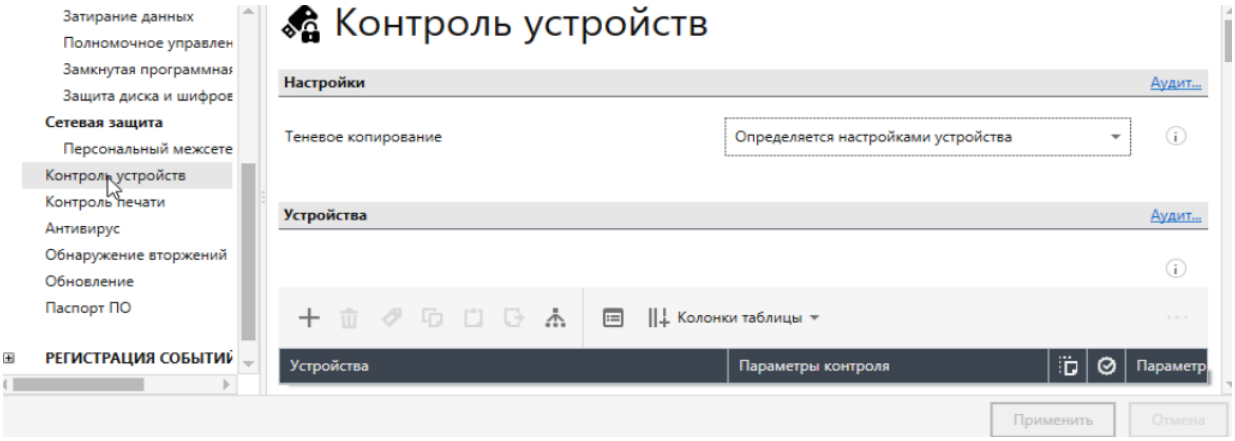

Рисунок Б.58. – Настройка контроля устройств: теневое копирование, продолжение

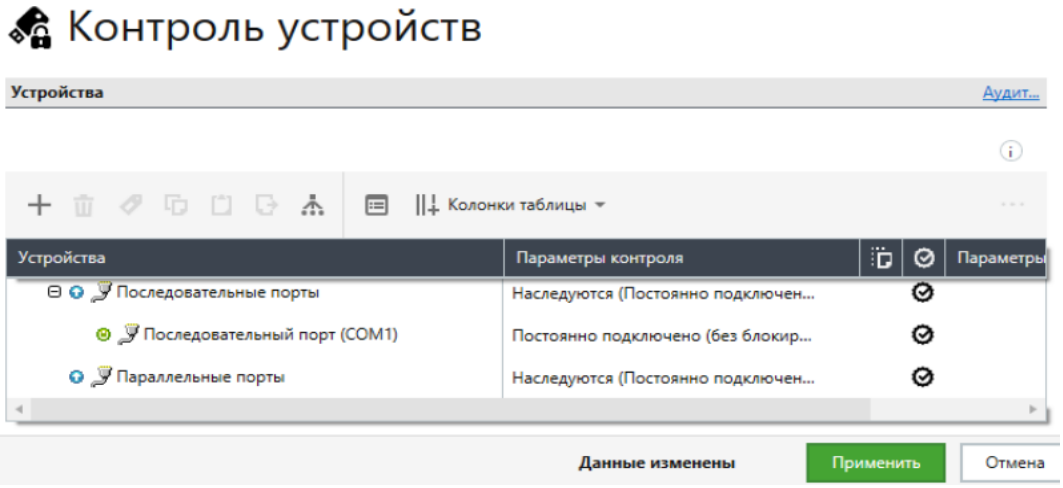

Рисунок Б.59. – Настройка контроля устройств: устройства

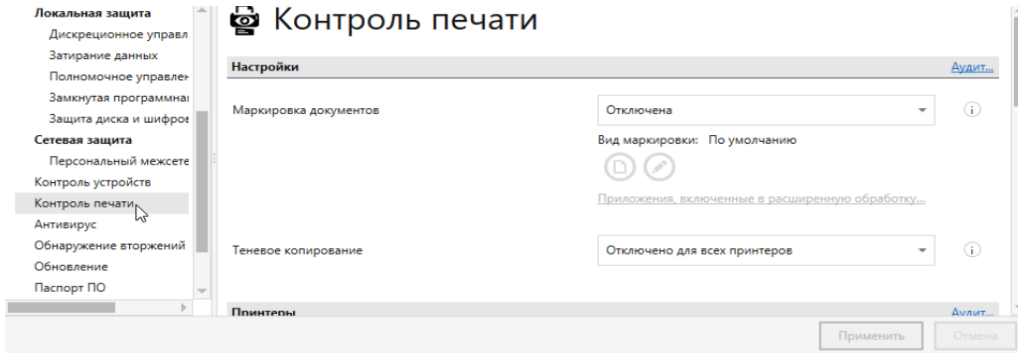

Рисунок Б.60. – Настройка контроля печати: настройки

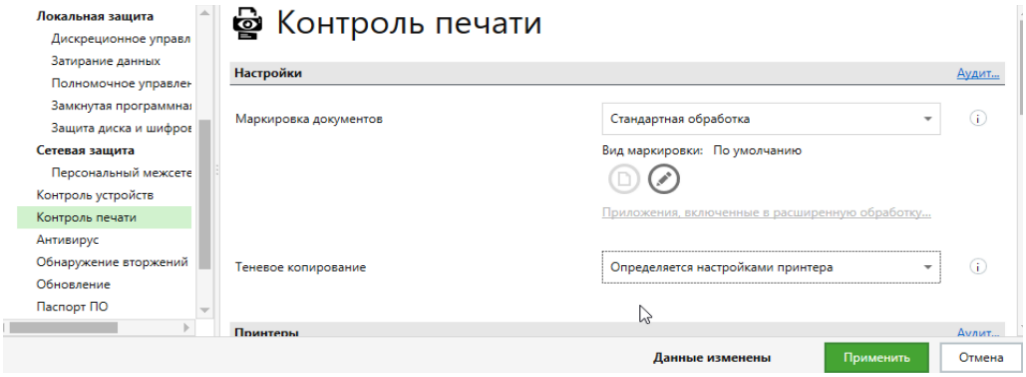

Рисунок Б.61. – Настройка контроля печати: настройки, продолжение

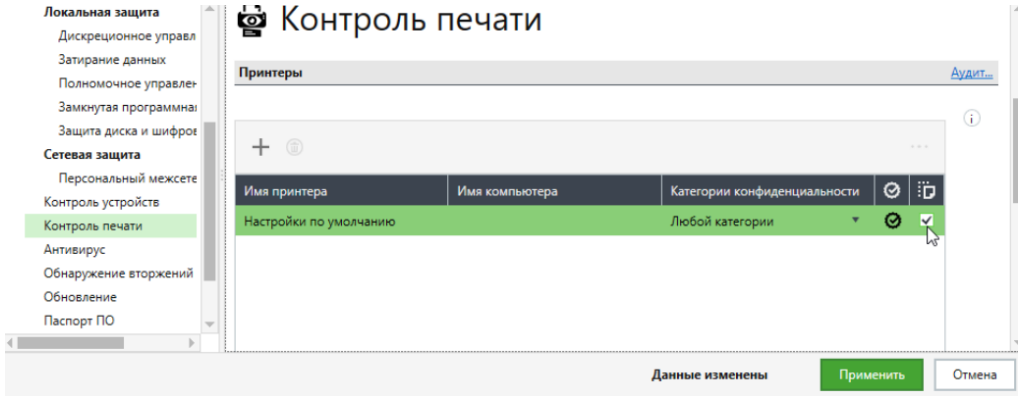

Рисунок Б.62. – Настройка контроля печати: принтеры

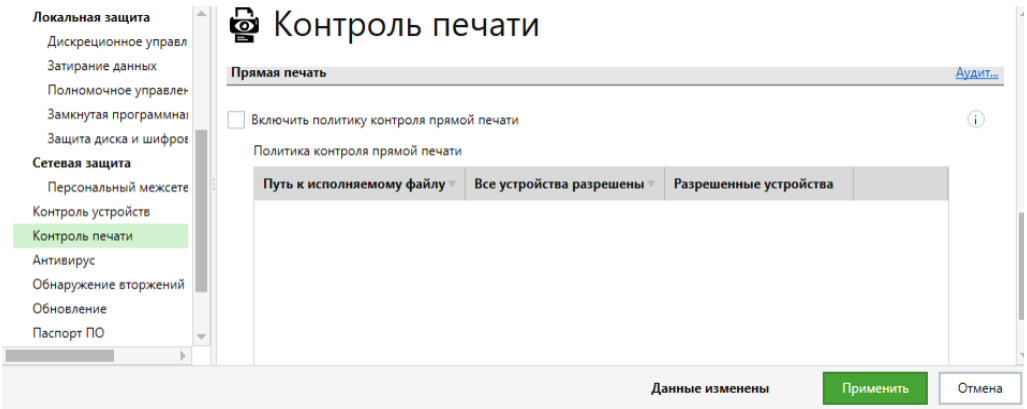

Рисунок Б.63.– Настройка контроля печати: прямая печать

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.

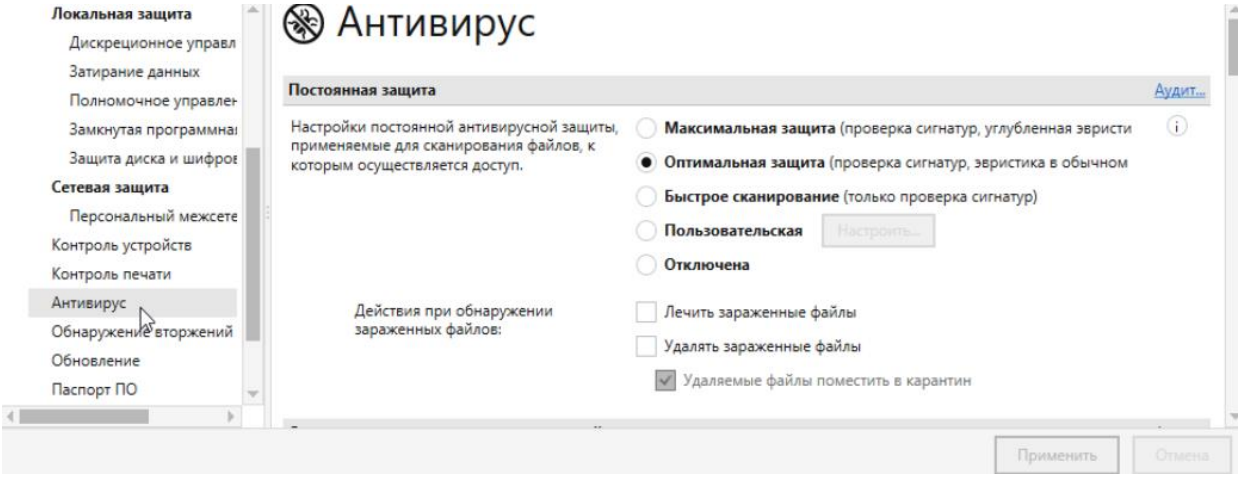

Рисунок Б.64. – Настройка антивируса: постоянная защита

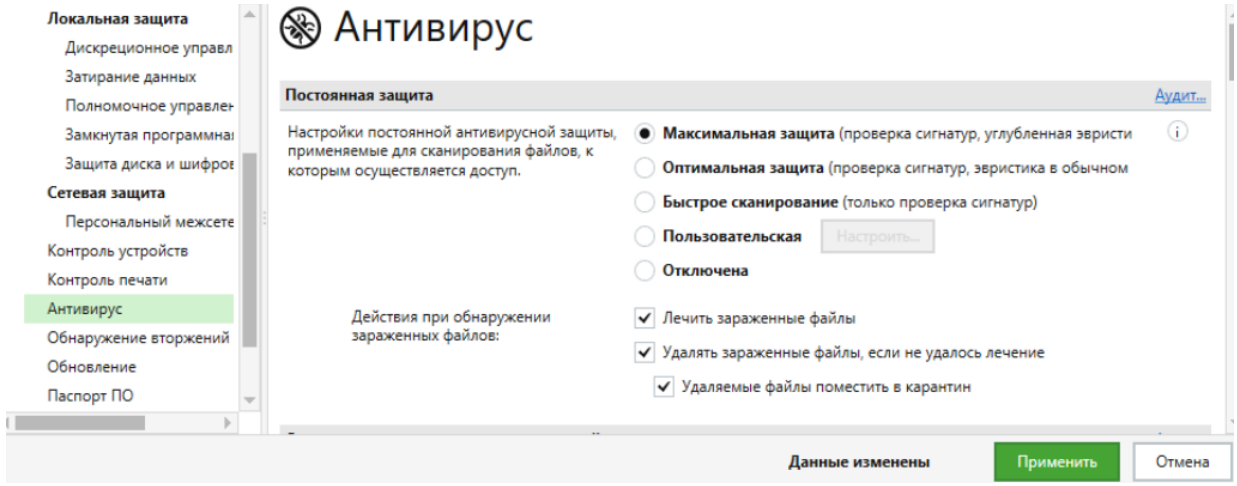

Рисунок Б.65. – Настройка антивируса: постоянная защита, продолжение

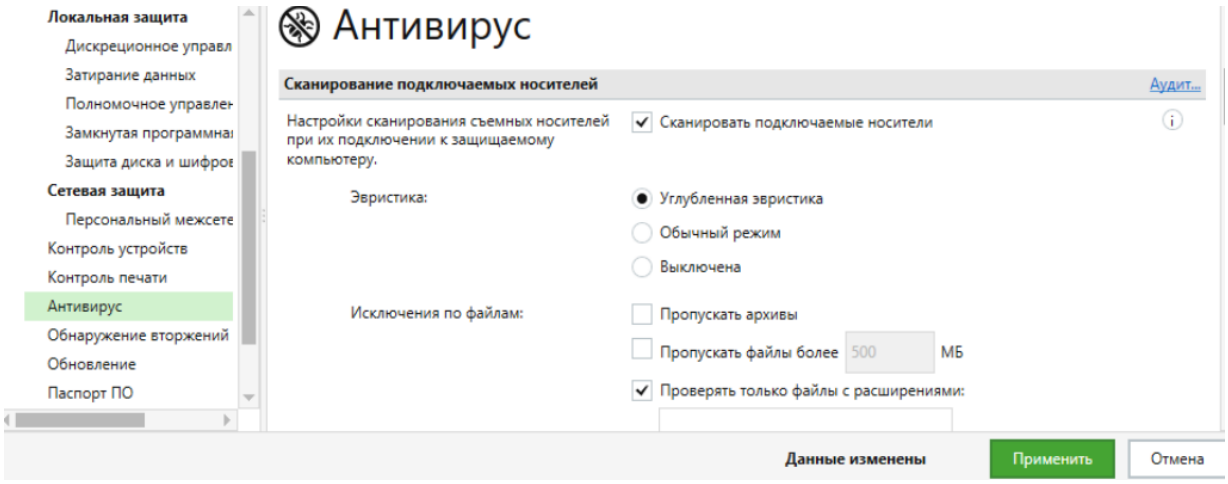

Рисунок Б.66. – Настройка антивируса: сканирование подключаемых носителей

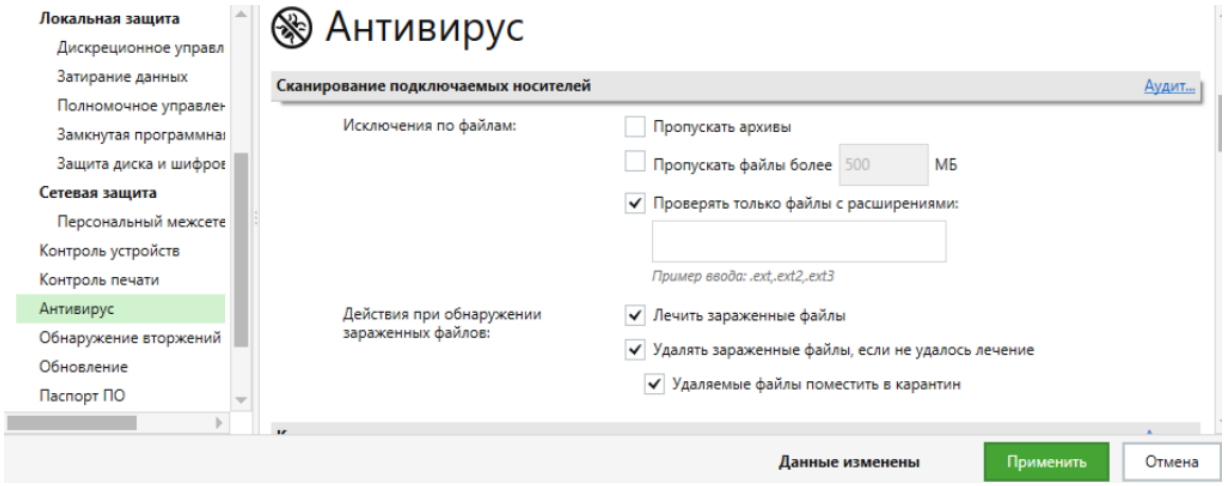

Рисунок Б.67. – Настройка антивируса: сканирование подключаемых носителей, продолжение

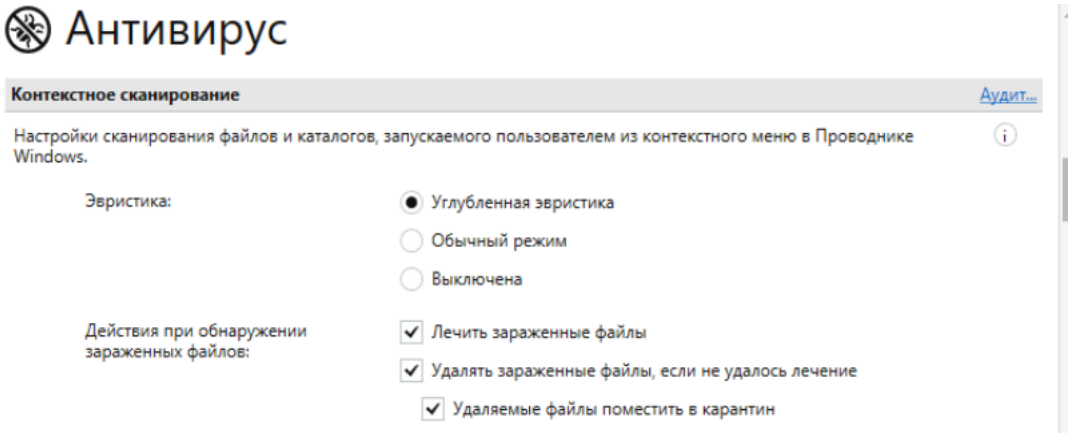

Рисунок Б.68.– Настройка антивируса: контекстное сканирование

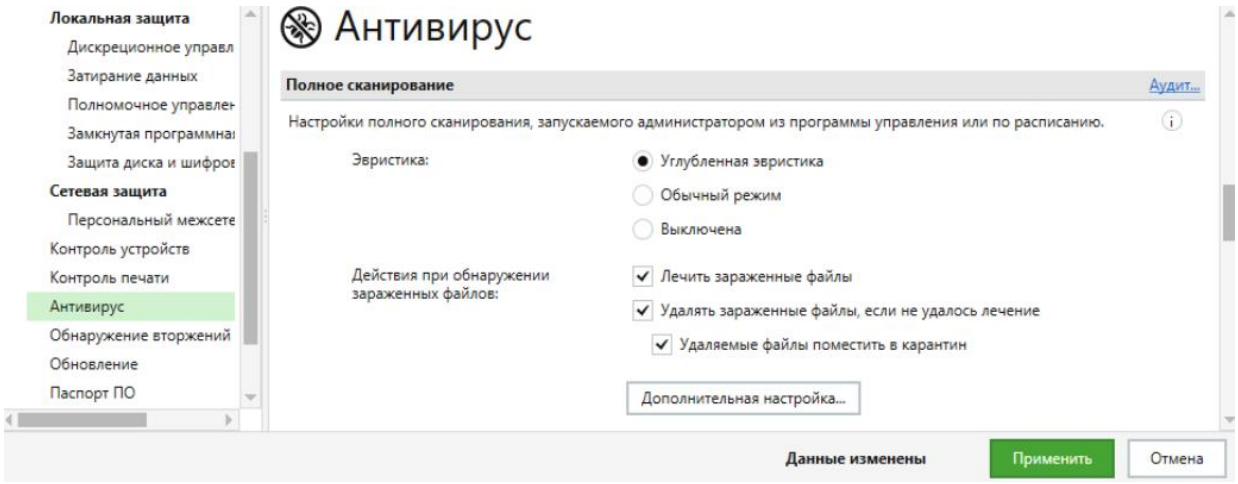

Рисунок Б.69. – Настройка антивируса: полное сканирование

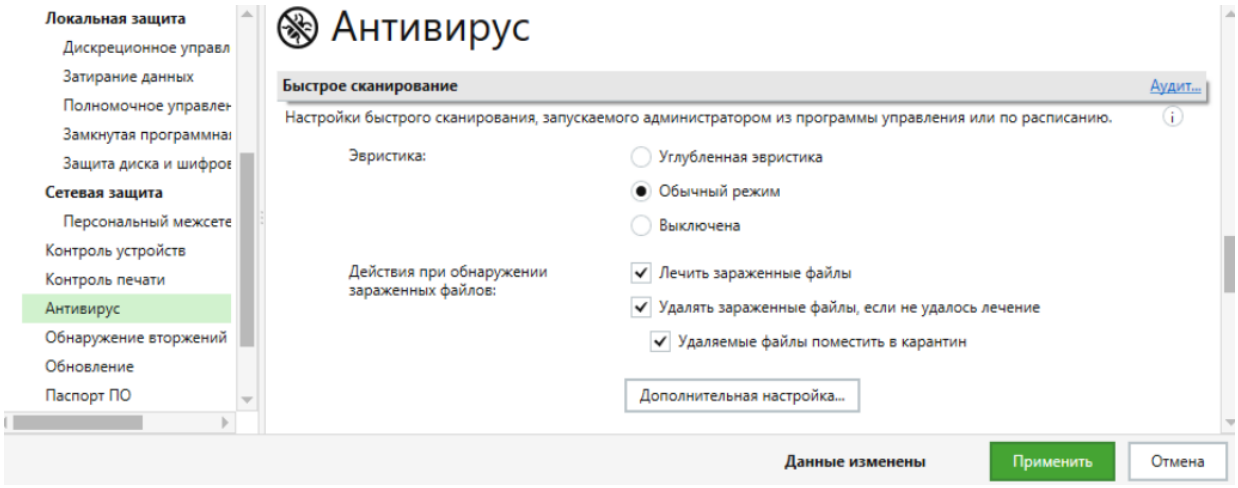

Рисунок Б.70. – Настройка антивируса: быстрое сканирование

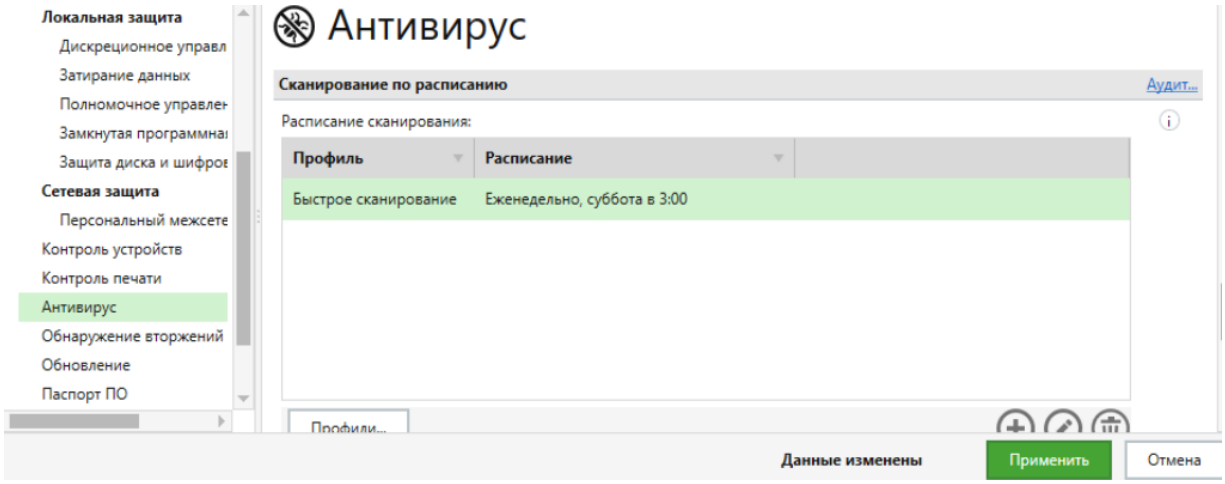

Рисунок Б.71. – Настройка антивируса: сканирование по расписанию

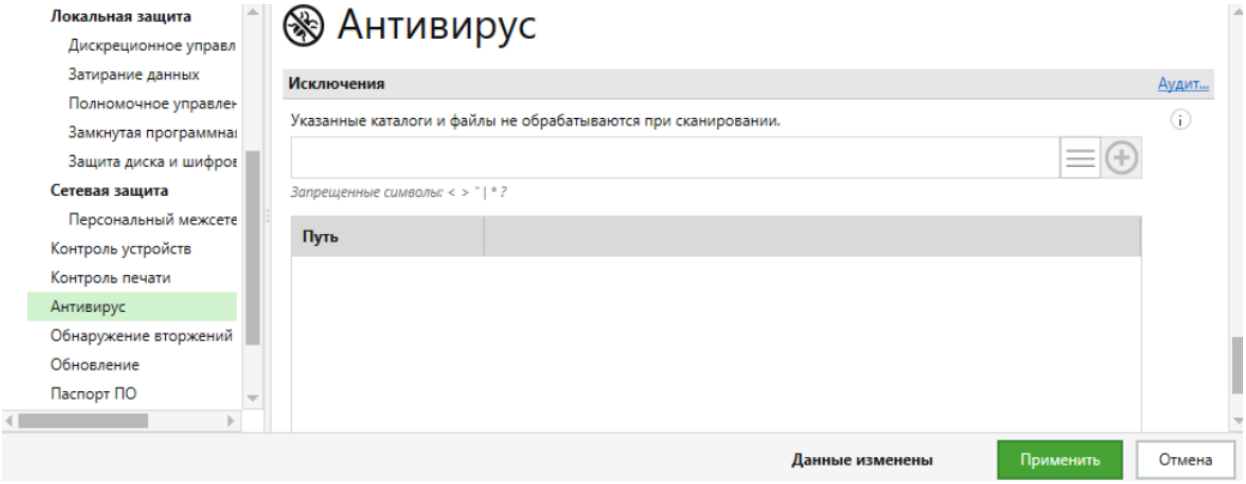

Рисунок Б.72. – Настройка антивируса: исключения

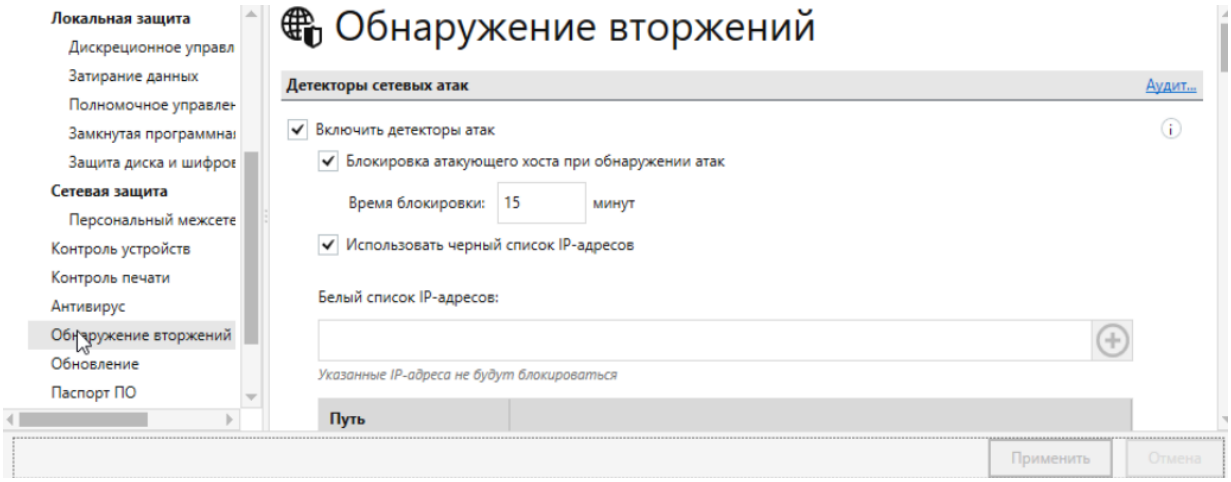

Рисунок Б.73. – Настройка обнаружения вторжений: начало

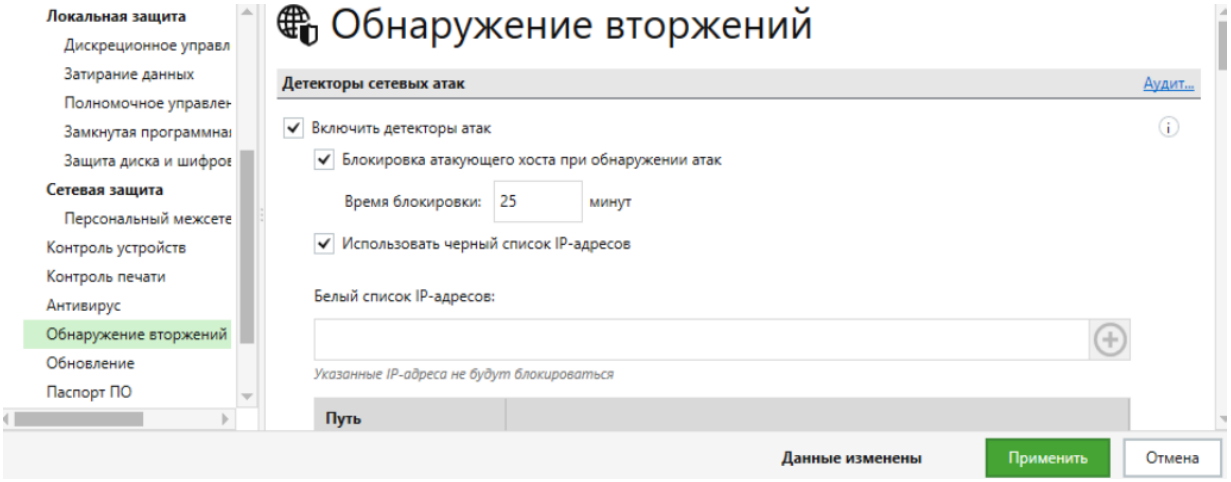

Рисунок Б.74. – Настройка обнаружения вторжений: детекторы сетевых атак

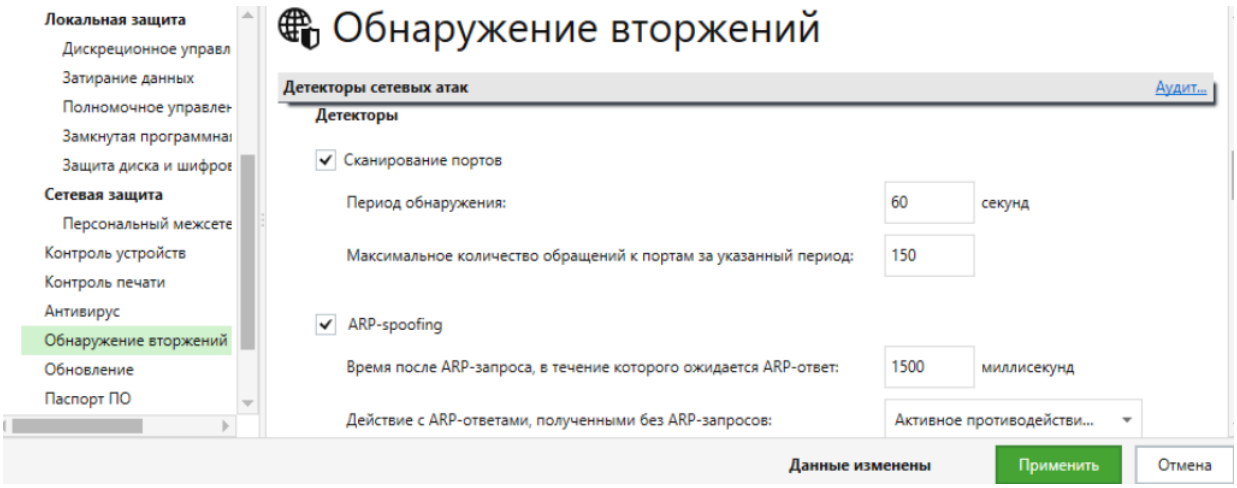

Рисунок Б.75. – Настройка детекторов сетевых атак: детекторы

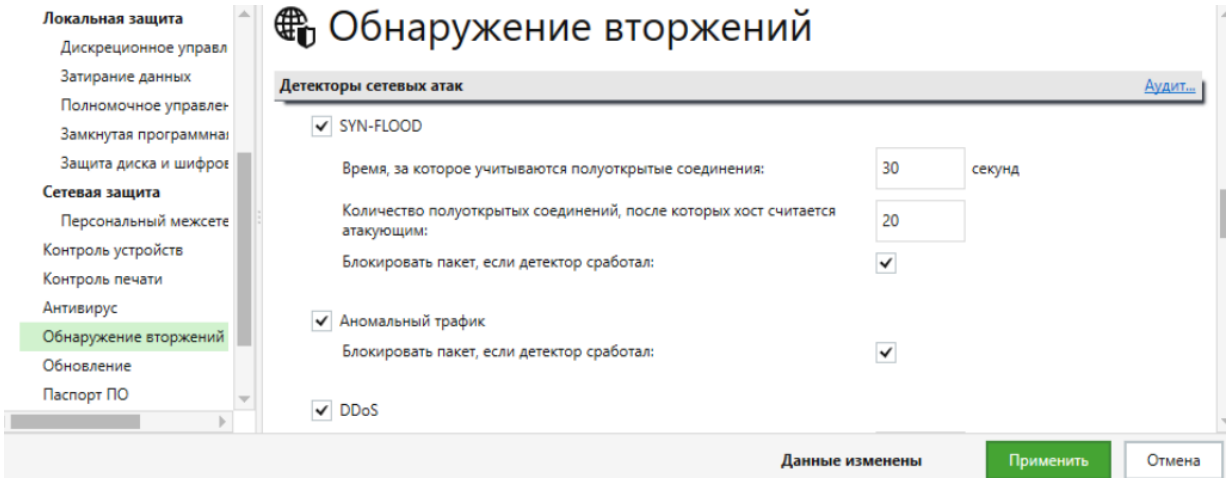

Рисунок Б.76. – Настройка детекторов сетевых атак: детекторы, продолжение

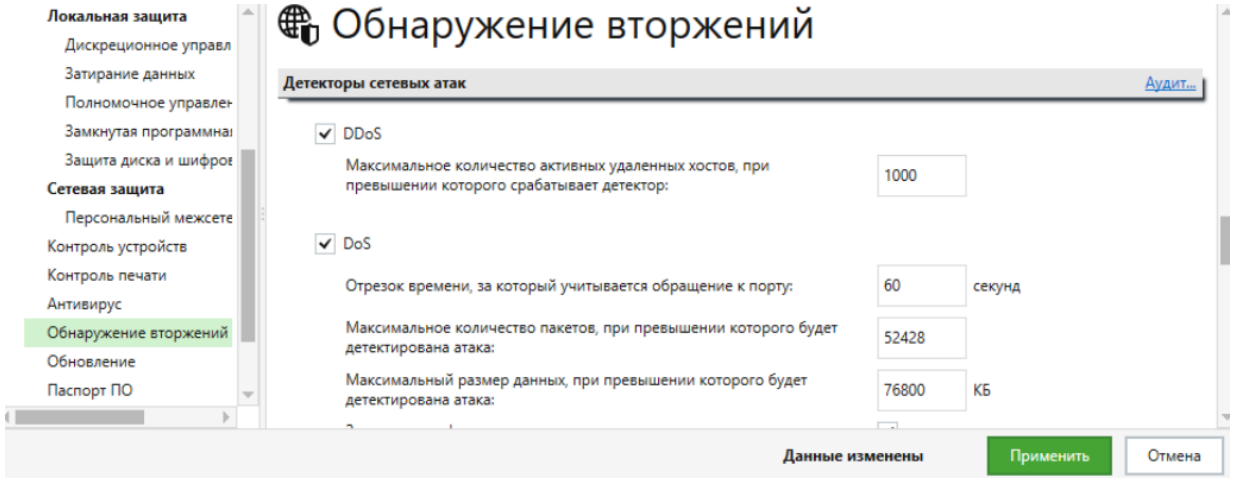

Рисунок Б.77. – Настройка детекторов сетевых атак: детекторы, завершение

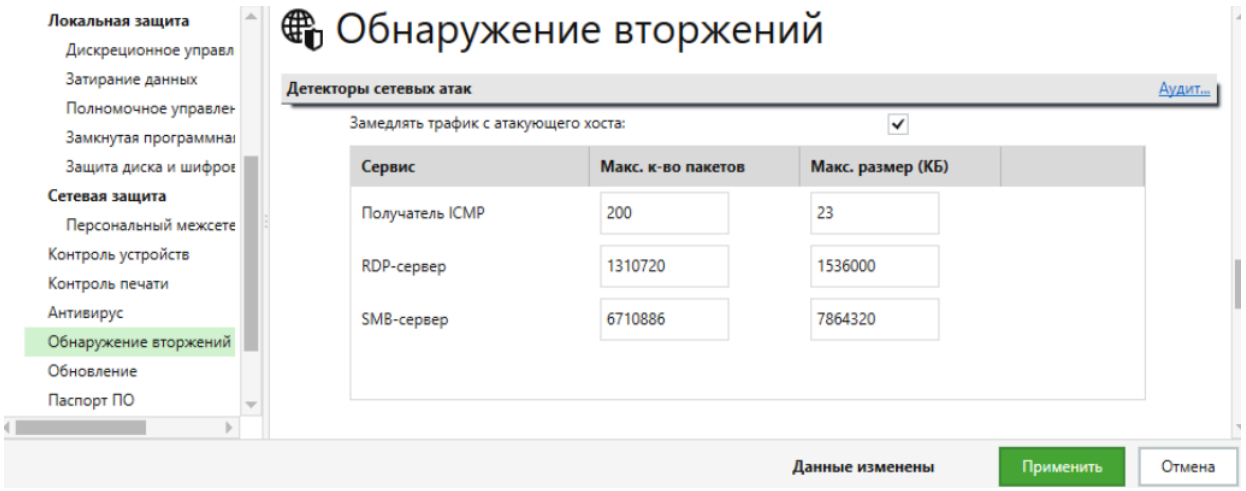

Рисунок Б.78. – Настройка детекторов сетевых атак: сервис (продолжение)

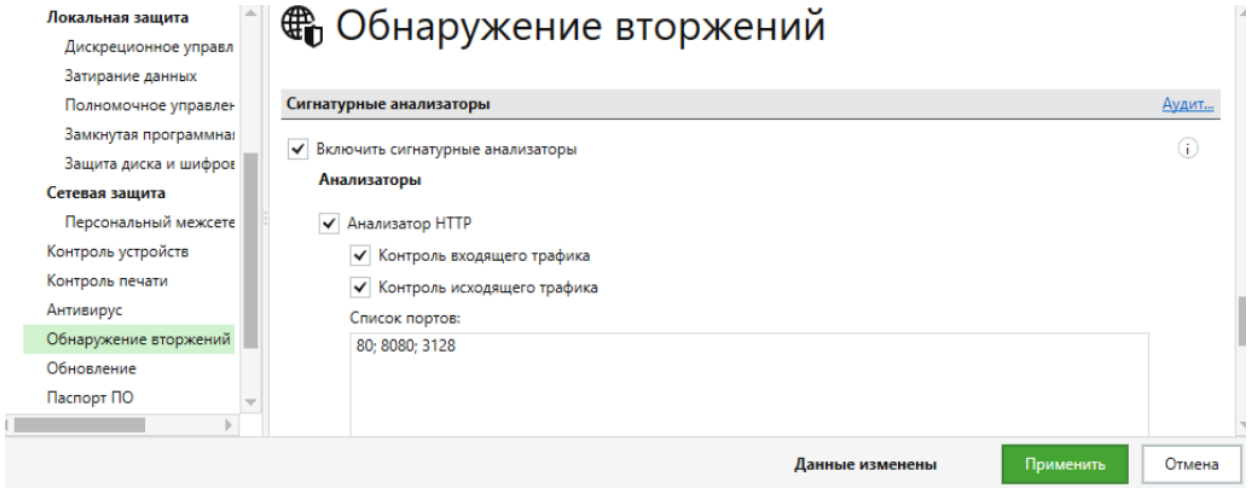

Рисунок Б.79. – Настройка обнаружения вторжений: сигнатурные анализаторы

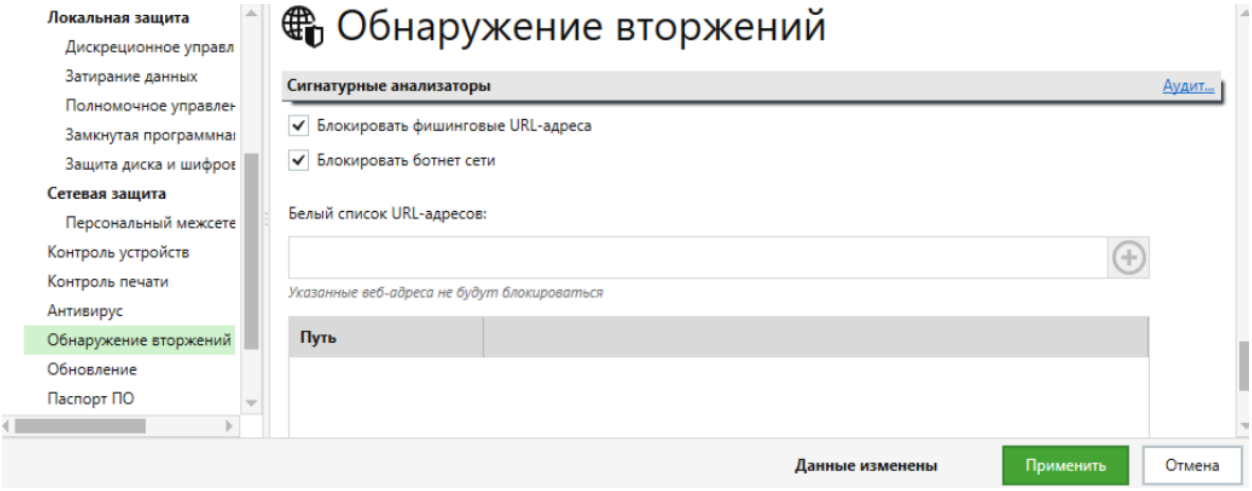

Рисунок Б.80. – Настройка обнаружения вторжений: сигнатурные анализаторы. продолжение

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.

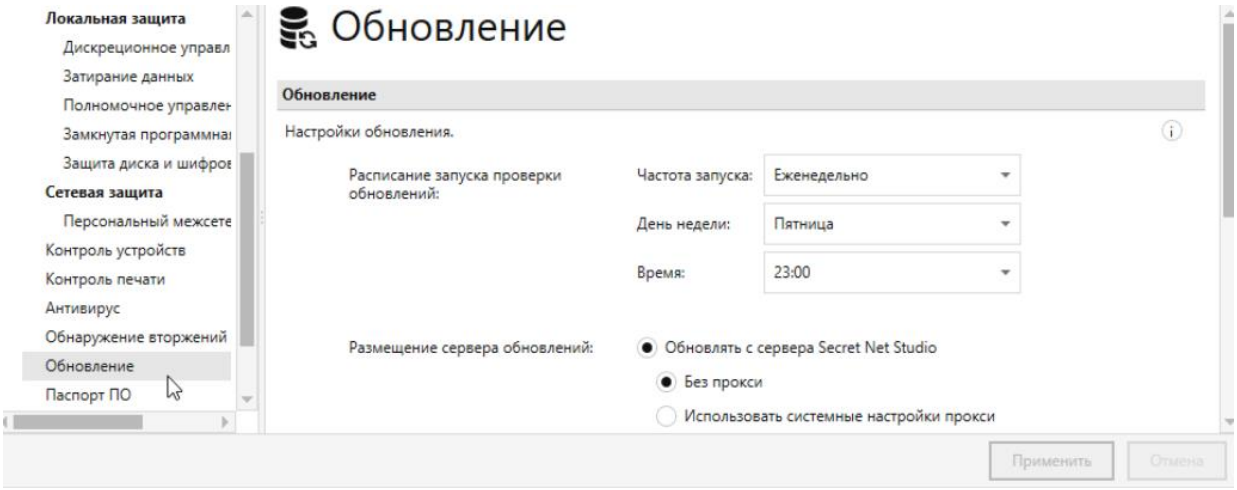

Рисунок Б.81. – Настройка обновлений

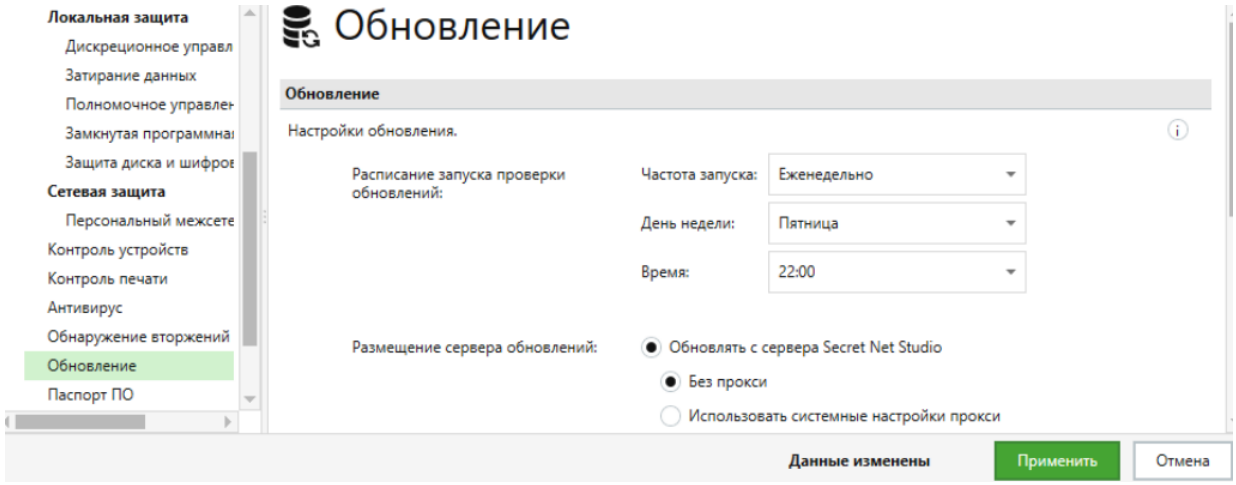

Рисунок Б.82. – Настройка обновлений, продолжение

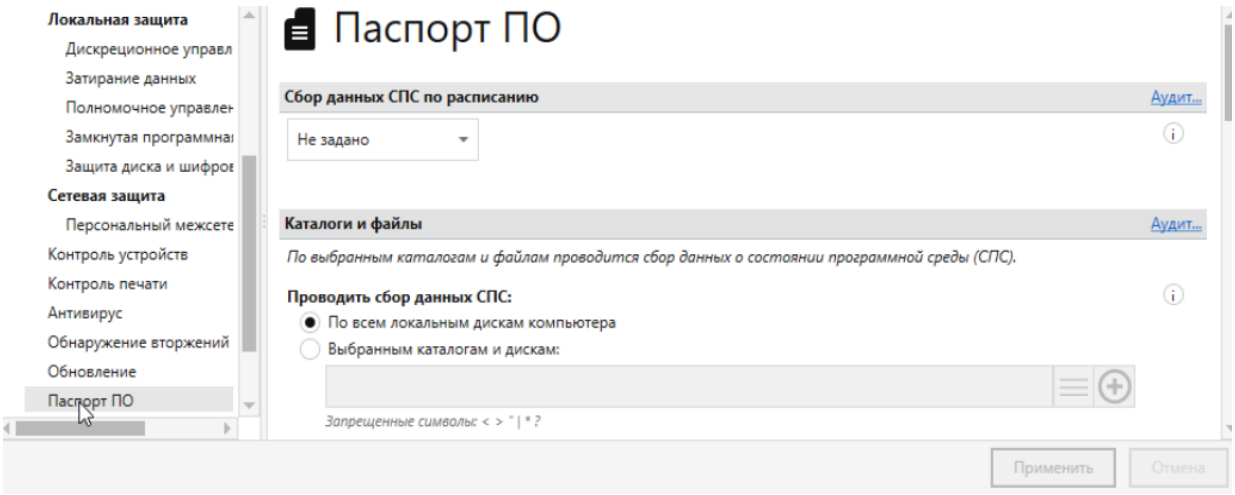

Рисунок Б.83. – Настройка паспорта ПО

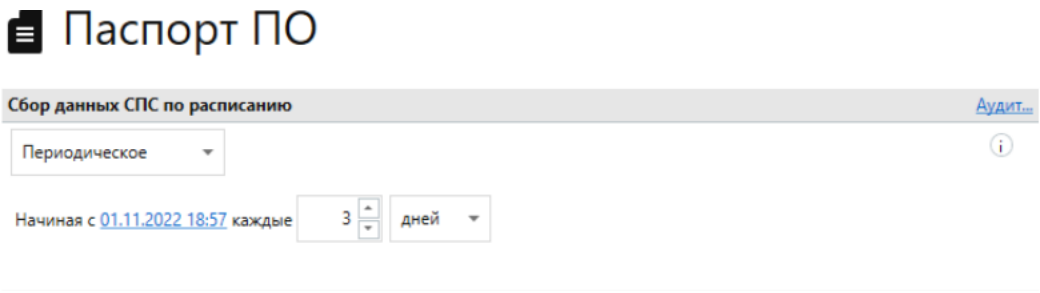

Рисунок Б.84. – Настройка паспорта ПО: сбор данных СПС по расписанию

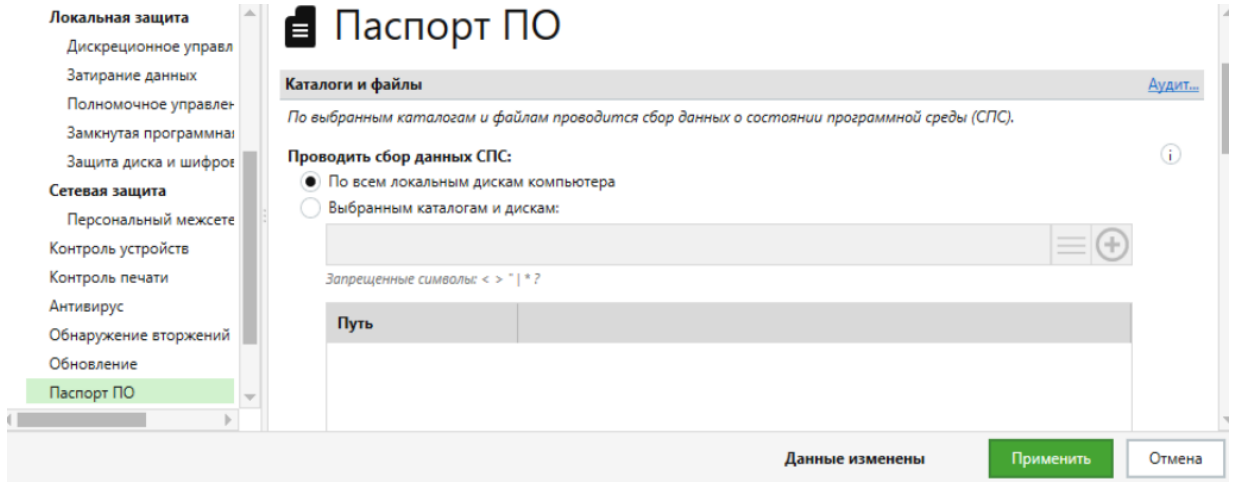

Рисунок Б.85. – Настройка паспорта ПО: каталоги и файлы

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

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 () 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.

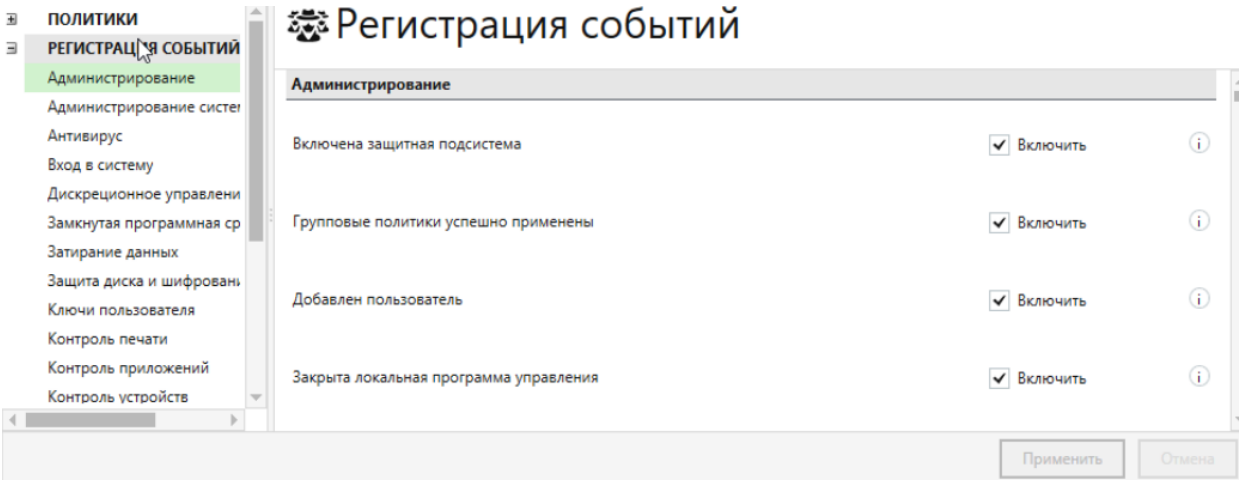

Рисунок Б.88. – Окно настройка регистрации событий

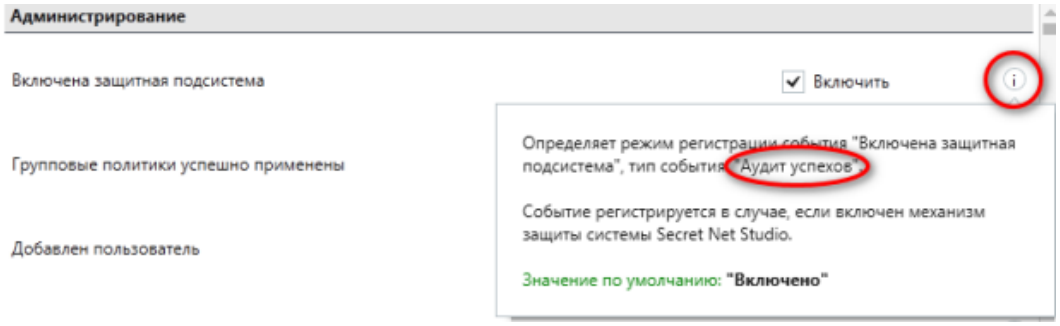

Рисунок Б.89. – Окно информации о событии

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 реализуется 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 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

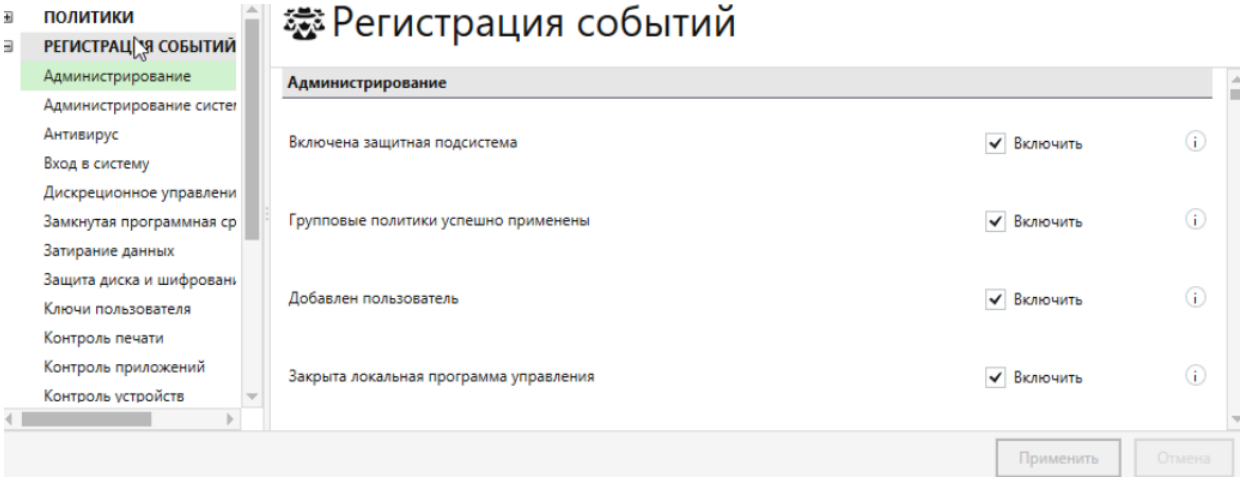

Рисунок Б.90. – Настройка администрирования, начало

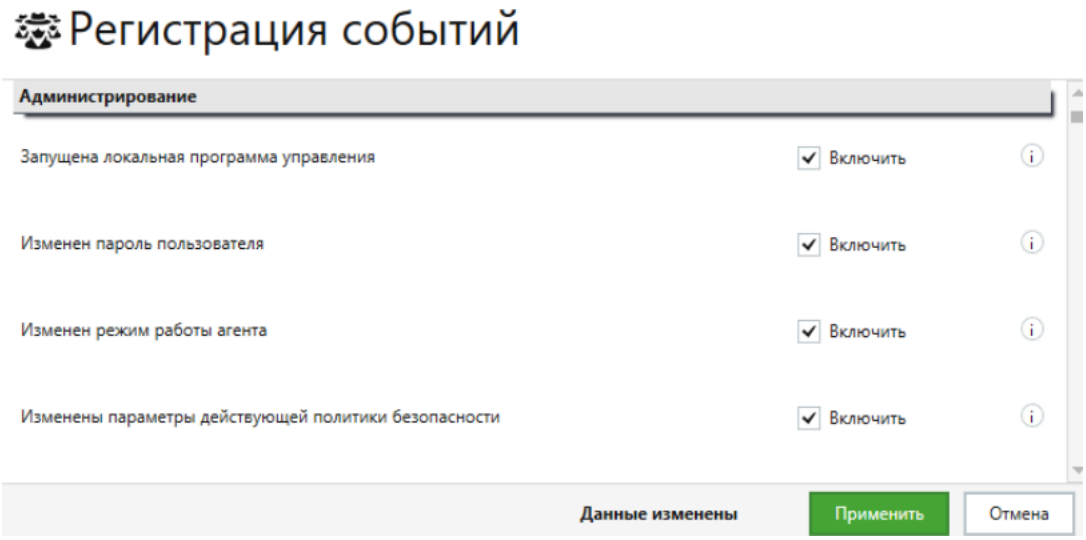

Рисунок Б.91. – Настройка администрирования,
продолжение первое

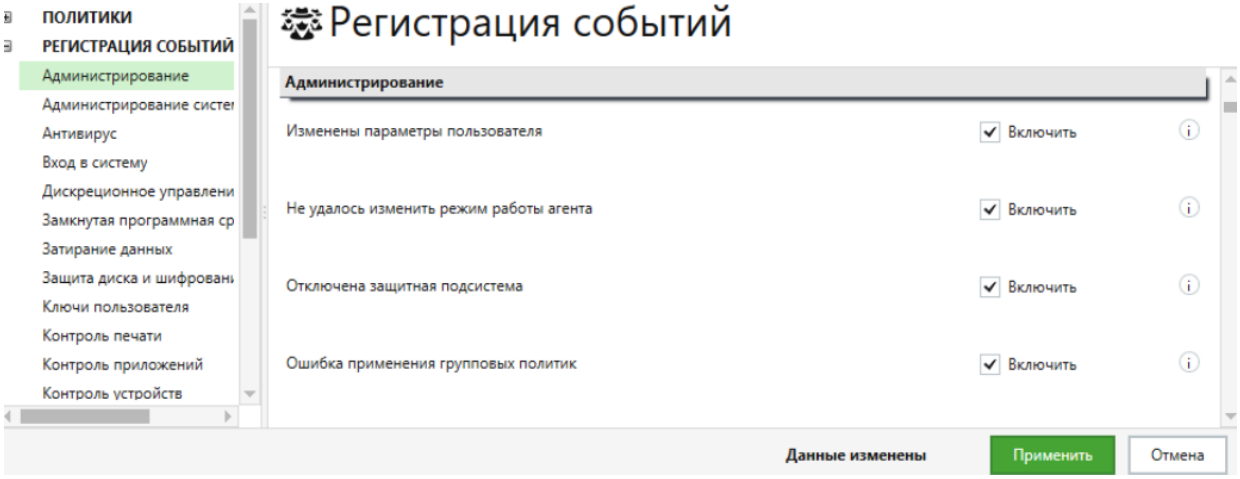

Рисунок Б.92. – Настройка администрирования,
продолжение второе

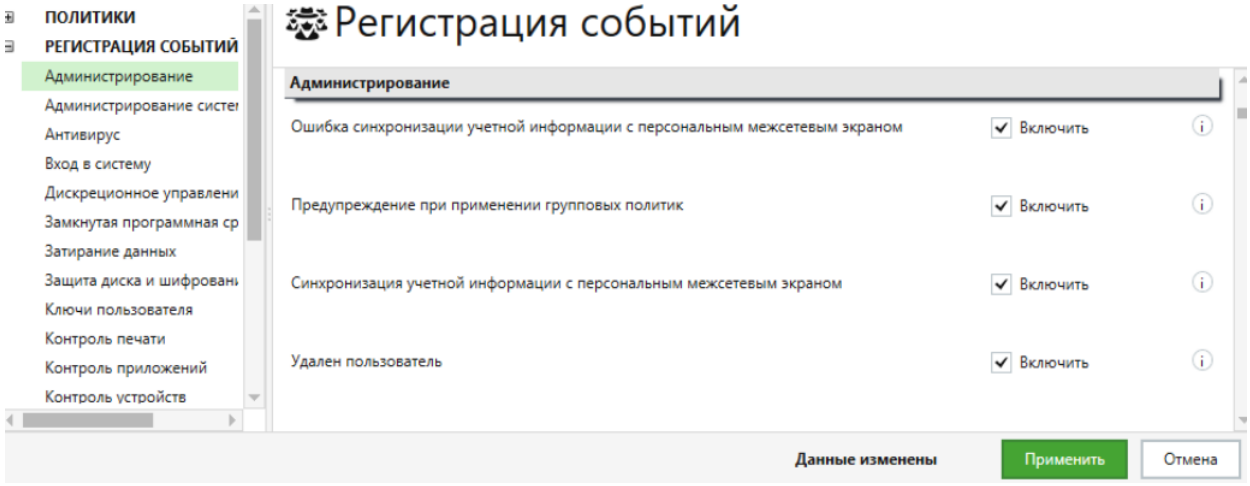

Рисунок Б.93. – Настройка администрирования, завершение

Настройка администрирования системы защиты

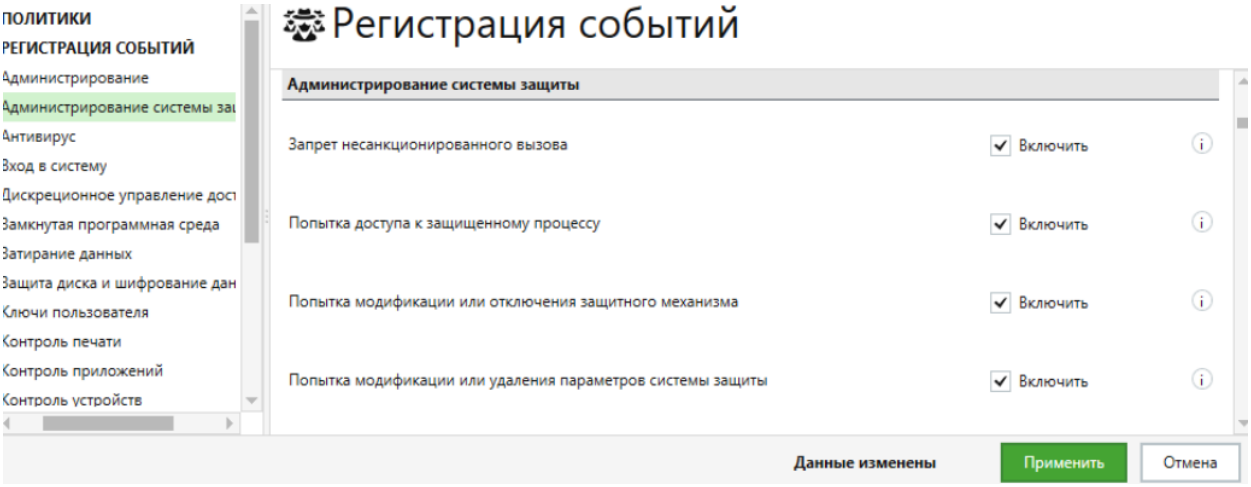

Рисунок Б.94. – Настройка администрирования системы защиты

Настройка антивируса

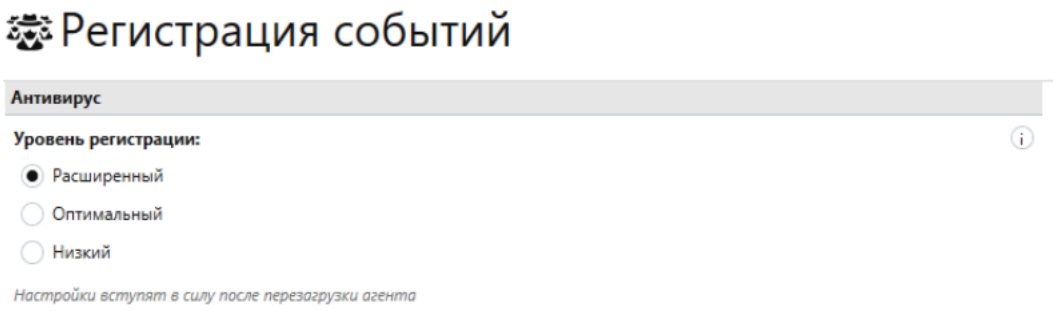

Рисунок Б.95. – Настройка антивируса

Настройка входа в систему

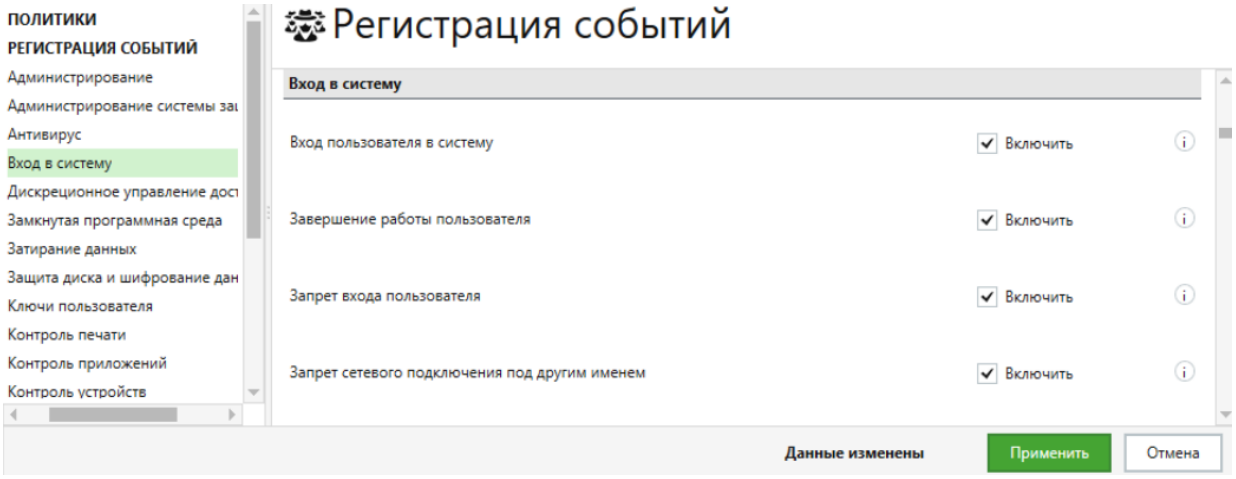

Рисунок Б.96. – Настройка входа в систему, начало

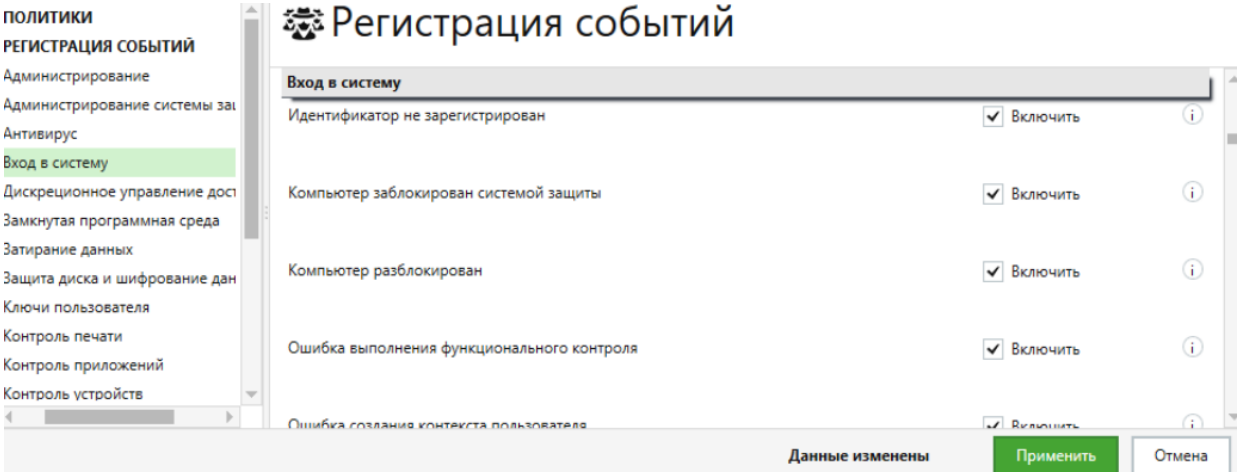

Рисунок Б.97. – Настройка входа в систему,
продолжение первое

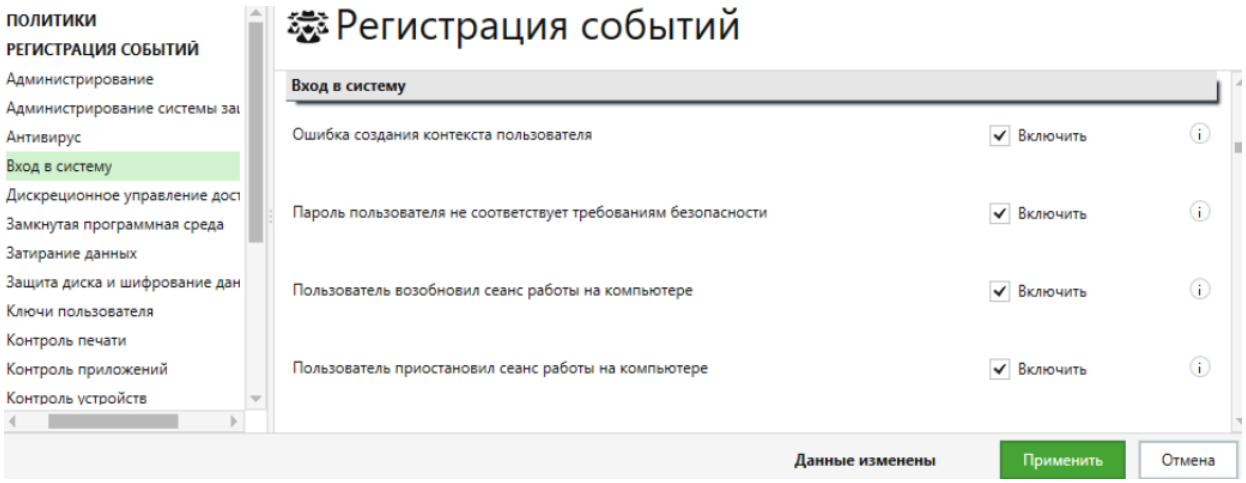

Рисунок Б.98. – Настройка входа в систему,
продолжение второе

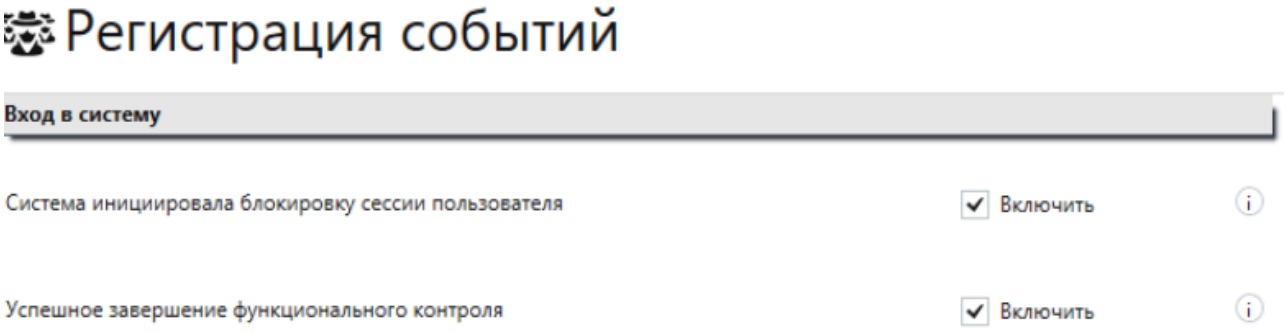

Рисунок Б.99. – Настройка входа в систему, завершение

Настройка дискреционного управления доступом

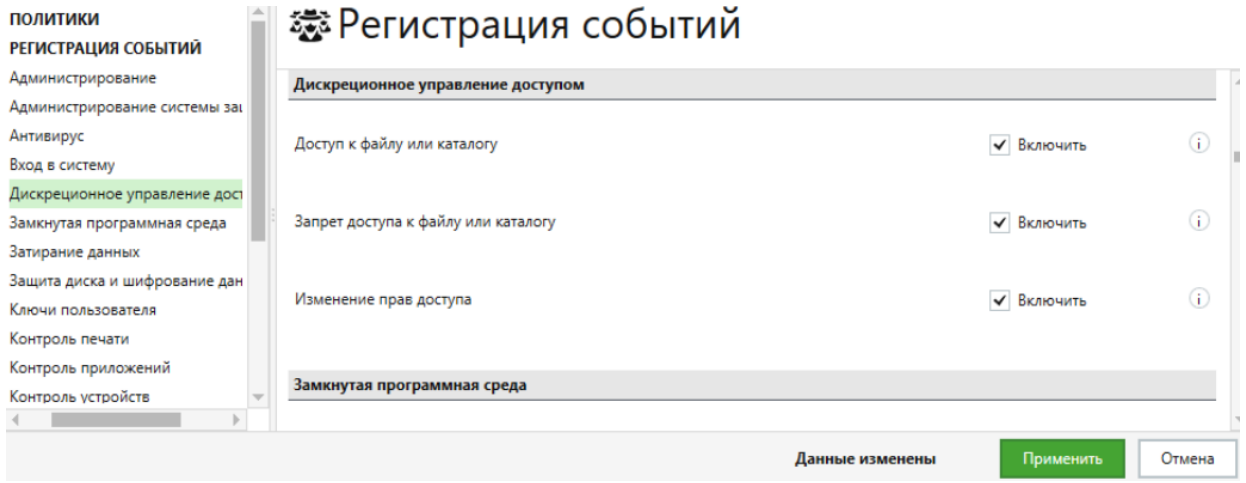

Рисунок Б.100. – Настройка дискреционного управления
доступом

Настройка замкнутой программной среды

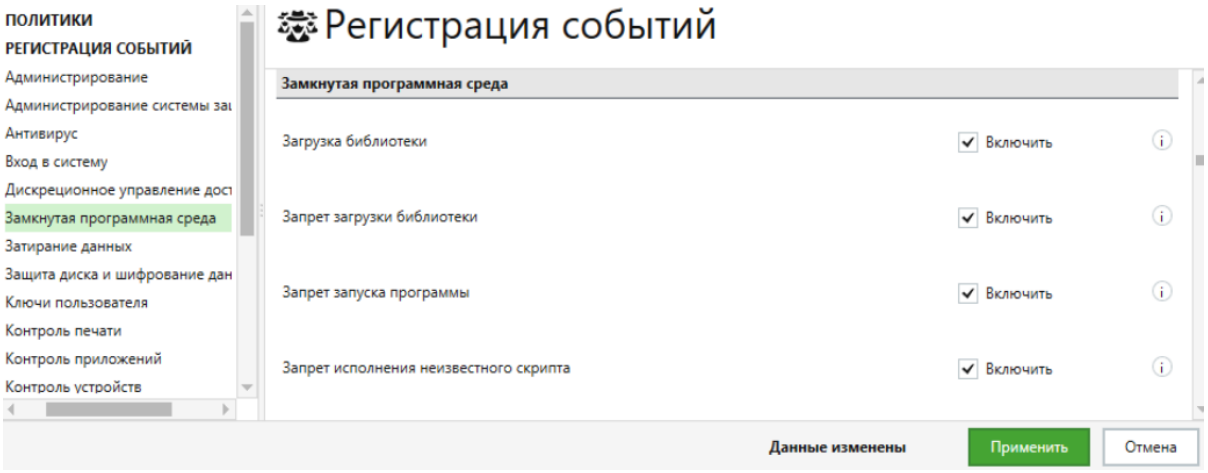

Рисунок Б.101. – Настройка замкнутой программной среды

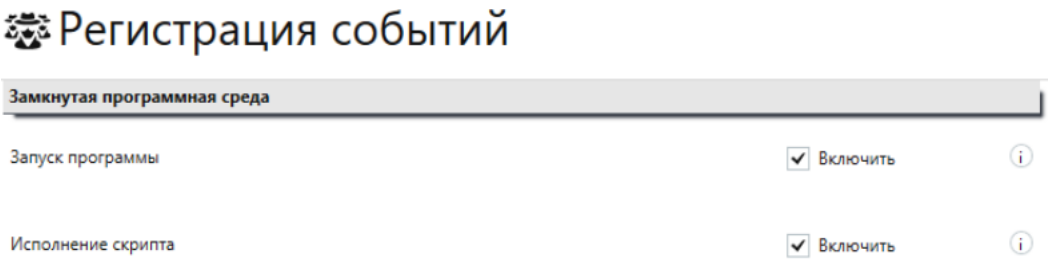

Рисунок Б.102. – Настройка замкнутой программной среды, продолжение

Настройка затирания данных

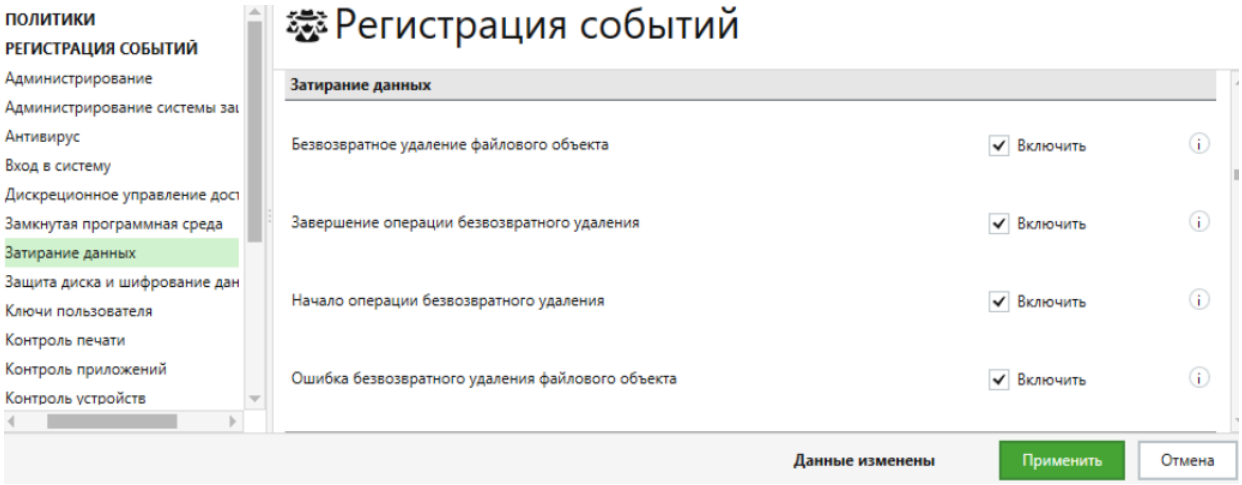

Рисунок Б.103. – Настройка затирания данных, начало

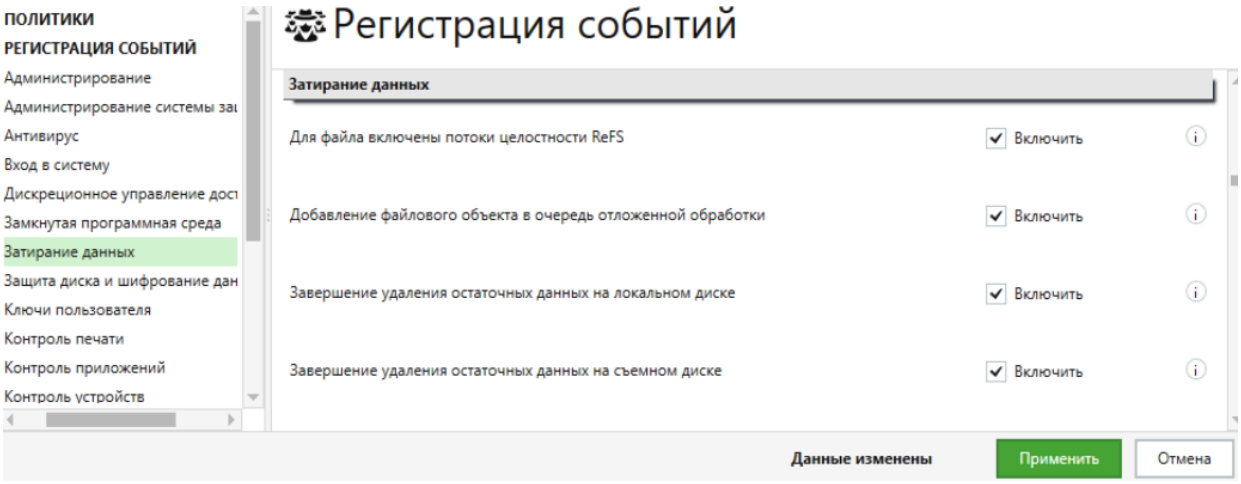

Рисунок Б.104. – Настройка затирания данных,
продолжение первое

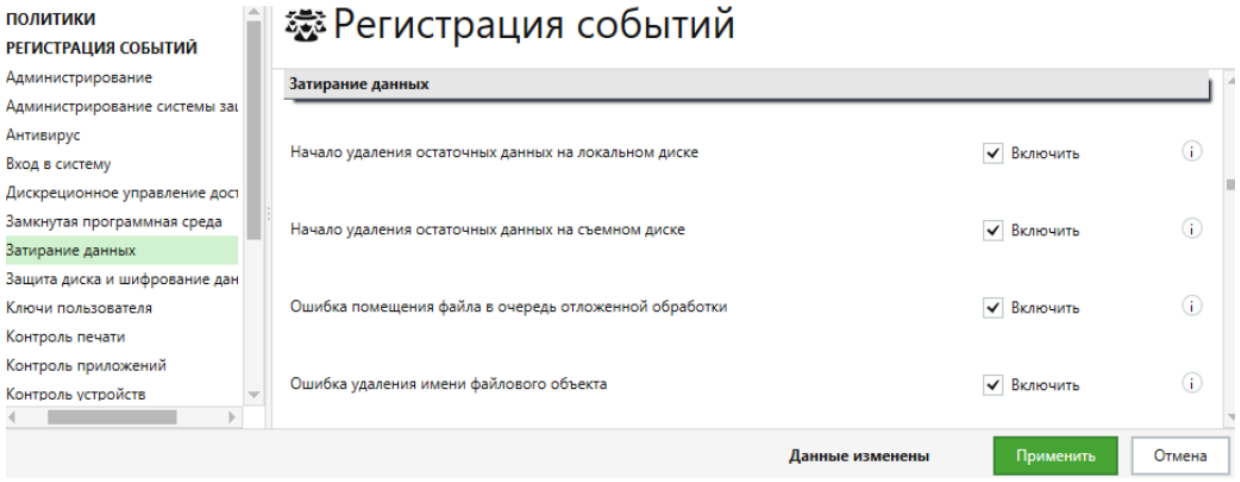

Рисунок Б.105. – Настройка затирания данных,
продолжение второе

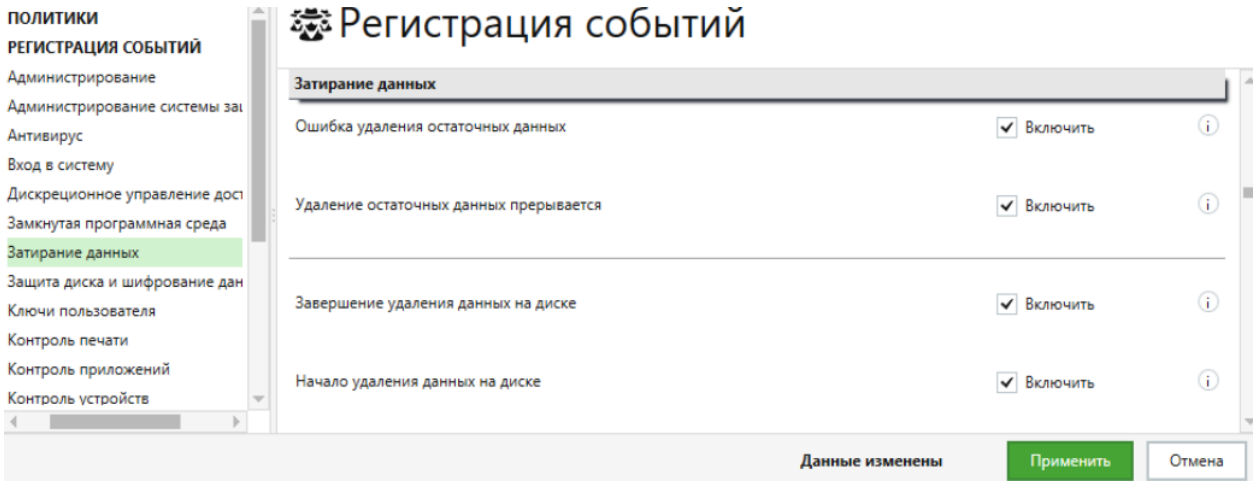

Рисунок Б.106. – Настройка затирания данных,
продолжение третье

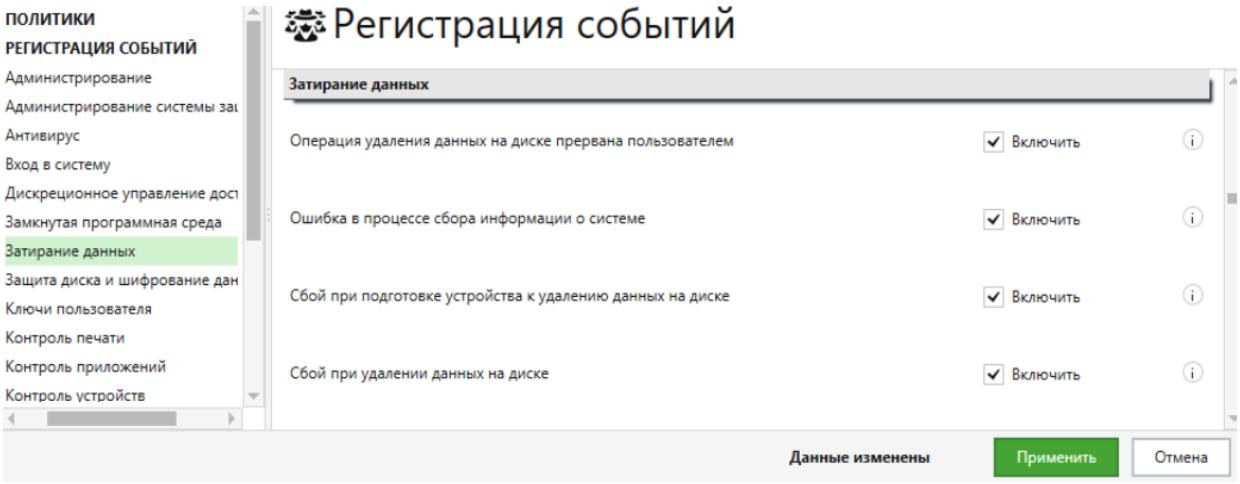

Рисунок Б.107. – Настройка затирания данных, завершение

Настройка защиты диска и шифрования данных

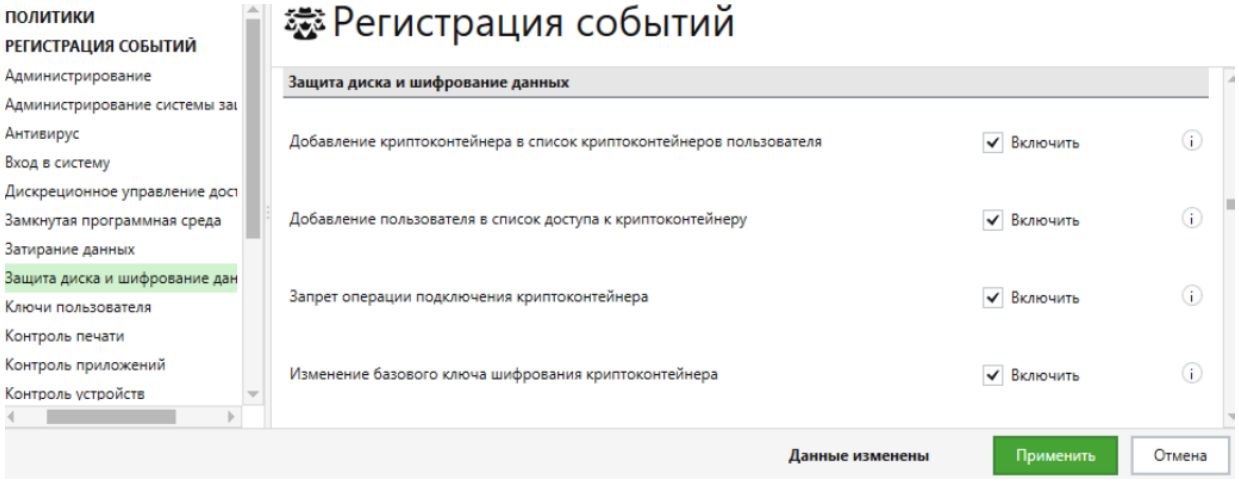

Рисунок Б.108. – Настройка защиты диска и шифрования данных, начало

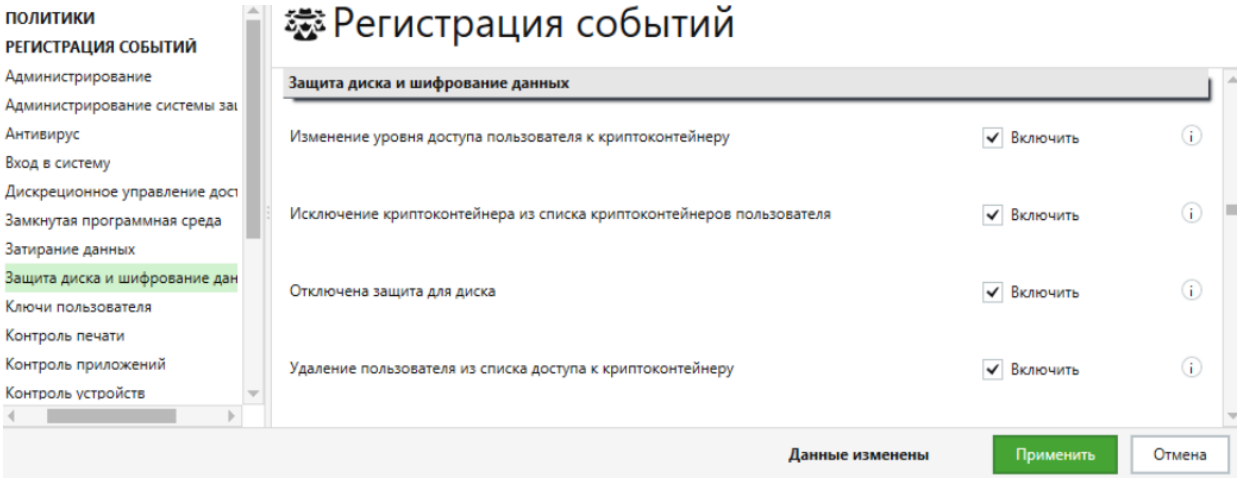

Рисунок Б.109. – Настройка защиты диска и шифрования данных, продолжение

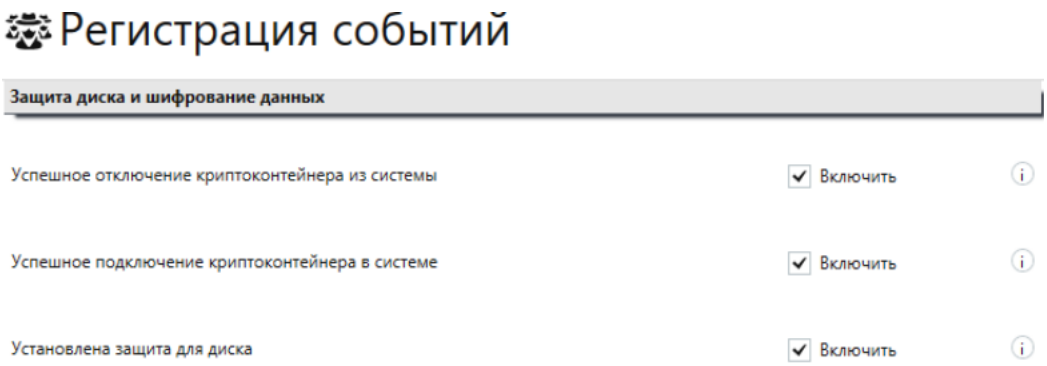

Рисунок Б.110. – Настройка защиты диска и шифрования данных, завершение

Настройка ключей пользователя

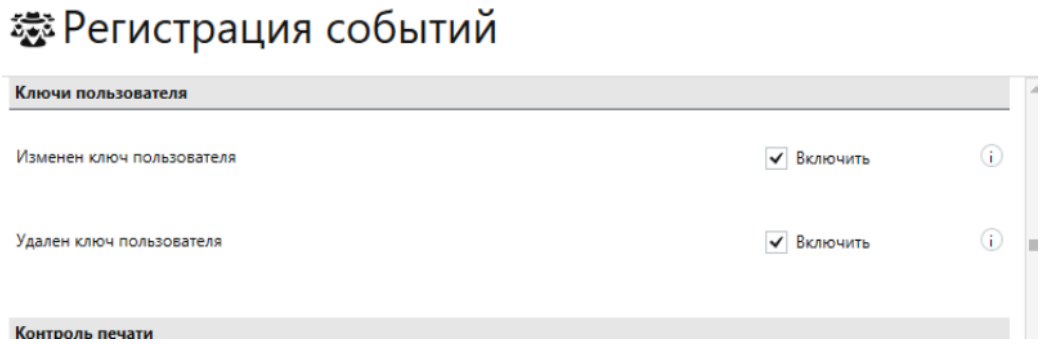

Рисунок Б.111. – Настройка ключей пользователя

Настройка контроля печати

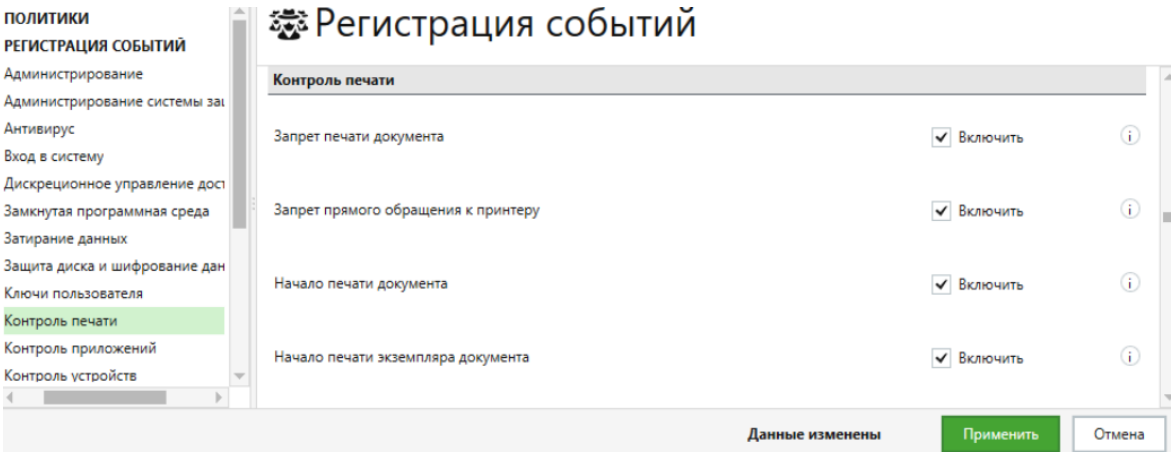

Рисунок Б.112. – Настройка контроля печати, начало

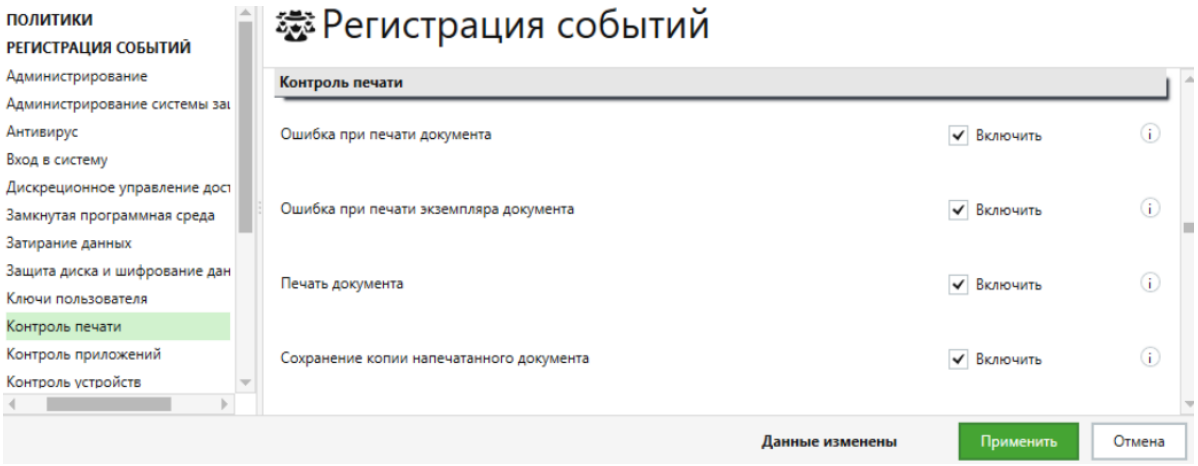

Рисунок Б.113. – Настройка контроля печати, продолжение

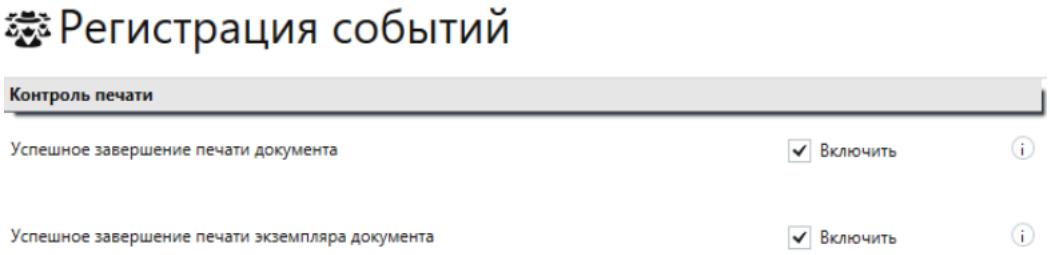

Рисунок Б.114. – Настройка контроля печати, завершение

Настройка контроля приложений

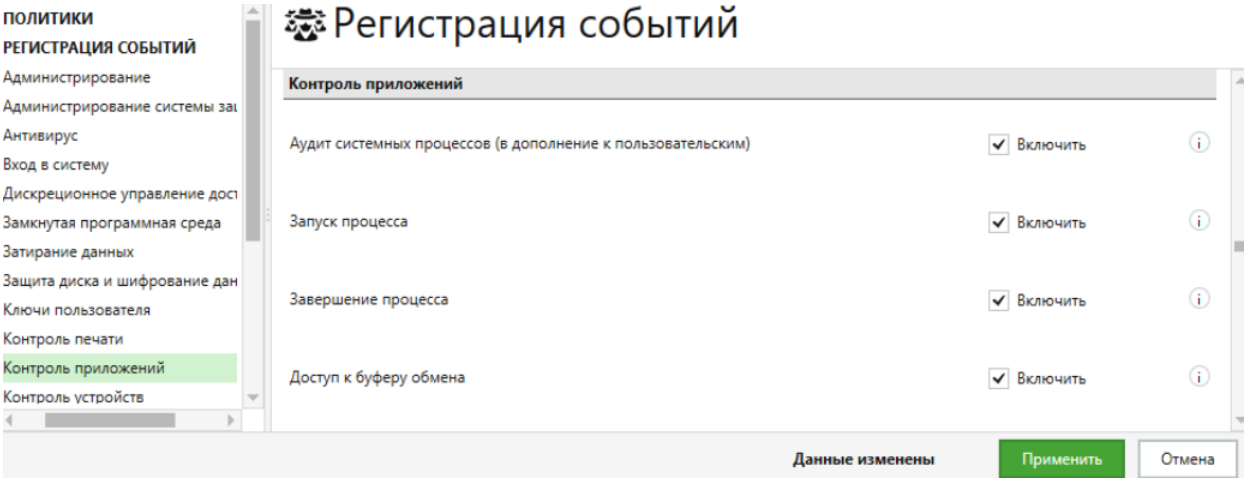

Рисунок Б.115. – Настройка контроля приложений, начало

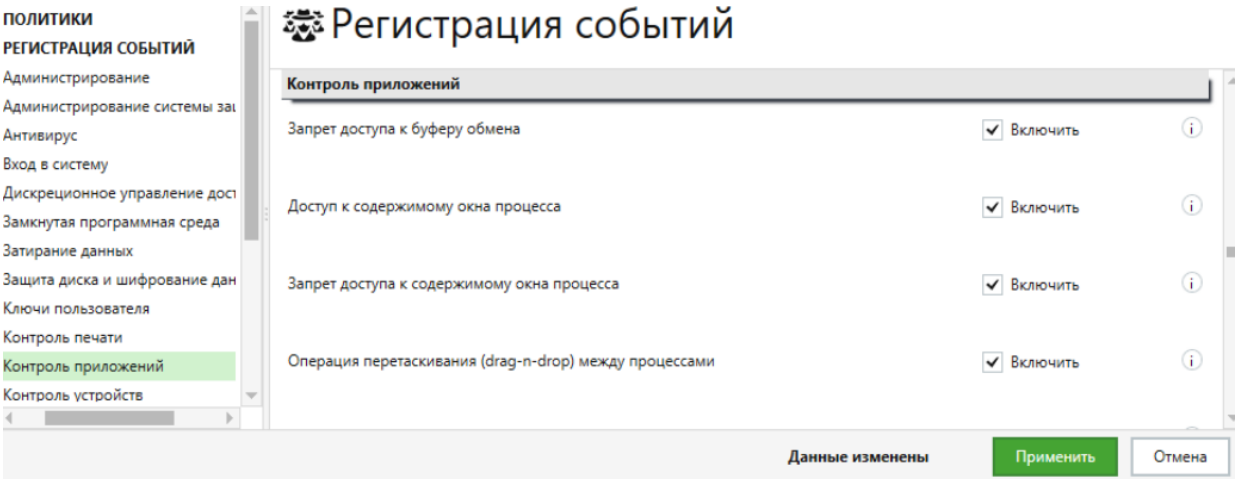

Рисунок Б.116. – Настройка контроля приложений, продолжение

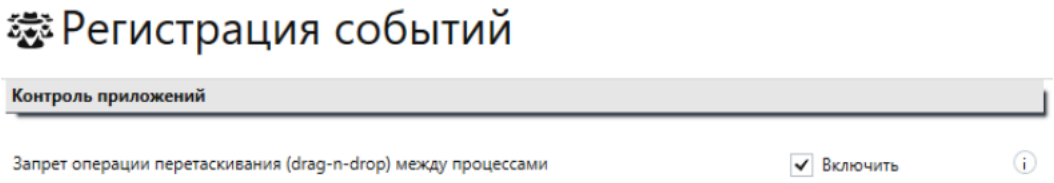

Рисунок Б.117. – Настройка контроля приложений, завершение

Настройка контроля устройств

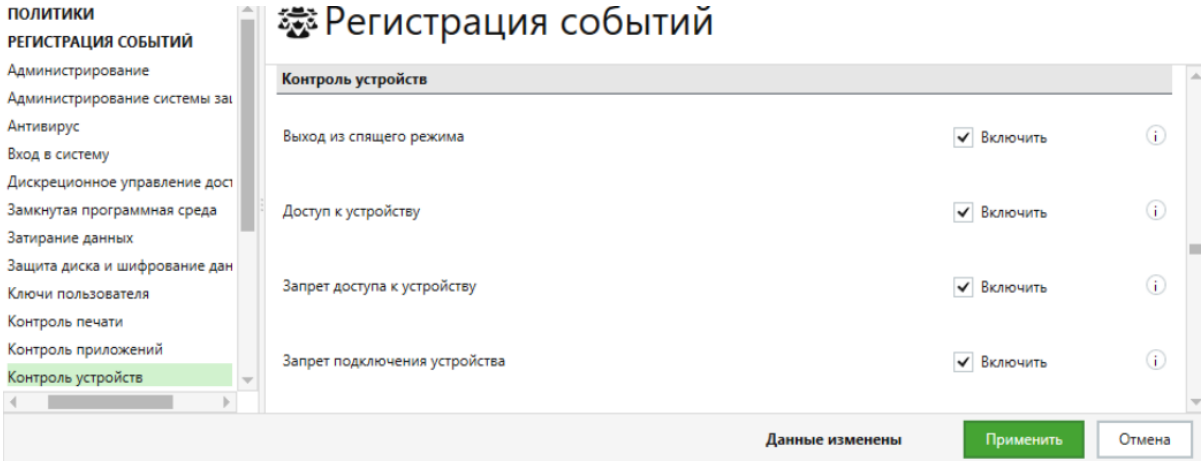

Рисунок Б.118. – Настройка контроля устройств, начало

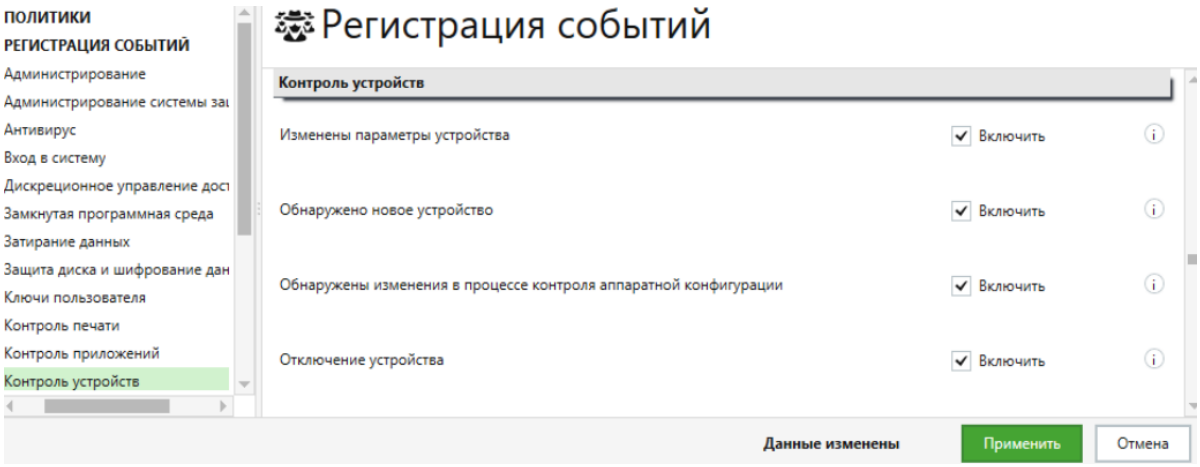

Рисунок Б.119. – Настройка контроля устройств, продолжение первое

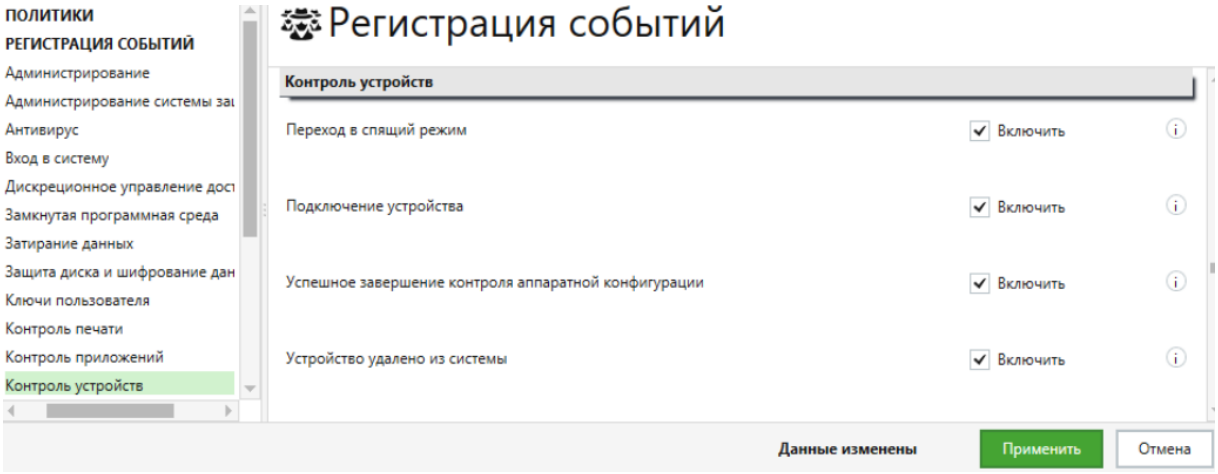

Рисунок Б.120. – Настройка контроля устройств, продолжение второе

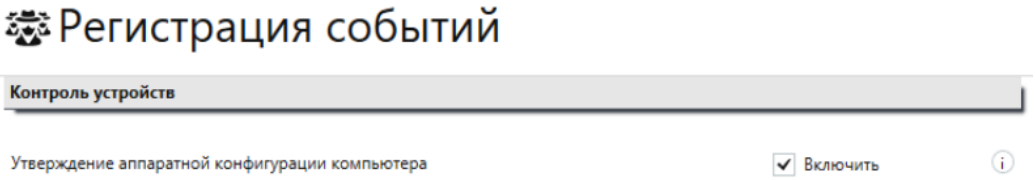

Рисунок Б.121. – Настройка контроля устройств, завершение

Настройка контроля целостности

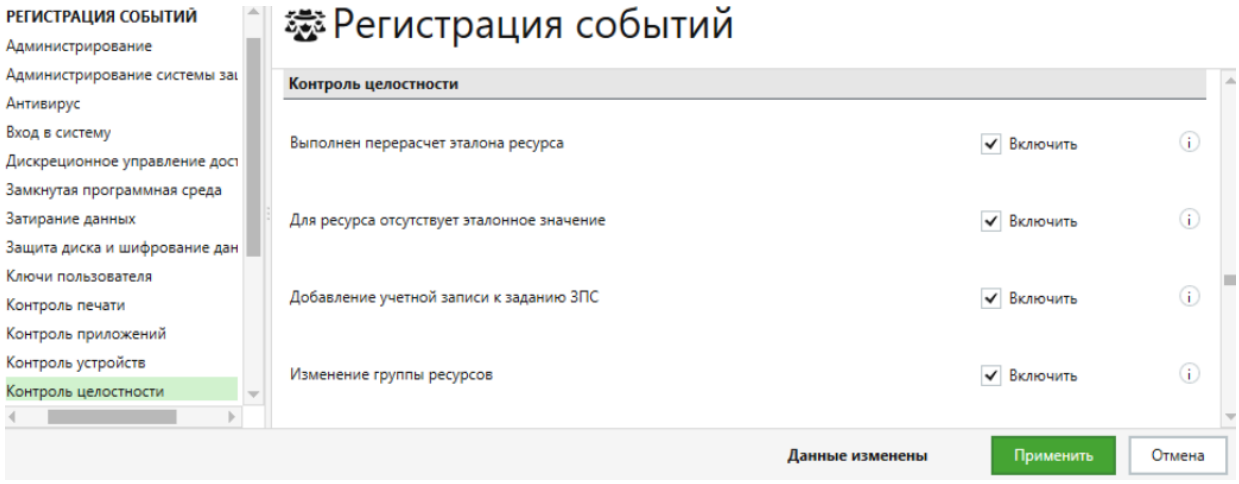

Рисунок Б.122. – Настройка контроля целостности, начало

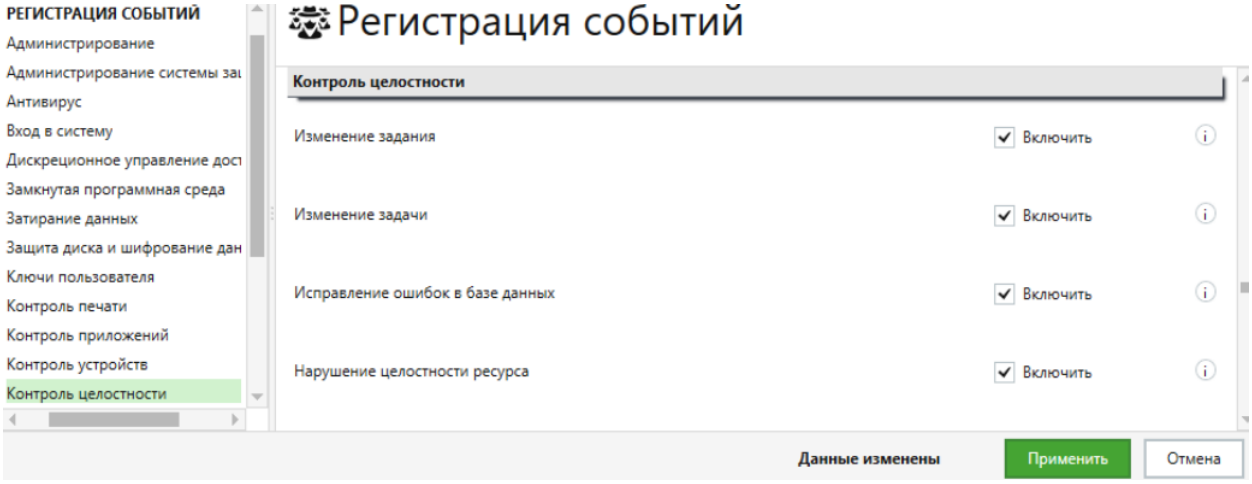

Рисунок Б.123. – Настройка контроля целостности,
продолжение первое

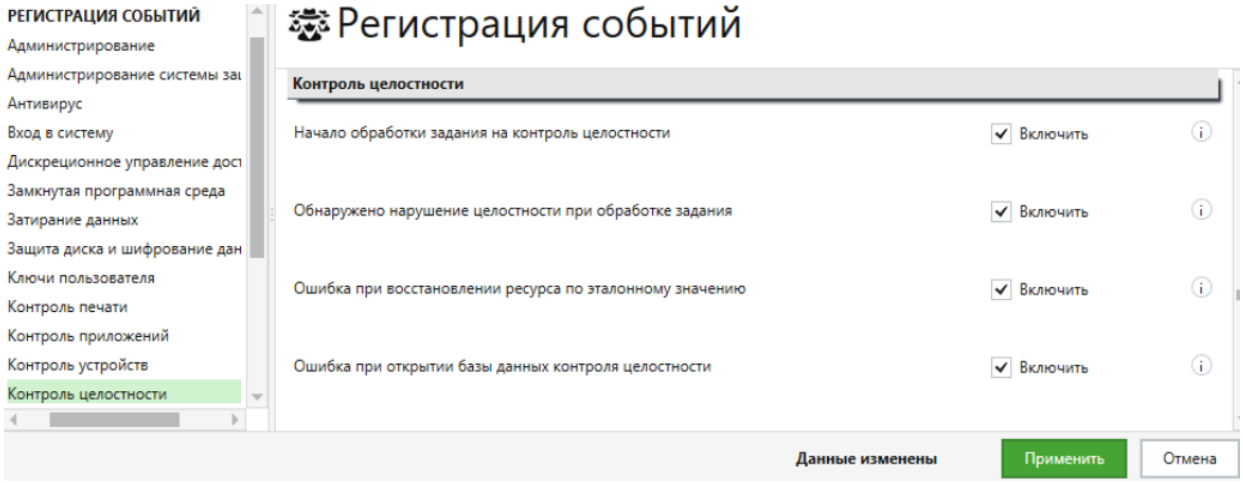

Рисунок Б.124. – Настройка контроля целостности,
продолжение второе

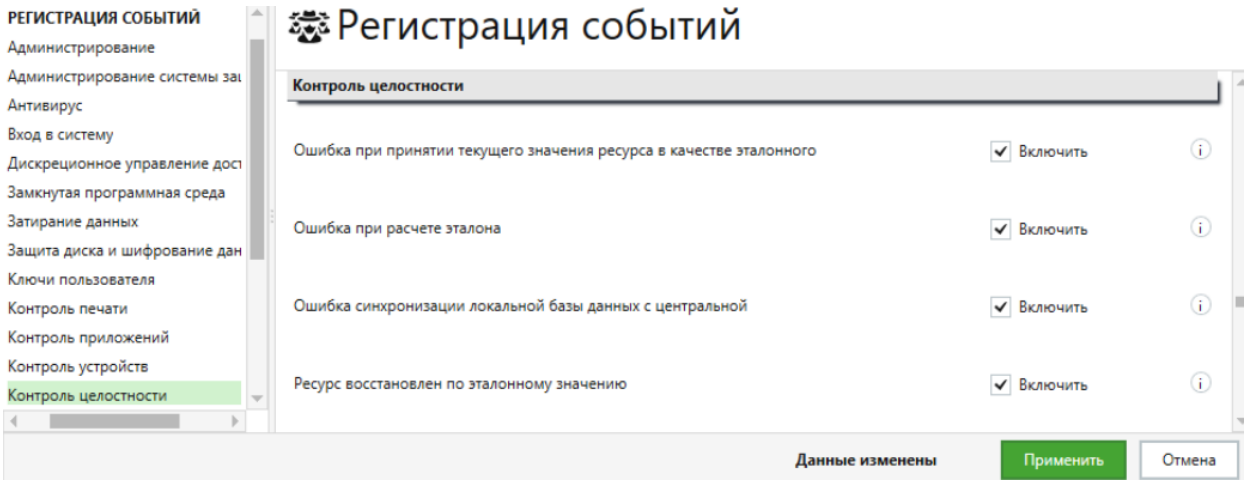

Рисунок Б.125. – Настройка контроля целостности,
продолжение третье

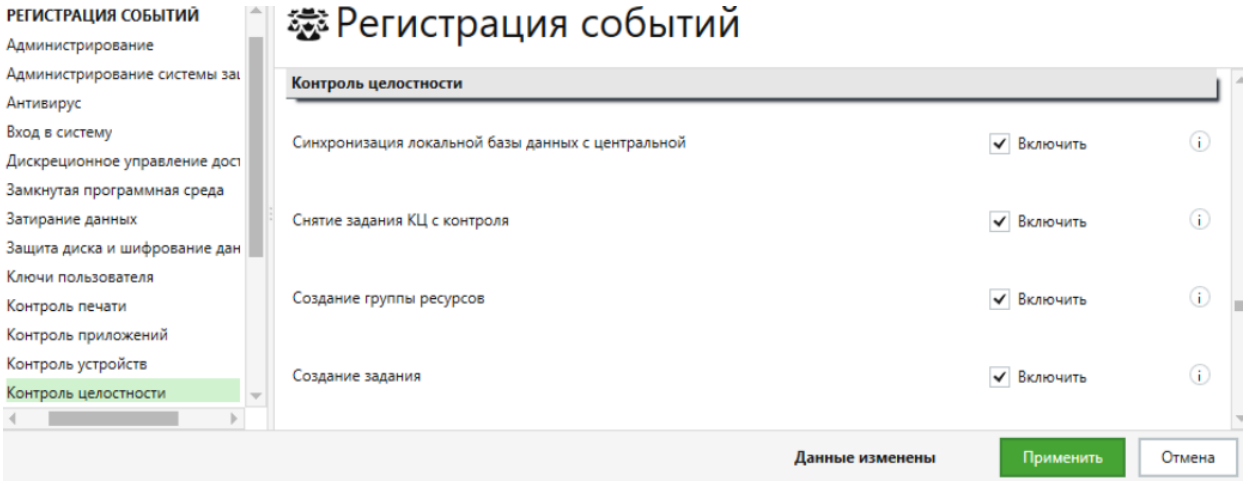

Рисунок Б.126. – Настройка контроля целостности,
продолжение четвёртое

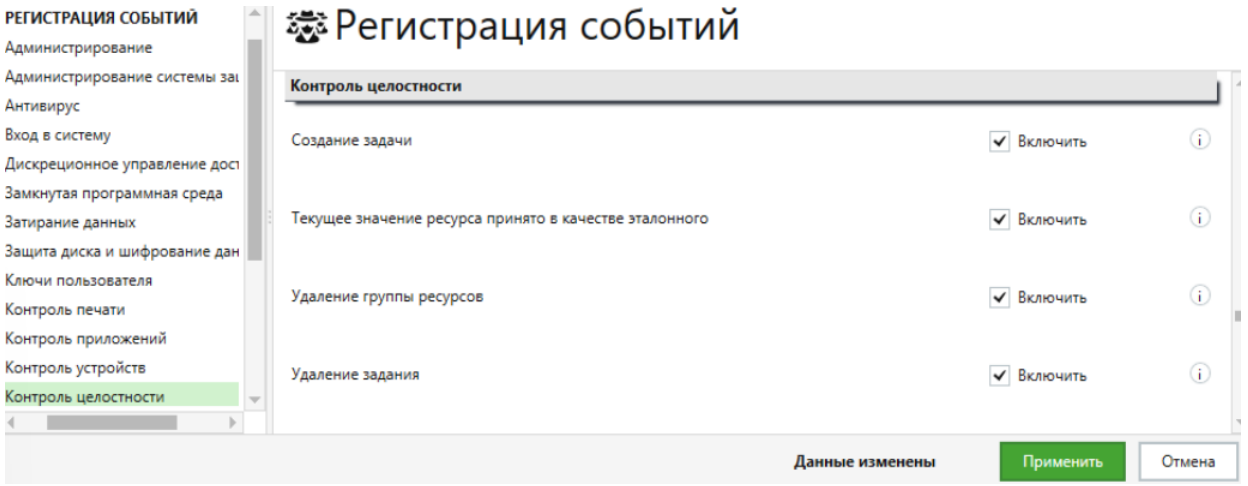

Рисунок Б.127. – Настройка контроля целостности,
продолжение пятое

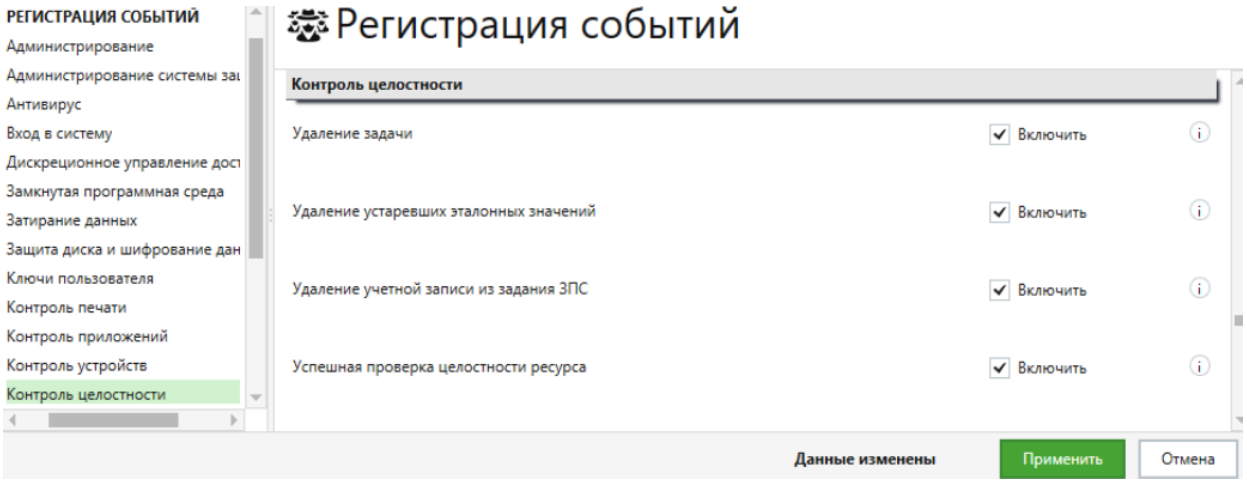

Рисунок Б.128. – Настройка контроля целостности, продолжение шестое

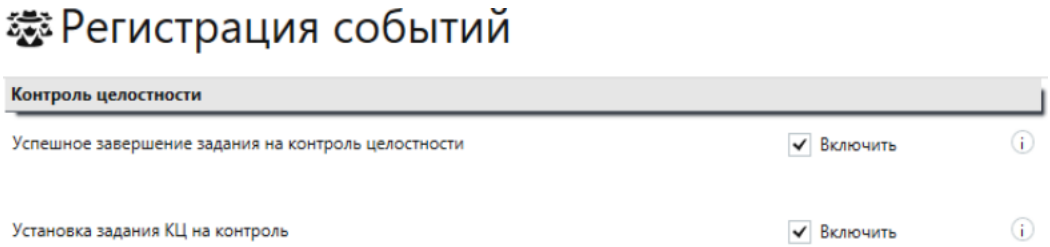

Рисунок Б.129. – Настройка контроля целостности, завершение

Настройка обнаружения вторжений

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

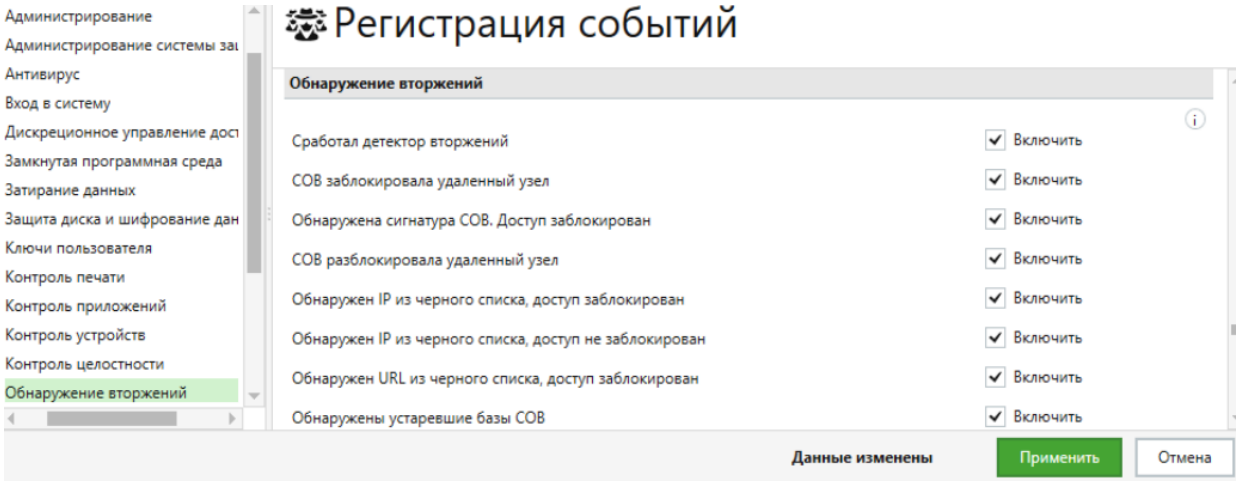

Рисунок Б.130. – Настройка обнаружения вторжений

Настройка общих событий

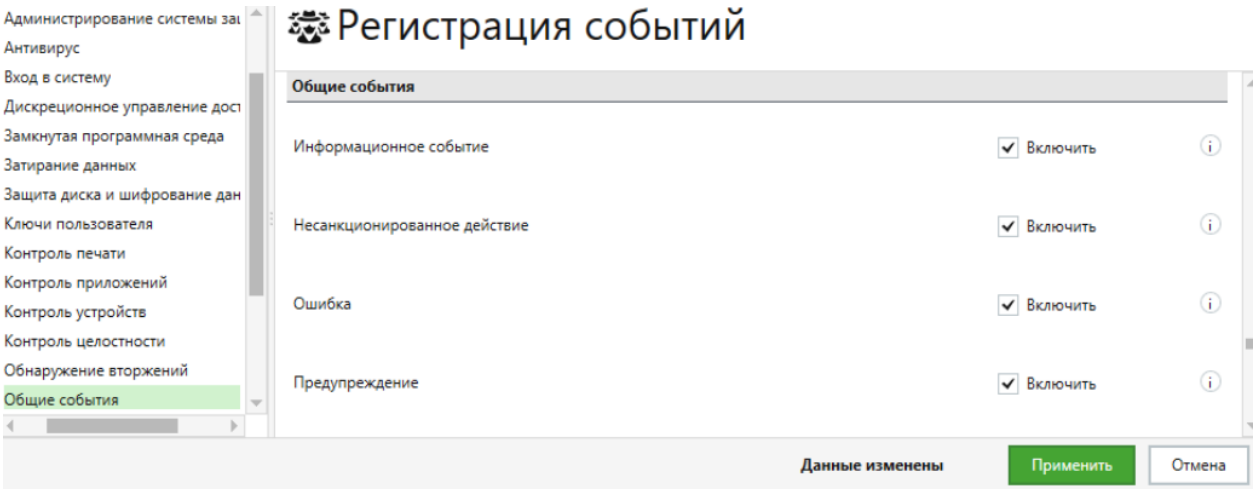

Рисунок Б.131. – Настройка общих событий

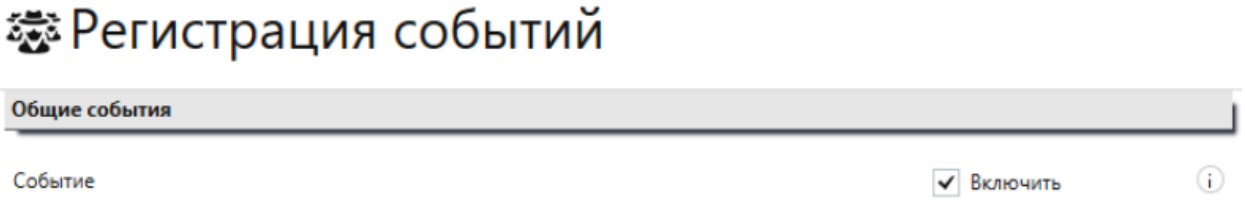

Рисунок Б.132. – Настройка общих событий, продолжение

Настройка паспорта ПО

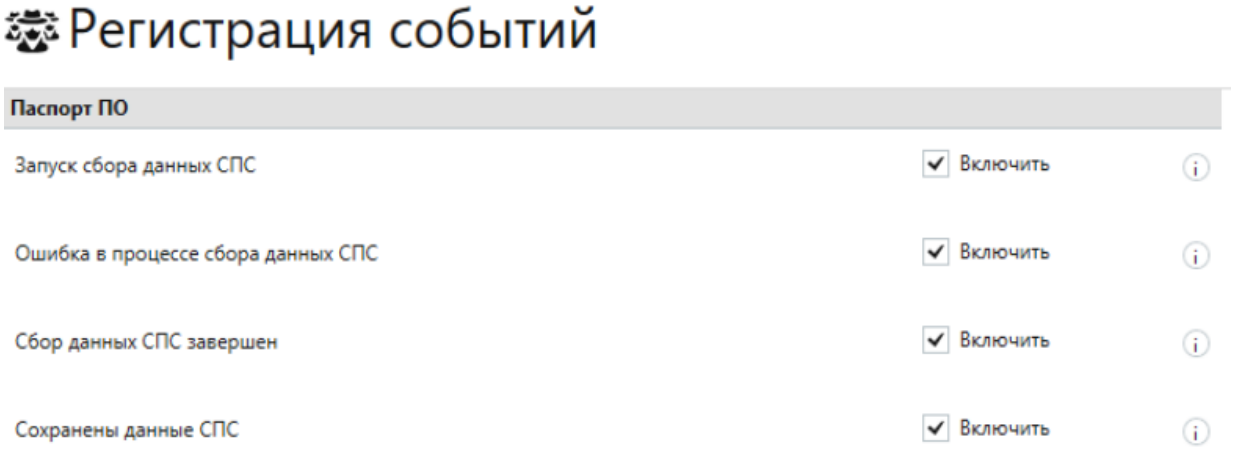

Рисунок Б.133. – Настройка паспорта ПО

Настройка полномочного управления доступом

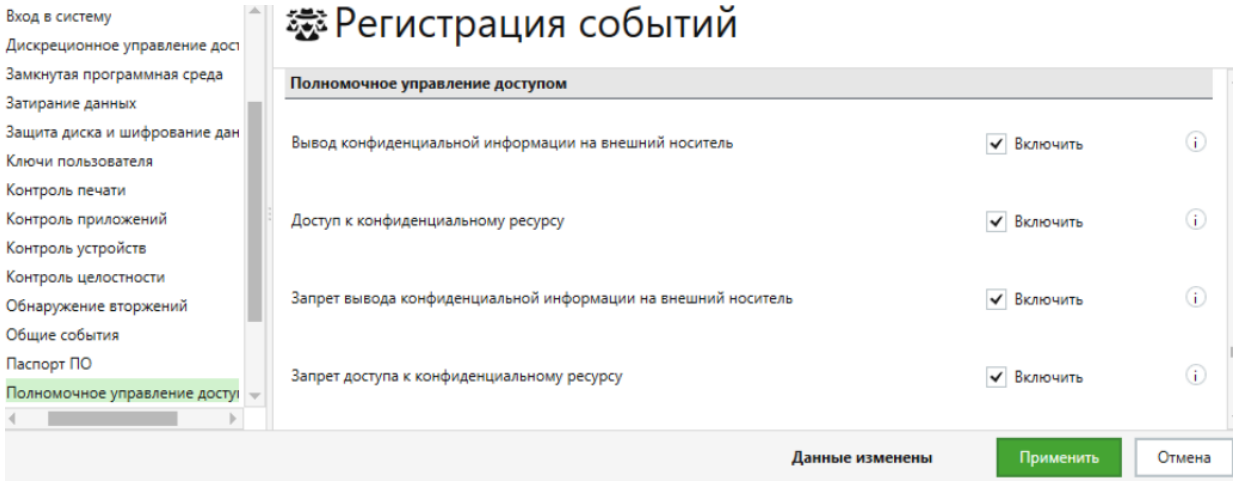

Рисунок Б.134. – Настройка полномочного управления доступом, начало

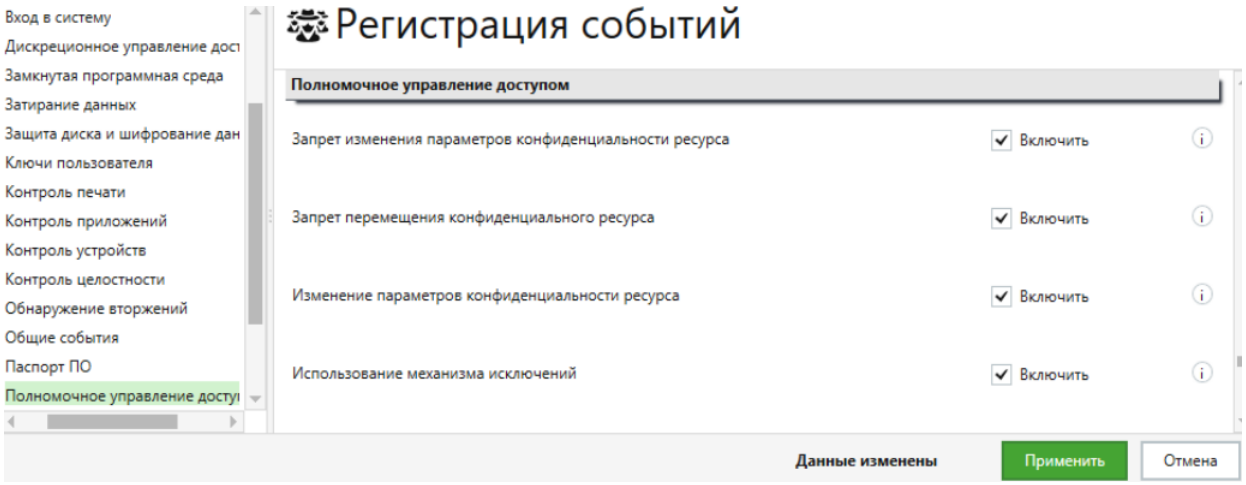

Рисунок Б.135. – Настройка полномочного управления доступом, продолжение

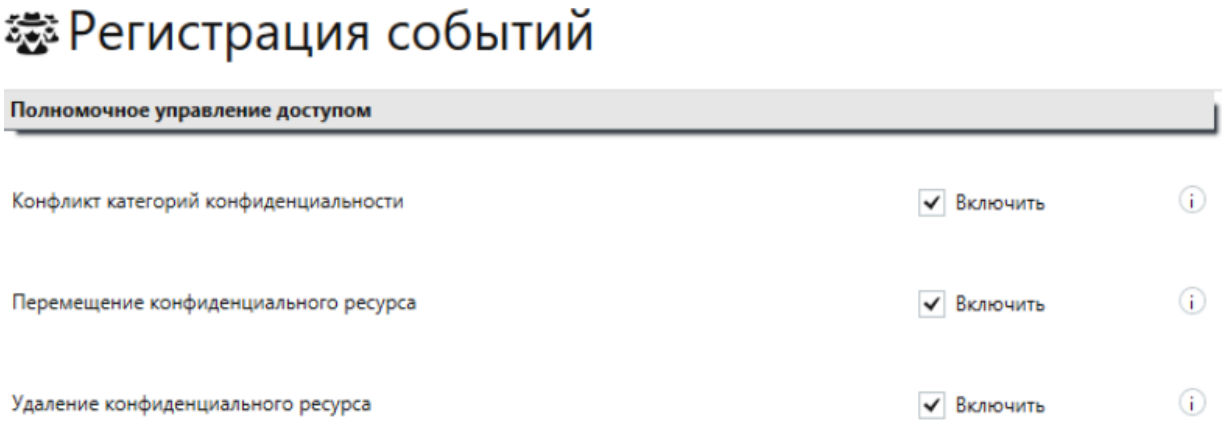

Рисунок Б.136. – Настройка полномочного управления доступом, завершение

Настройка теневого копирования

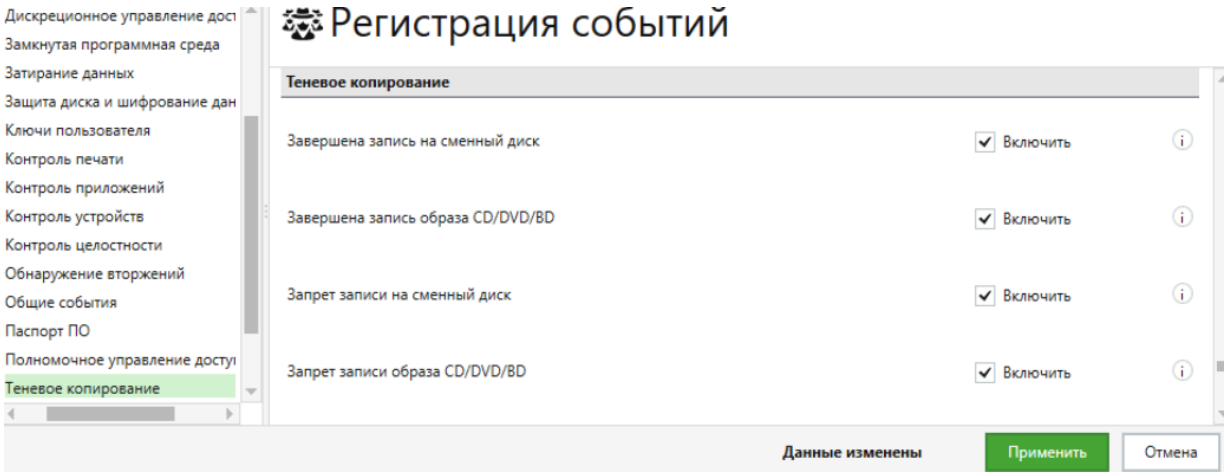

Рисунок Б.137. – Настройка теневого копирования

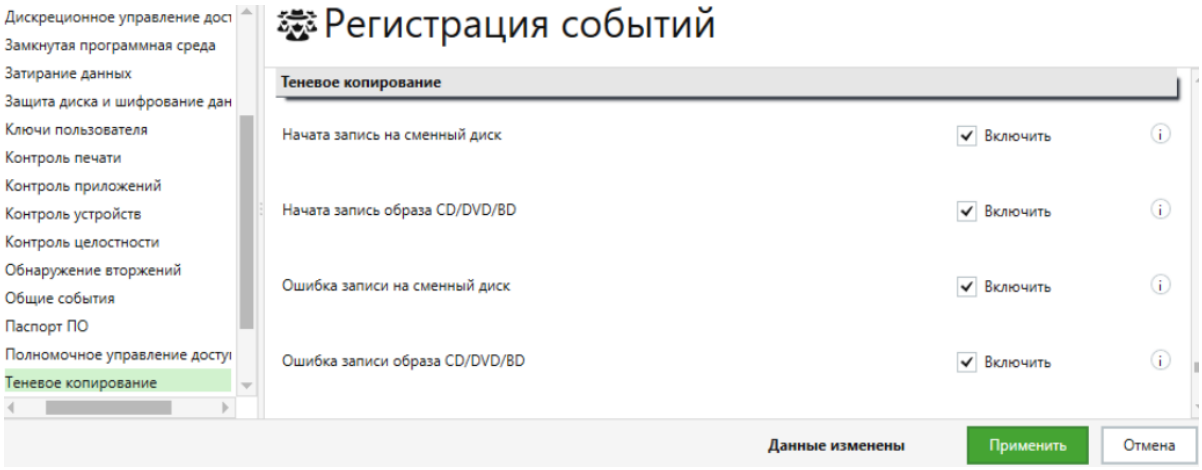

Рисунок Б.138. – Настройка теневого копирования, продолжение

Настройка ЦУ КЦ-ЗПС

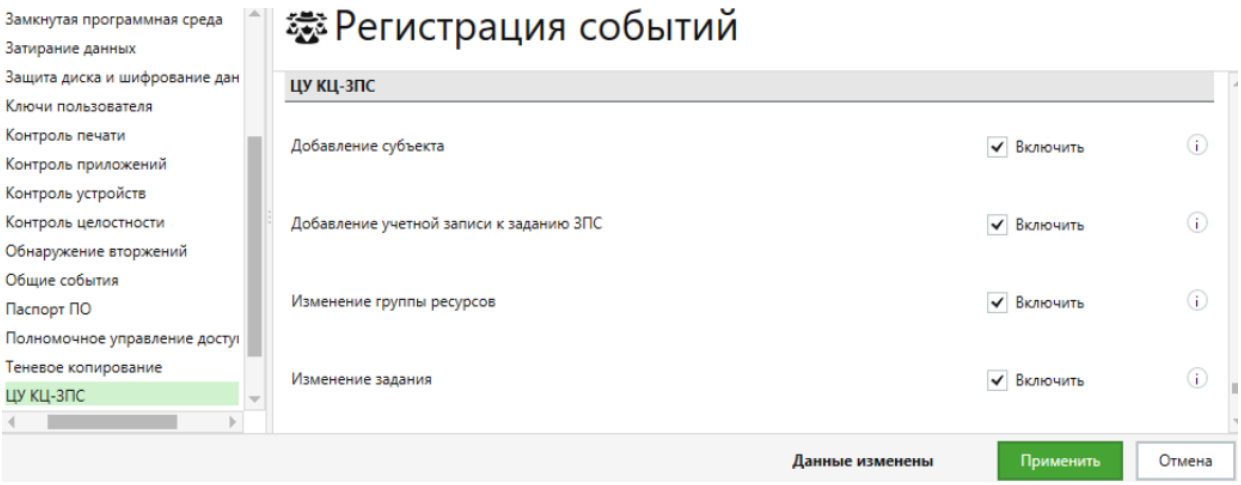

Рисунок Б.139. – Настройка ЦУ КЦ-ЗПС, начало

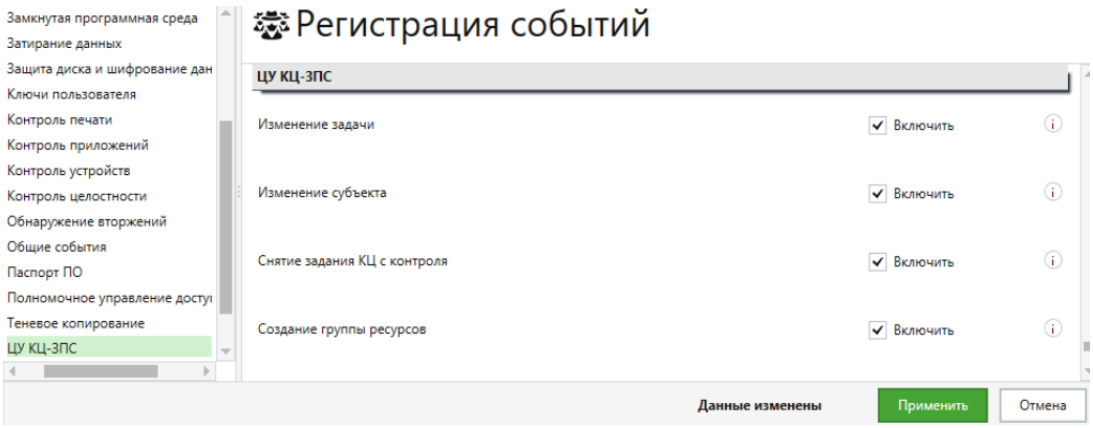

Рисунок Б.140. – Настройка ЦУ КЦ-ЗПС, продолжение первое

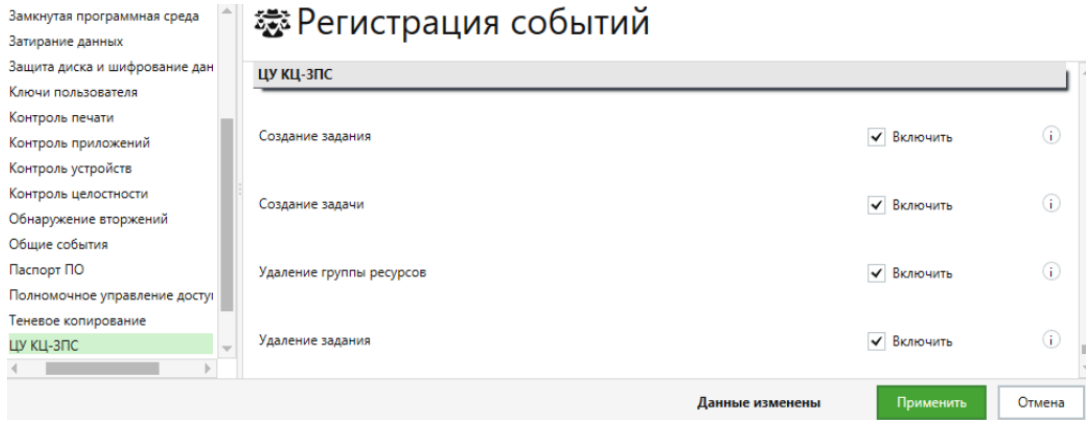

Рисунок Б.141. – Настройка ЦУ КЦ-ЗПС, продолжение второе

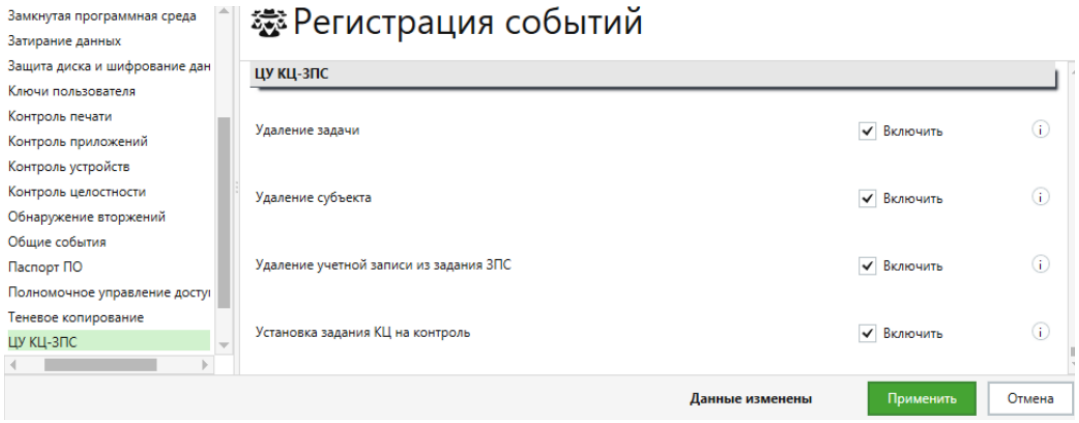

Рисунок Б.142. – Настройка ЦУ КЦ-ЗПС, завершение

Настройка группы «Параметры»

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

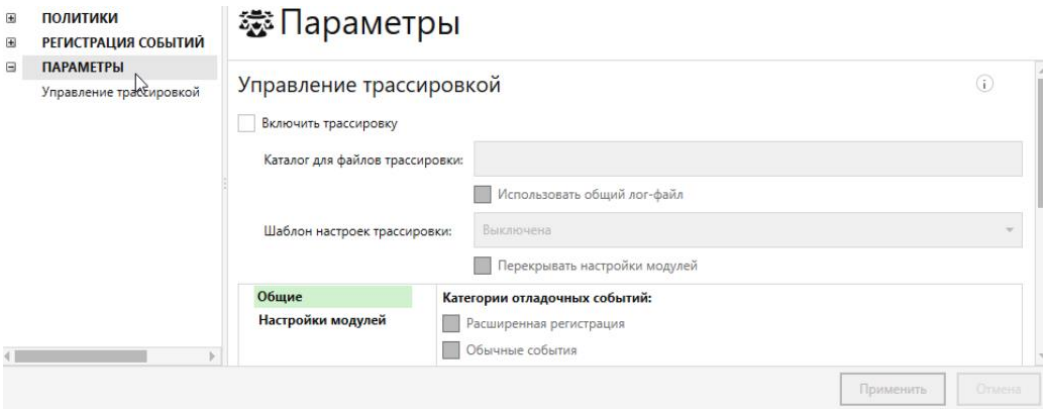

Рисунок Б.143. – Настройка параметров:
управления трассировкой

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 PIN администратора безопасности (пароль). Последовательный порядок действия при завершении процедуры активации представлен на рисунках Б.144. ÷ Б.147..

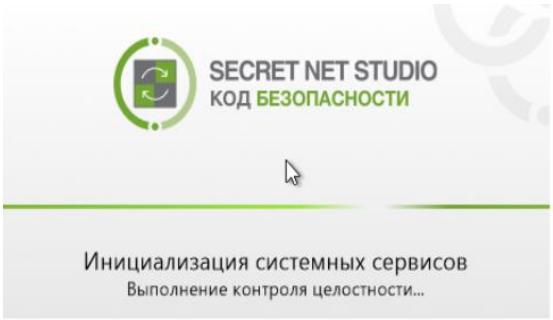

Рисунок Б.144. – Запуск «Secret Net Studio»

Рисунок Б.145. – Запуск ОС

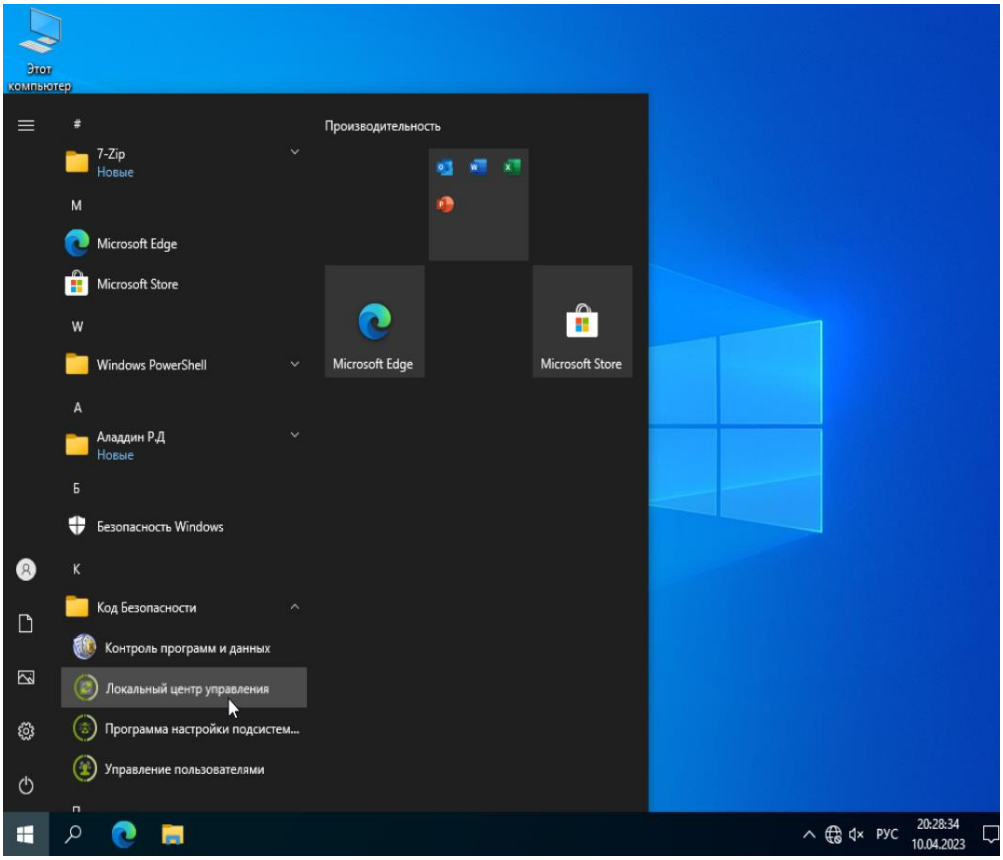

Рисунок Б.146. – Запуск «Локальный центр управления»

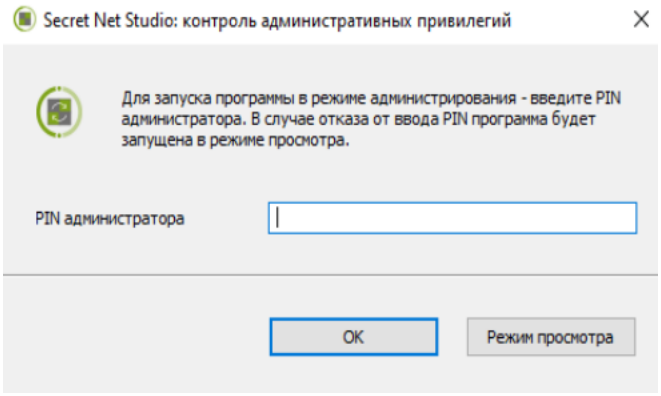

Рисунок Б.147. – Окно запроса PIN администратора безопасности

Просмотр локальных Журналов и Запросов

Журналы

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

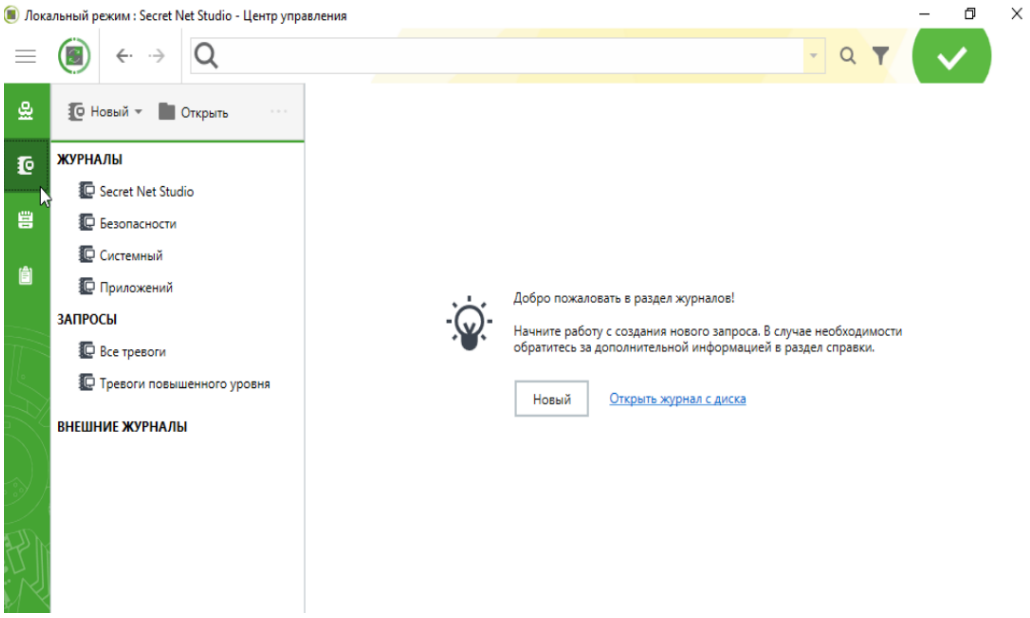

Рисунок Б.148. – Интерфейс «Журналы»

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.

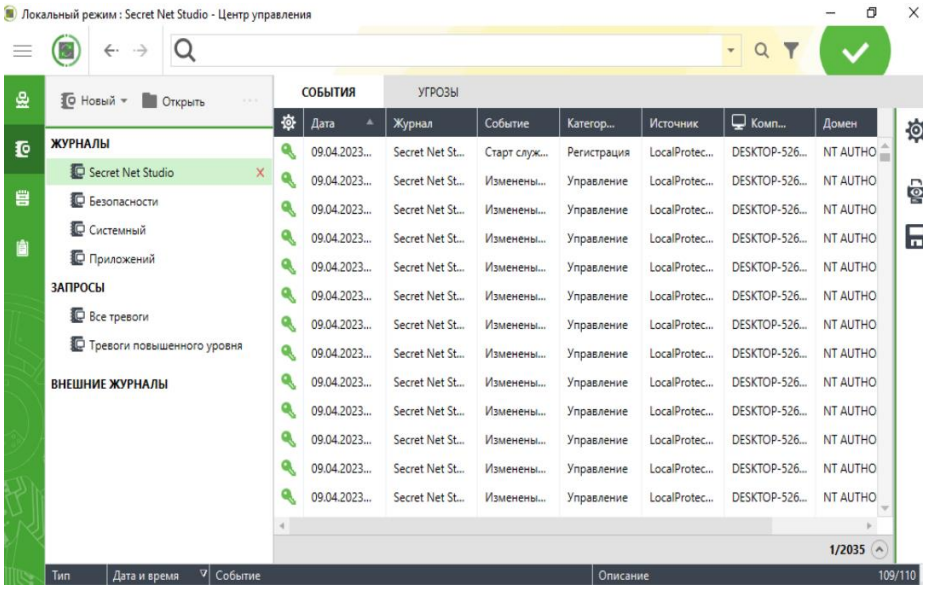

Рисунок Б.149. – Отчёт журнала «Secret Net Studio»

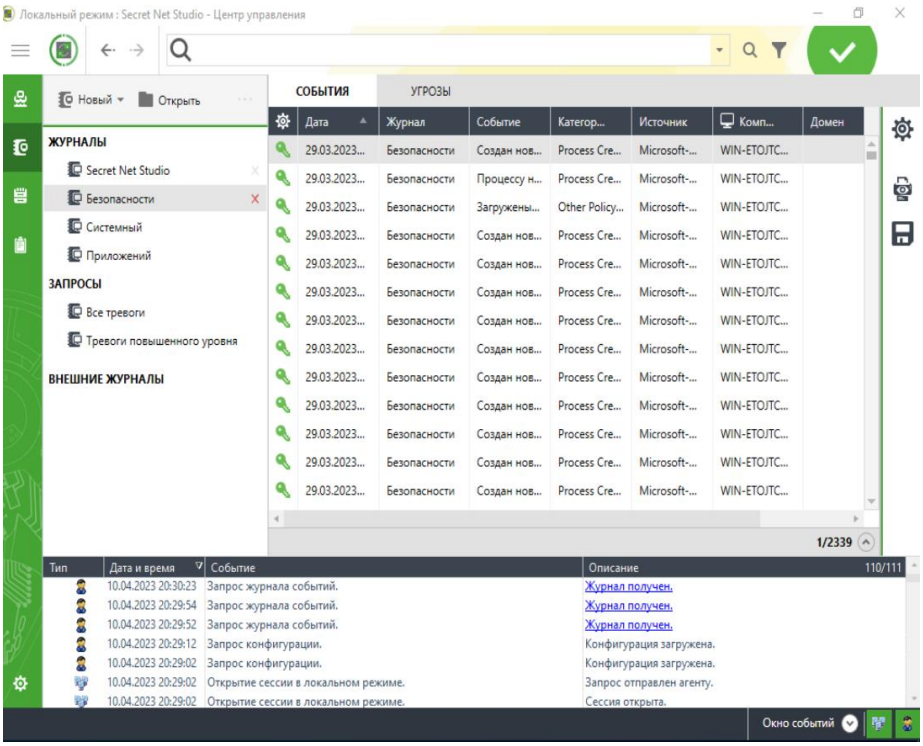

Рисунок Б.150. – Отчёт журнала безопасности

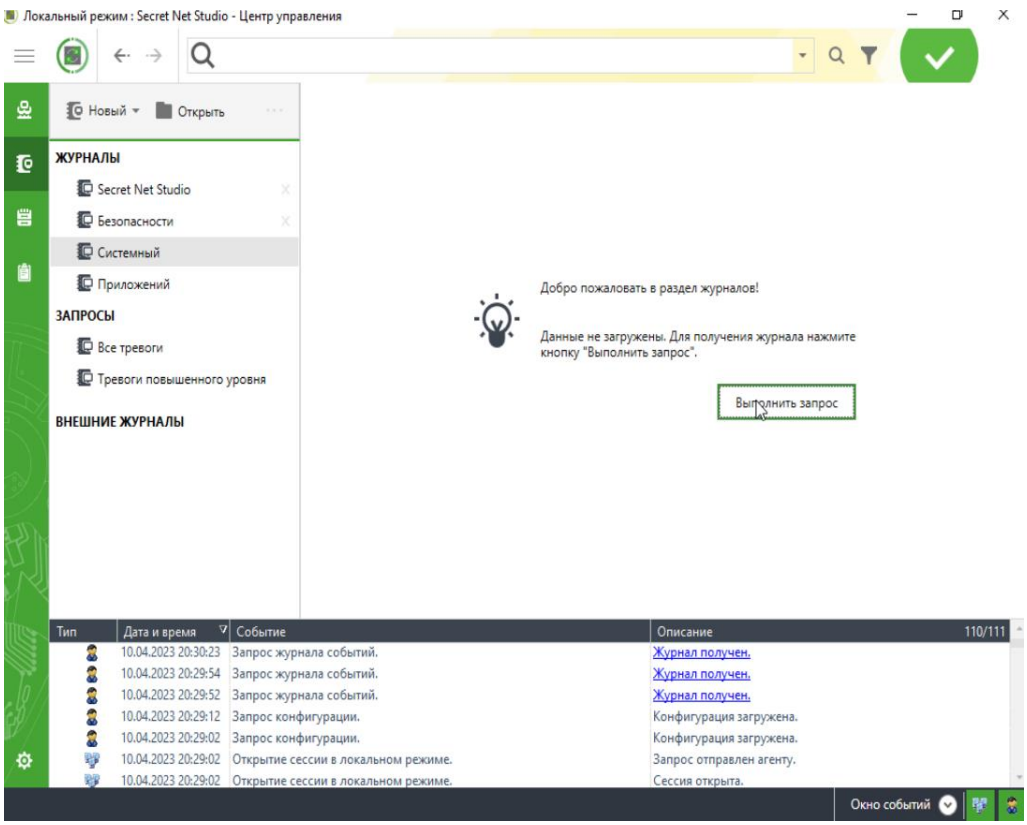

Рисунок Б.151. – Запуск системного журнала: процесс «выполнить запрос»

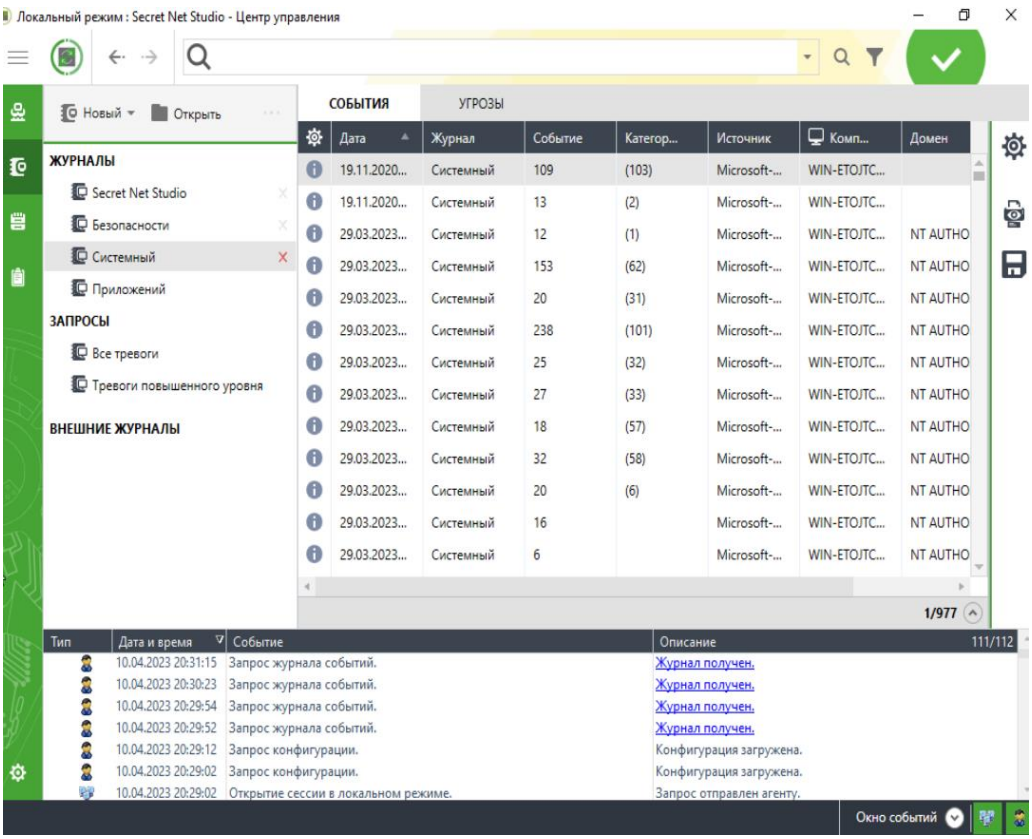

Рисунок Б.152. – Отчёт системного журнала

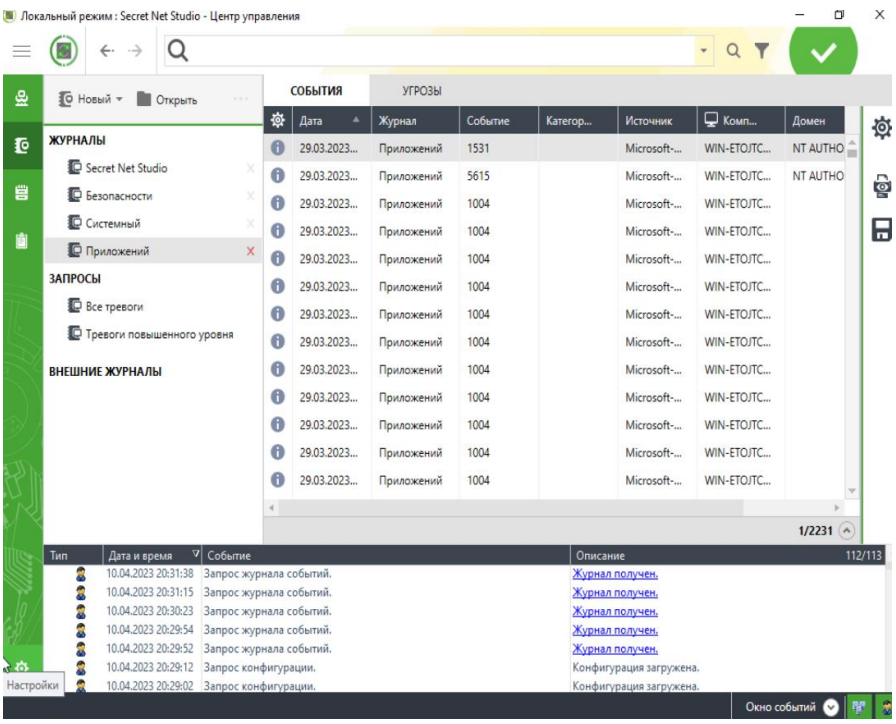

Рисунок Б.153. – Отчёт журнала приложений

В случае необходимости получить конкретную выборку записей журнала можно составить запрос на формирование выборки по определенным условиям: в правой части окна кнопка «Запрос» → открылась панель → С помощью кнопки «Добавить правило» ввести следующие сведения (по заданию): «Дата» → «Интервал» → «За последние 24 часа» → → «Агент» → «Содержит» → «Secret Net Studio» (см. рисунок Б.154.).

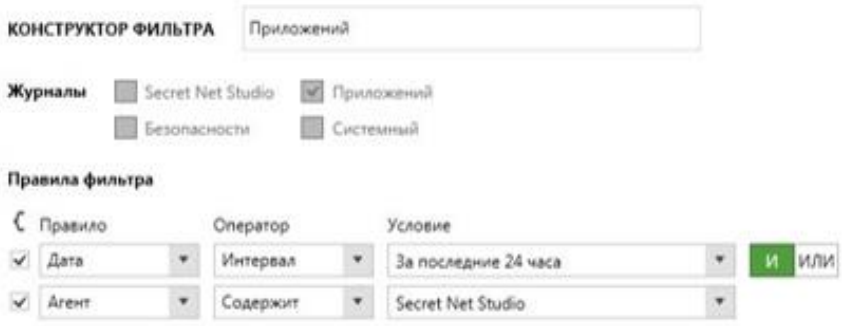

Рисунок Б.154. – Окно настройки выборки журнала

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.

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.155. и Б.156.).

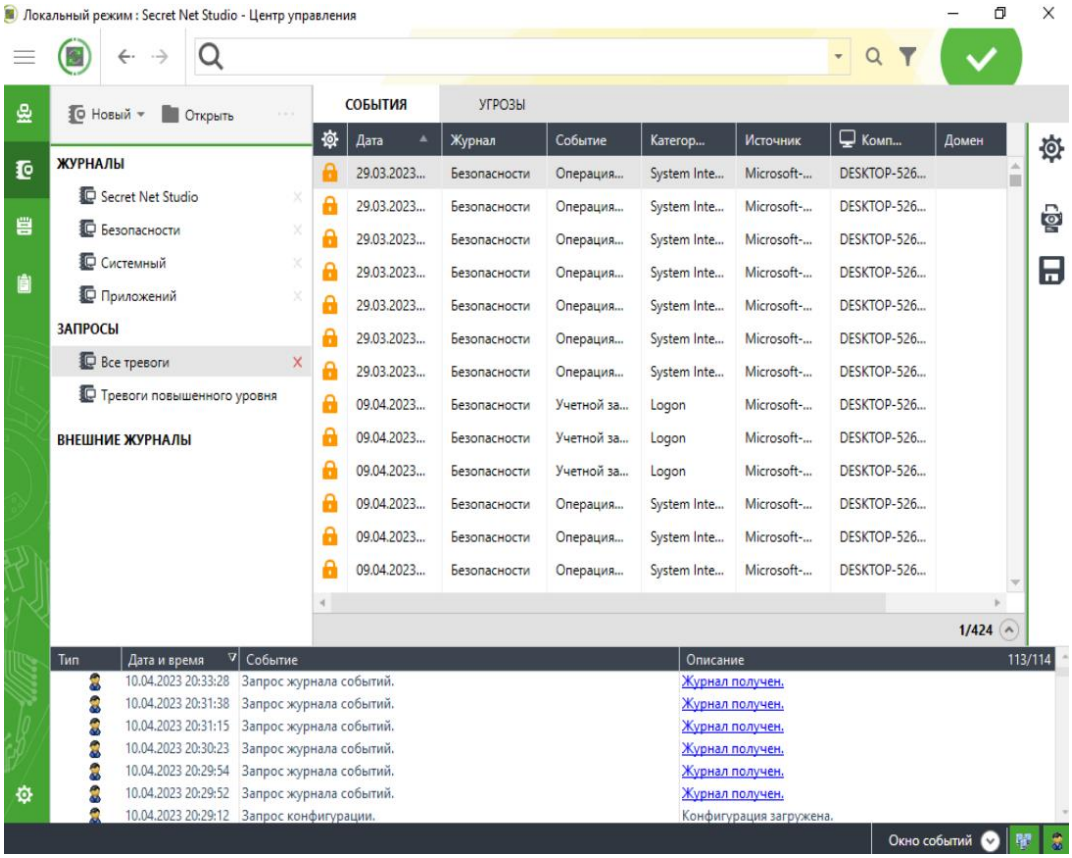

Рисунок Б.155. – Отчёт запросов «Журнал всех тревог»

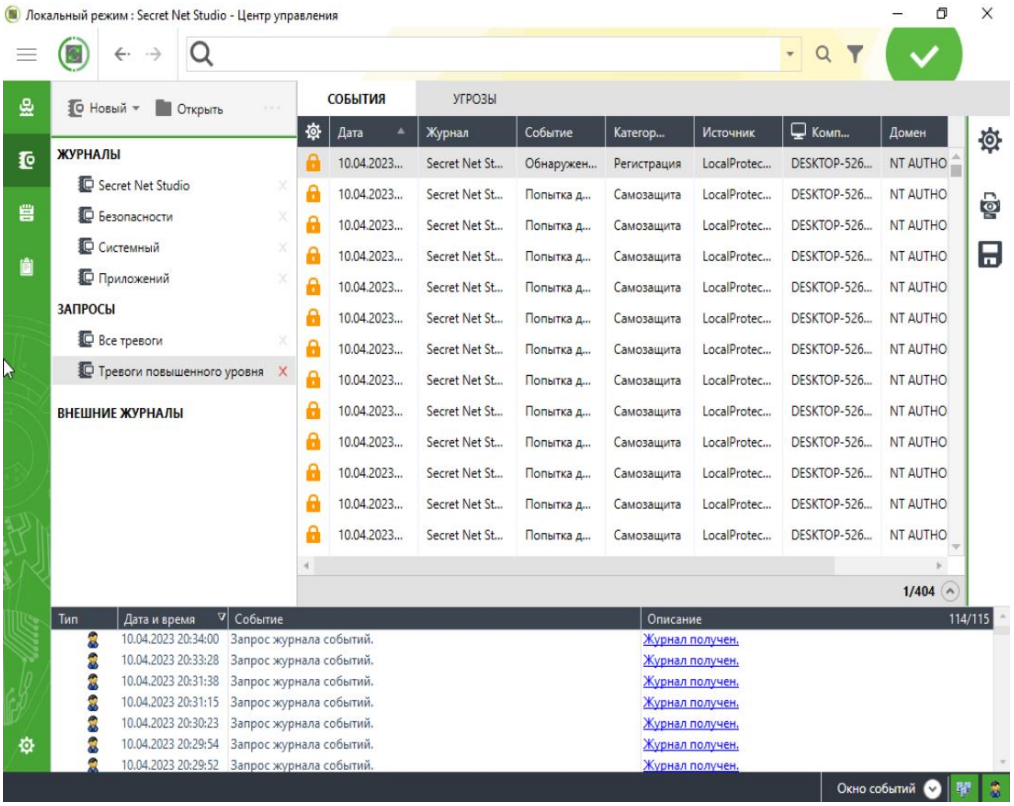

Рисунок Б.156. – Отчёт запросов «Журнал тревог повышенного уровня»

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

Параметры системы показаны на рисунке В.1..

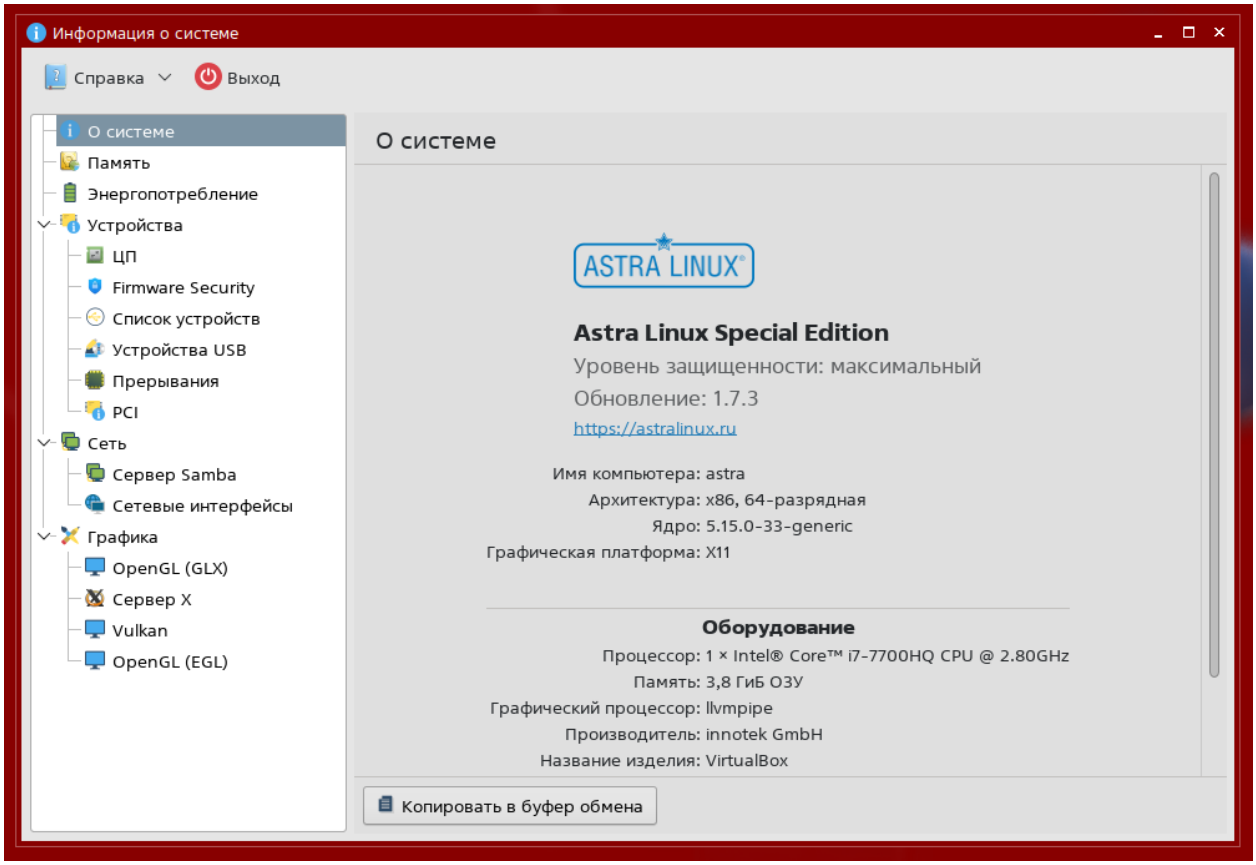

Рисунок В.1. – Параметры системы Astra Linux 1.7.3

Создание пользователя системы:

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

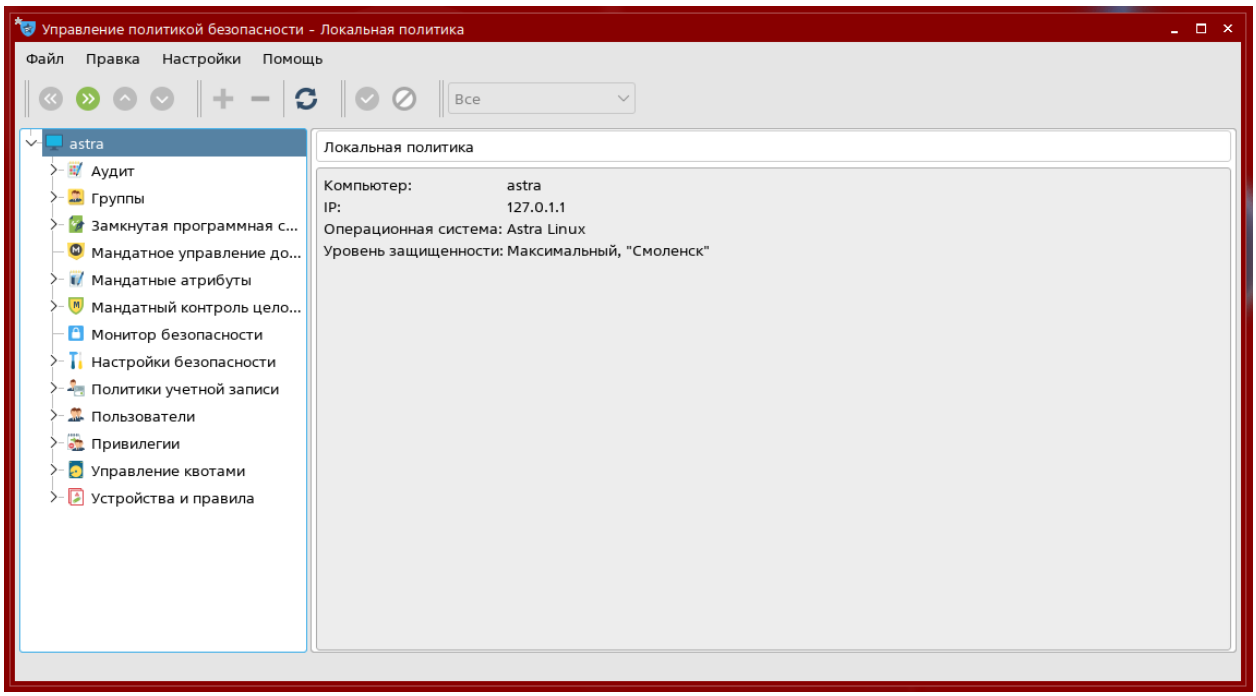

Рисунок В.2. – Окно управления политикой безопасности

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

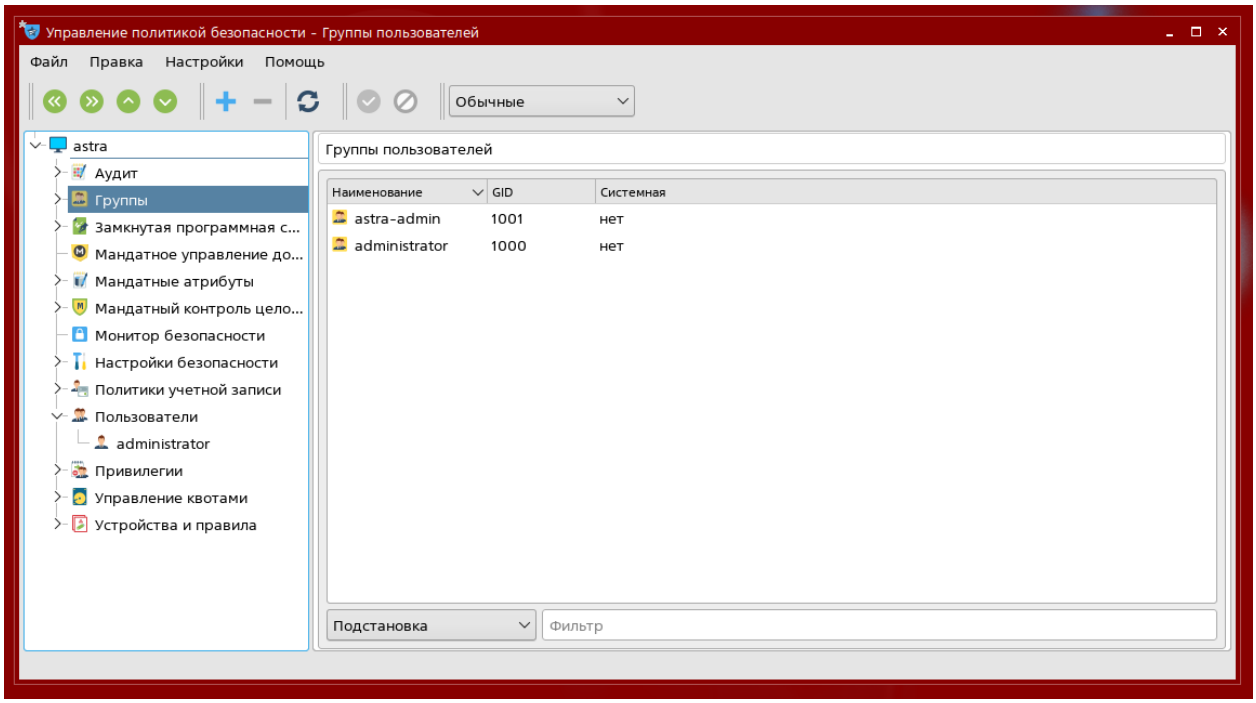

Рисунок В.3. – Окно управления группами

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.).

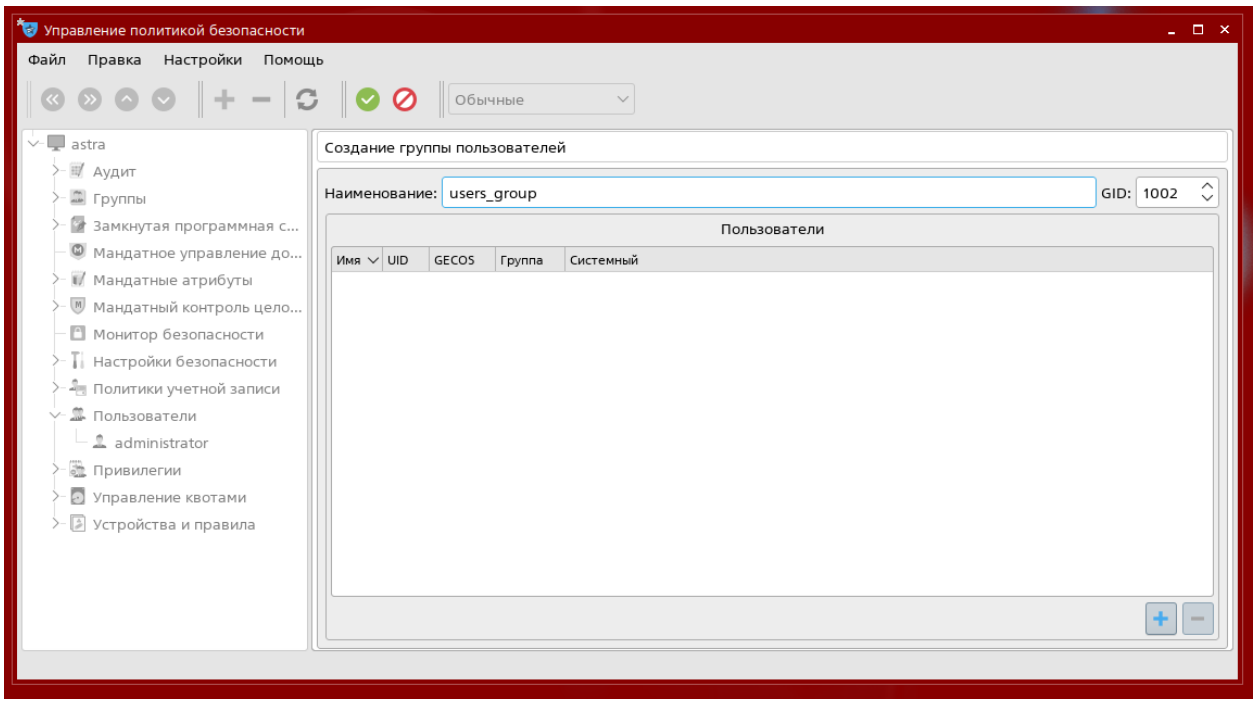

Рисунок В.4. – Создание группы пользователей

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

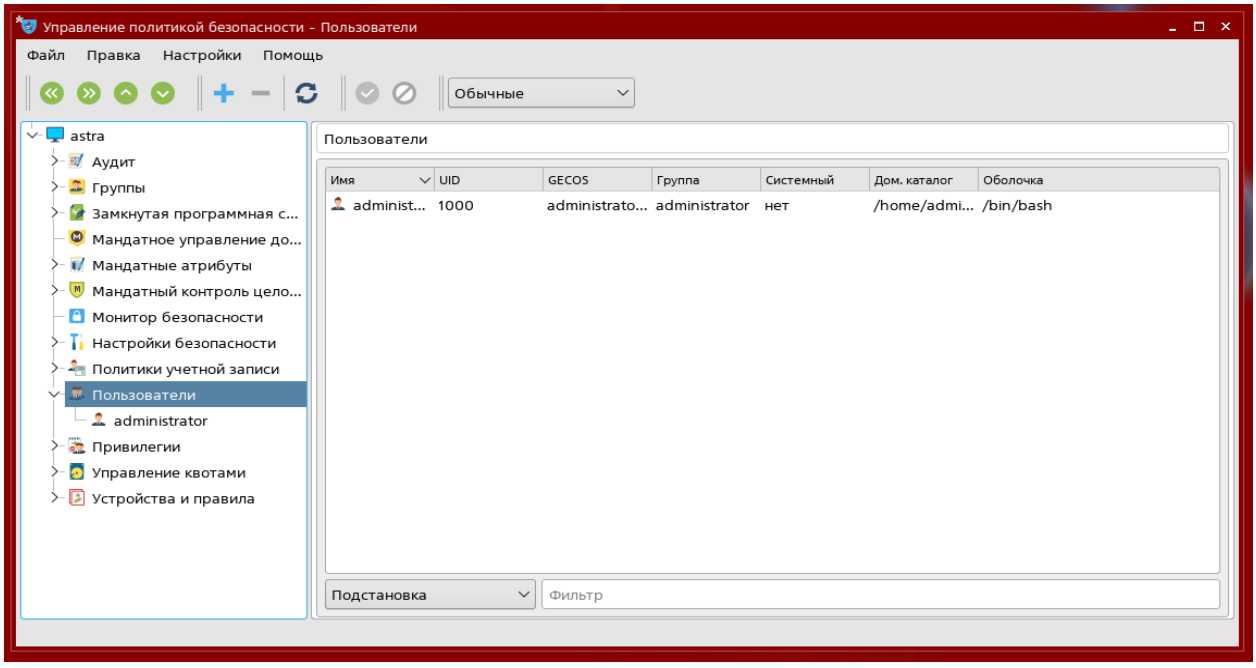

Рисунок В.5. – Список пользователей

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.).

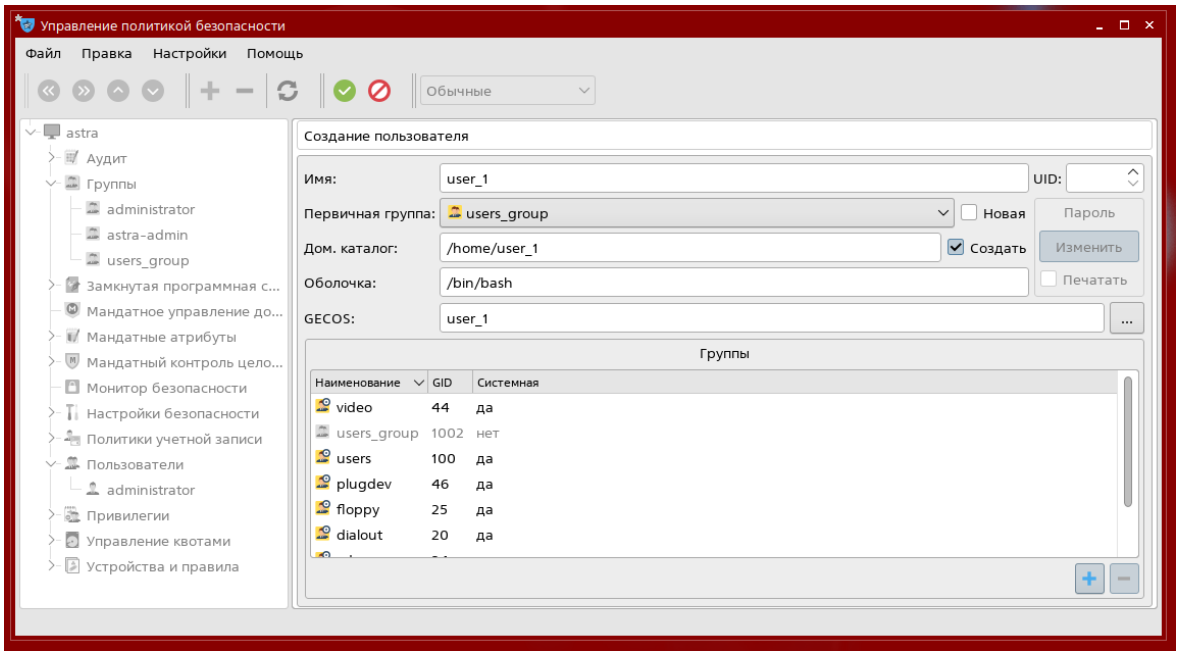

Рисунок В.6. – Создание пользователя

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

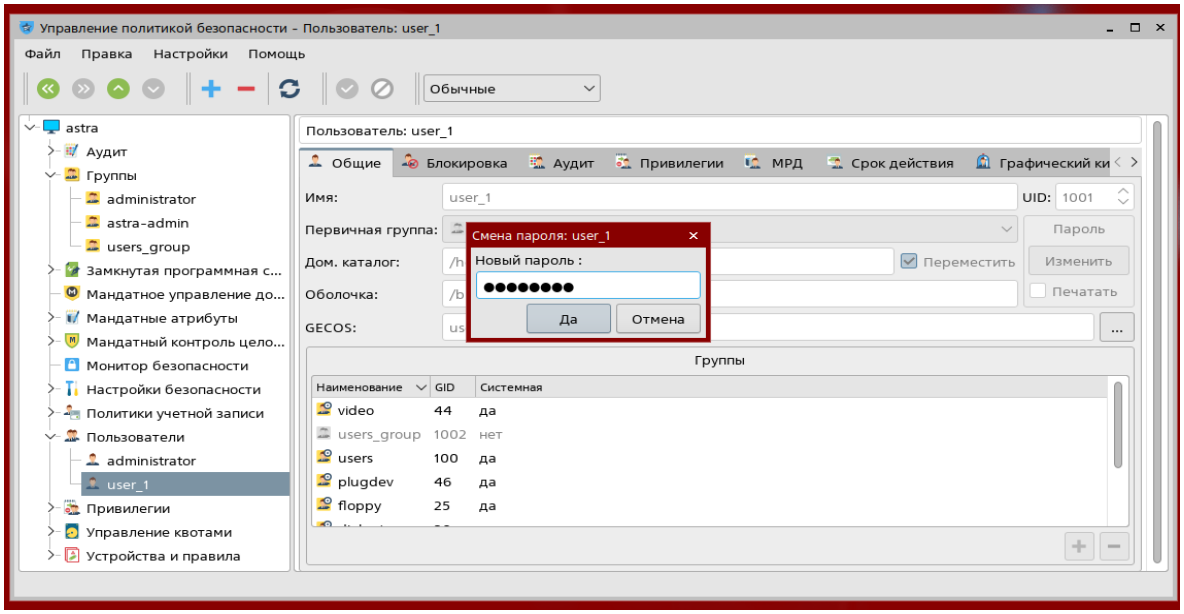

Рисунок В.7. – Смена пароля пользователя

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.)

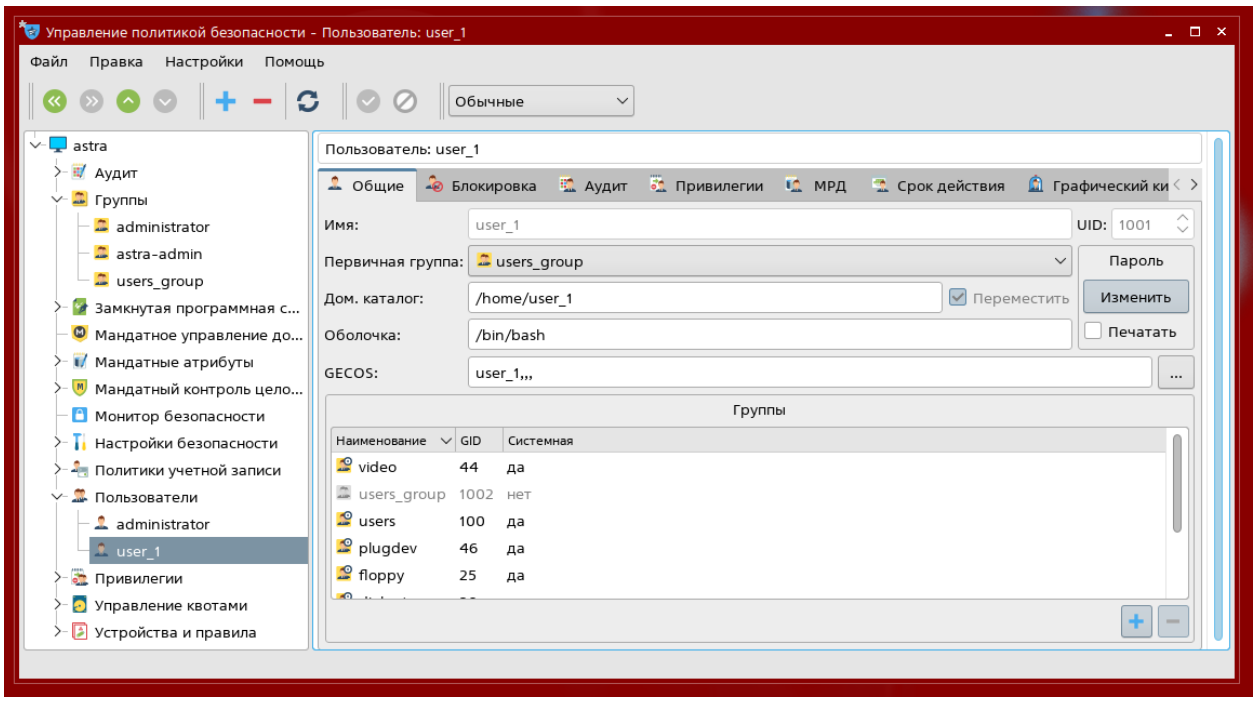

Рисунок В.8. – Общие настройки пользователя

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.).

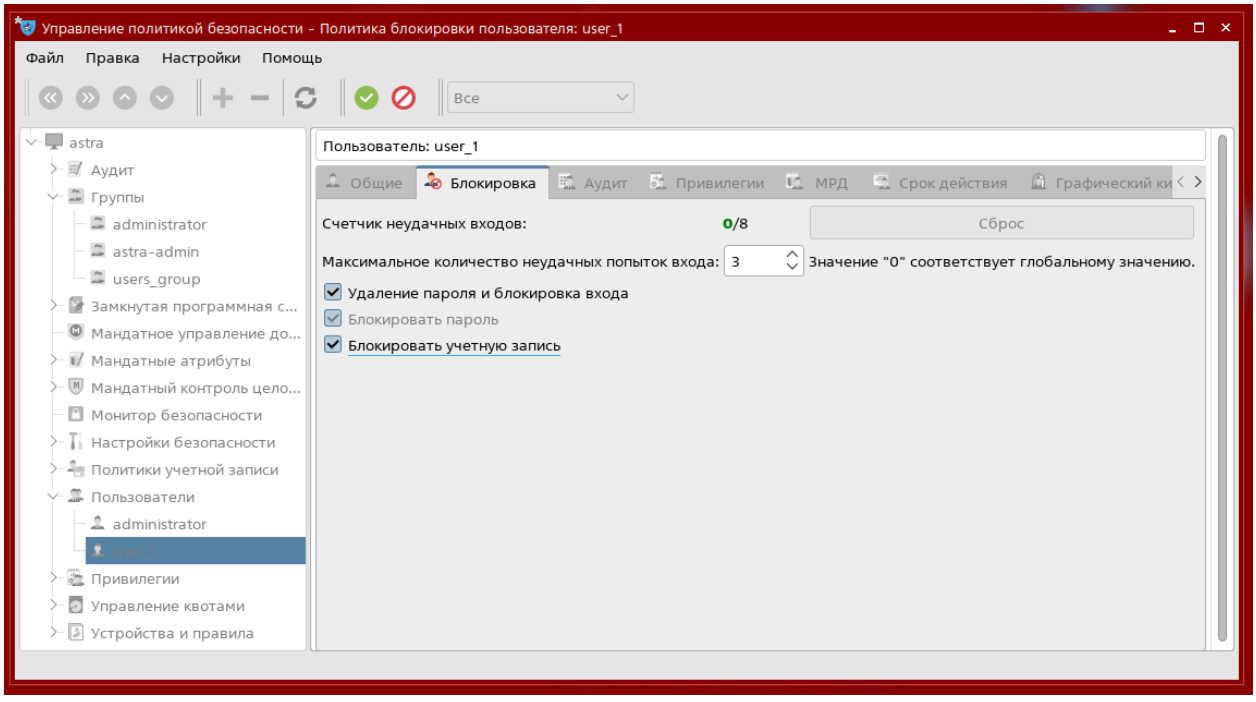

Рисунок В.9. – Настройка блокировки пользователя

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

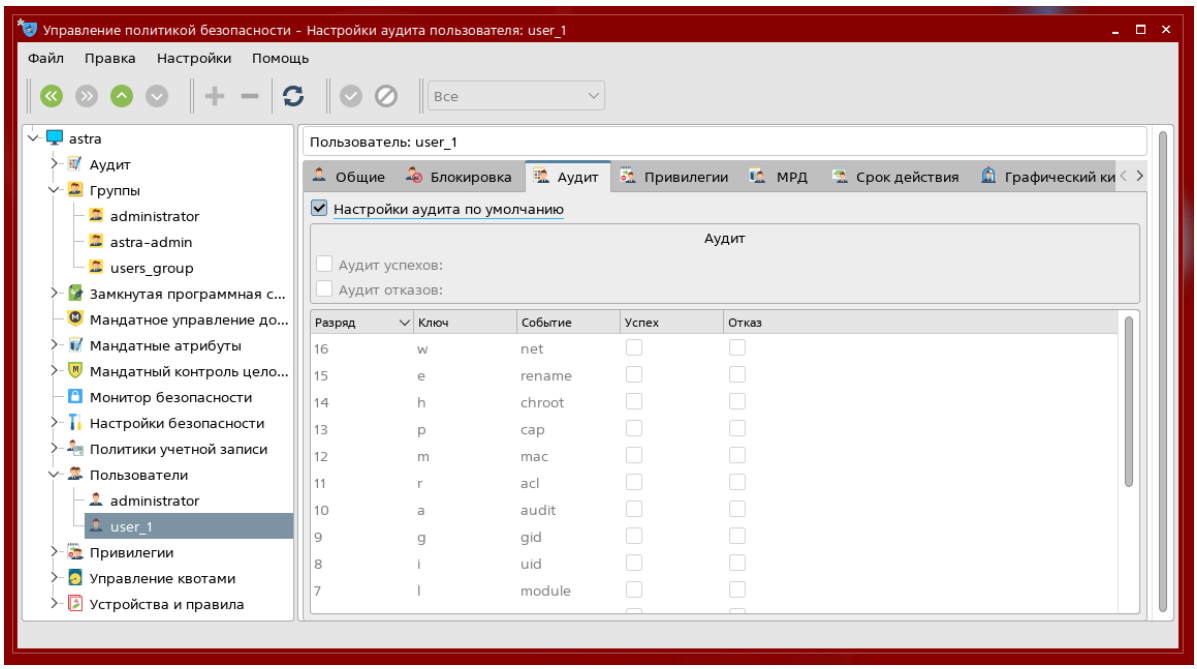

Рисунок В.10. – Настройка аудита пользователя

Во вкладке «МРД» настроить уровни и категории доступа. (см. рисунок В.11.)

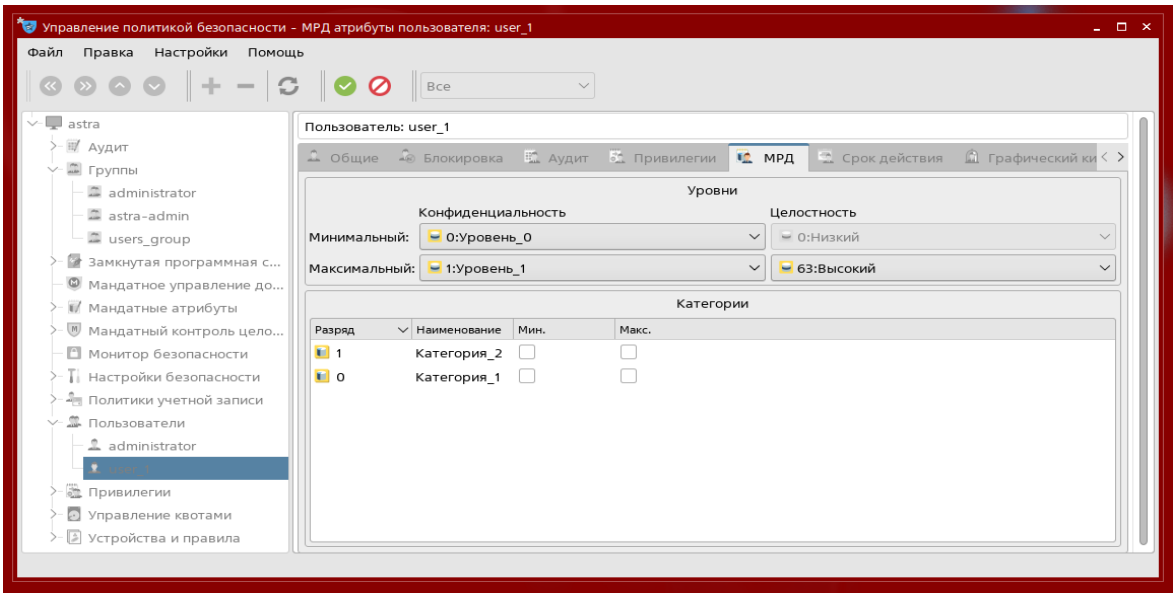

Рисунок В.11. – Настройка МРД пользователя

Во вкладке «Срок действия» настраиваются 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 В.12.):

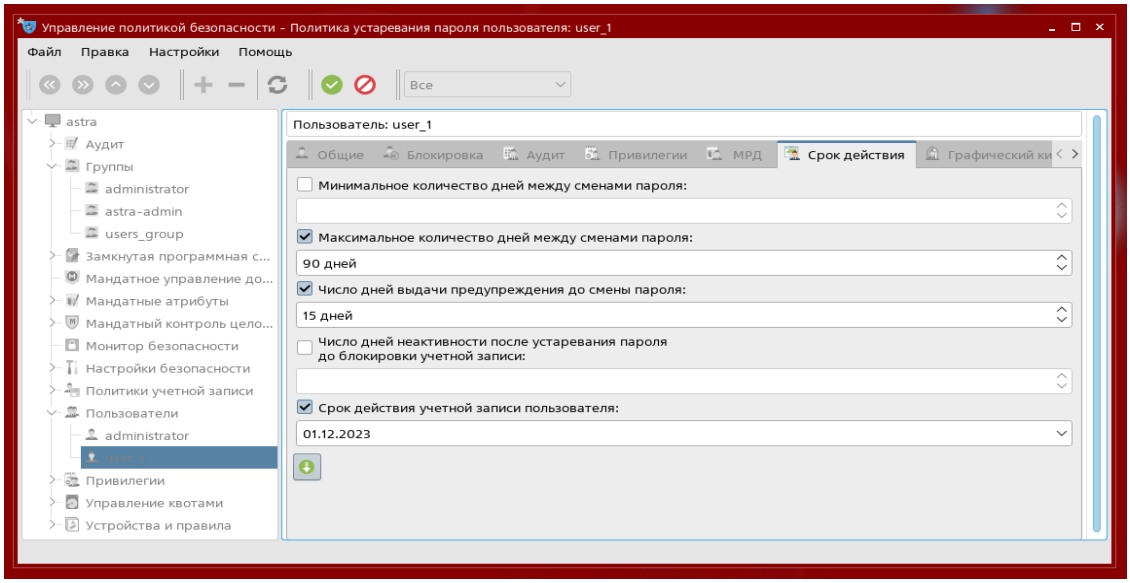

Рисунок В.12. – Настройка срока действия учетной записи пользователя

Настройка идентификации и аутентификации

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

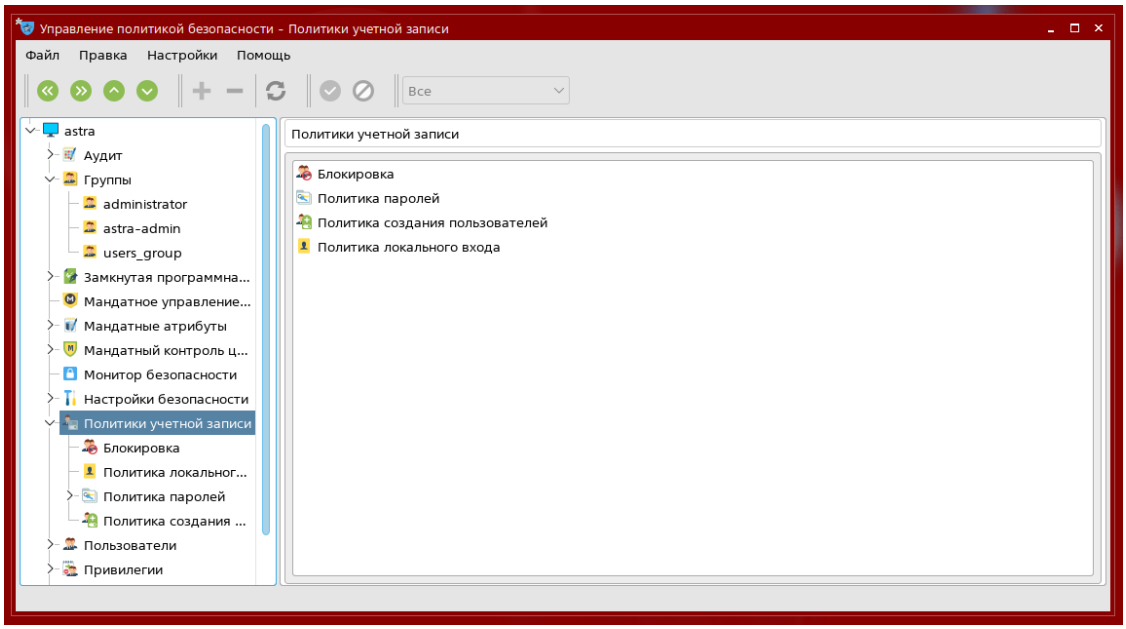

Рисунок В.13. – Окно политик учетной записи

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.)

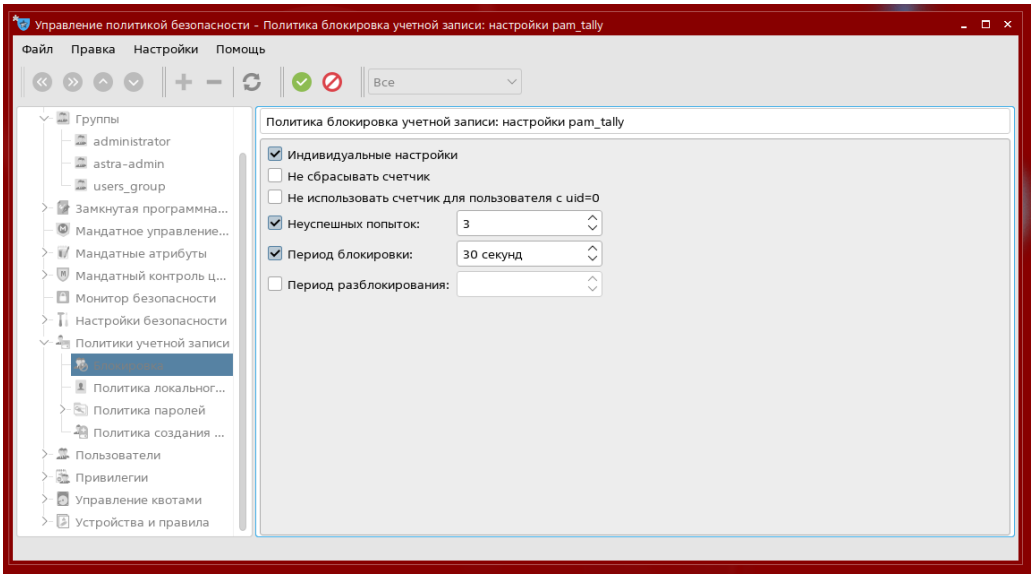

Рисунок В.14. – Настройка блокировки учетной записи

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.):

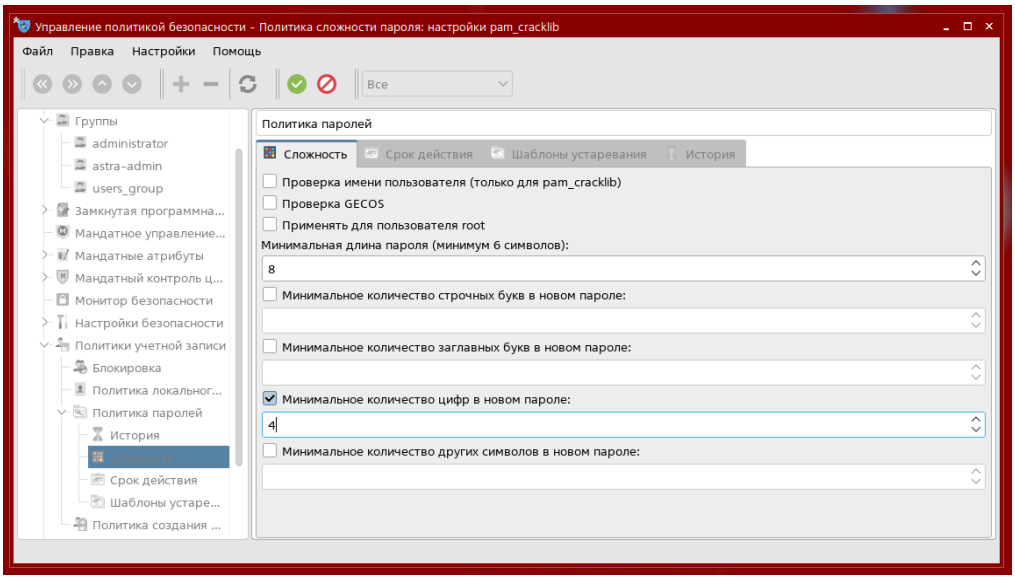

Рисунок В.15. – Настройка сложности пароля

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.):

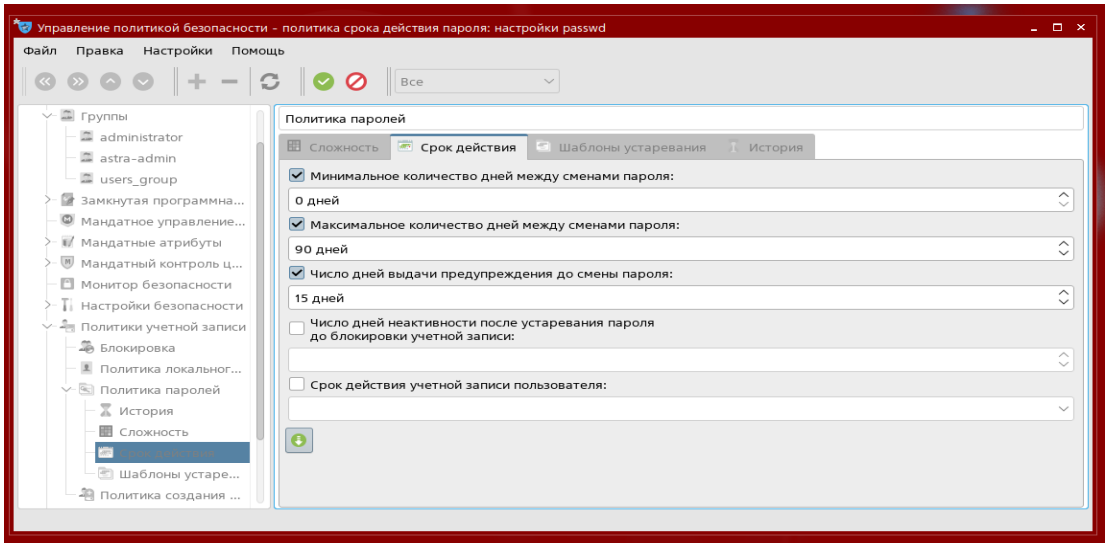

Рисунок В.16. – Настройка срока действия пароля

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 В.17.).

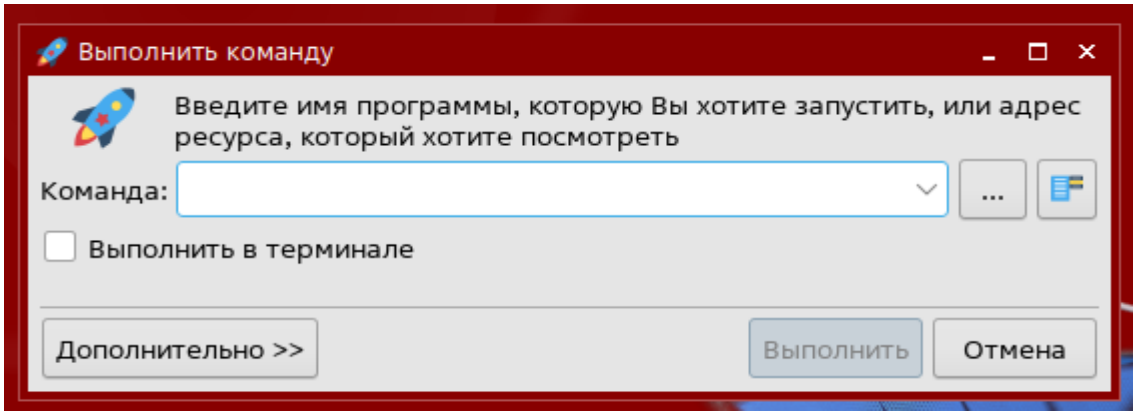

Рисунок В.17. – Окно ввода команд

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

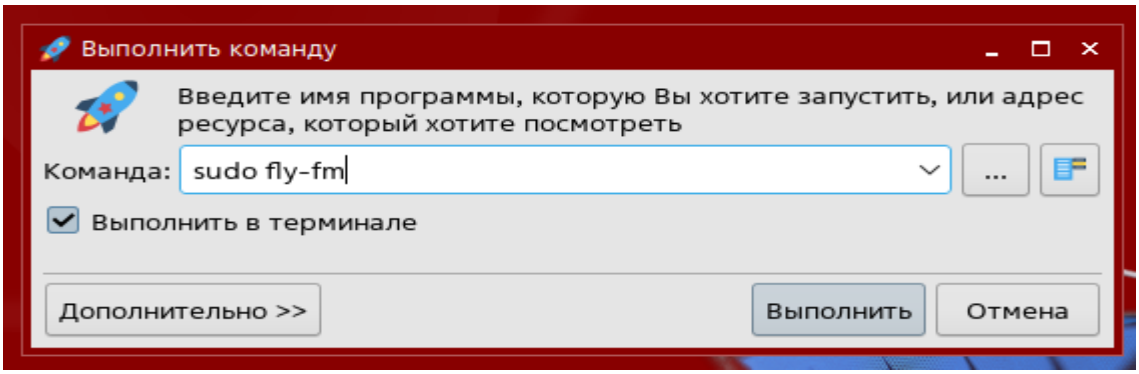

Рисунок В.18. – Ввод команды

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

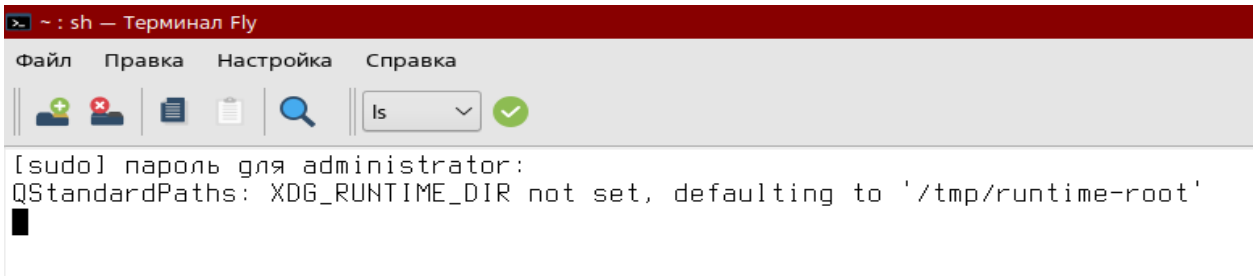

Рисунок В.19. – Ввод пароля для «sudo»

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

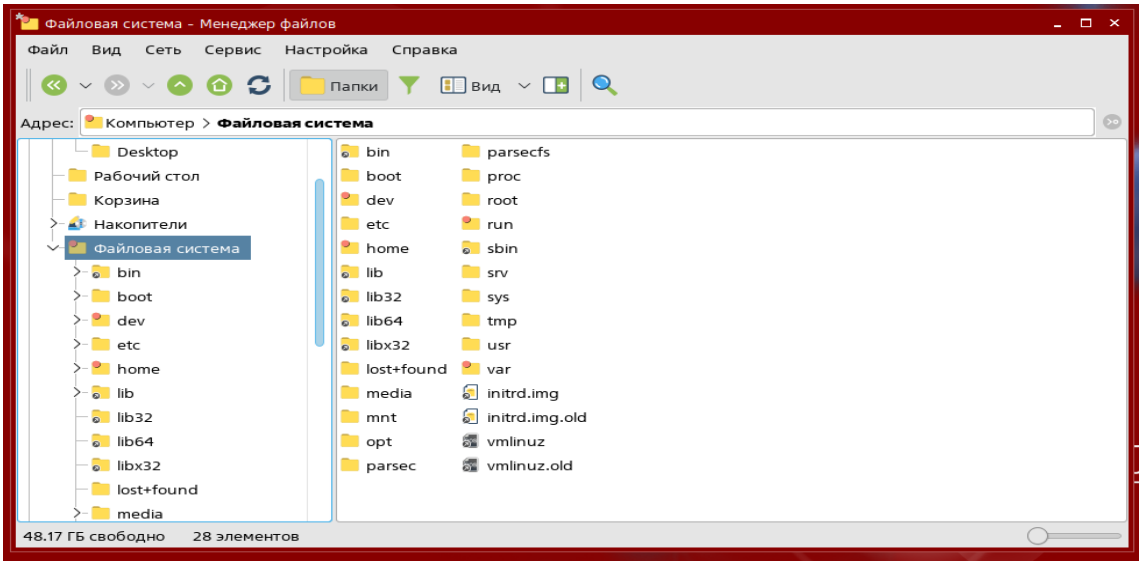

Рисунок В.20. – Окно менеджера файлов

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.).

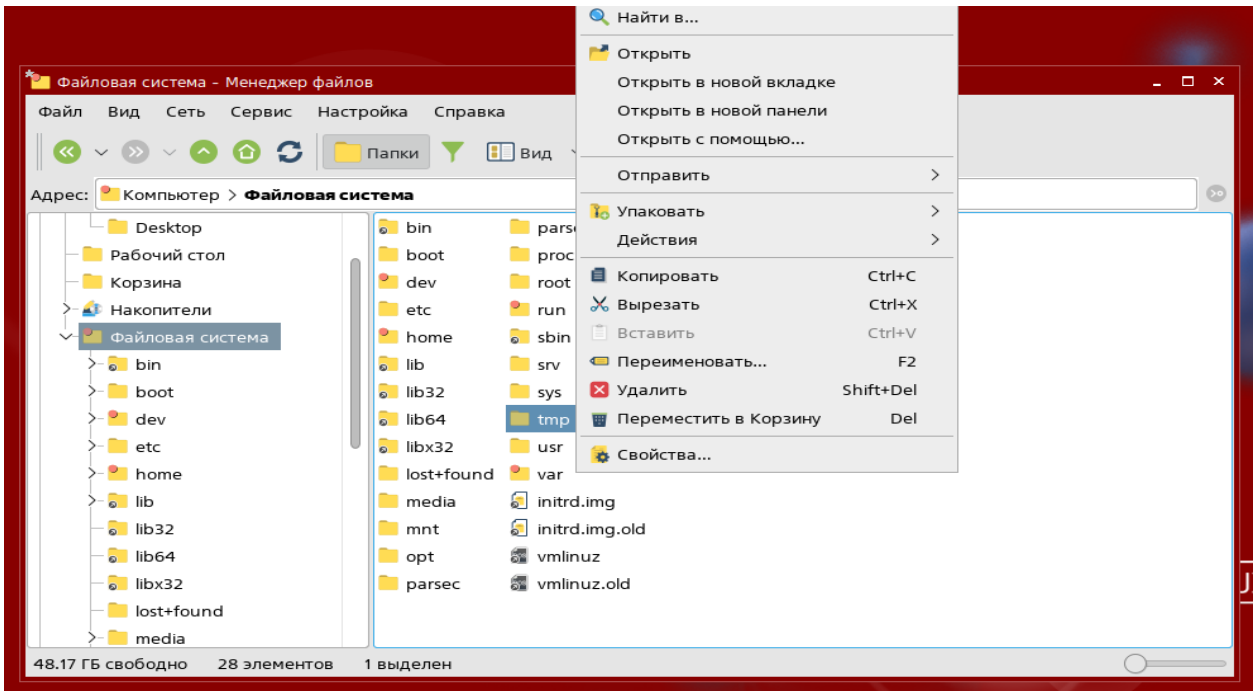

Рисунок В.21. – Контекстное меню папки

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

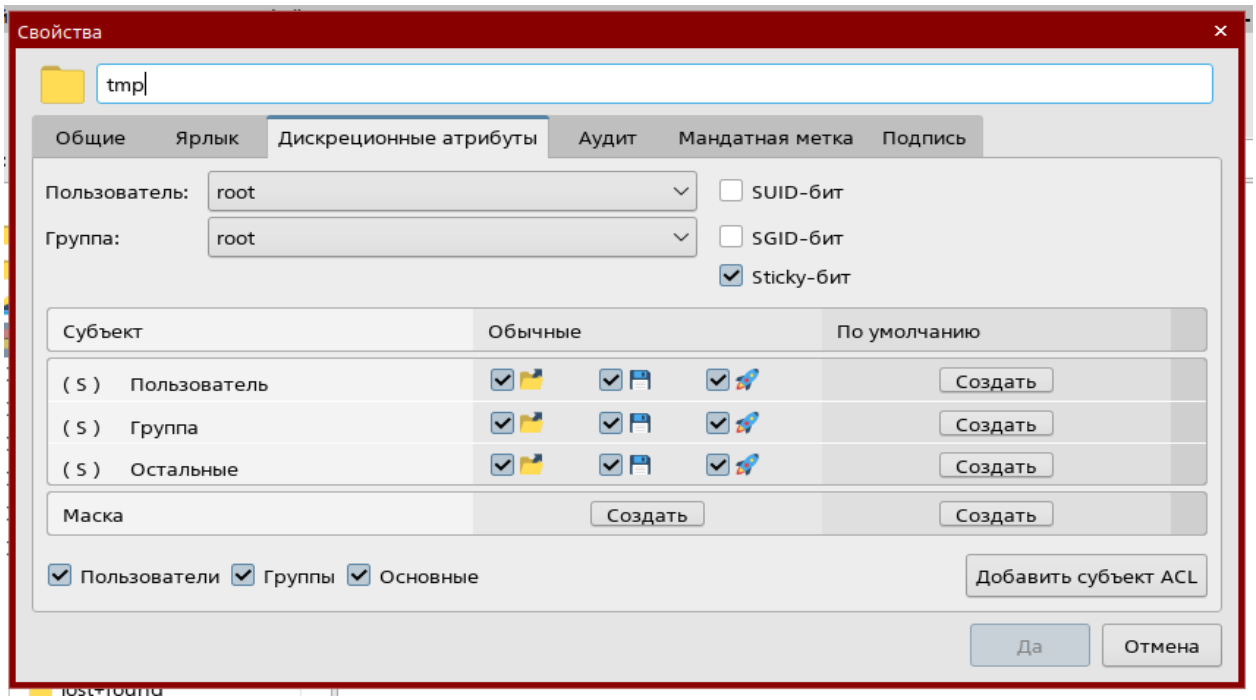

Рисунок В.22. – Дискреционный атрибуты папки

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

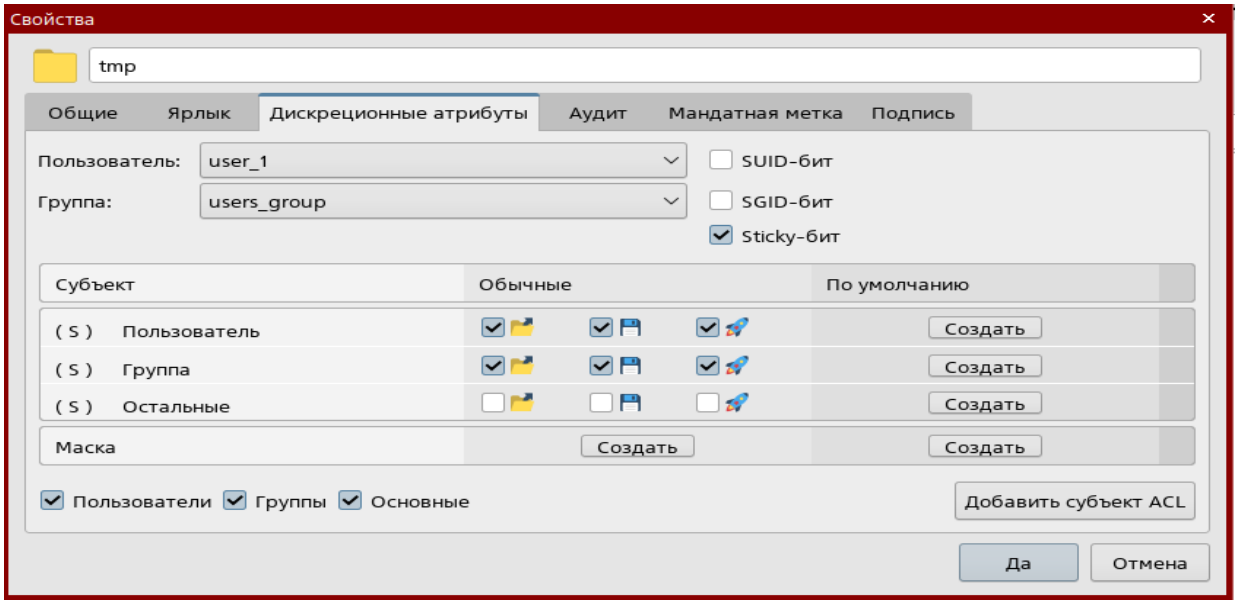

Рисунок В.23. – Настройка дискреционных атрибутов

Настройка очистки остаточной информации

Открыть управление политикой безопасности

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

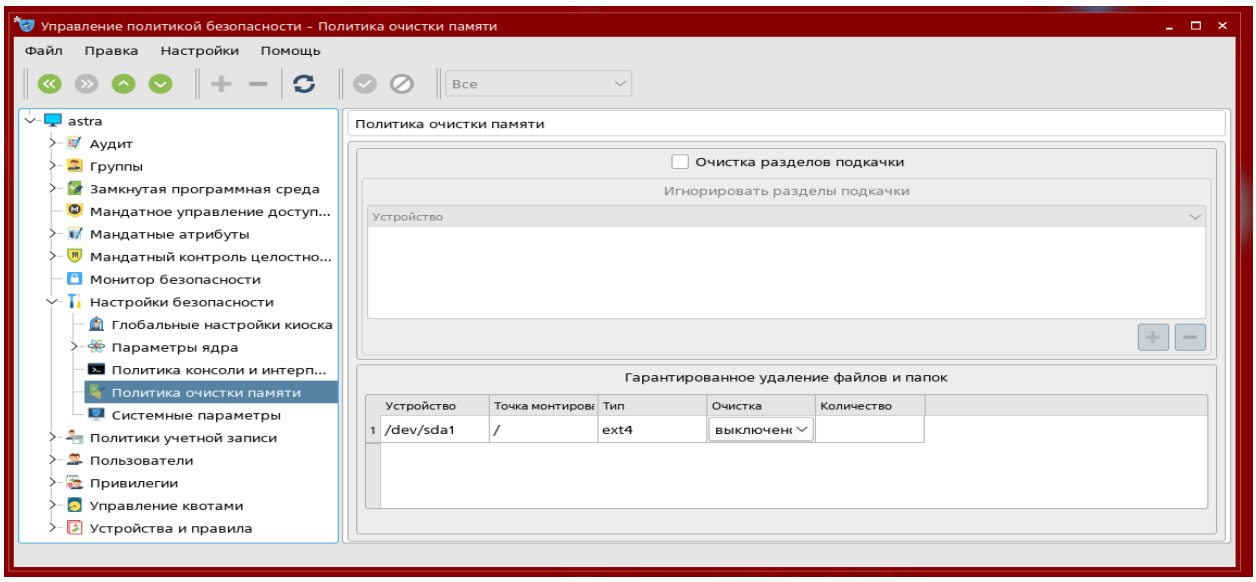

Рисунок В.24. – Окно политики очистки памяти

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.).

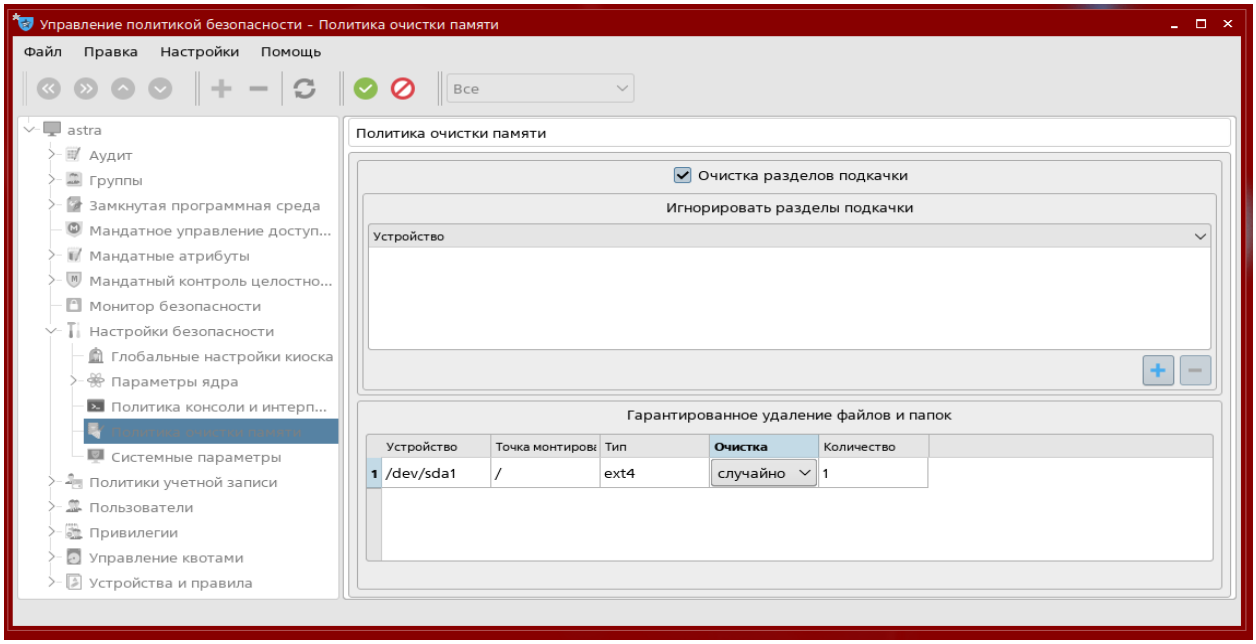

Рисунок В.25. – Настройка гарантированного удаления

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 В.26.)

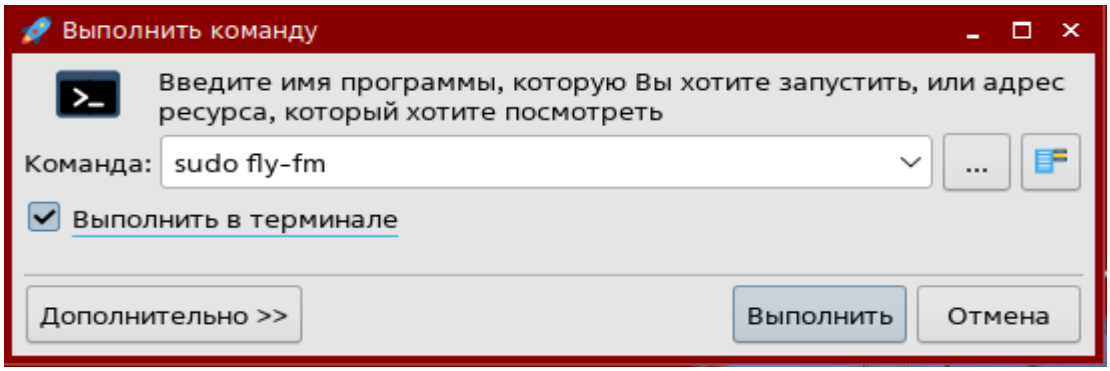

Рисунок В.26. – Ввод команды

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.).

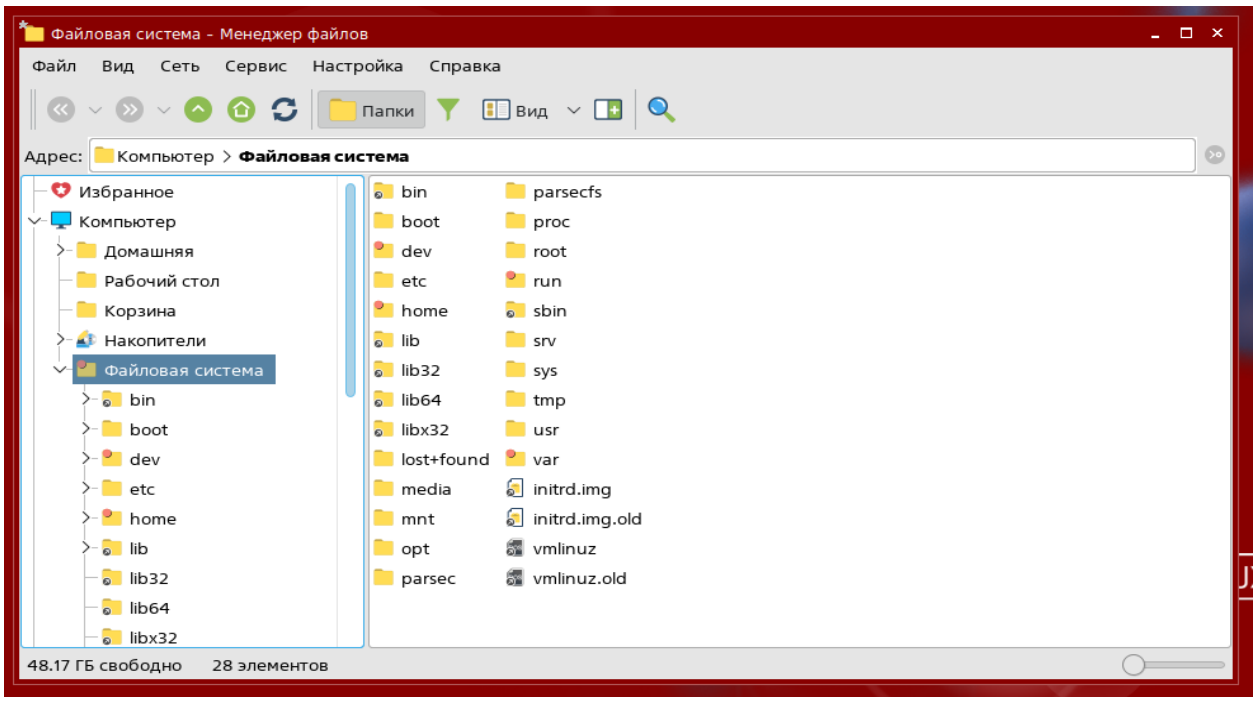

Рисунок В.27. – Менеджер файлов

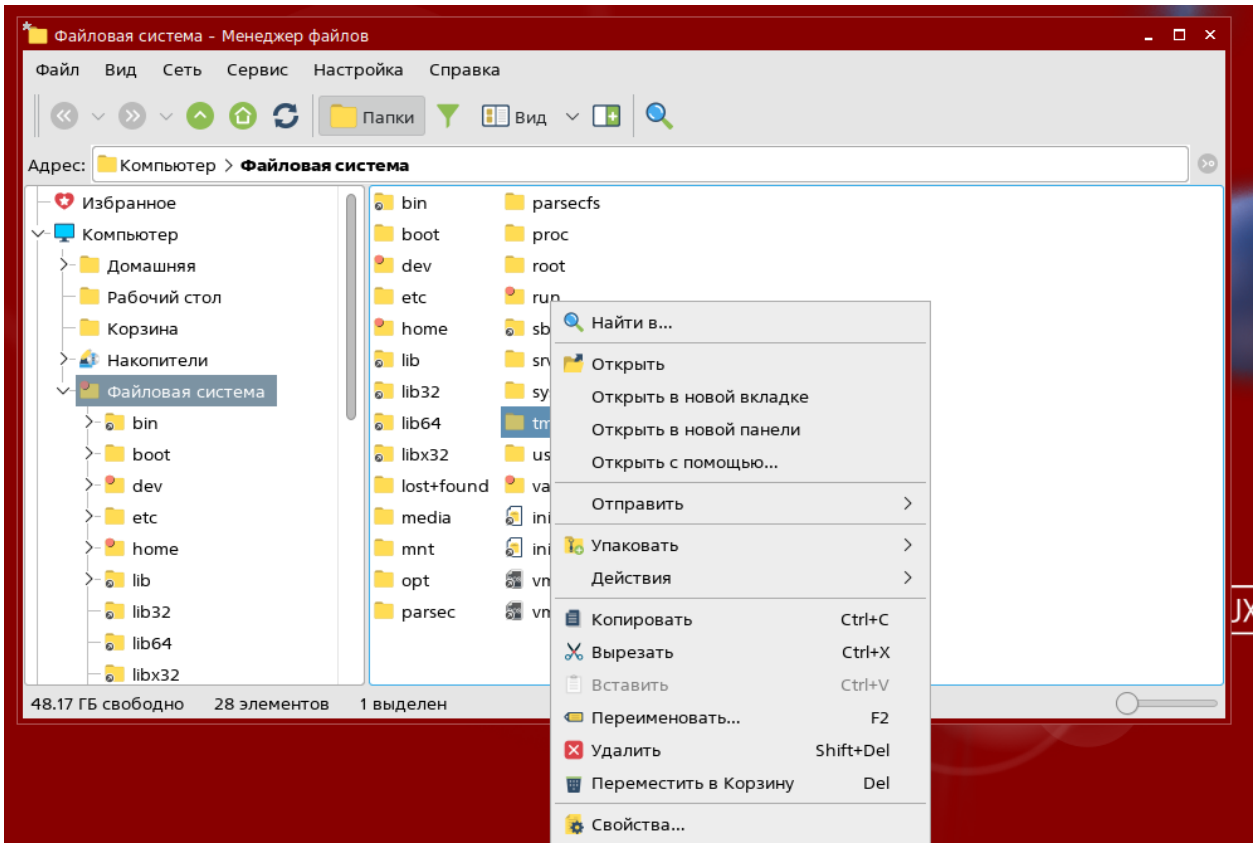

Рисунок В.28. – Контекстное меню

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

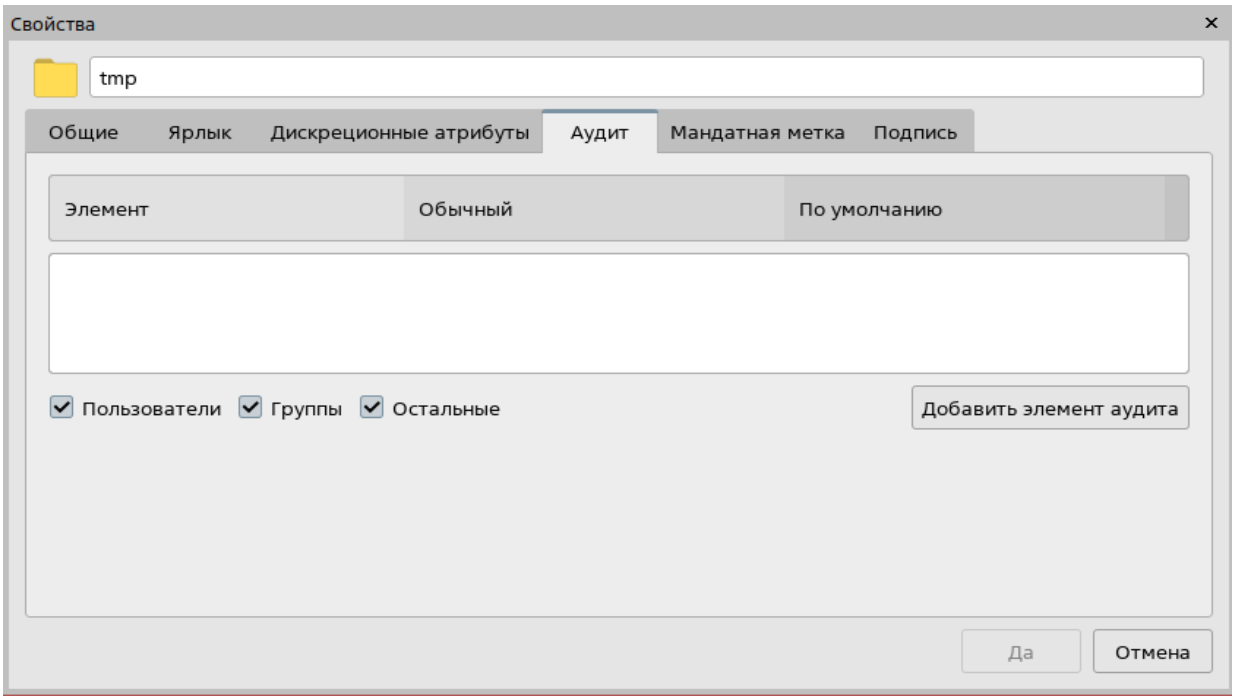

Рисунок В.29. – Аудит папки

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.).

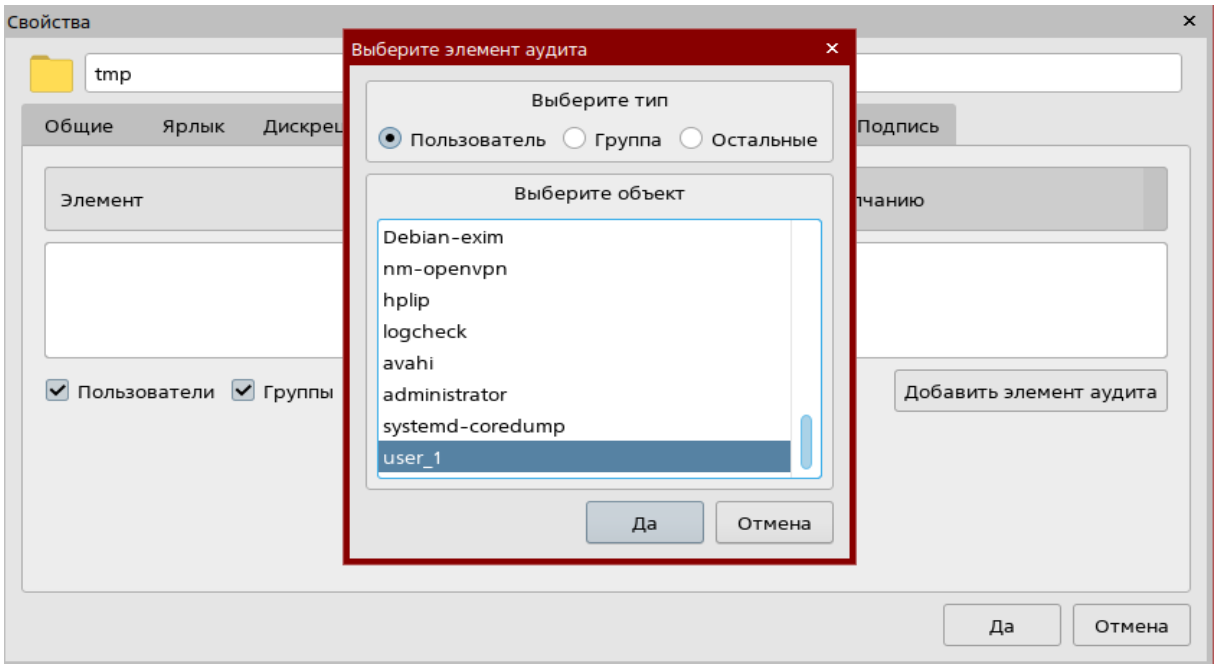

Рисунок В.30. – Добавление аудита

В примере (см. рисунок В.31.) были установлены права для субъектов user_1, root, и остальные:

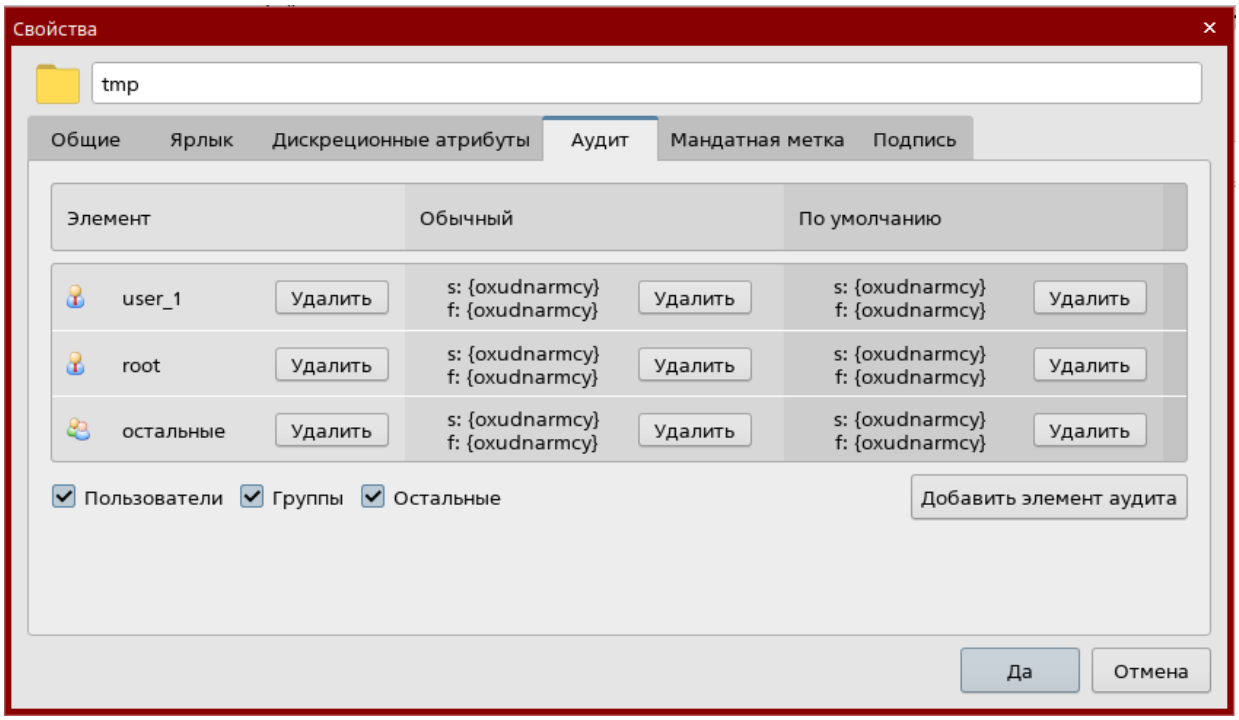

Рисунок В.31. – Настройка аудита

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

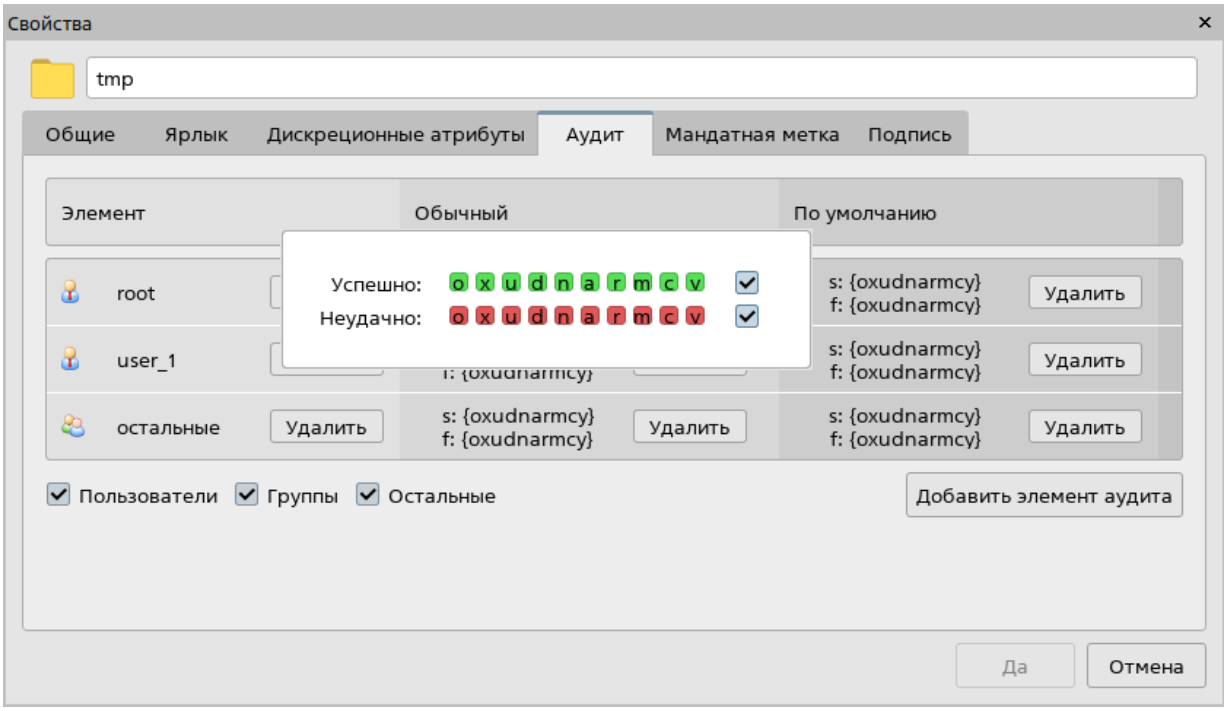

Рисунок В.32. – Установка права доступа

Настройка контроля целостности файловой системы и программно-аппаратной среды.

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

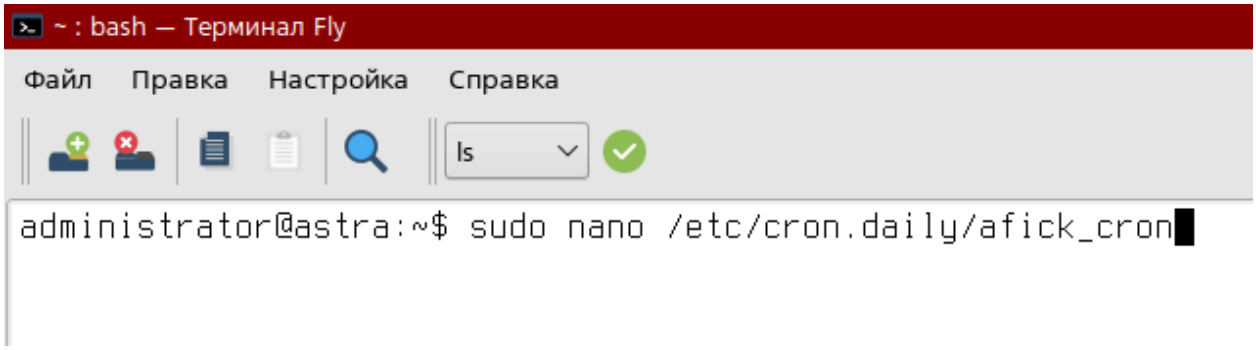

Рисунок В.33. – Ввод команды в терминал

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

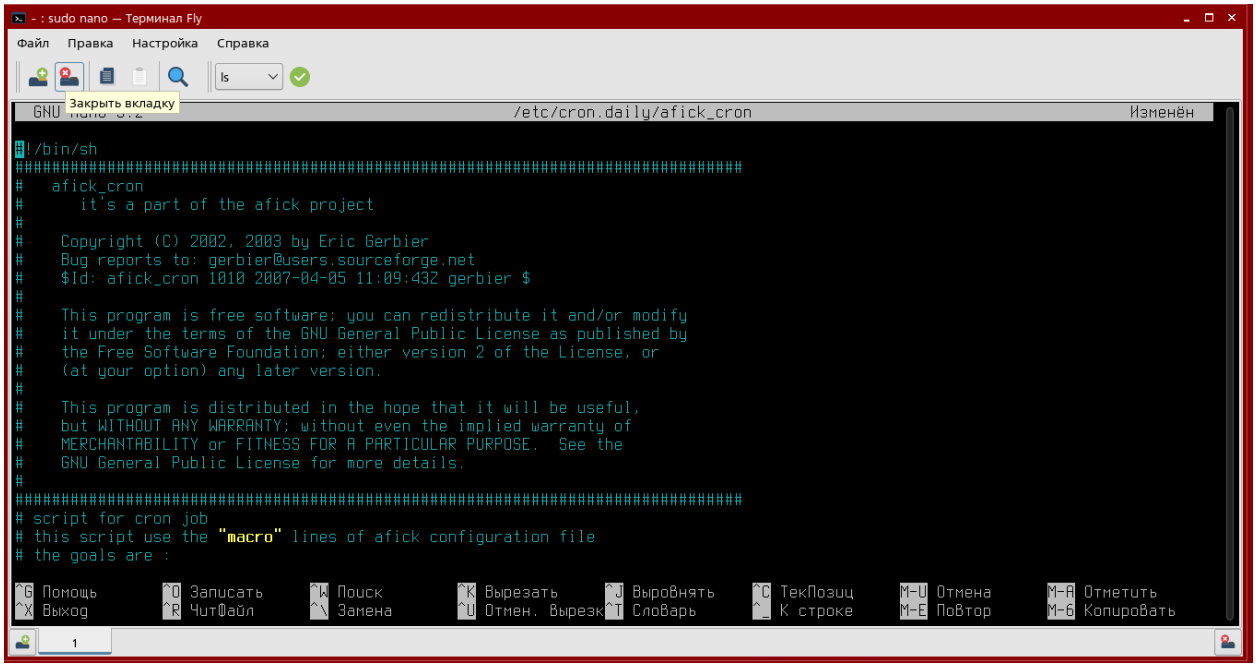

Рисунок В.34. – Результат выполнения команды

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 В.36.):

```
nice -n $NICE $AFICK -c $CONFFILE -k > $LOGFILE
2>$ERRORLOG
```

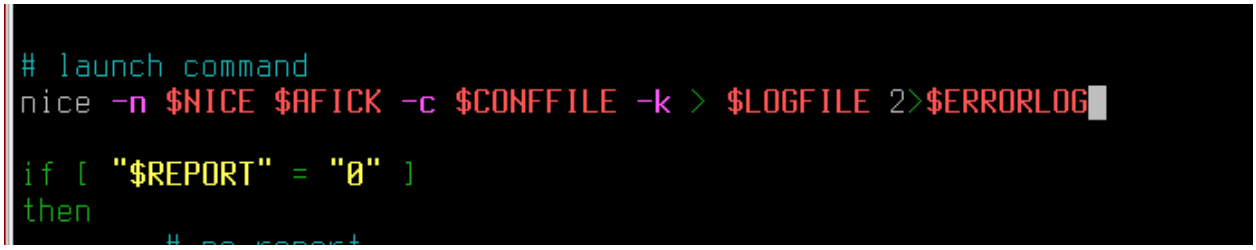

Рисунок В.36. – Изменение команды запуска

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

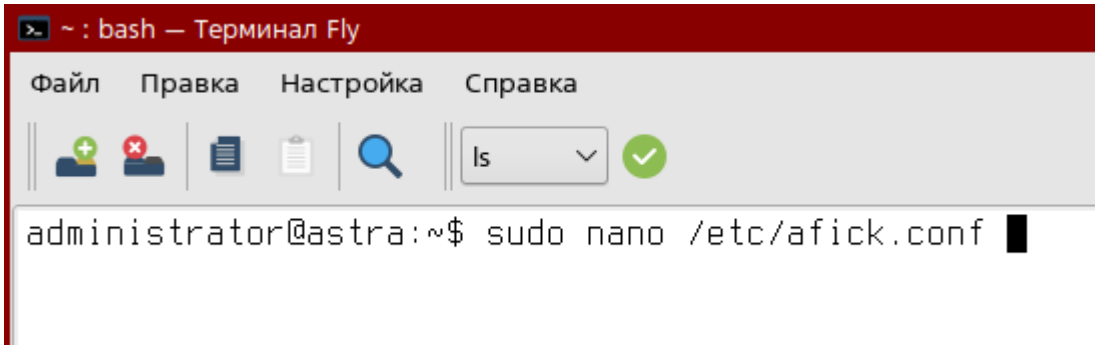

Рисунок В.37. – Открытие файла «/etc/afick.conf»

Результат выполнения команды – на рисуноке В.38..

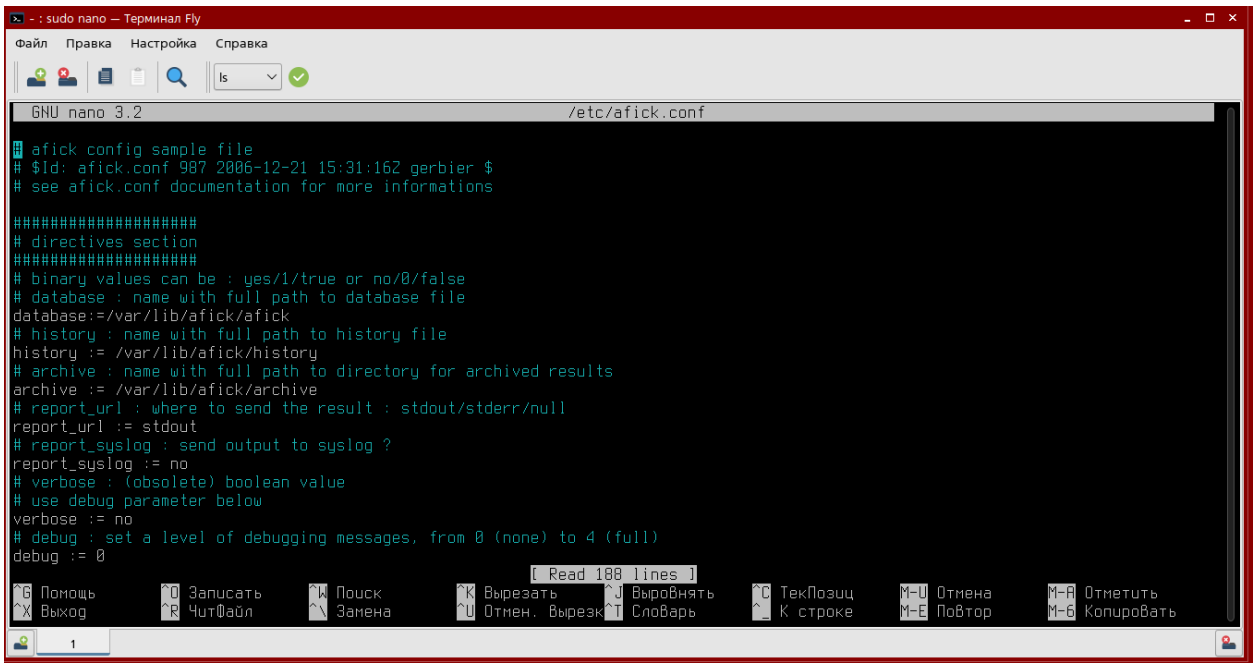

Рисунок В.38. – Файл «/etc/afick.conf»

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»

```
# ! /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.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
```

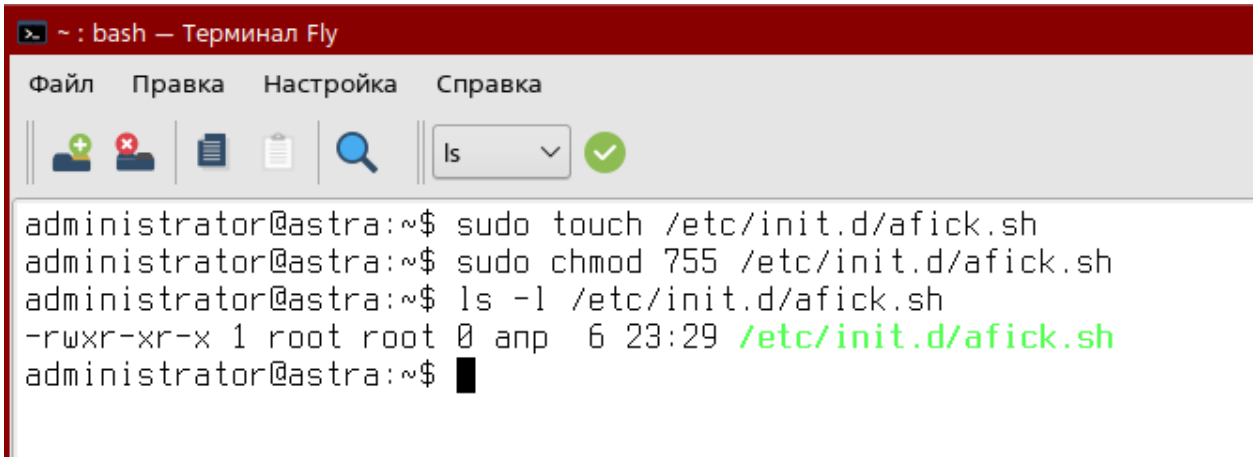

Рисунок В.41. – Создание и настройка прав файла «affick.sh»

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"
```

```
    log_end_msg $status
    if [ $status -ne "0" ];
    then
        sleep 2
    fi
    ;;

    *)
    echo "Для использования данного скрипта необходимо запустить его с параметром start. Например: afick.sh start"
    ;;
esac
```

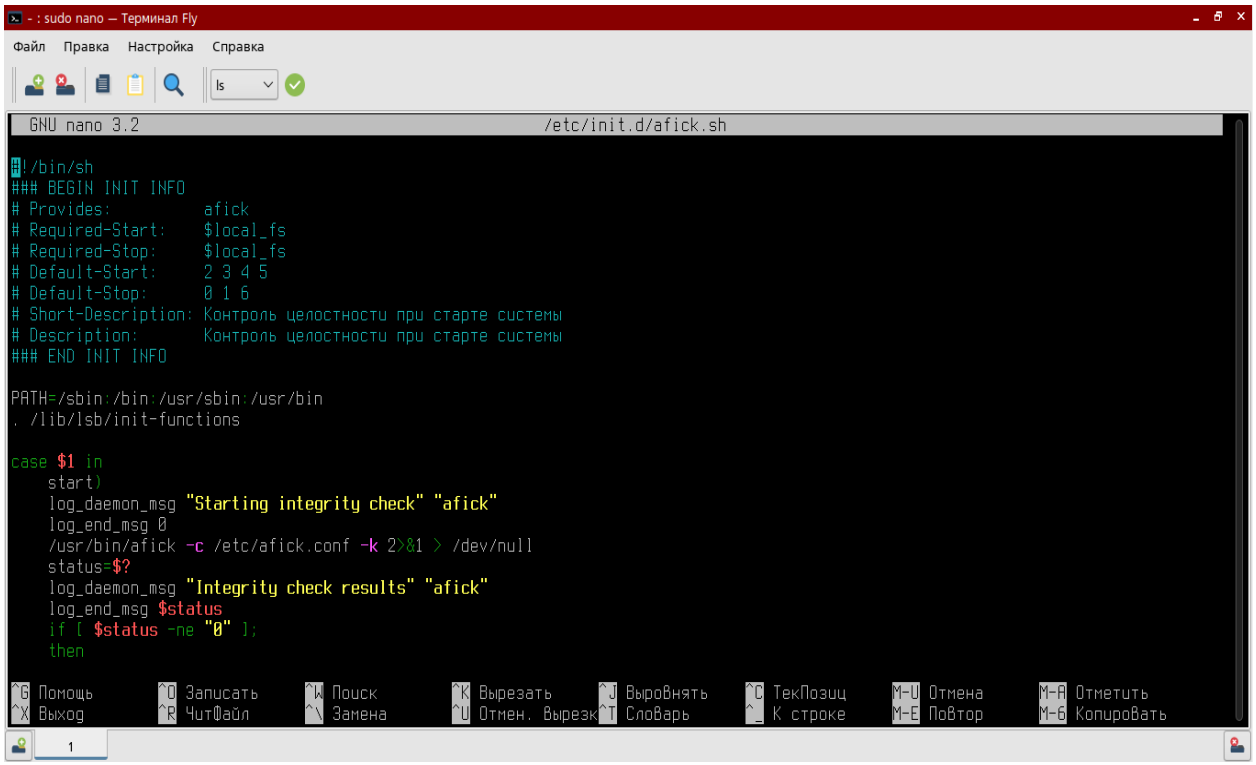

Рисунок В.42. – Первая часть созданного файла

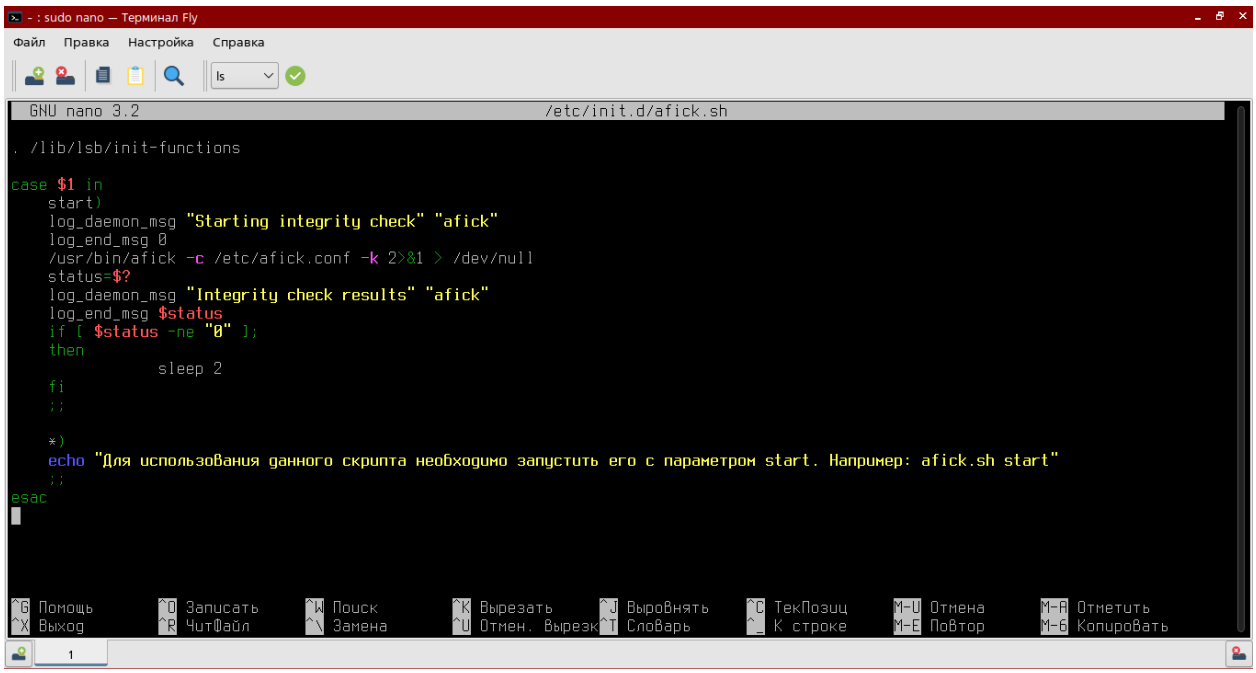

Рисунок В.43. – Вторая часть созданного файла

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

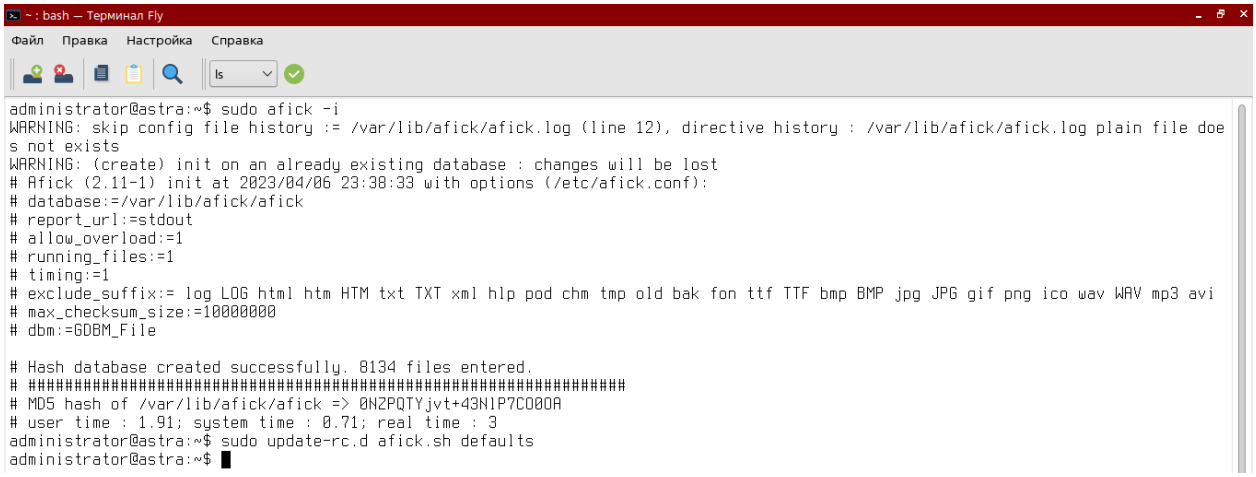

Рисунок В.44. – Выполнение команд

Аналогичного результата можно добиться, используя графическую утилиту afick.

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

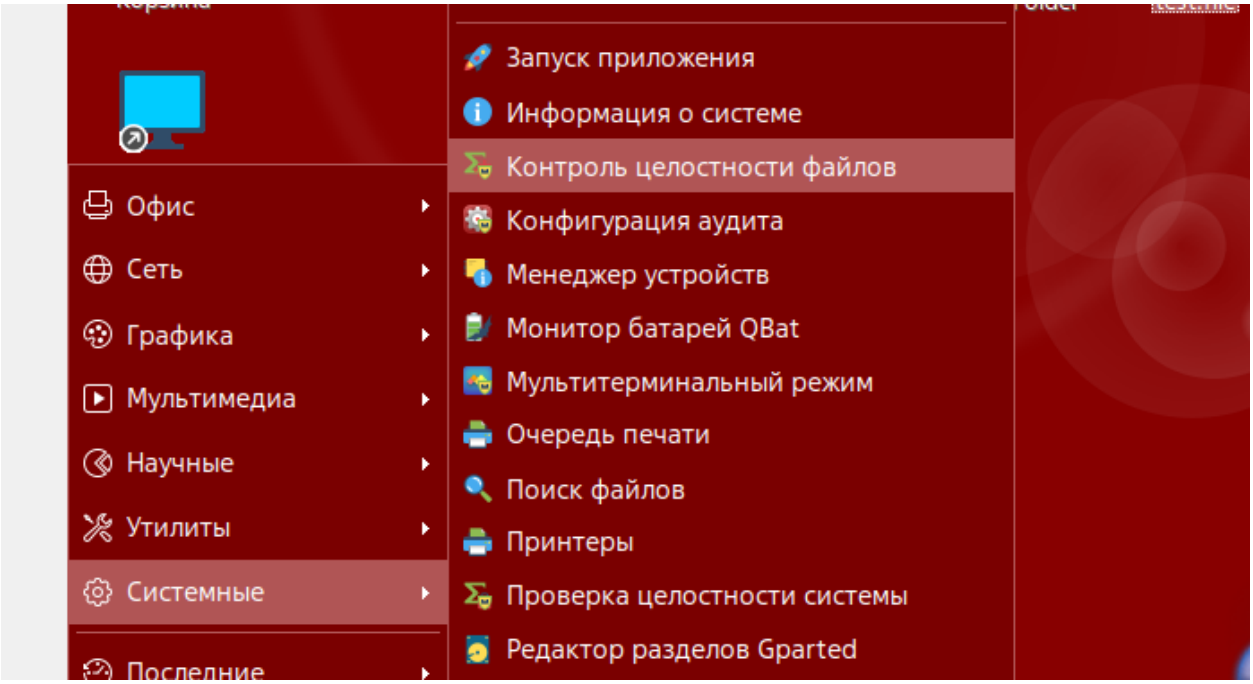

Рисунок В.45. – Запуск утилиты контроля целостности файлов

Откроется утилита как на рисунке В.46.:

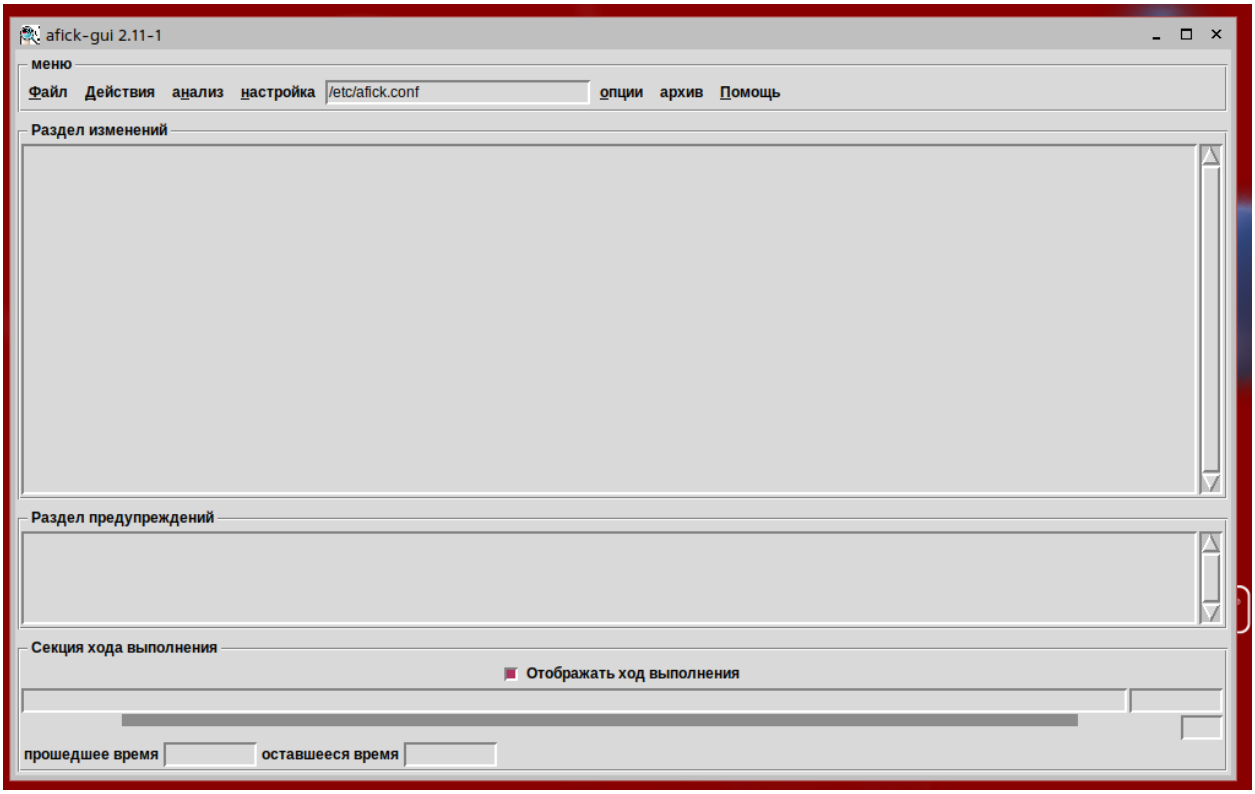

Рисунок В.46. – Утилита affick

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

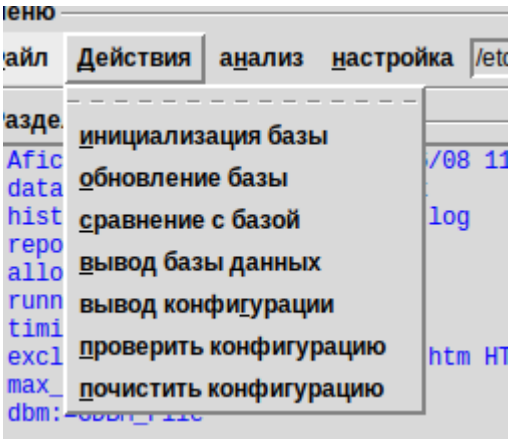

Рисунок В.47. – Инициализация БД affick

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.):

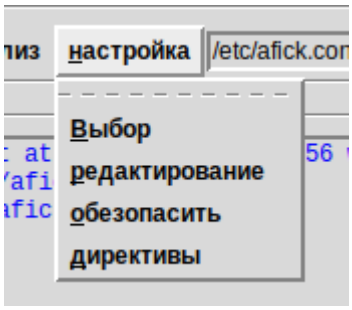

Рисунок В.48. – Выбор в меню

```
# ! /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.)

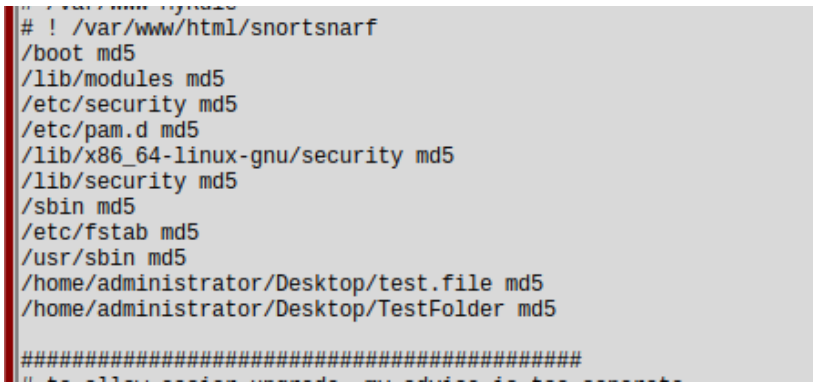

Рисунок В.50. – Настройка контроля целостности для файла и папки

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

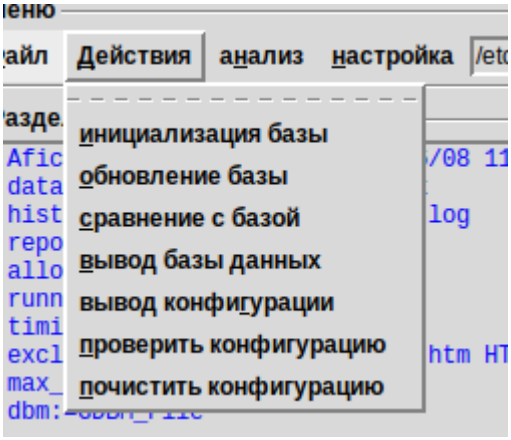

Рисунок В.51. – Обновление базы

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

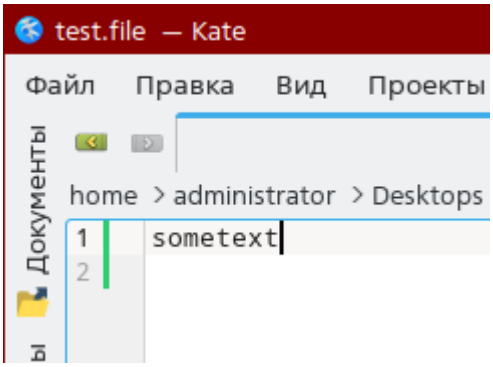

Рисунок В.52. – Редактирование файла

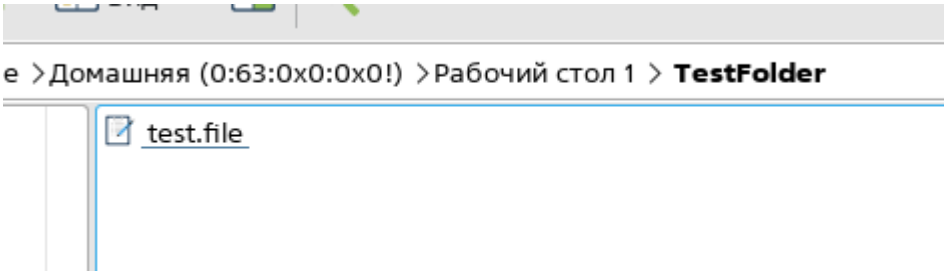

Рисунок В.53 – Добавление файла в проверяемую папку

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

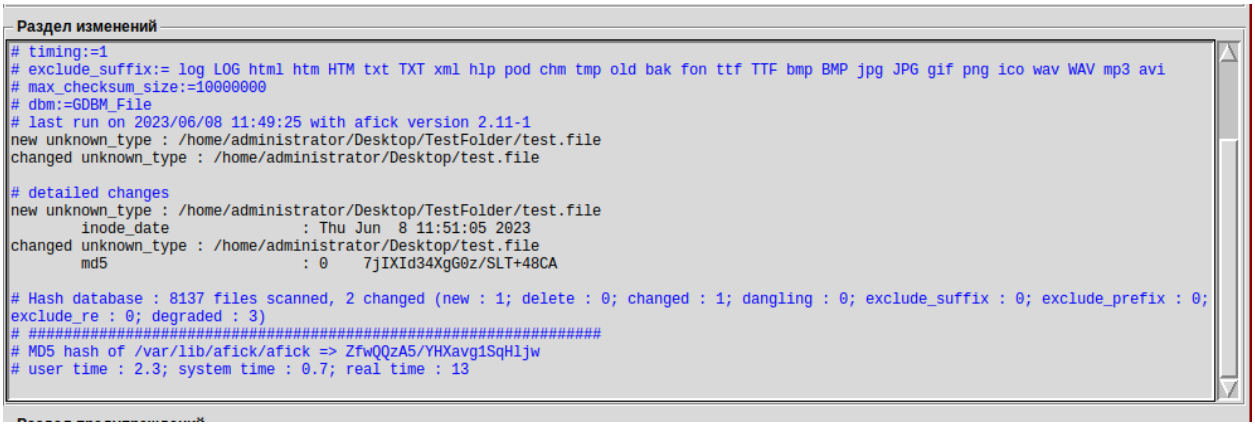

Рисунок В.54. – Проверка контроля целостности

Необходимо обратить внимание, что в конфигурационном файле указываются расширения файлов, которые будут игнорироваться (см. рисунок В.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.):

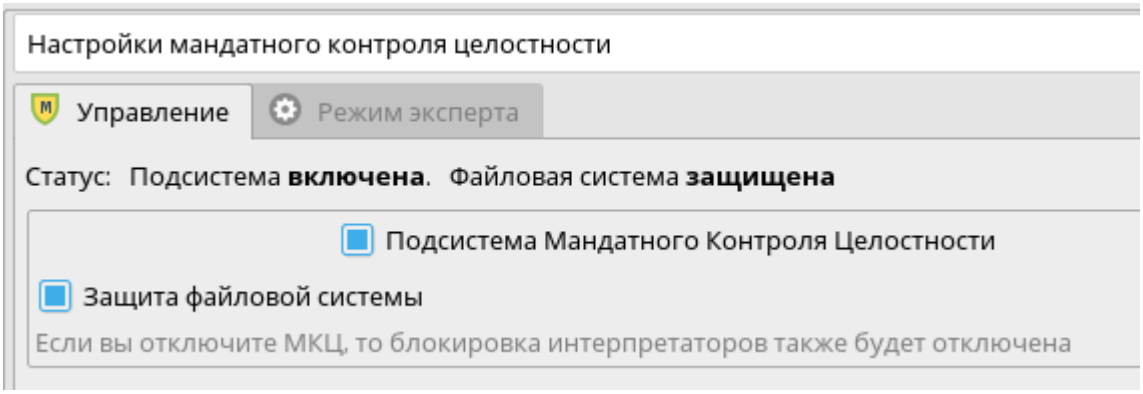

Рисунок В.56. – Включение защиты ФС

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

```
leti@astra:~$ sudo astra-mic-control status
АКТИВНО
leti@astra:~$
```

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

```
leti@astra:~$ sudo set-fs-ilev status
АКТИВНО
leti@astra:~$
```

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

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

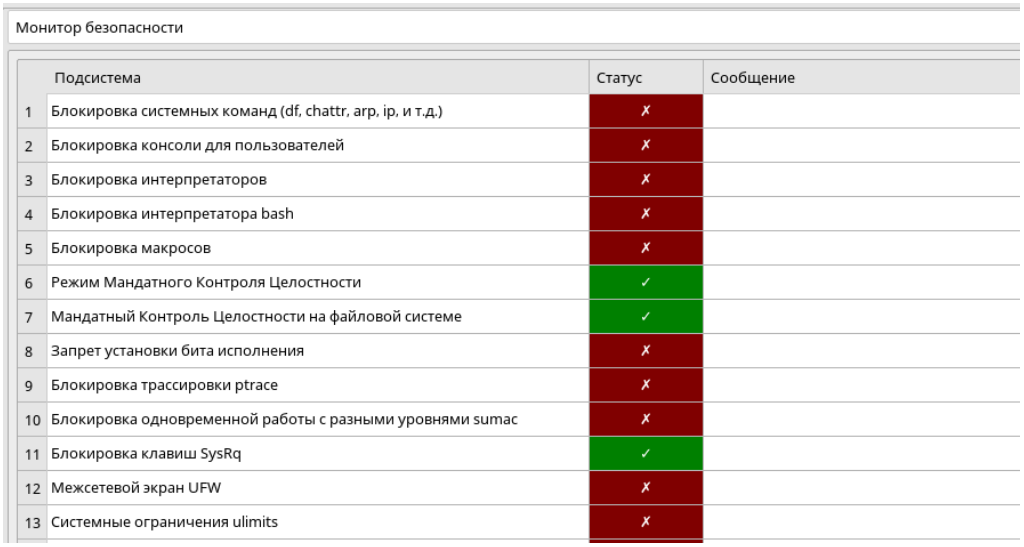

Рисунок В.59. – проверка статус в графической утилите

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

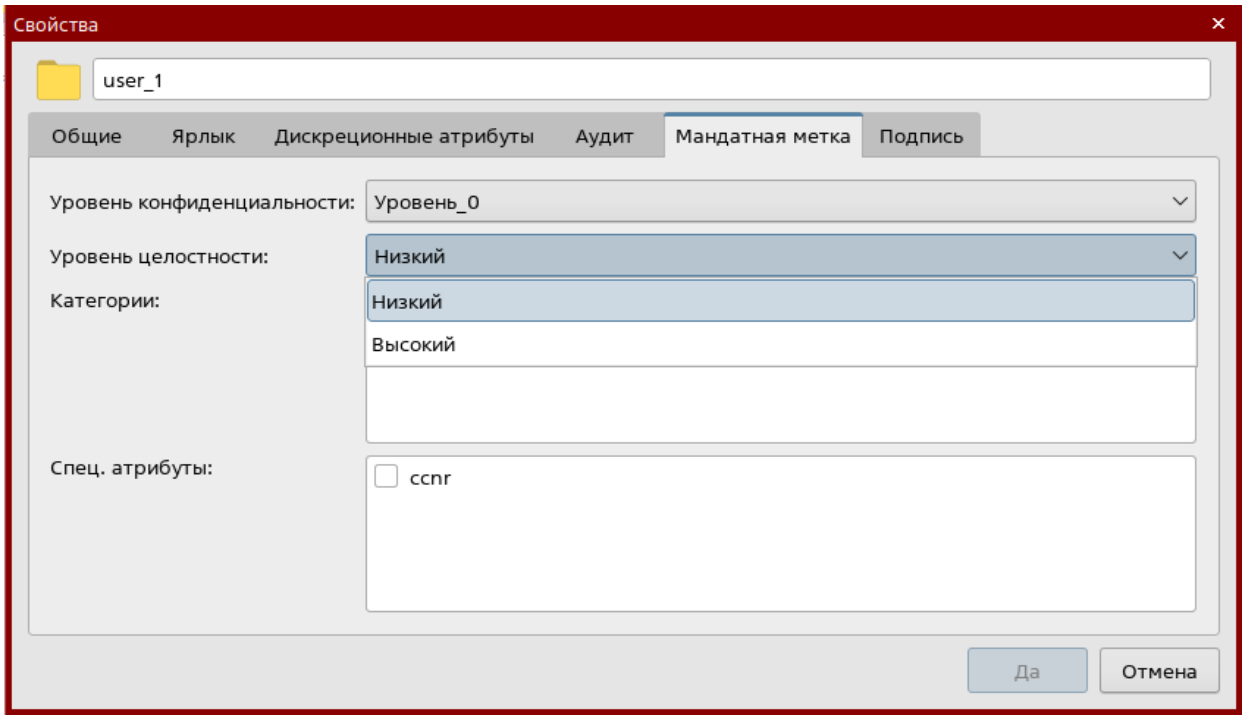

Рисунок В.60. – Создание каталога с требуемым уровнем целостности

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

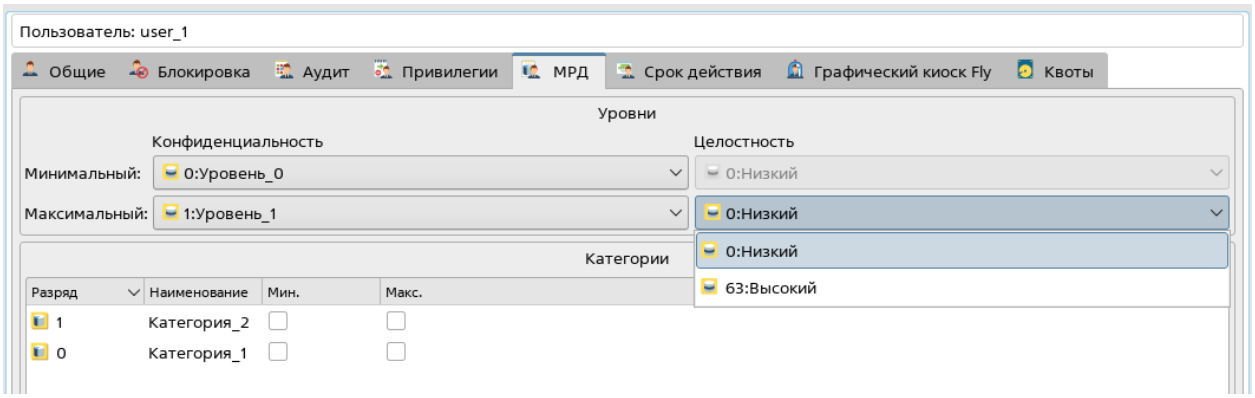

Рисунок В.61. – Настройка уровня целостности пользователя

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

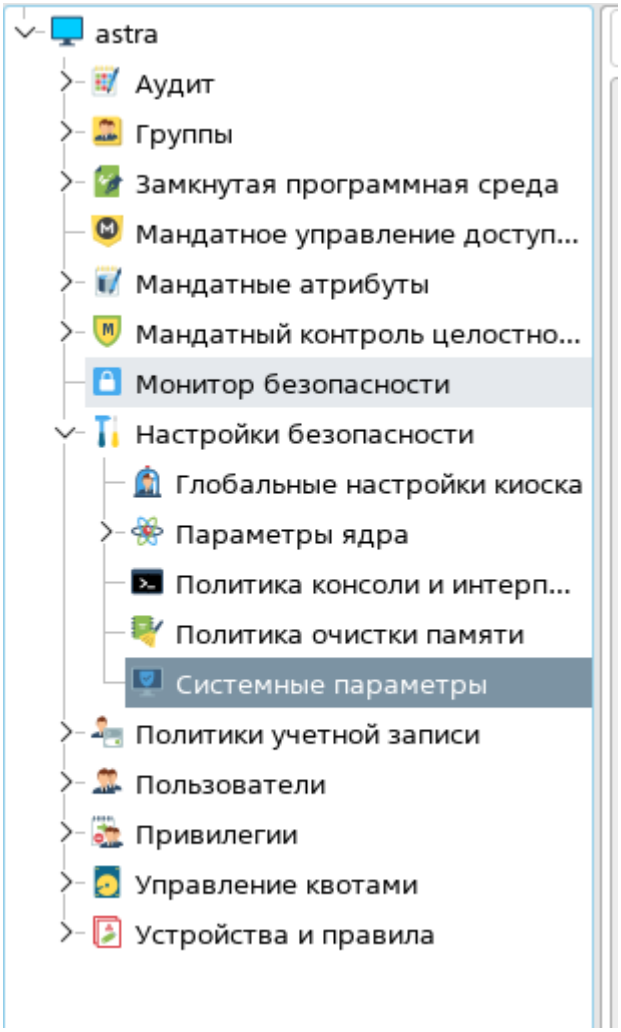

Рисунок В.62. – Путь к системным параметрам

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.):

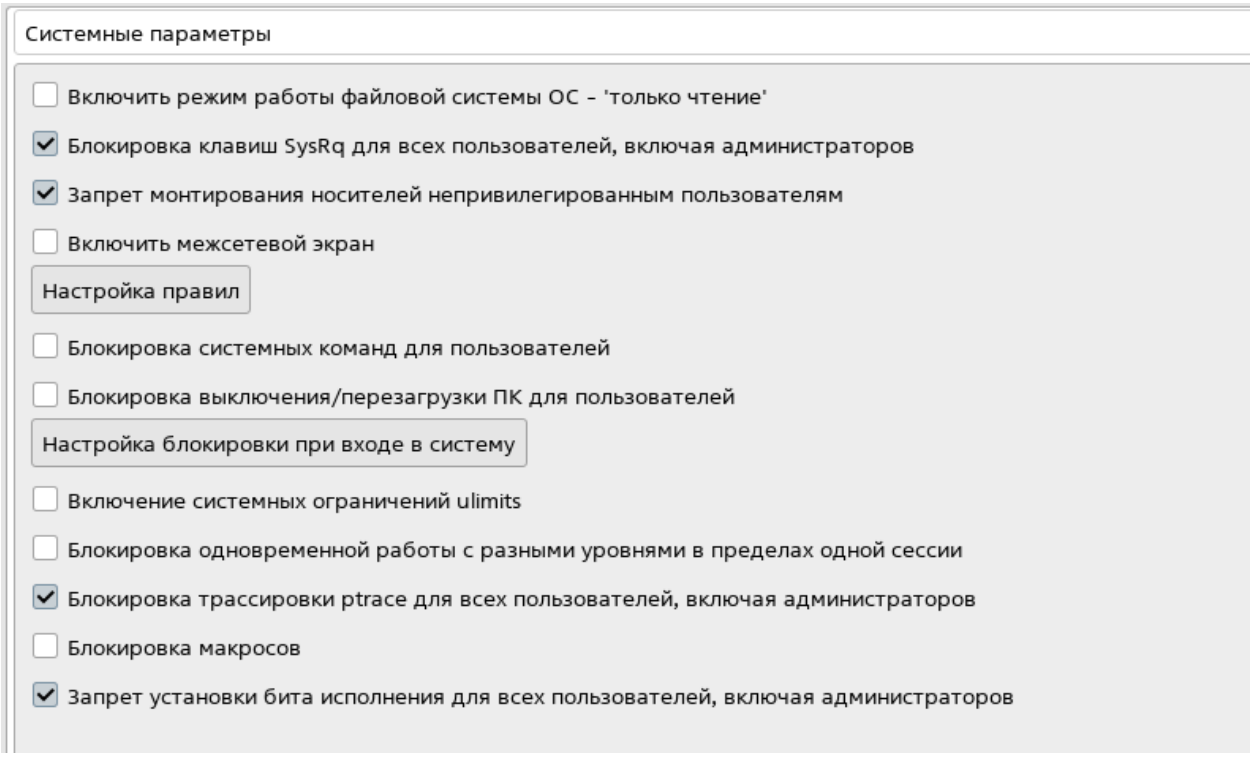

Рисунок В.63. – Настройка монитора безопасности

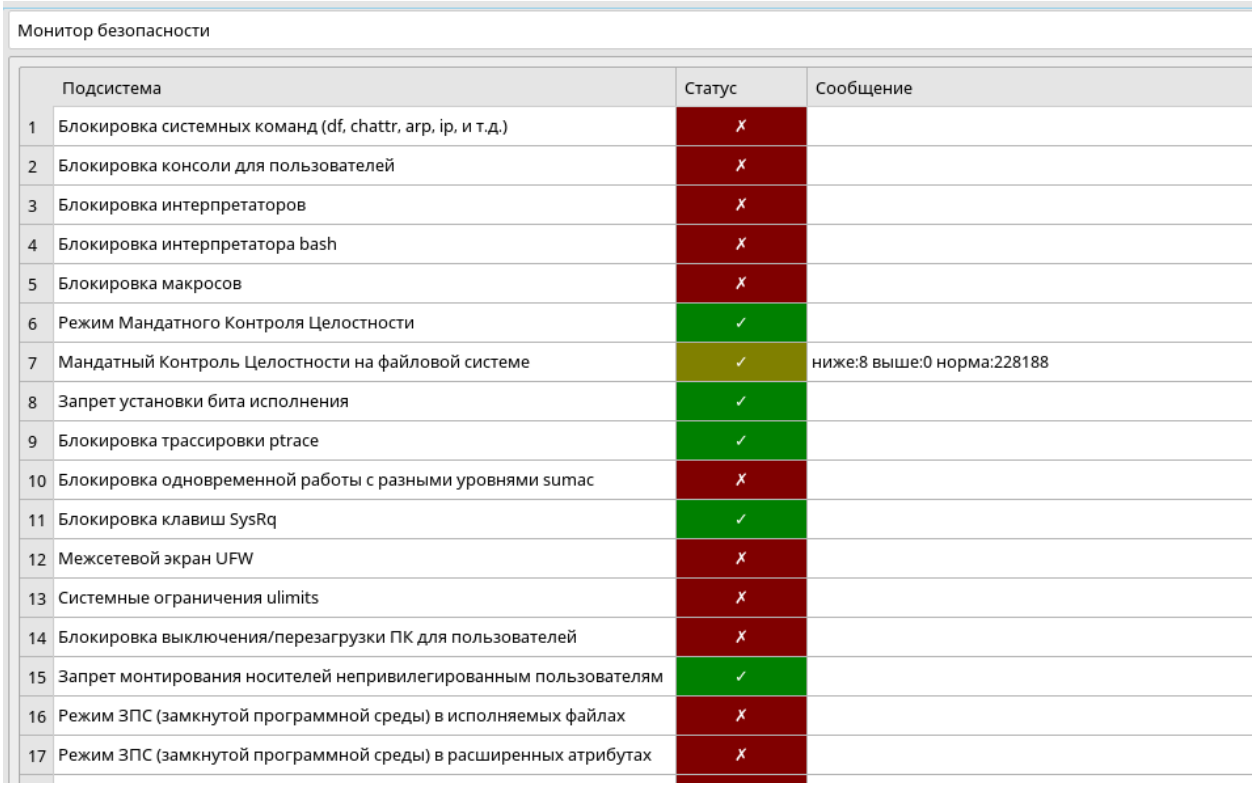

Рисунок В.64. – Результат настройки монитора безопасности

Настройка прав разграничения доступа для внешних носителей информации

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

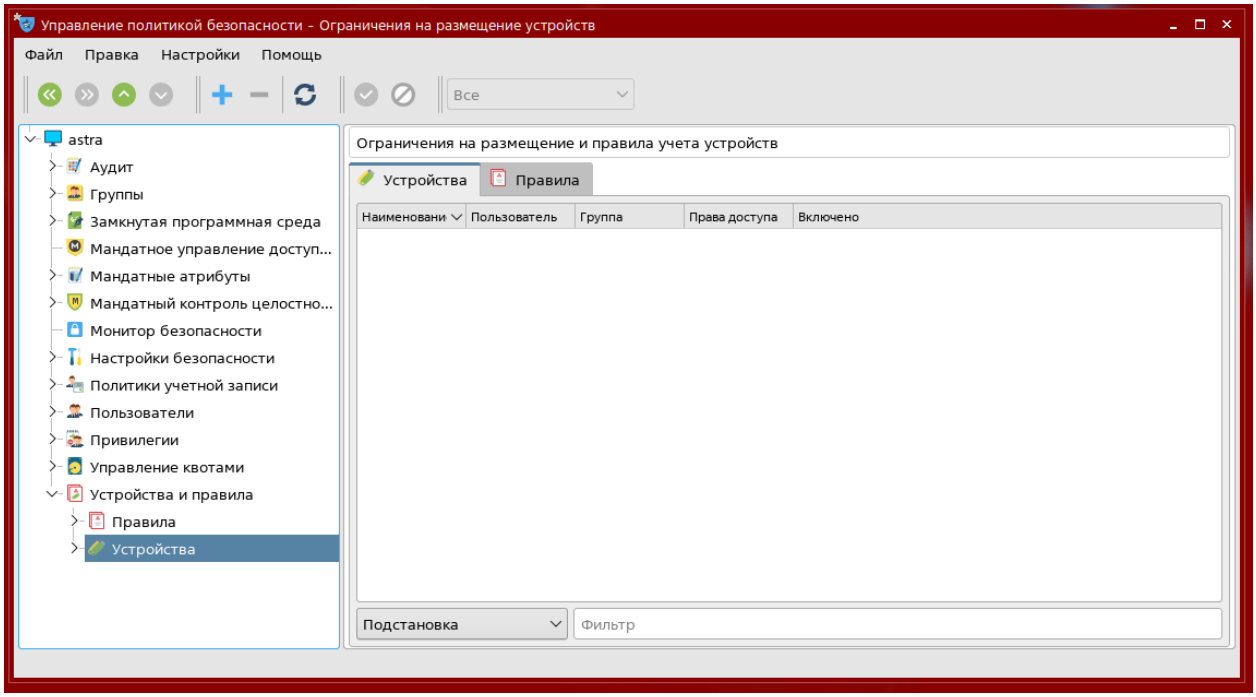

Рисунок В.65. – Окно ограничение на размещения и правила учета устройств

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

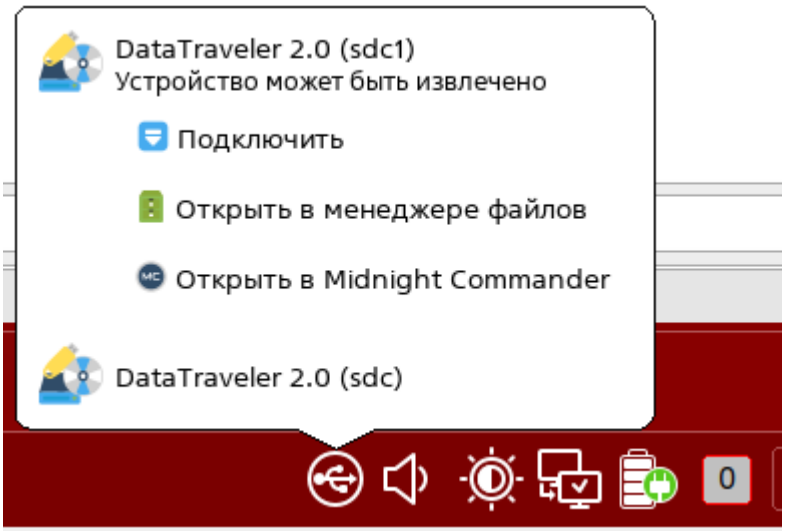

Рисунок В.66. – Подключение устройства

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

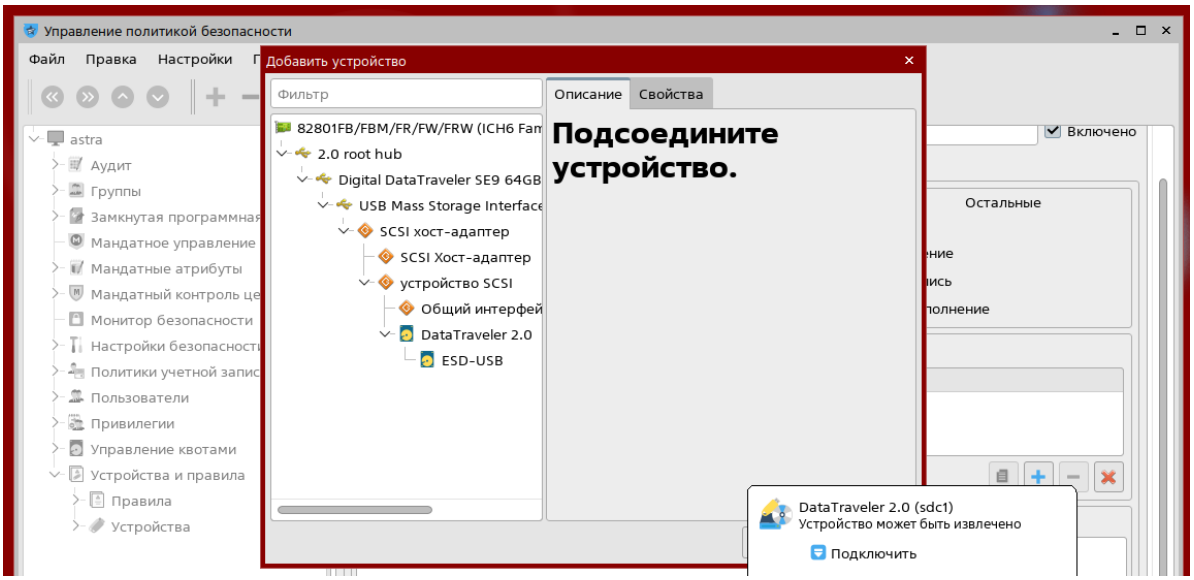

Рисунок В.67. – Список устройств

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

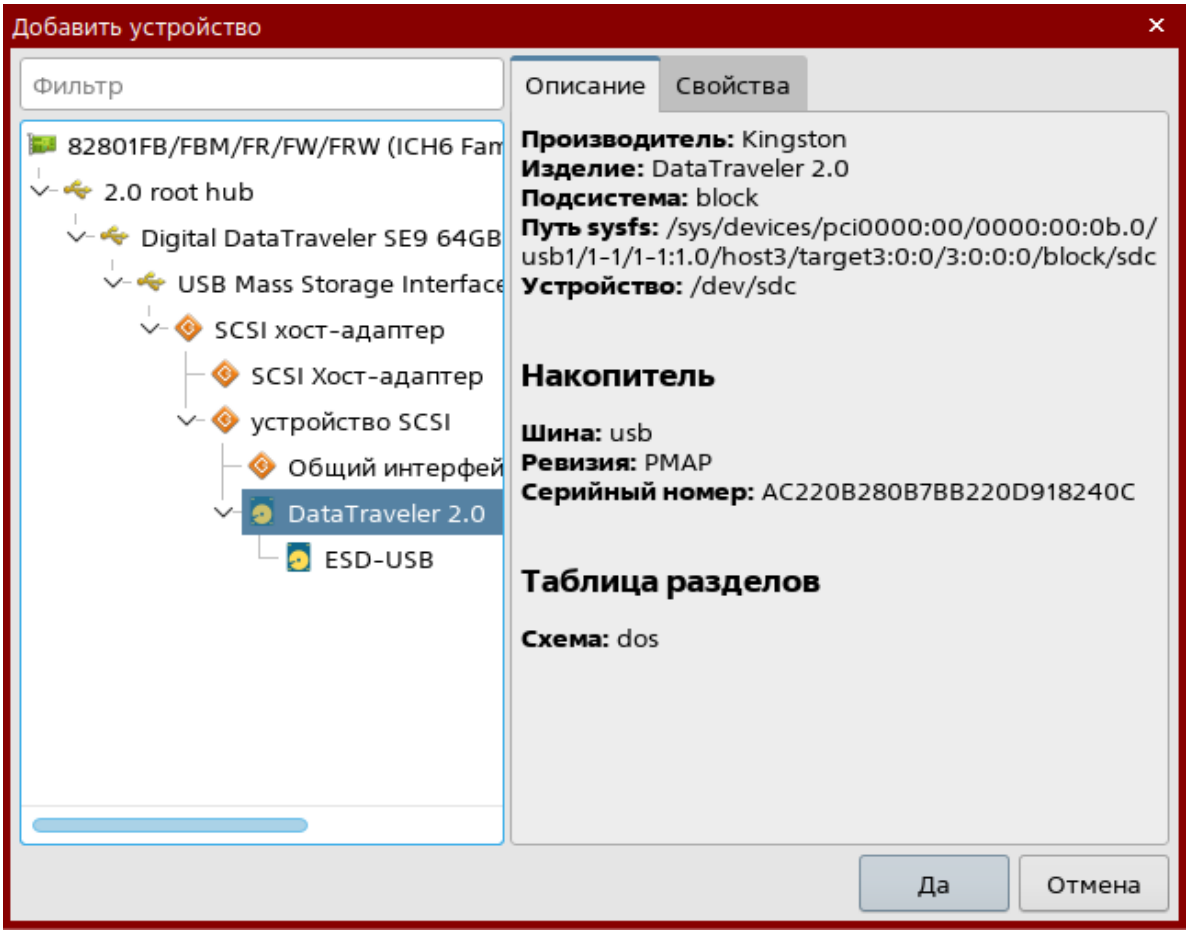

Рисунок В.68. – Выбор необходимого устройства из списка

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

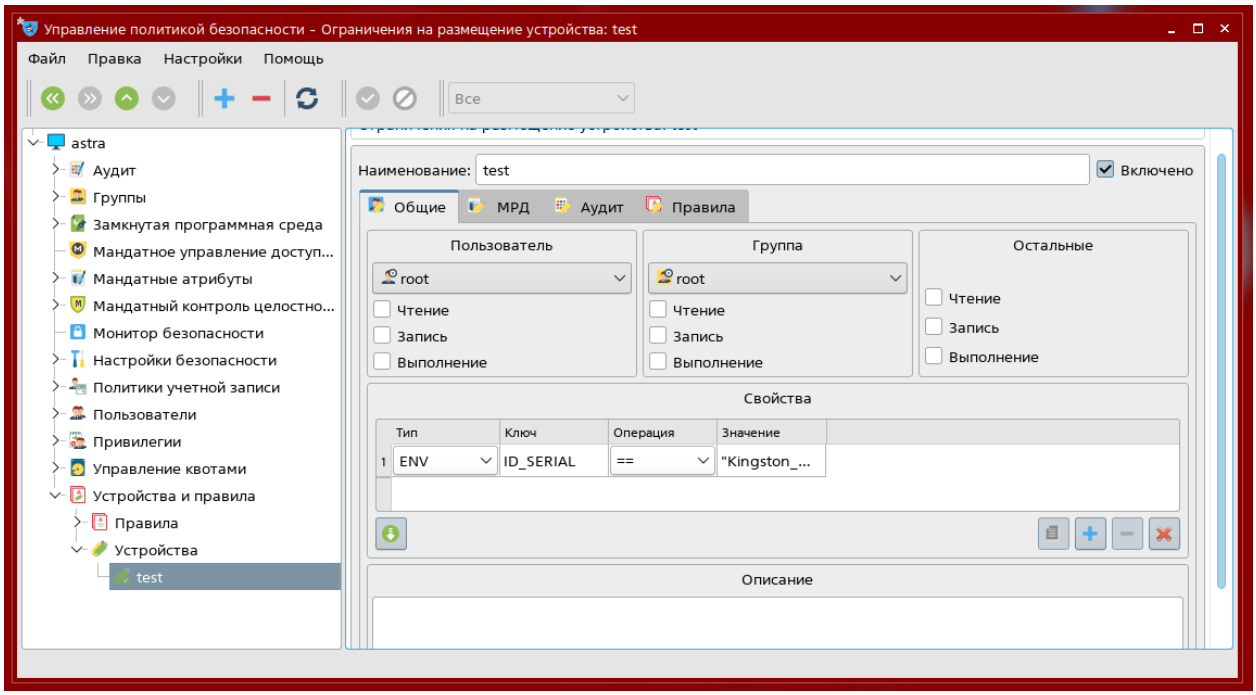

Рисунок В.69. – Результат настройки устройства

ПРИЛОЖЕНИЕ Г

Пример настройки САВЗ «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 ВТ, 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.);

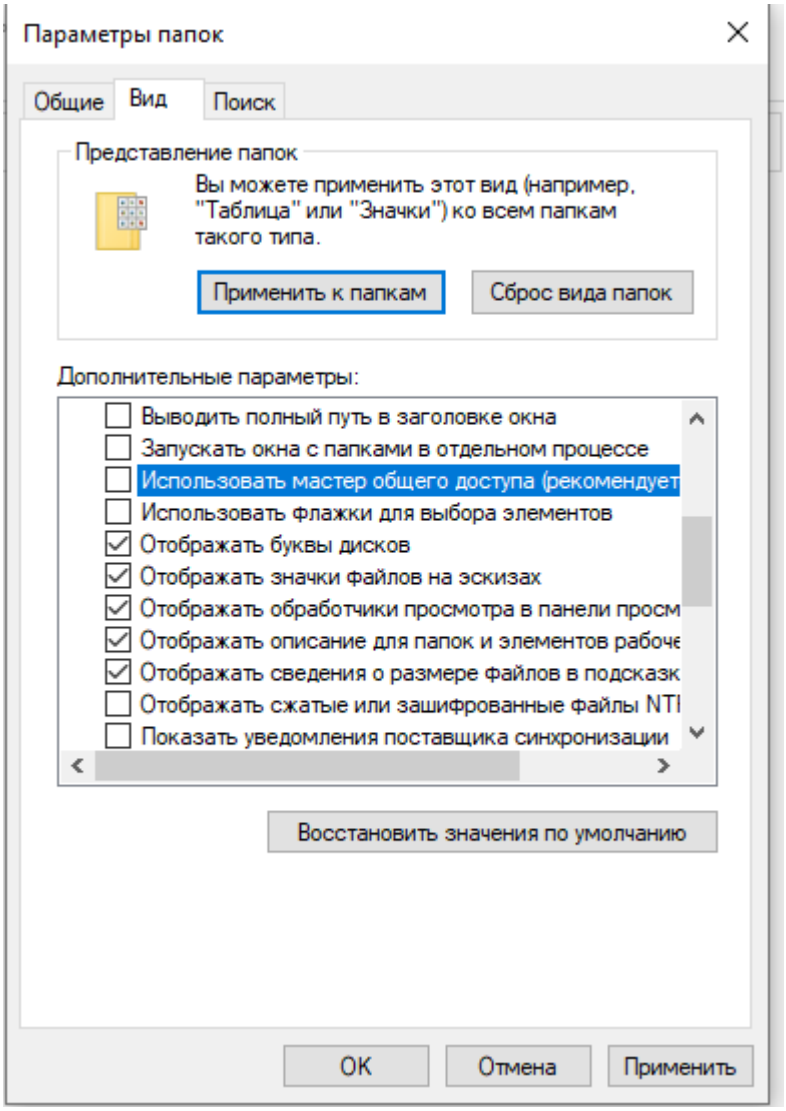

Рисунок Г.1. – Флаг «Использовать мастер общего доступа (рекомендуется)»

– произвести настройку прав доступа к данной директории (Нажать правой кнопкой «мыши» по директории «C:\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.).

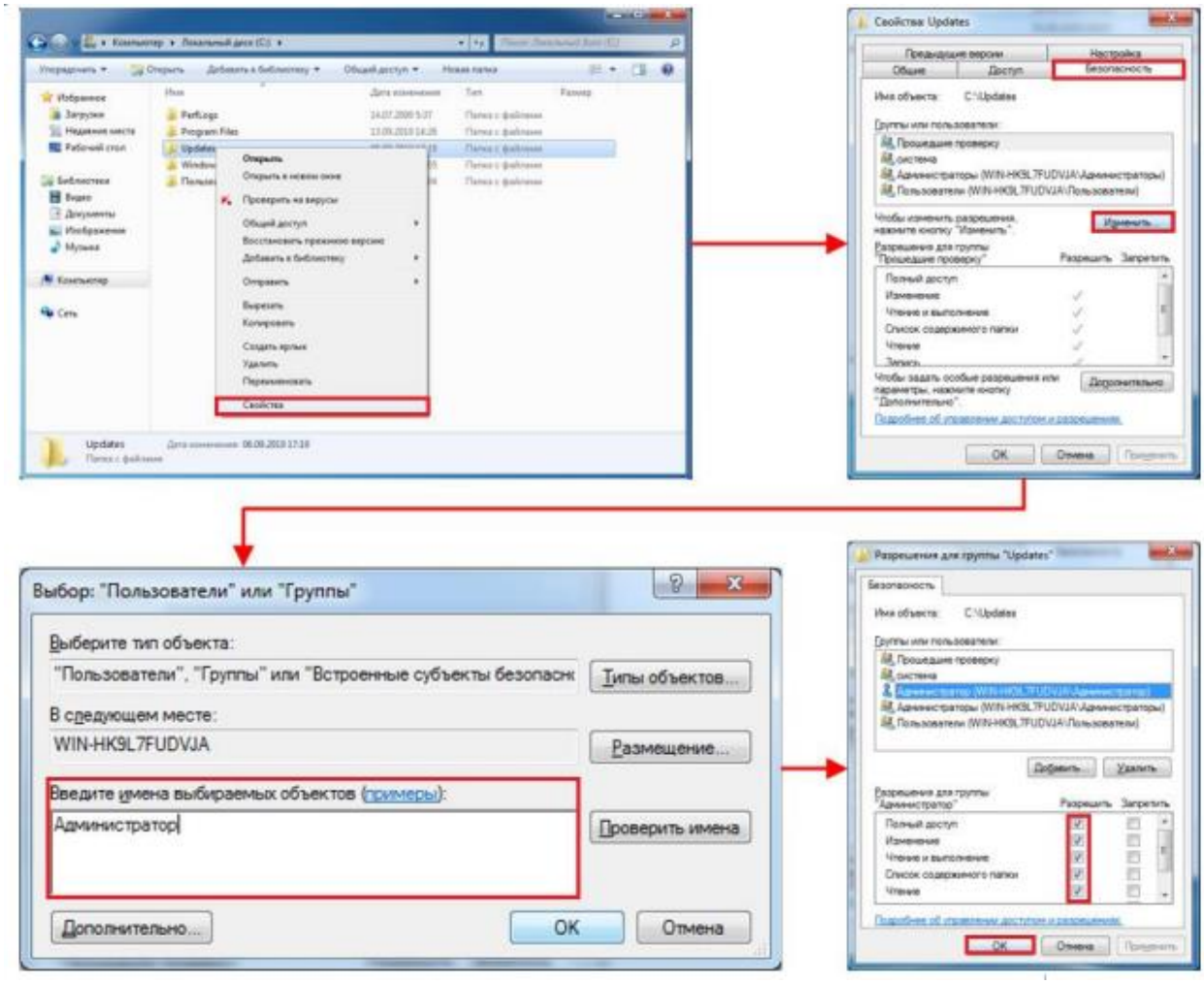

Рисунок Г.2. – Настройка прав доступа к директории

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.);

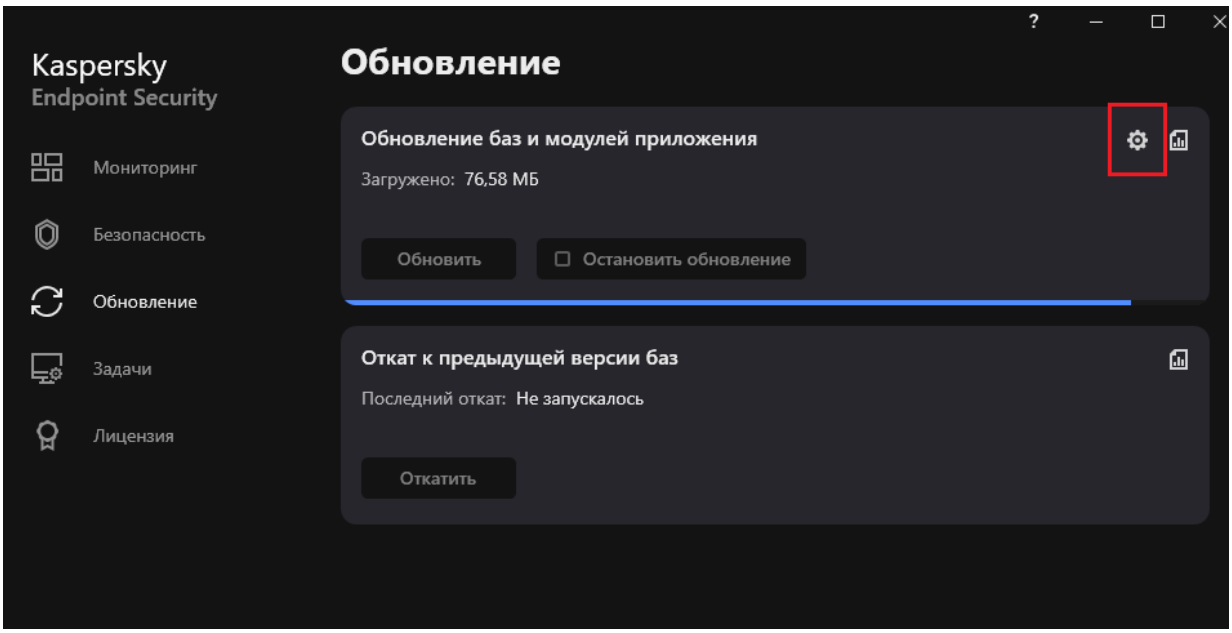

Рисунок Г.3. – Настройка компонента «Обновления»

– 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.);

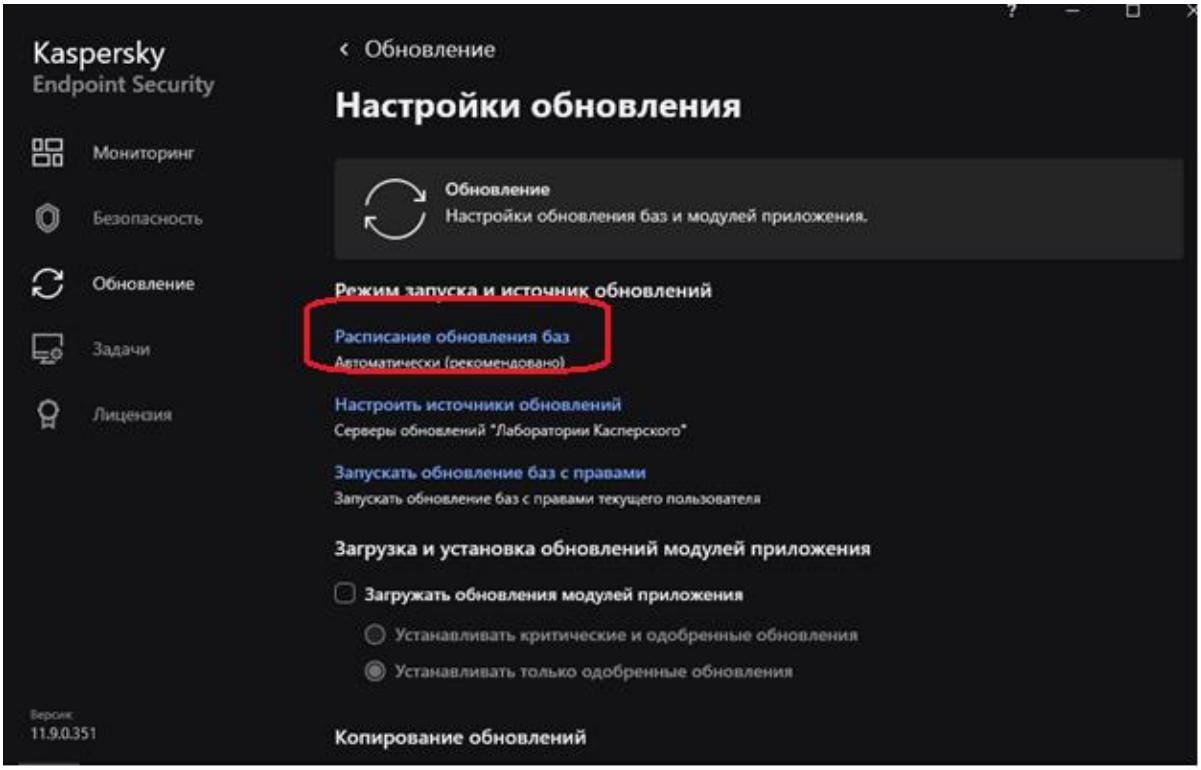

Рисунок Г.4. – Настройка обновлений

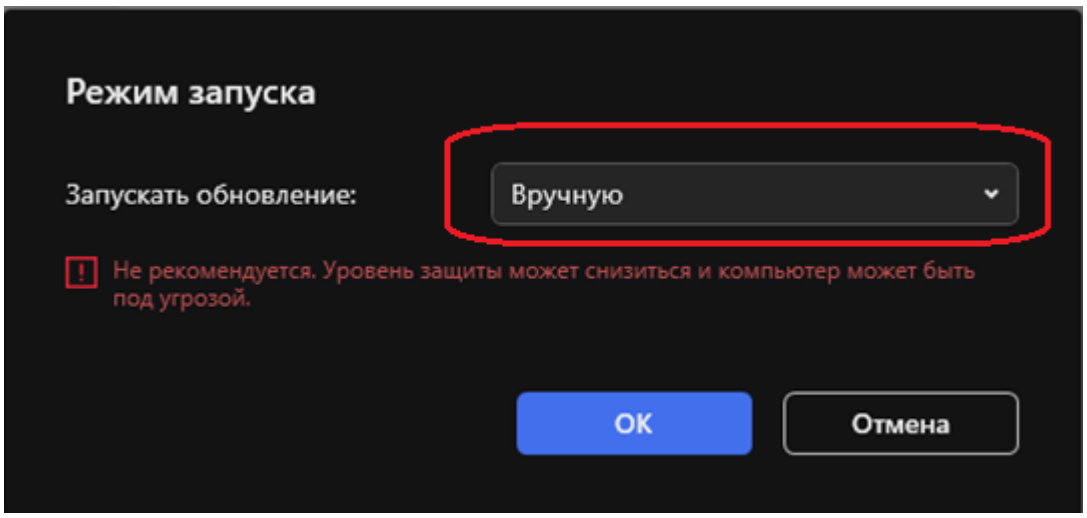

Рисунок Г.5. – Выбор режима запуска обновления

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

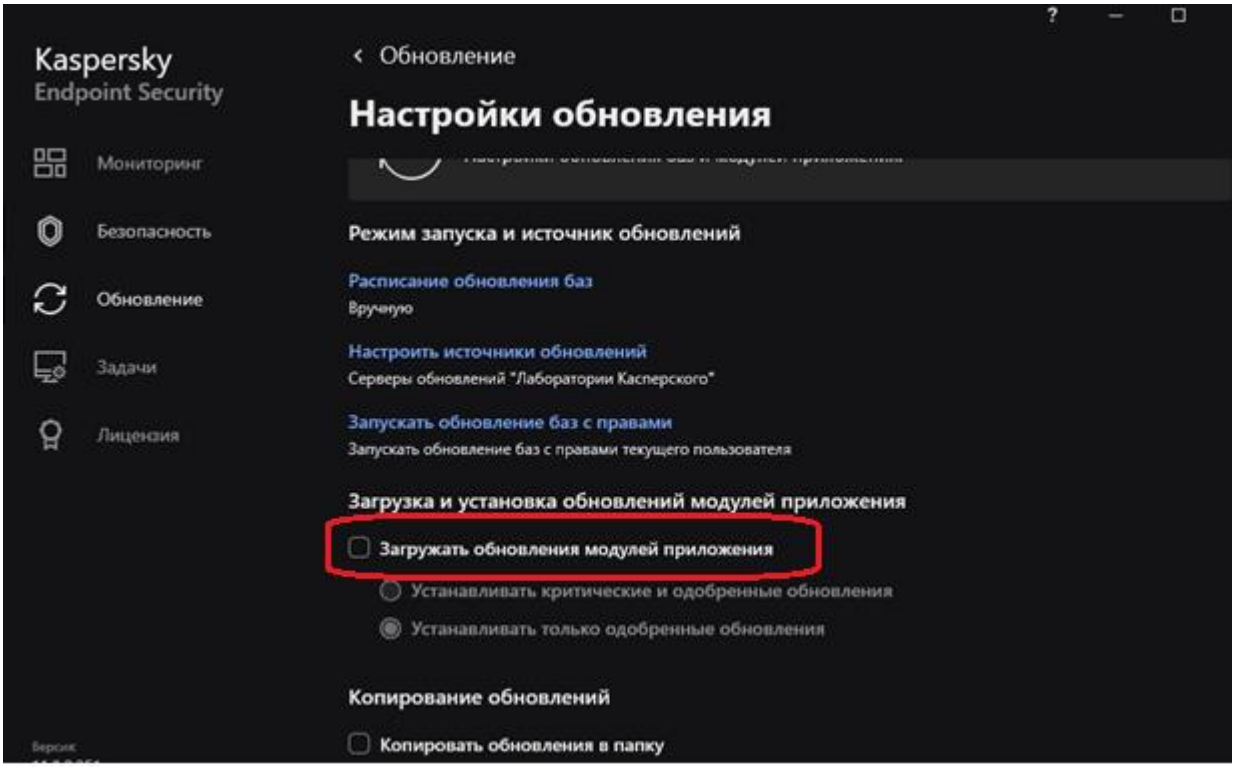

Рисунок Г.6. – Настройка обновлений

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

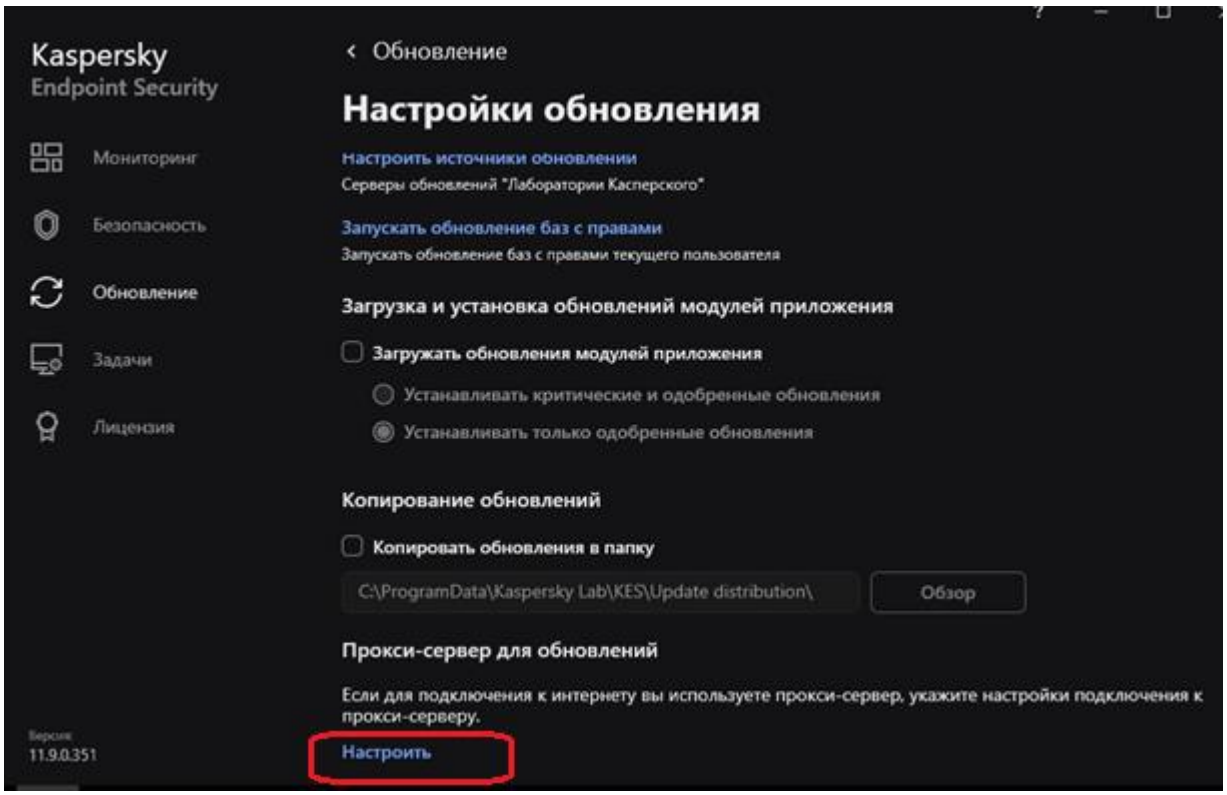

Рисунок Г.7. – Настройка обновлений

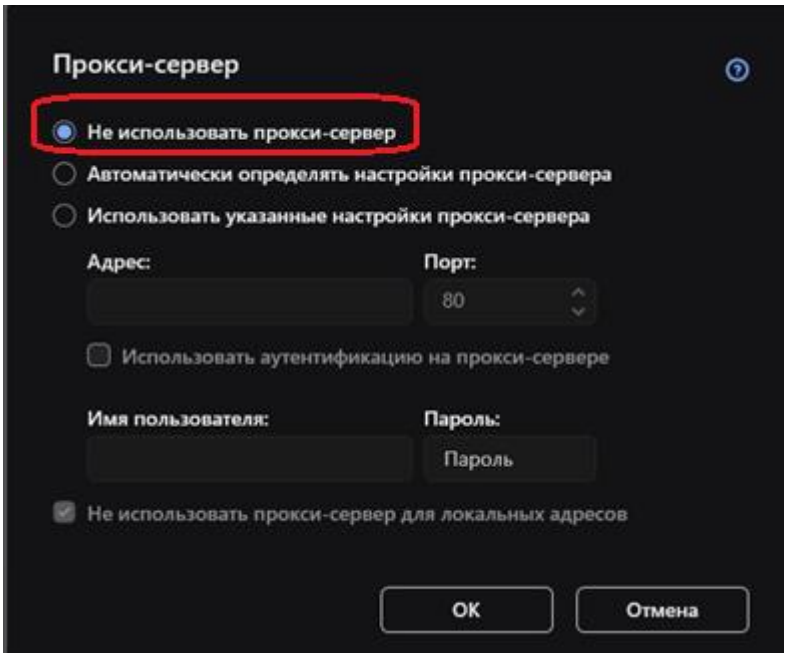

Рисунок Г.8. – Настройка параметров обновлений

– 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.);

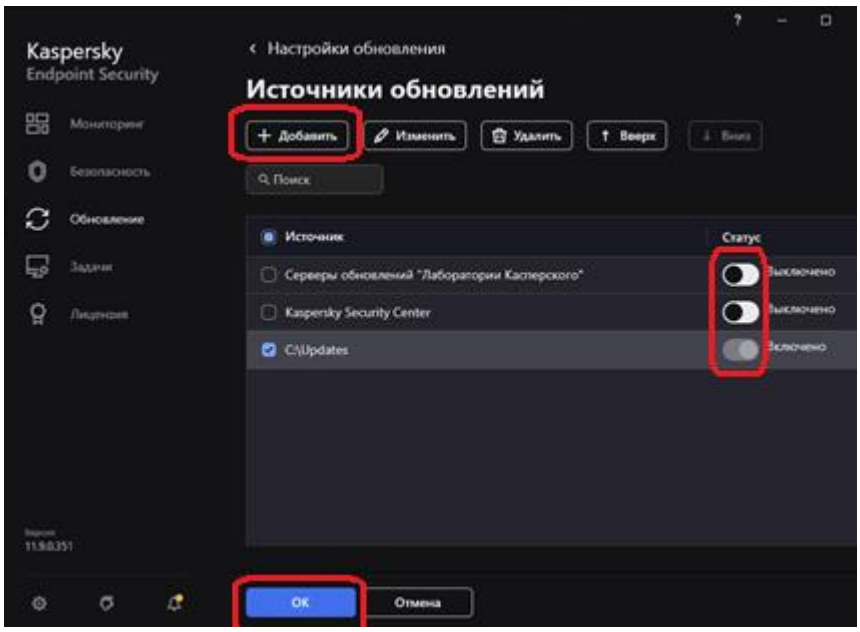

Рисунок Г.9. – Выбор источника обновлений

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

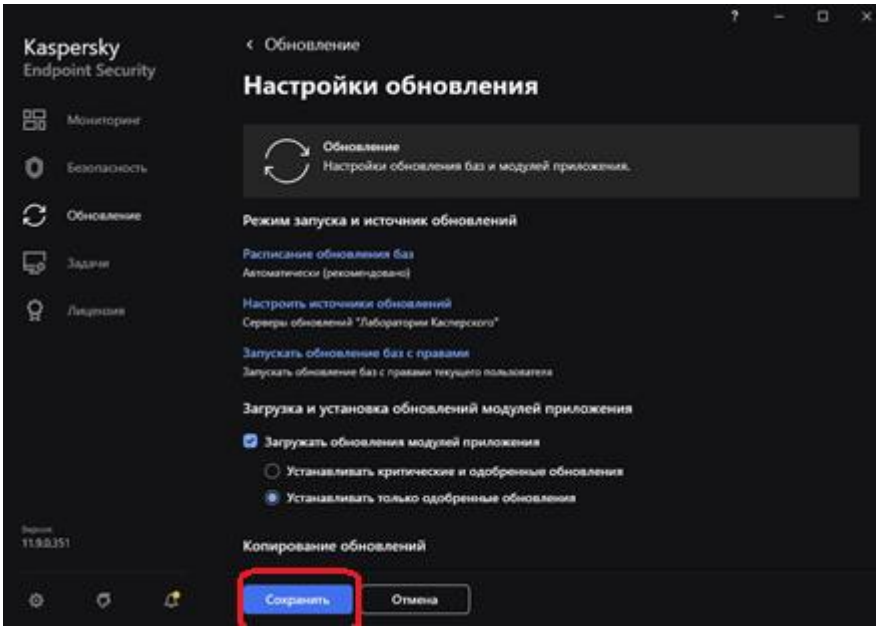

Рисунок Г.10. – Сохранение обновлений

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

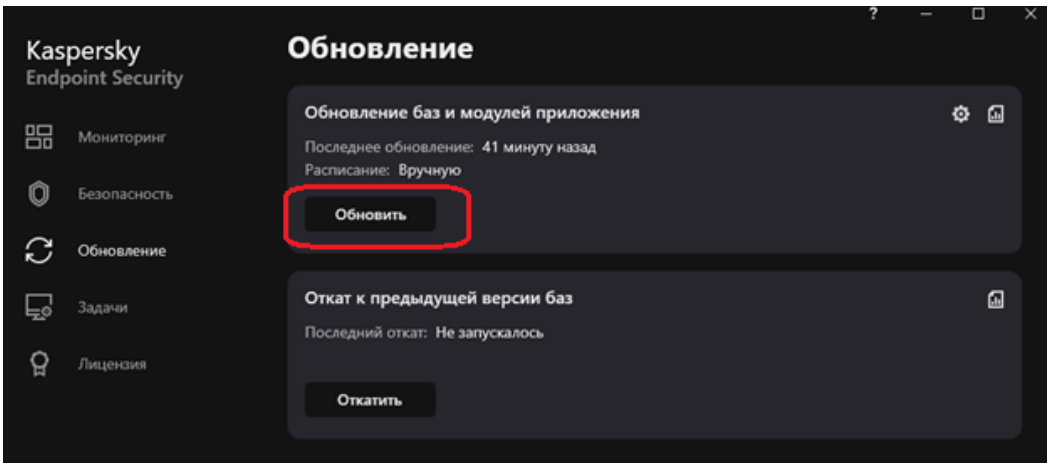

Рисунок Г.11. – Запуск обновлений БВС в ручном режиме

– 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.).

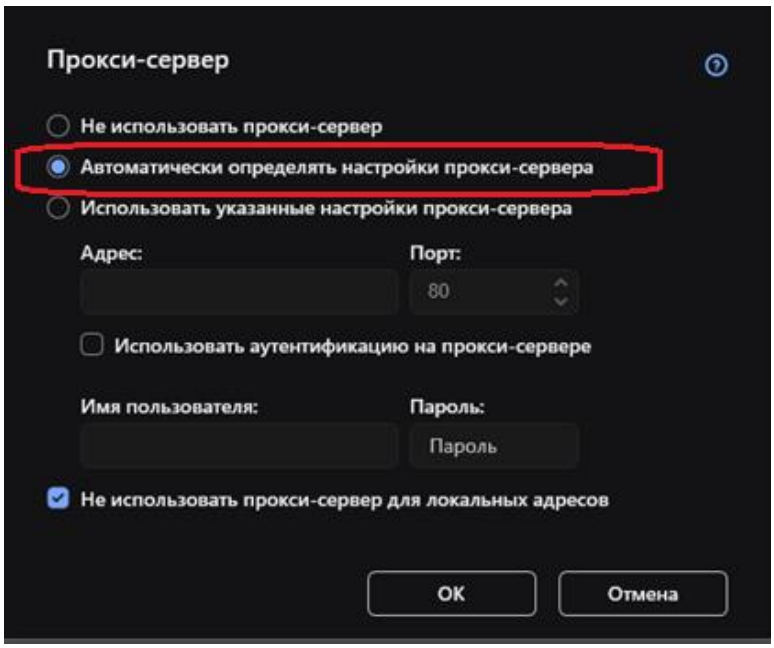

Рисунок Г.12. – Настройка параметров прокси-сервера

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.).

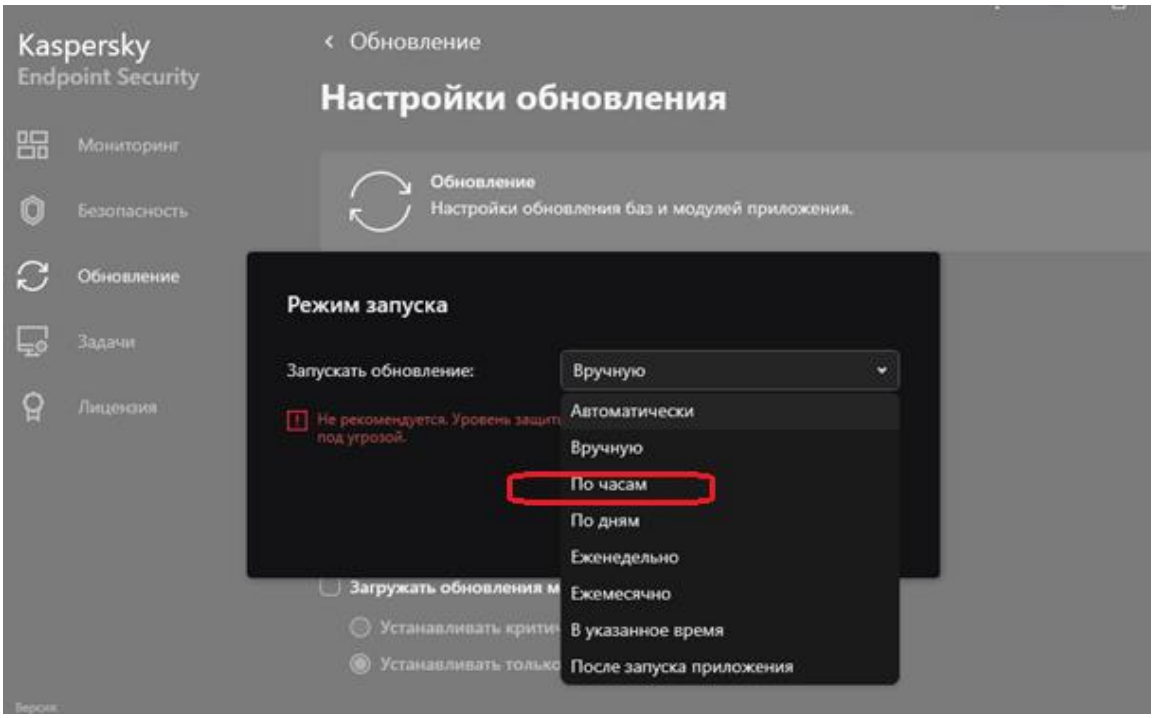

Рисунок Г.13. – Настройка задачи обновления самостоятельного АП сети Интернет

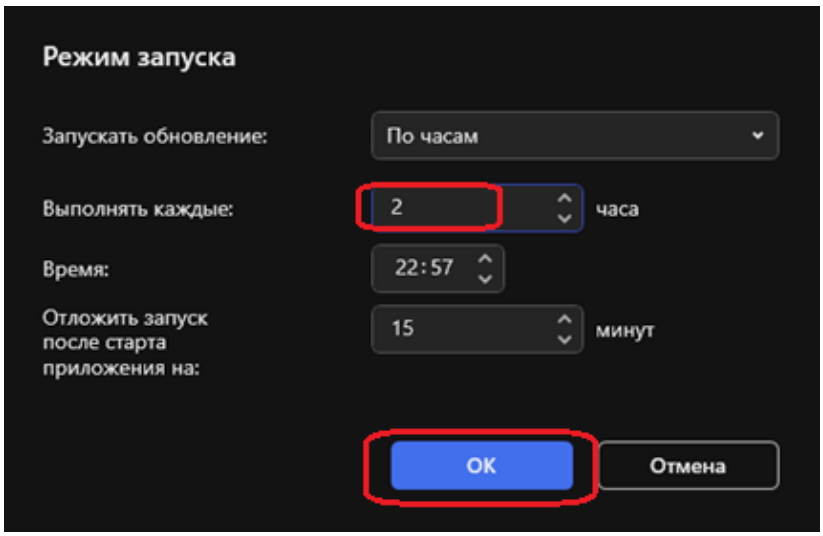

Рисунок Г.14. – Настройка задачи обновления самостоятельного АП сети Интернет

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.).

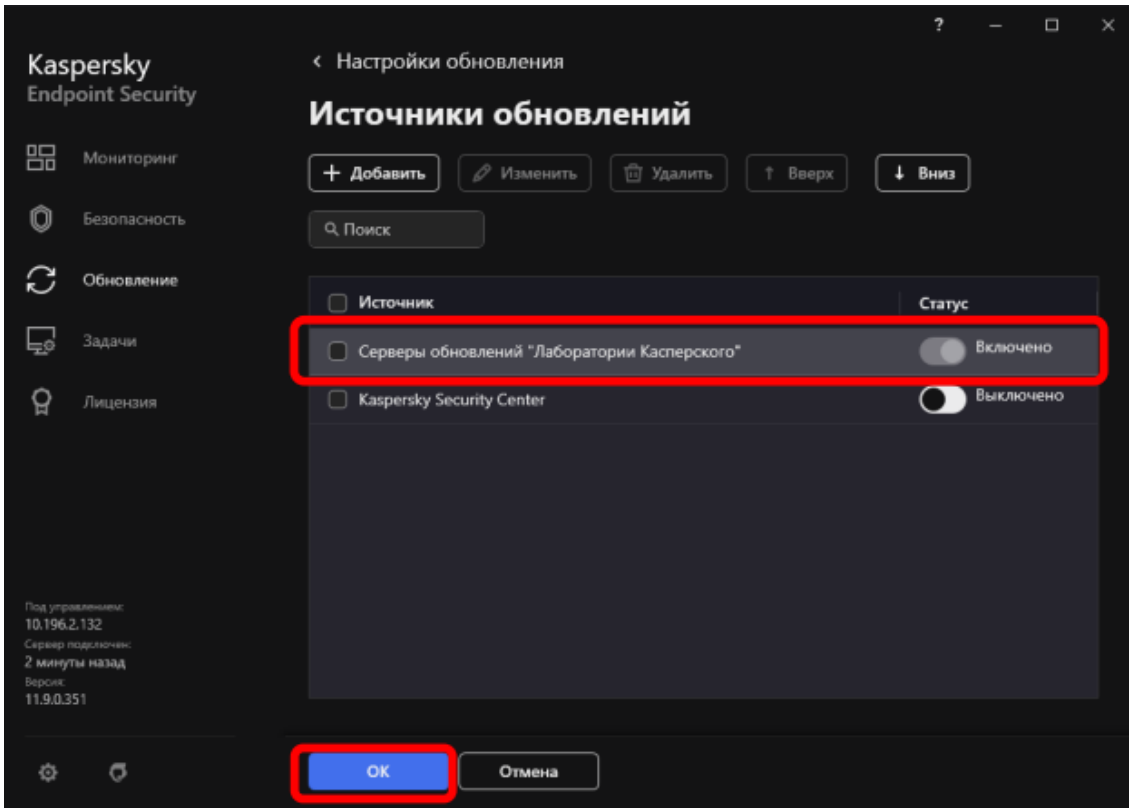

Рисунок Г.15. – Настройка источника обновлений

4) В окне «Настройки обновлений» нажать кнопку «Сохранить» (см. рисунок Г.16.).

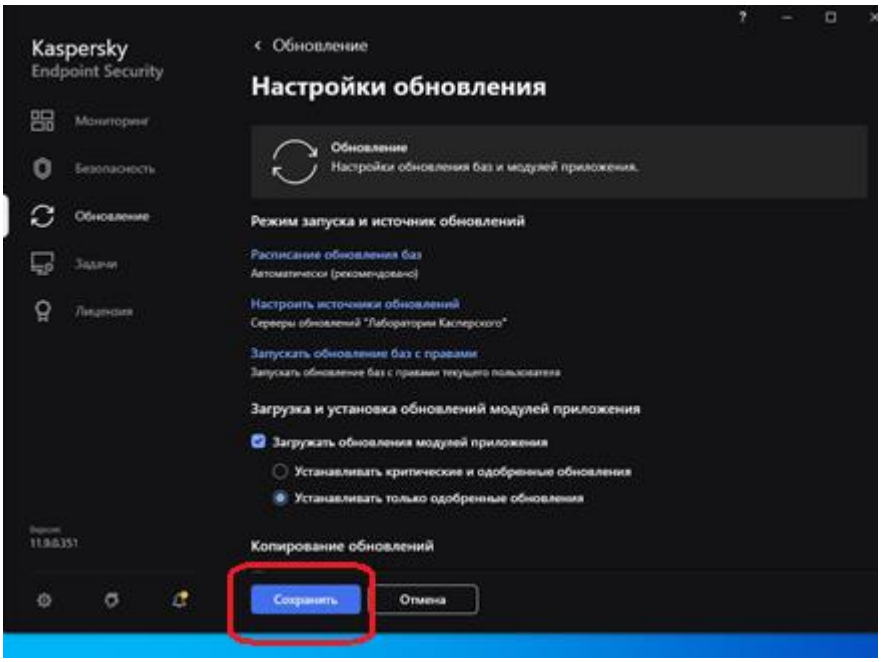

Рисунок Г.16. – Сохранение обновлений

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 Г.17.).

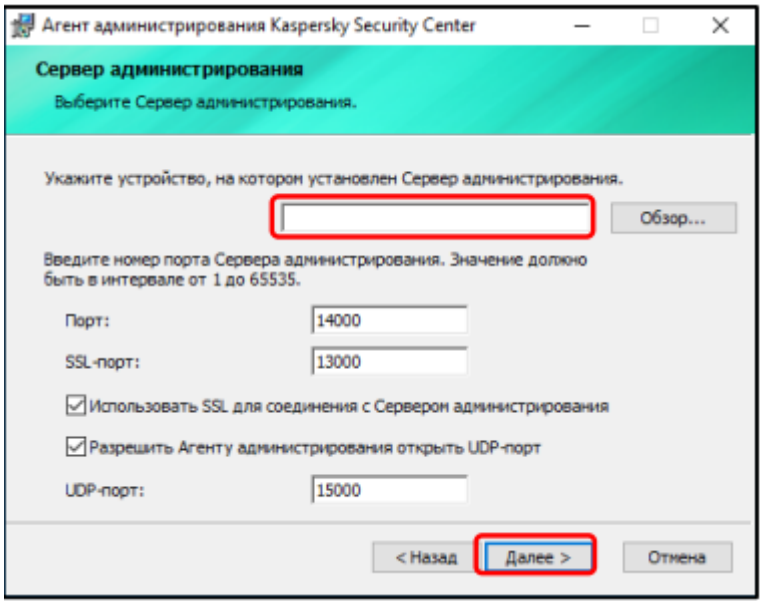

Рисунок Г.17. – Выбор сервера администрирования

В дальнейшем следует до завершения установки нажимать кнопку «Далее», оставляя все параметры по умолчанию.

После установки САВЗ 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.).

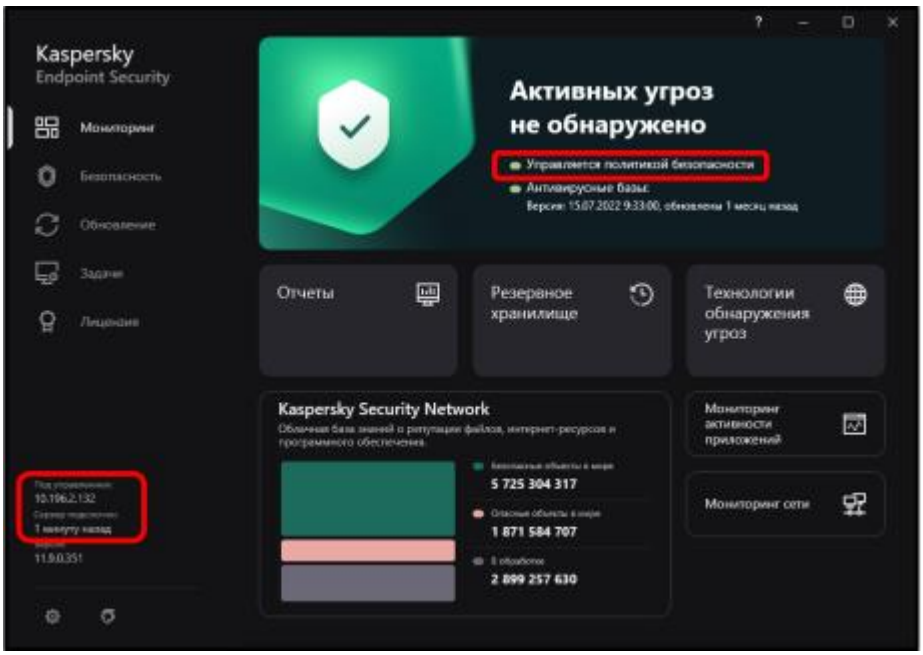

Рисунок Г.18. – Проверка подключения к серверу
«Kaspersky Security Center»

Если через 10 минут запись не появилась, целесообразно провести проверку соединения с сервером «Kaspersky Security Center». Для этого необходимо:

1) 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.);

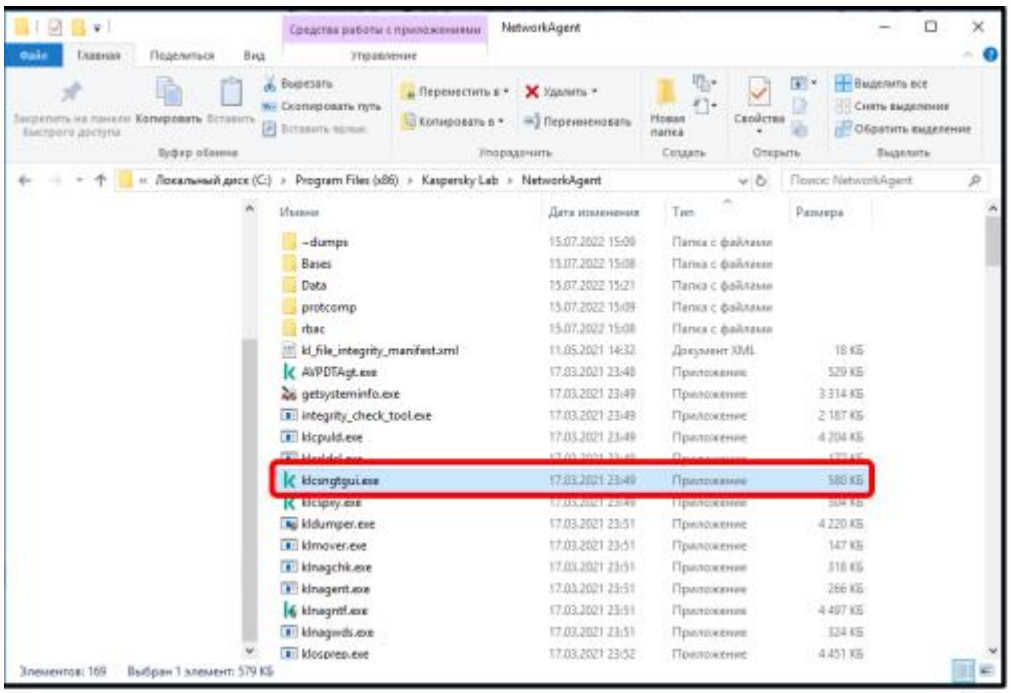

Рисунок Г.19. – Запуск утилиты «klcsngtgui.exe»

3) в открывшемся окне выбрать «Запустить утилиту klnagchk» (см. рисунок Г.20.).

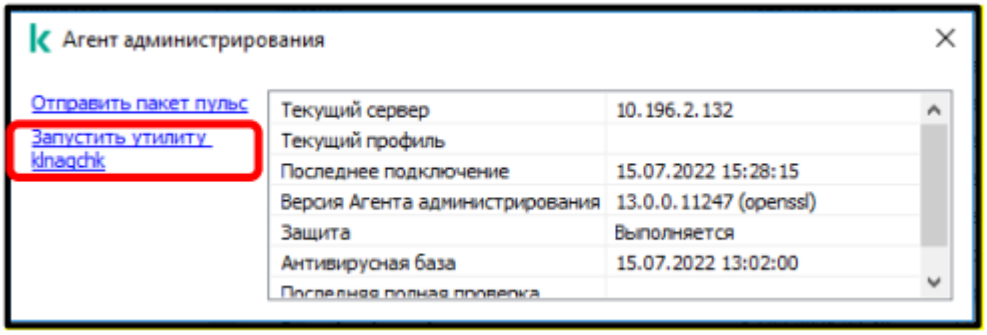

Рисунок Г.20. – Запуск утилиты «klnagchk»

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.).

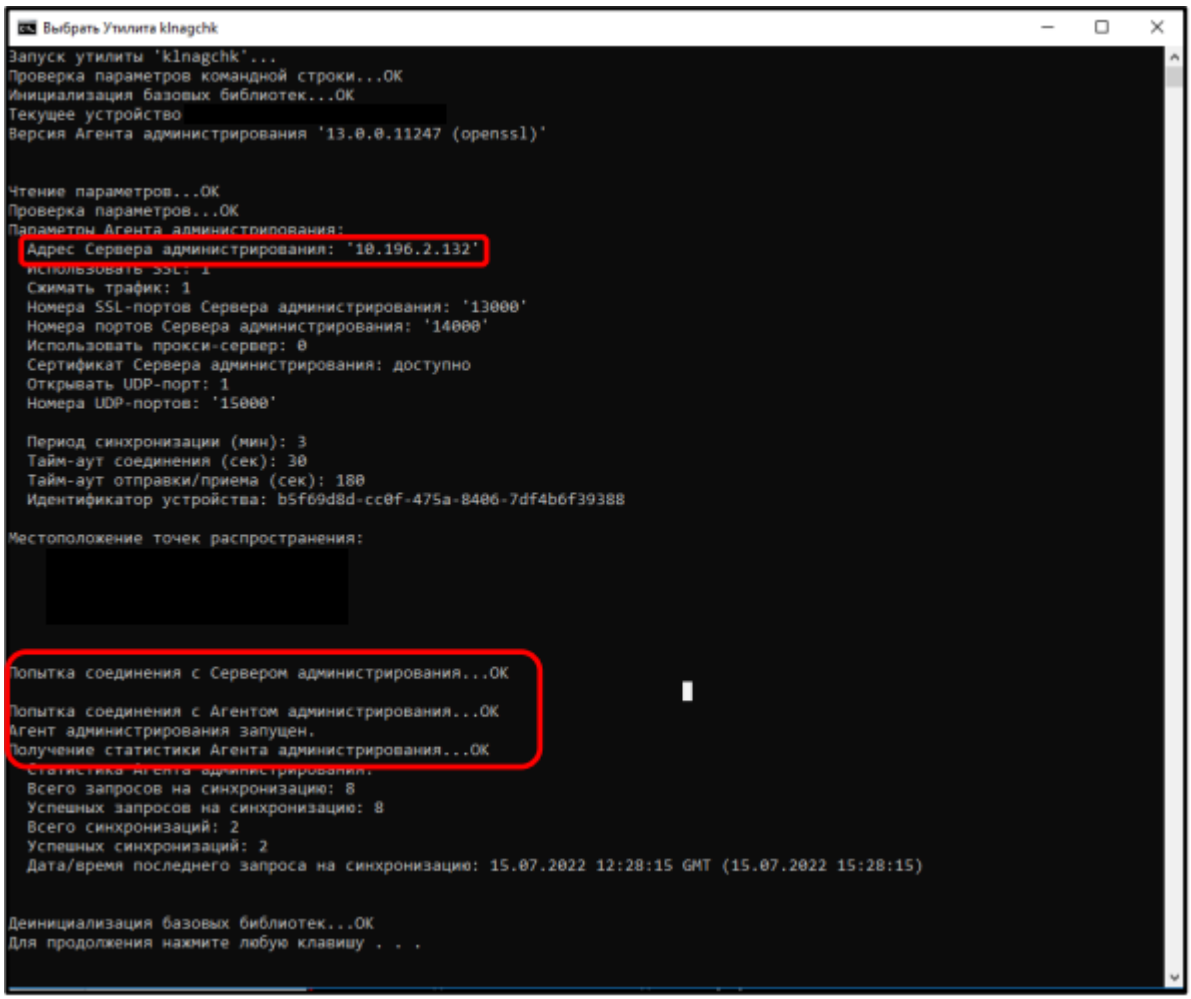

Рисунок Г.21. – Вывод утилиты «klnagchk.exe»

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.).

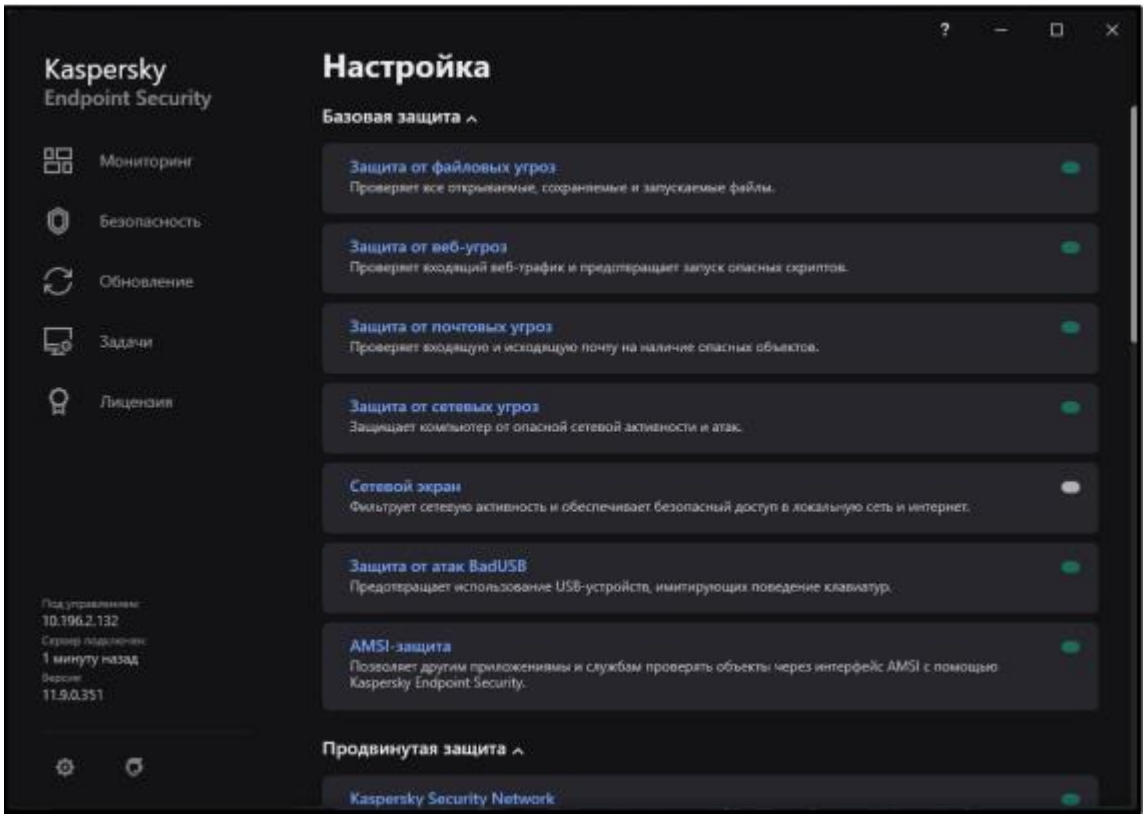

Рисунок Г.22. – Общий вид раздела настроек «Базовая защита»

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.);

3) далее в поле «Действие при обнаружении угрозы» выбрать пункт необходимый пункт и нажать кнопку «Расширенная настройка» (см. рисунок Г.23.);

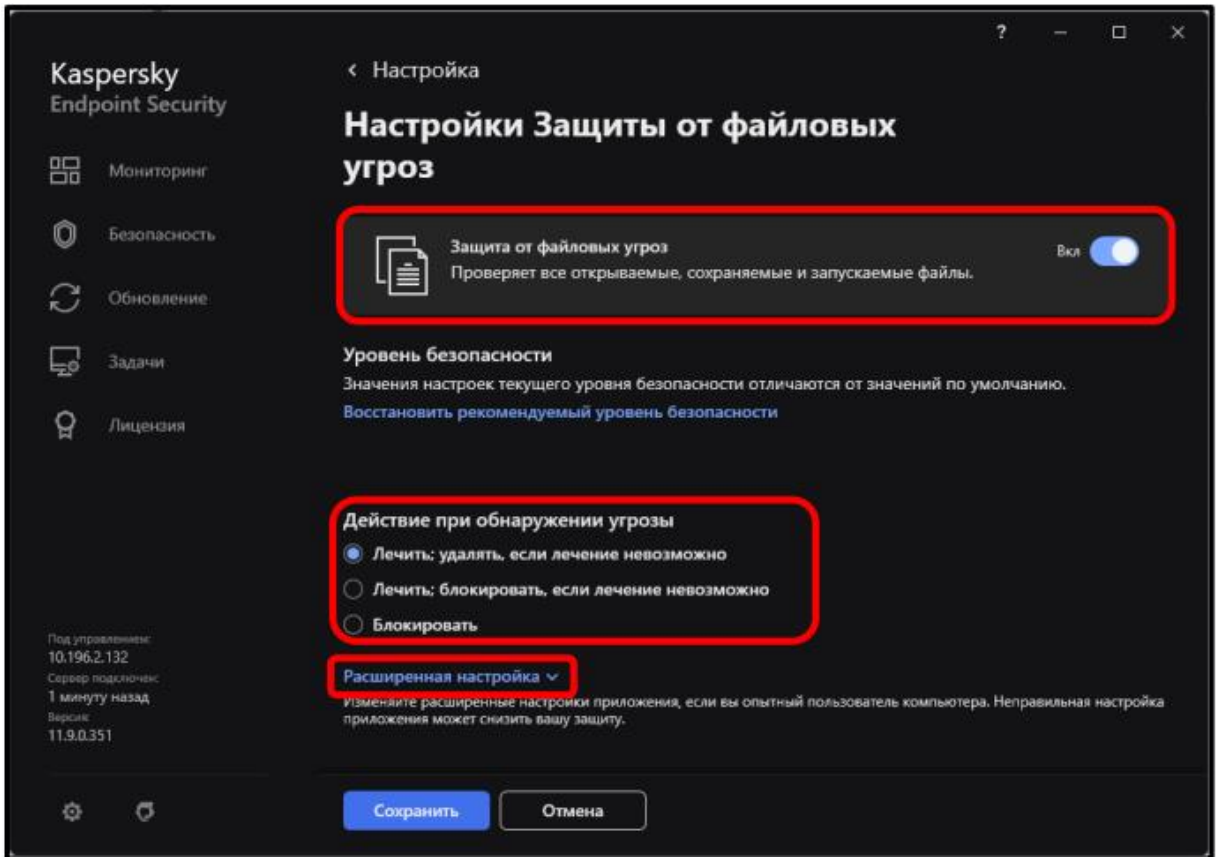

Рисунок Г.23. – Настройка компонента «Защита от файловых угроз»

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»;

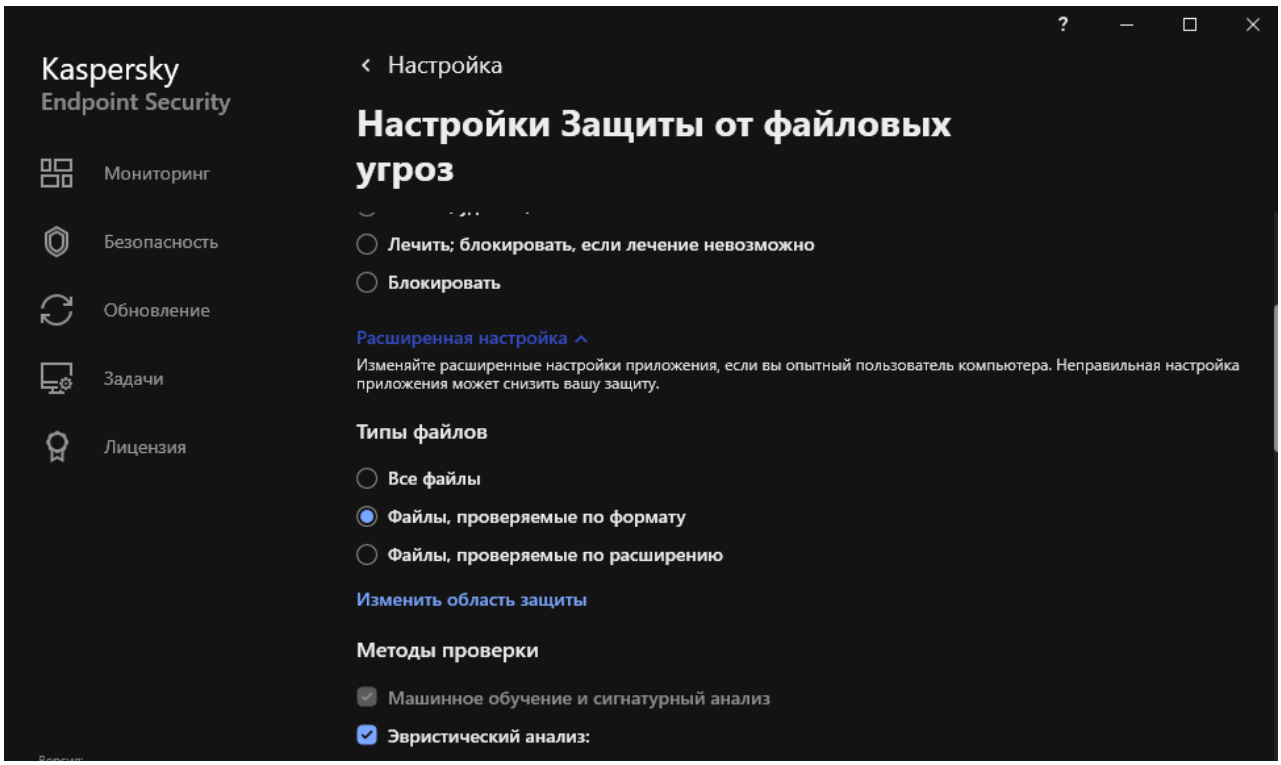

Рисунок Г.24. – Настройка компонента «Защита от файловых угроз»

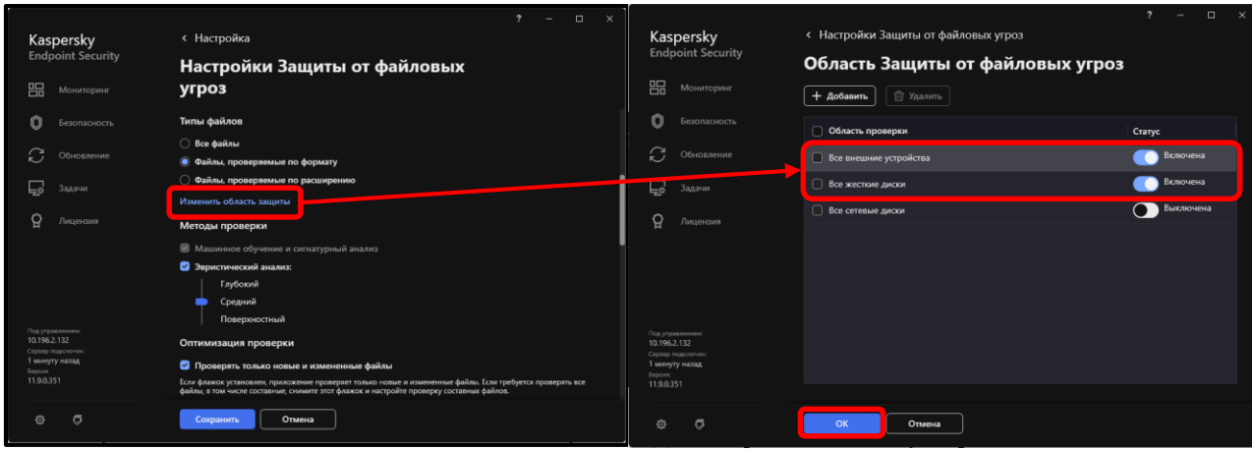

Рисунок Г.25. – Настройка области защиты

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.);

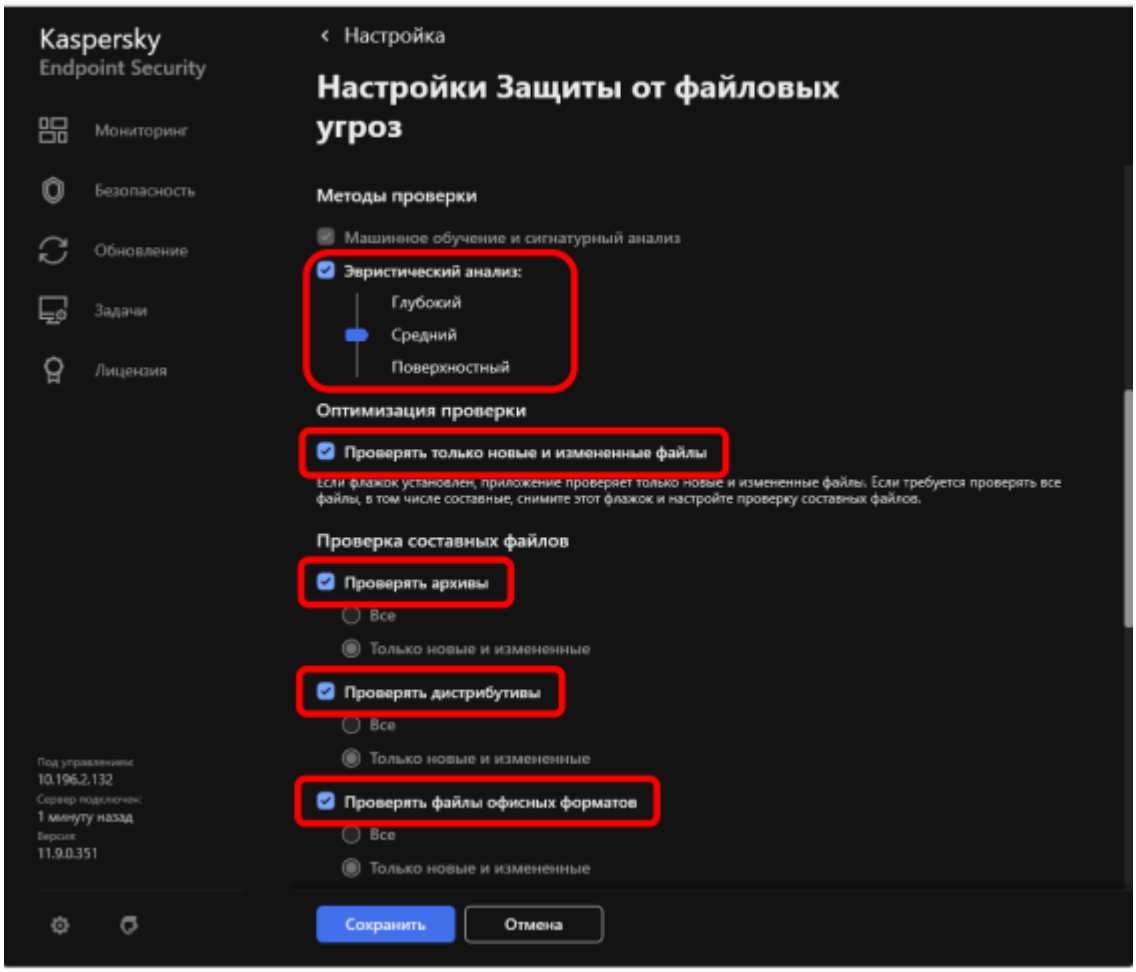

Рисунок Г.26. - Настройка компонента «Защита от файловых угроз»

6) выбрать пункт «Не распаковывать составные файлы большого размера», определить максимальный размер файла, выбрать пункт «Распаковывать составные файлы в фоновом режиме», определить минимальный размер файла, активировать «Технология iSwift» и «Технология «iChecker» в разделе «Технологии проверки» и нажать «Сохранить» (см. рисунок Г.27.);

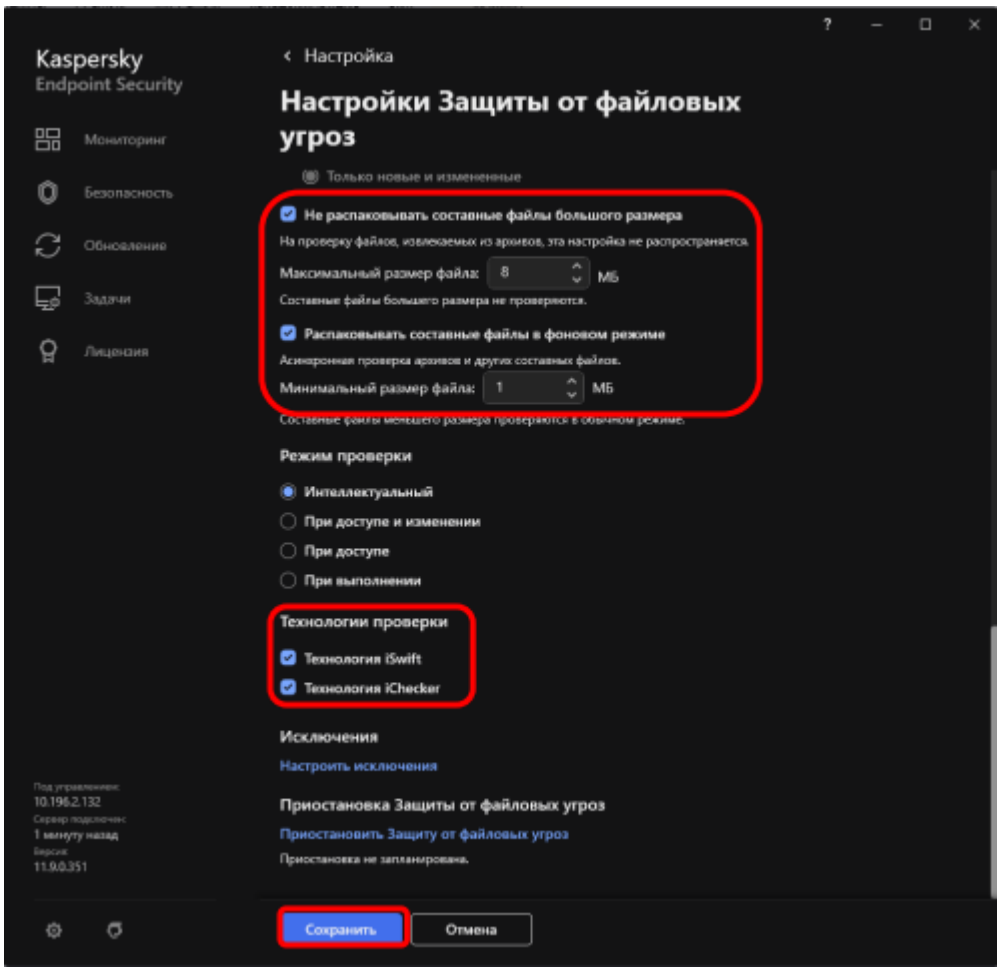

Рисунок Г.27. – Настройка проверки составных файлов

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.);

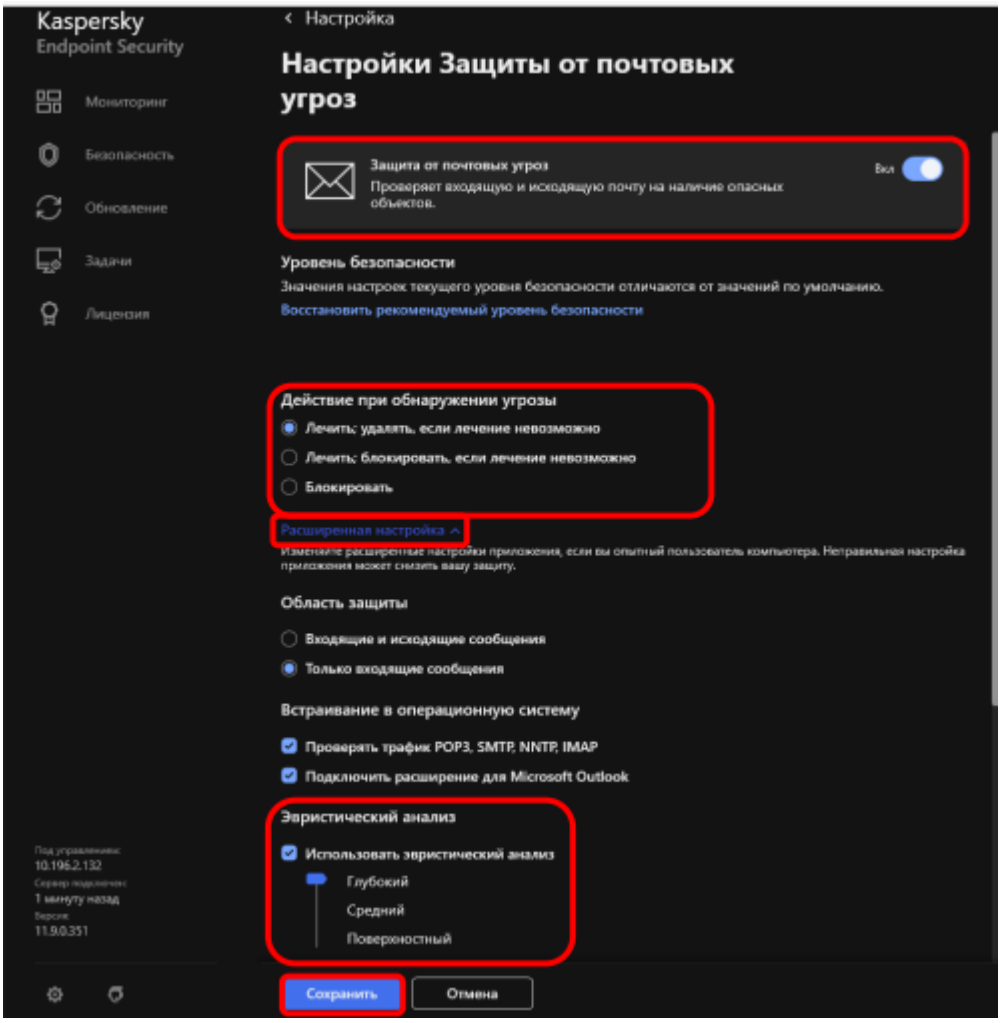

Рисунок Г.28. – Настройка компонента «Защита от почтовых угроз»

Компонент «Защита от веб-угроз»

Компонент «Защита от веб-угроз» предназначен для защиты информации, поступающей на средство ВТ по HTTP-протоколу, а также для предотвращения запуска на средстве ВТ опасных скриптов, полученных через браузер.

Защита от веб-угроз предусматривает контроль HTTP-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.);

2) в появившемся окне активировать «Защиту от веб-угроз» (см. рисунок Г.29.);

3) в поле «Действие при обнаружении угрозы» выбрать пункт «Запрещать загрузку» и нажать на кнопку «Расширенная настройка» (см. рисунок Г.29.);

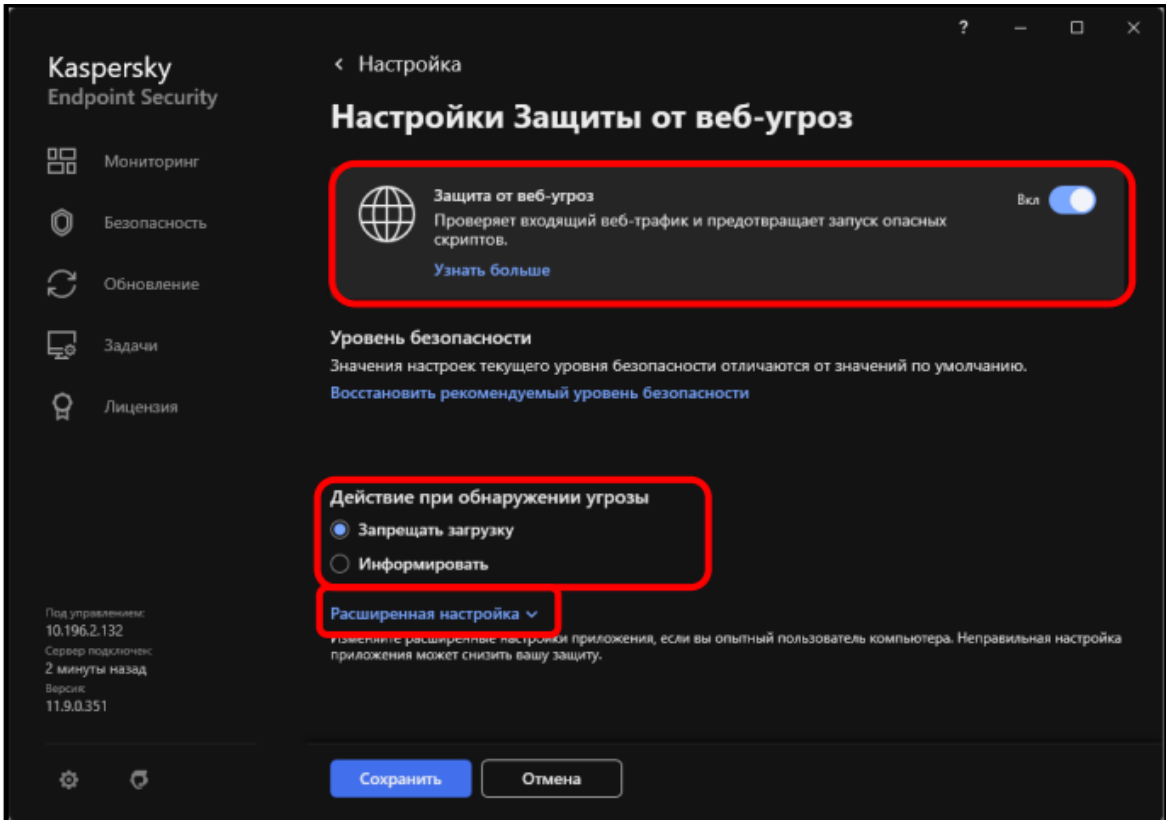

Рисунок Г.29. – Настройка компонента «Защита от веб-угроз»

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.

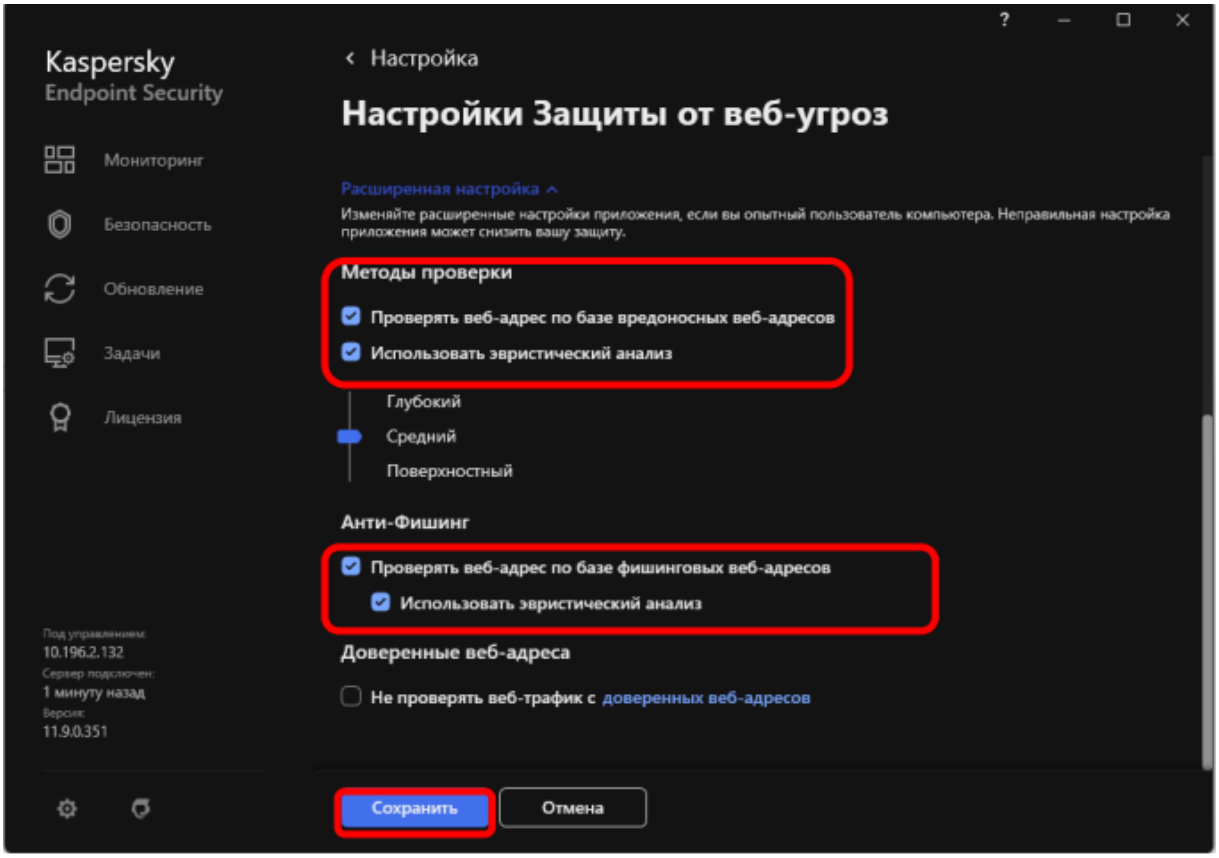

Рисунок Г.30. – Настройка компонента «Защита от веб-угроз»

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 «AMSI-защита» (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.).

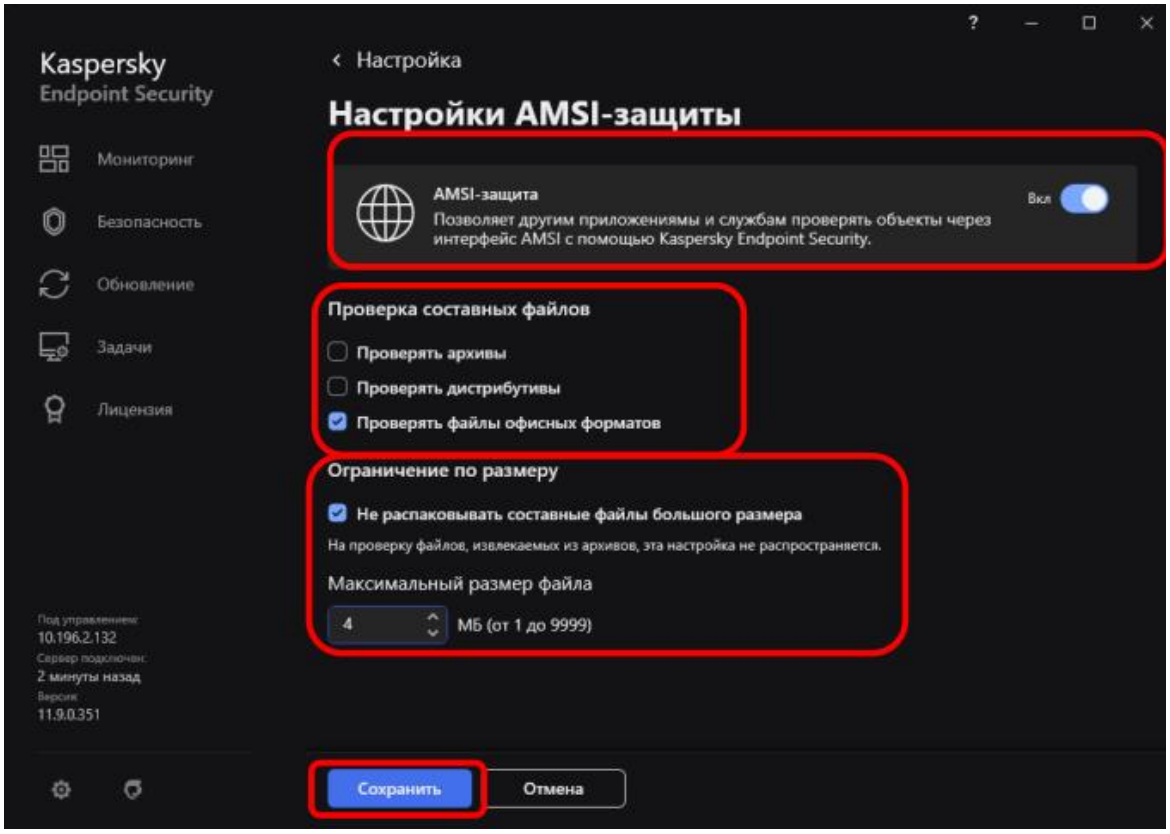

Рисунок Г.31. – Настройка компонента «AMSI-защита»

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.):

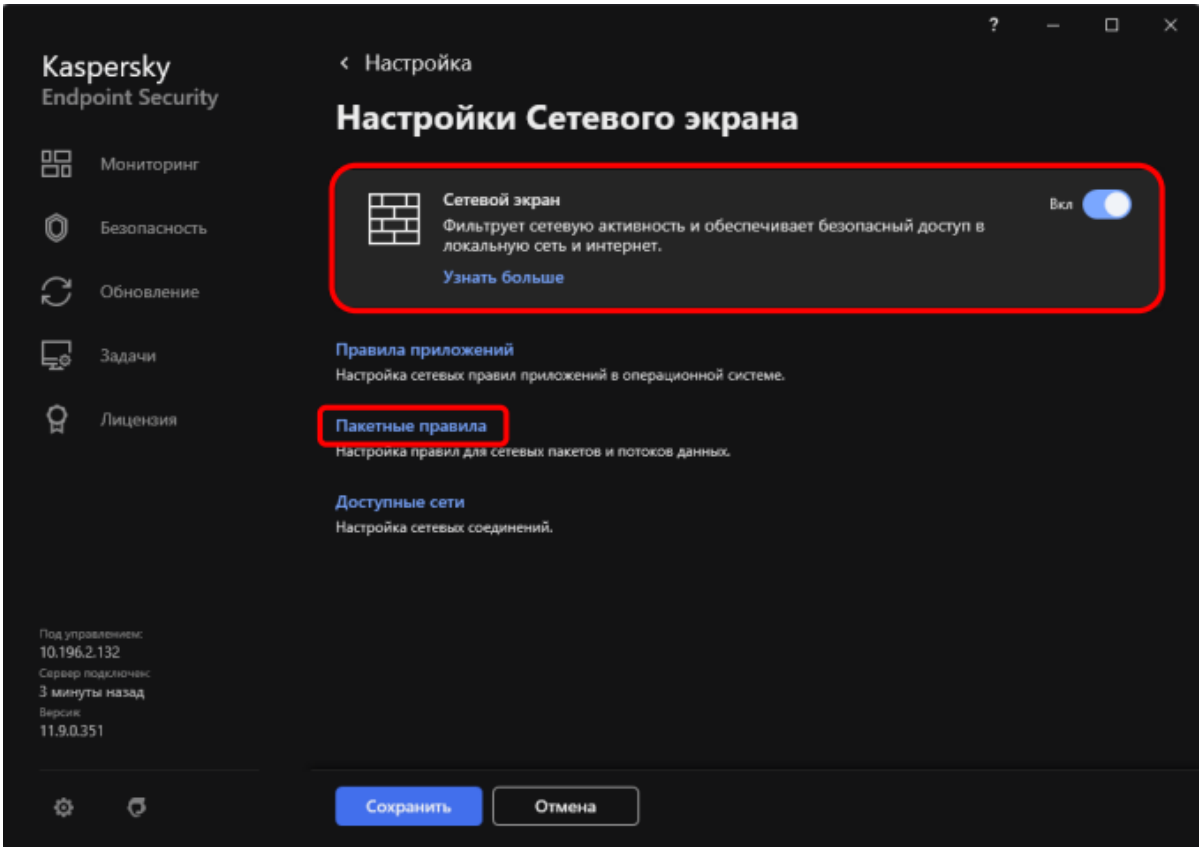

Рисунок Г.32. – Настройка компонента «Сетевой экран»

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.);

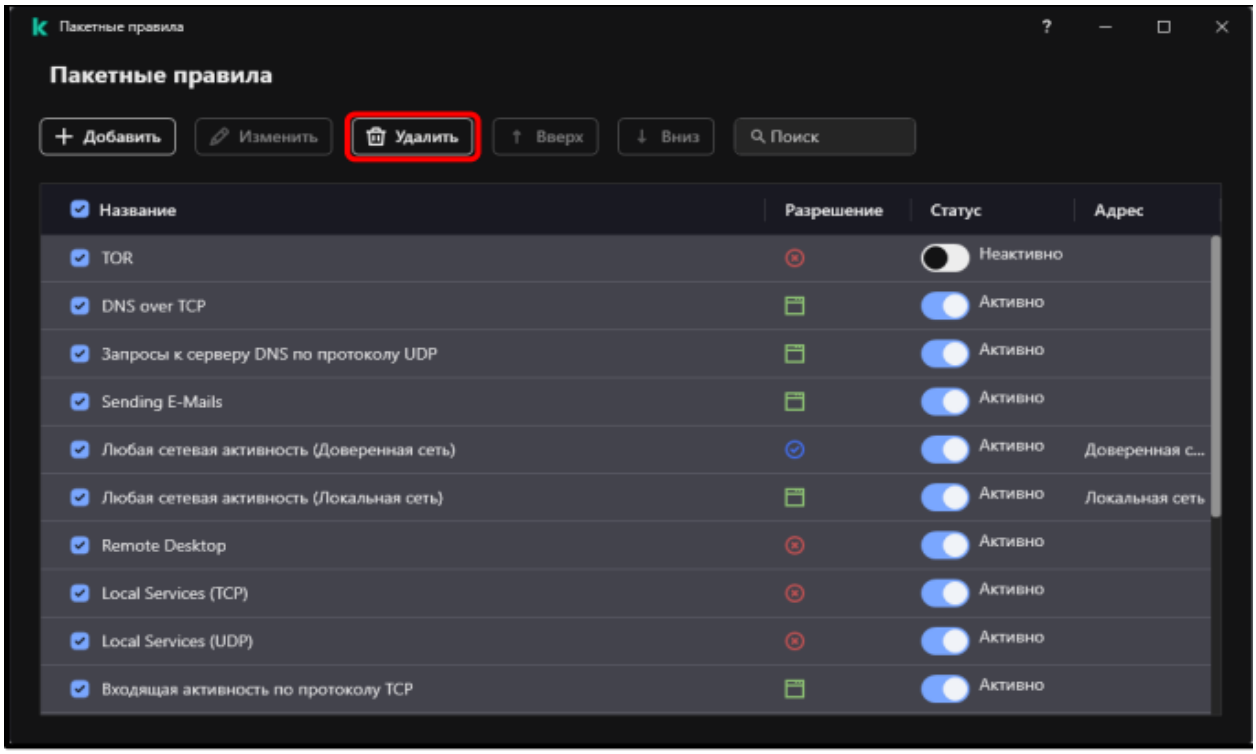

Рисунок Г.33. – Удаление пакетных правил

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.);

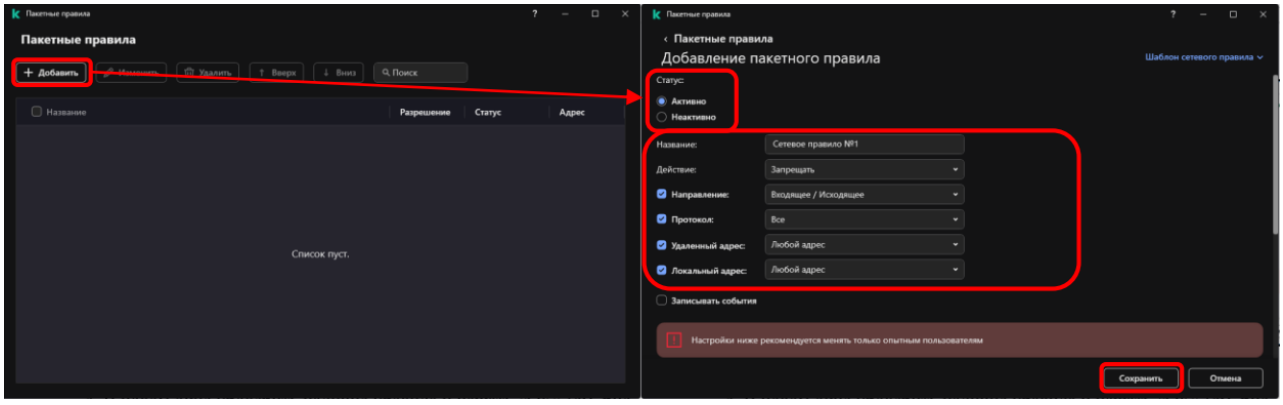

Рисунок Г.34. – Настройка сетевых пакетных правил

5) в новом окне проверить наличие правила и нажать «Закрыть» (см. рисунок Г.35.).

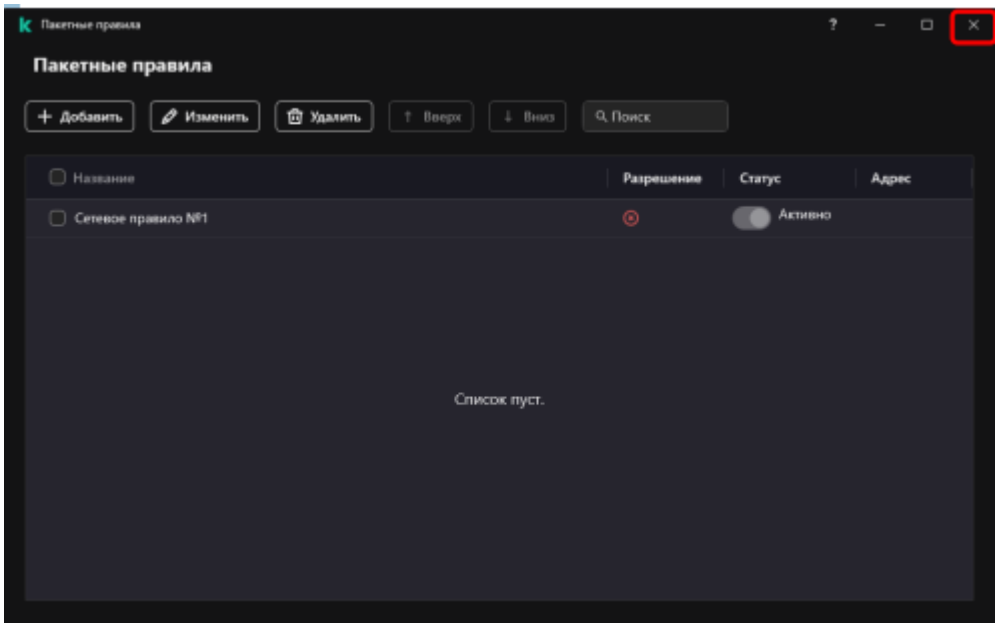

Рисунок Г.35.– Результат создания правила, запрещающего любую сетевую

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 MAC-спуфинга», выбрать пункт «Только уведомлять» в разделе «При обнаружении атаки MAC-спуфинг» и нажать кнопку «Сохранить» (см. рисунок Г.36.).

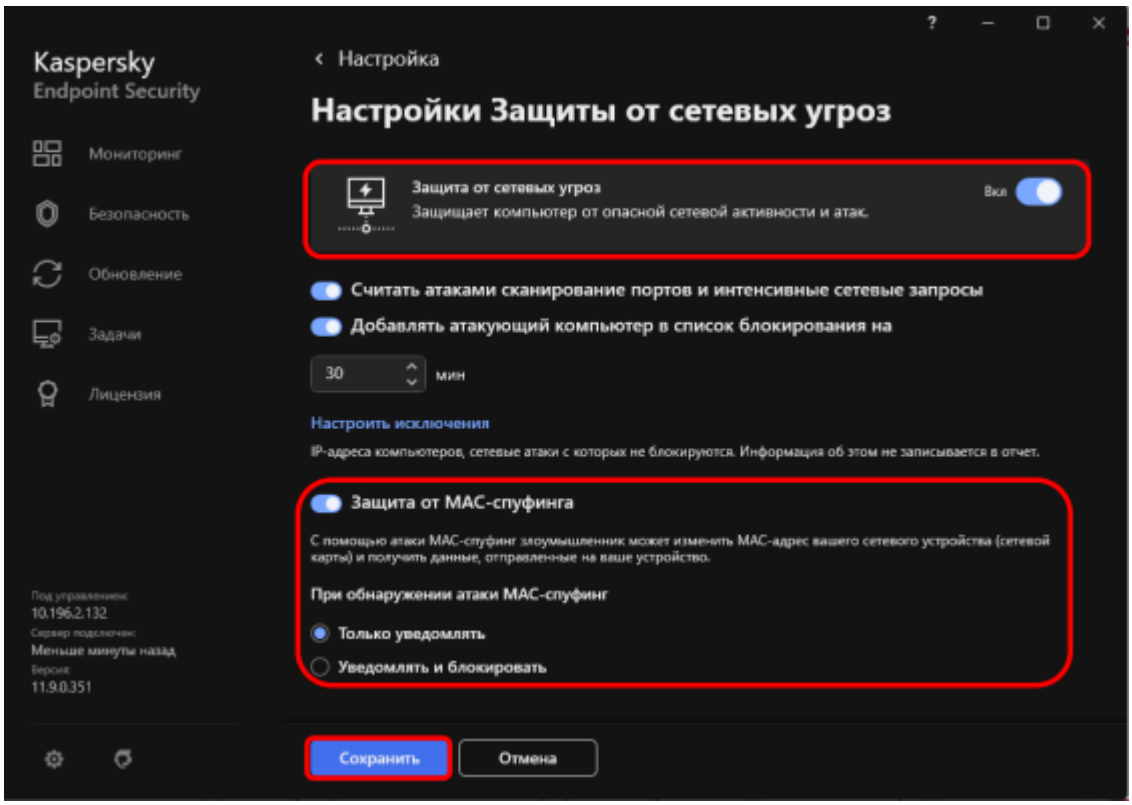

Рисунок Г.36. – Настройка компонента «Защита от сетевых угроз»

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 USB-устройств» в разделе «Авторизация USB-устройств при подключении» (см. рисунок Г.37.);

3) в поле «Максимальное количество попыток авторизации USB-устройства» указать необходимое значение, и в поле «Таймаут при достижении максимального количества попыток» указать требуемое значение (см. рисунок Г.37.).

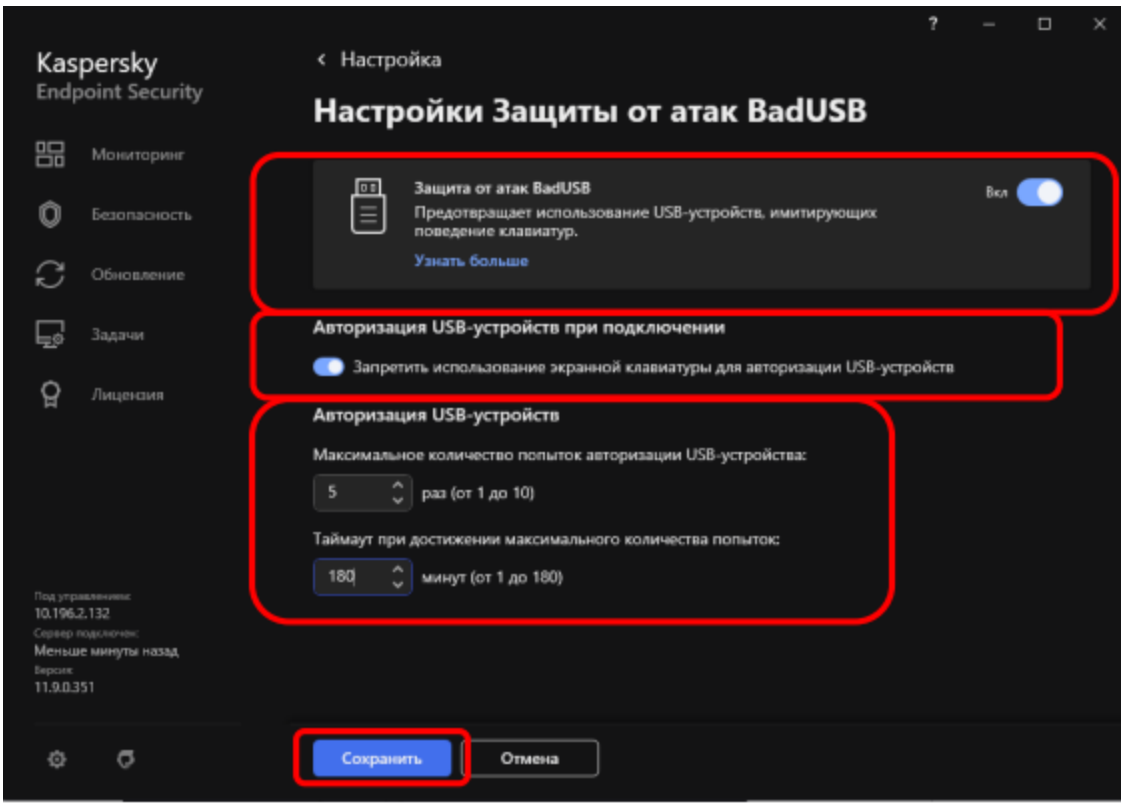

Рисунок Г.37. – Настройка компонента «Защита от атак BadUSB»

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.).

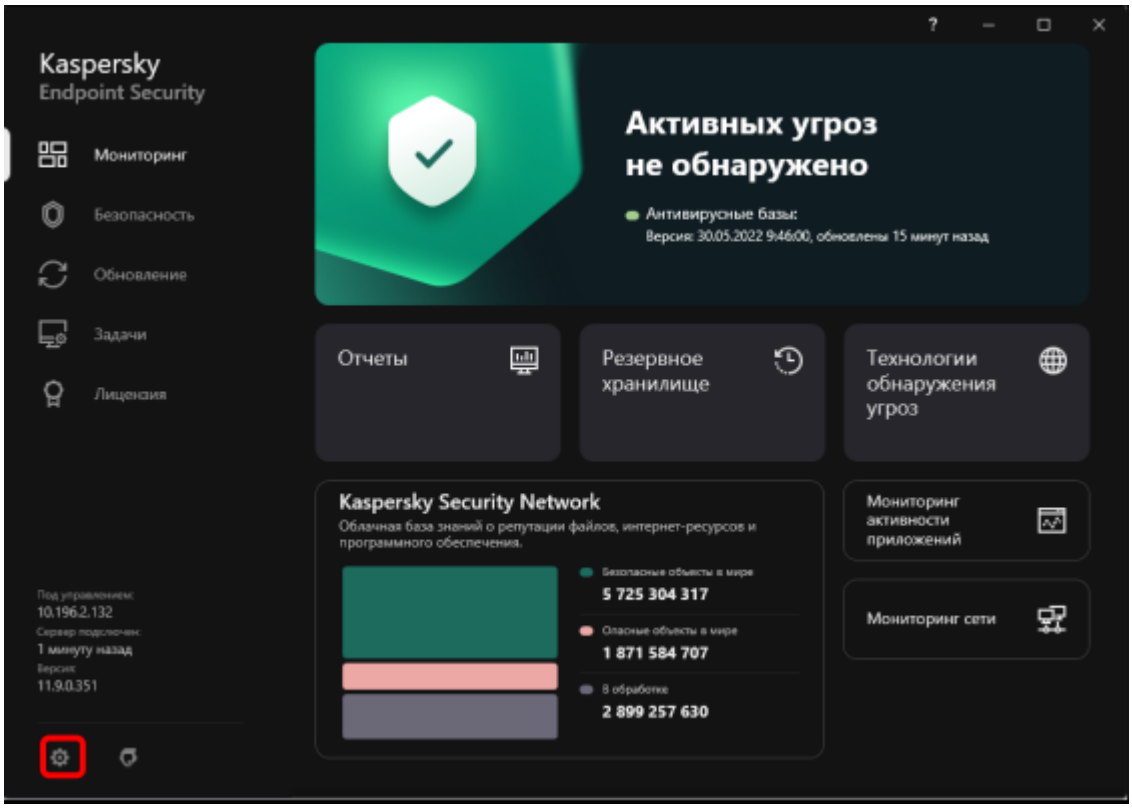

Рисунок Г.38. – Главное окно «Kaspersky Endpoint Security 11 для Windows»

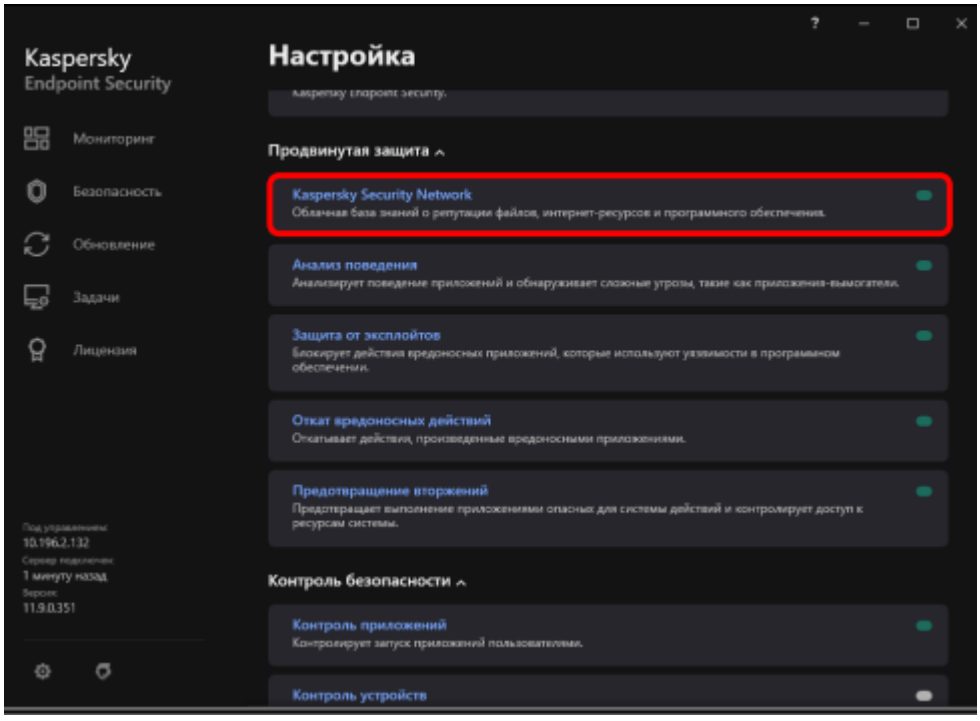

Рисунок Г.39. – Общий вид раздела настроек «Продвинутая защита»

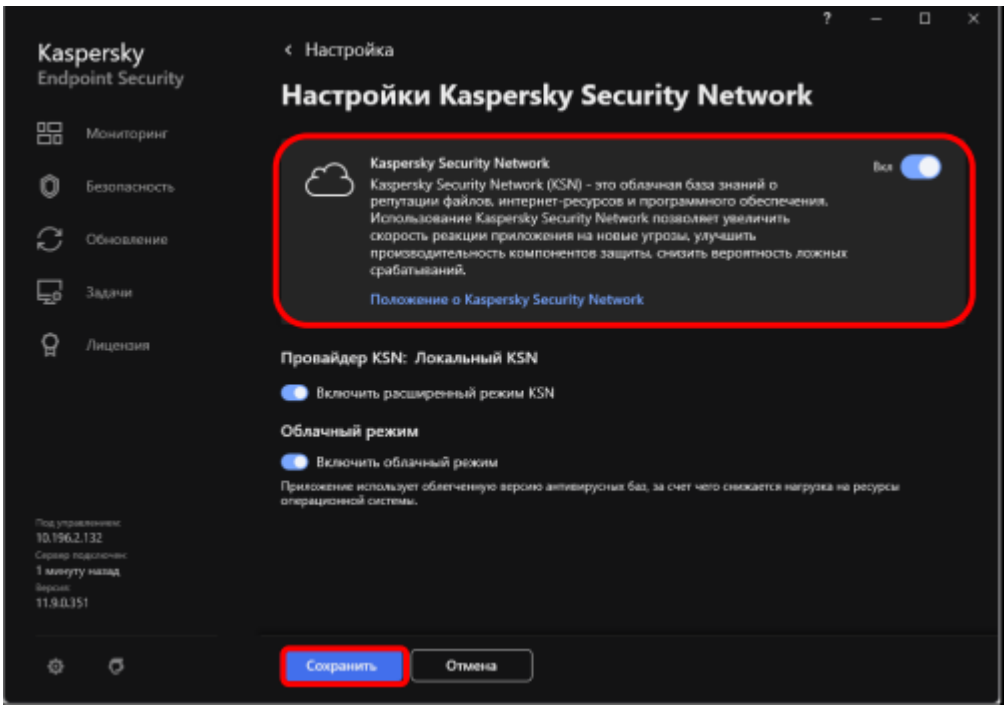

Рисунок Г.40. – Компонент «Kaspersky Security Network»

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.).

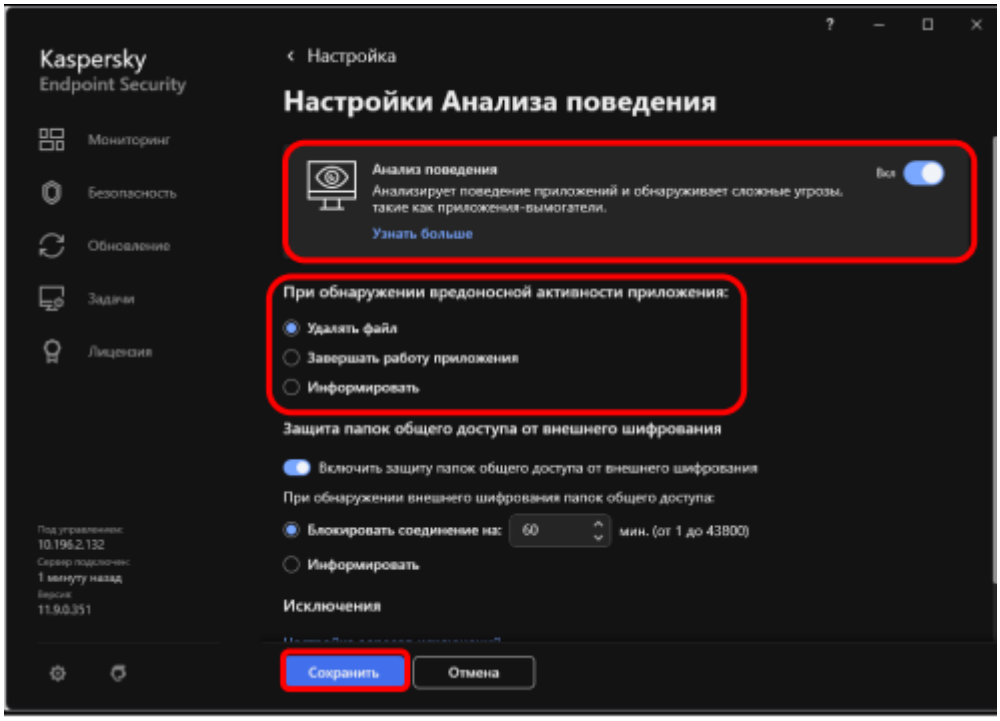

Рисунок Г.41. – Настройка компонента «Анализ поведения»

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.).

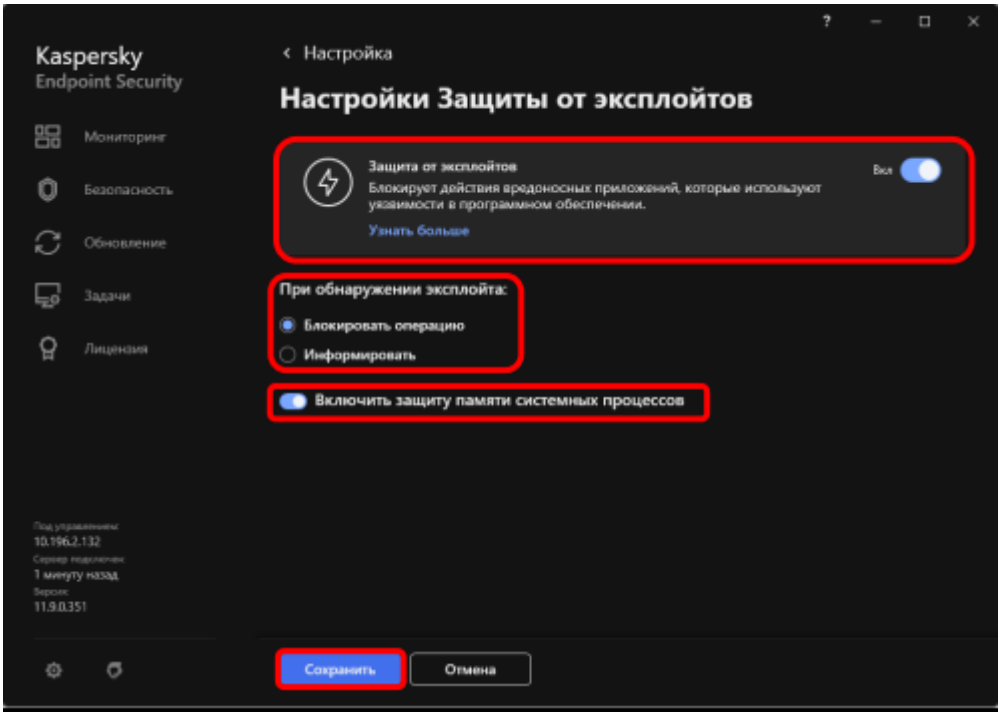

Рисунок Г.42. – Настройка компонента «Защита от эксплойтов»

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.).

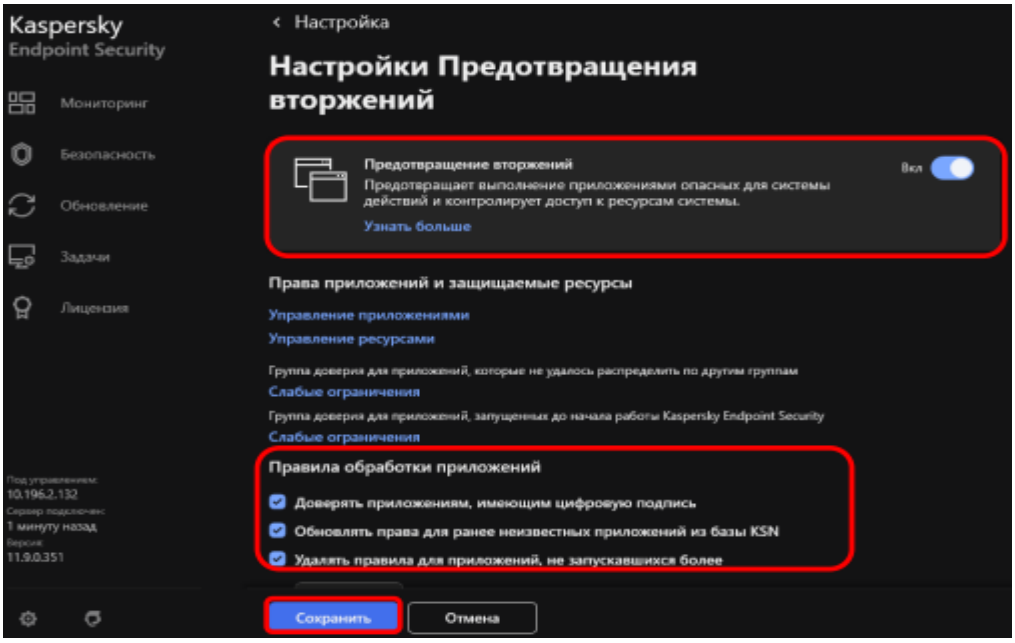

Рисунок Г.43. – Настройка компонента «Предотвращение вторжений»

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.).

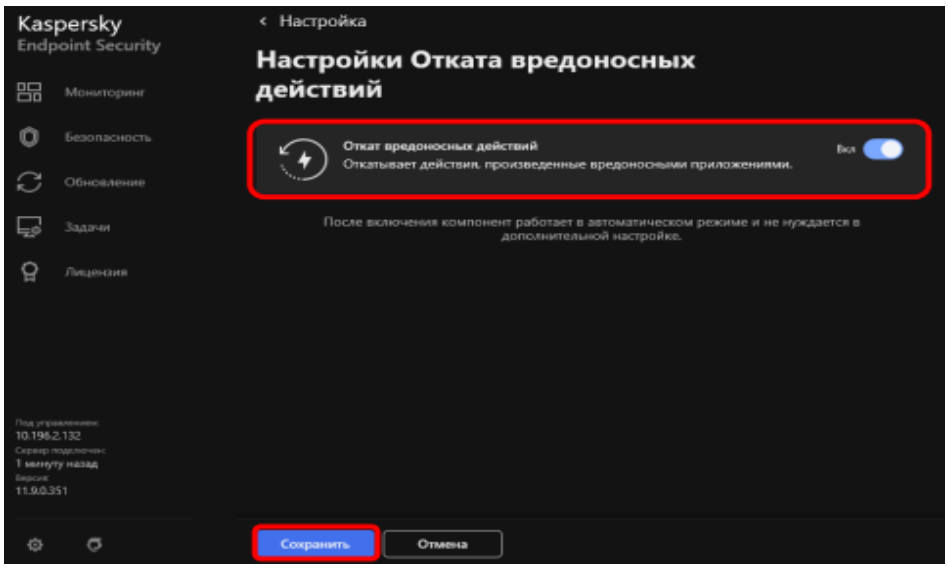

Рисунок Г.44. – Настройка компонента «Откат вредоносных воздействий»

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.).

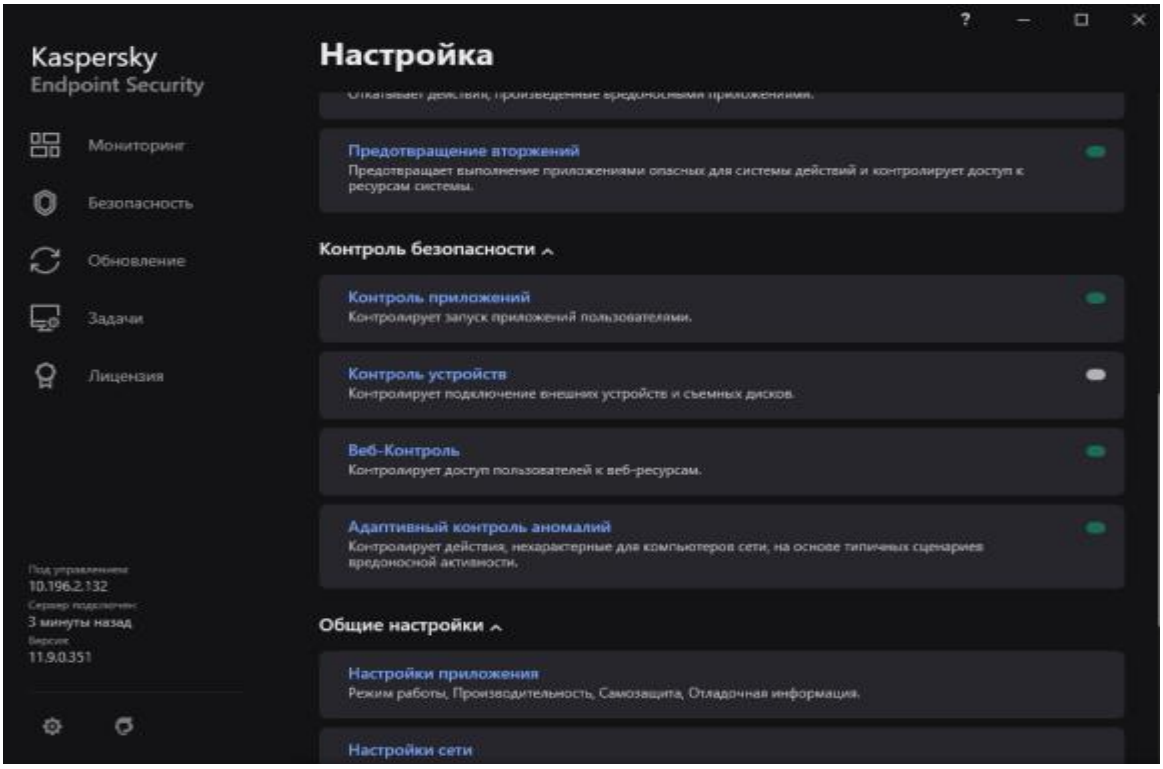

Рисунок Г.45. – Меню настроек «Контроль безопасности»

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).

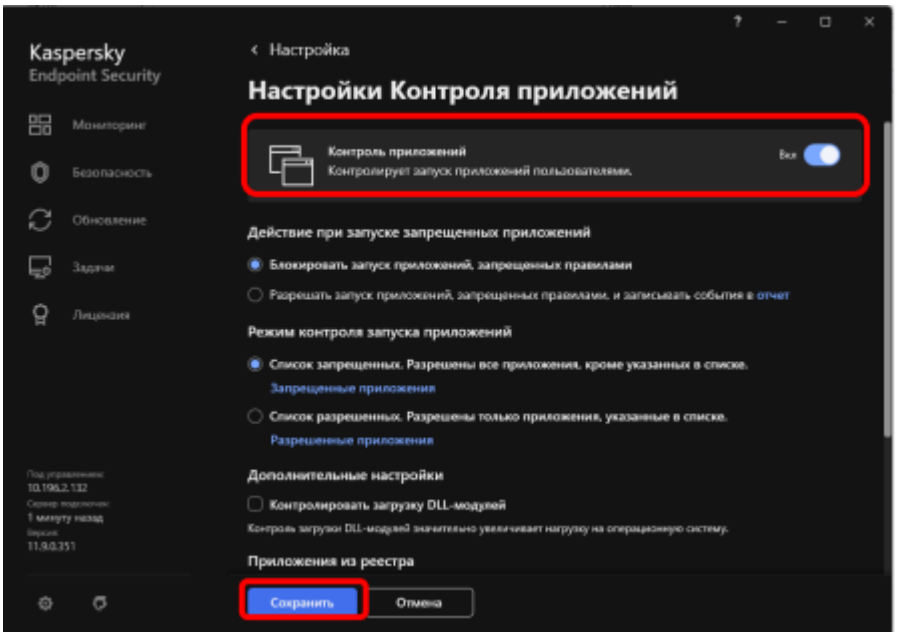

Рисунок Г.46. – Настройка компонента «Контроль приложений»

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;

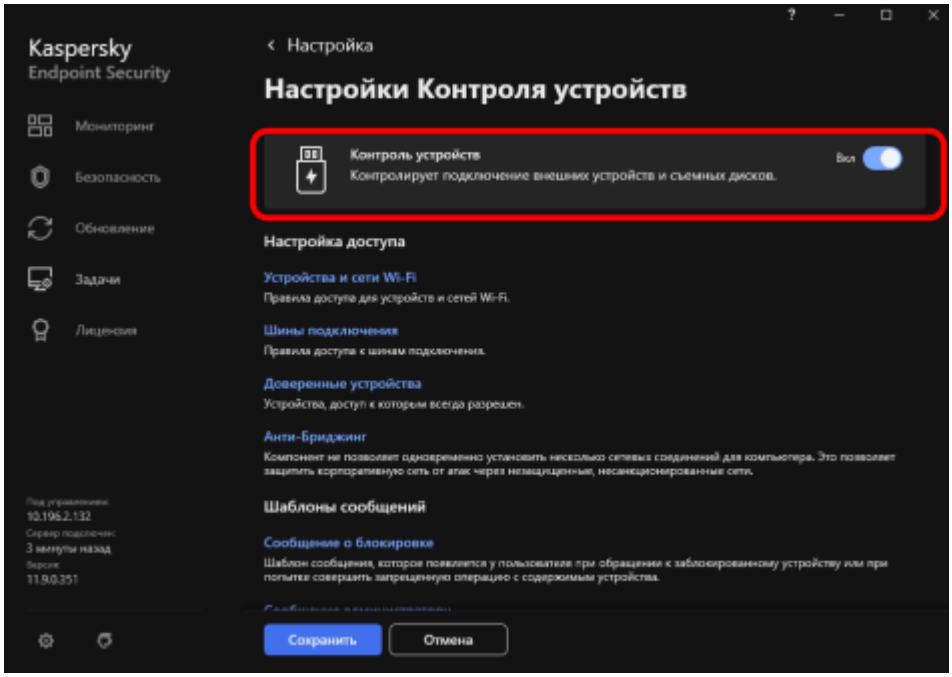

Рисунок Г.47. – Настройка компонента «Контроль устройств»

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»;

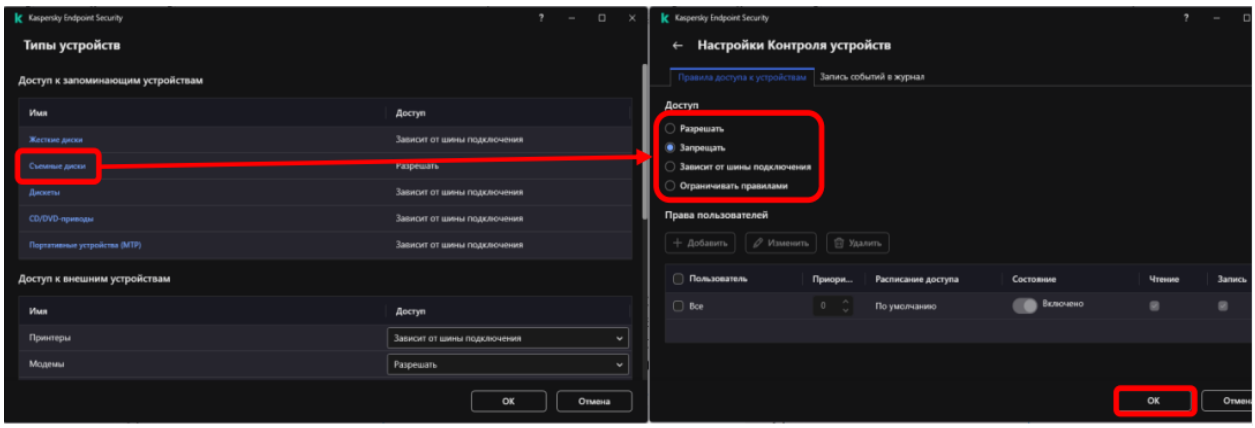

Рисунок Г.48. – Запрет использования устройств

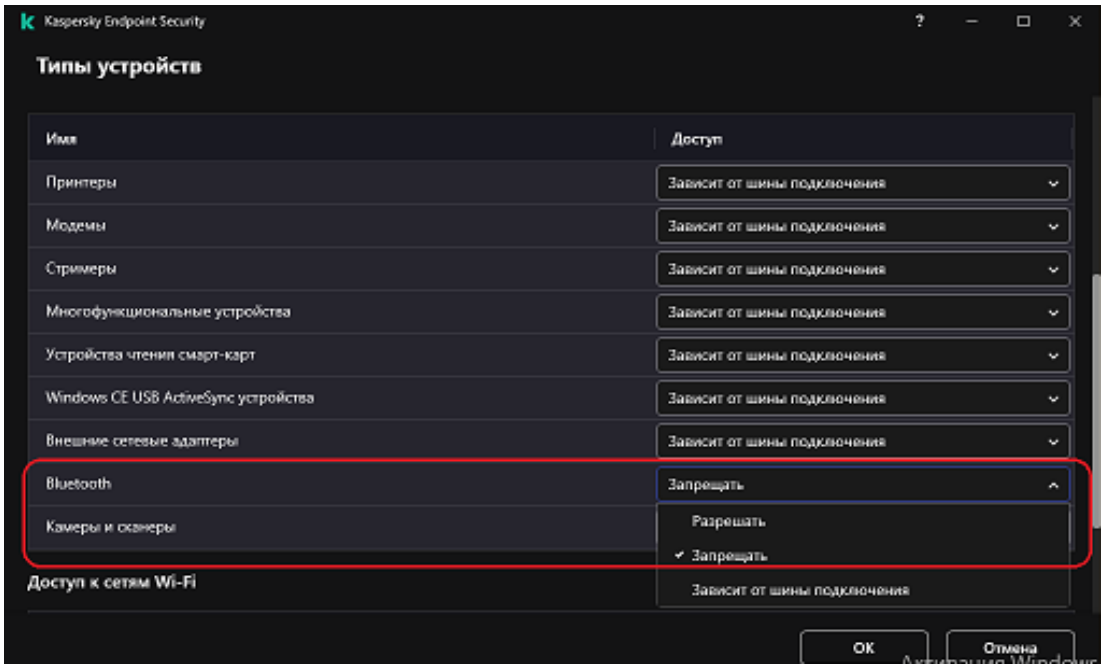

Рисунок Г.49. – Запрет использования устройств

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.);

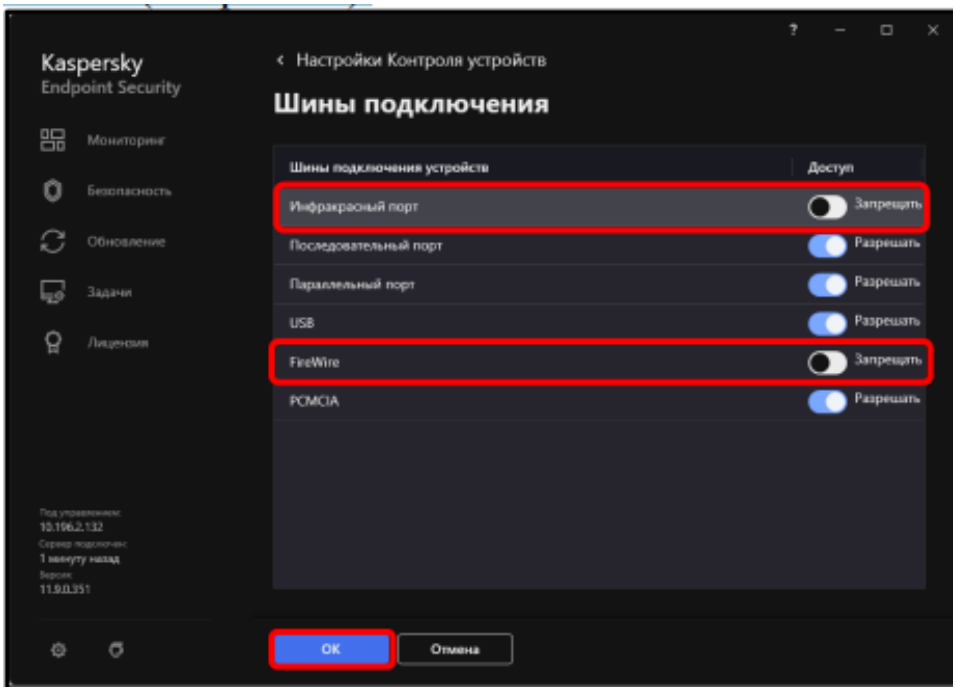

Рисунок Г.50. – Запрет использования шин «Инфракрасный порт» и «FireWire»

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.

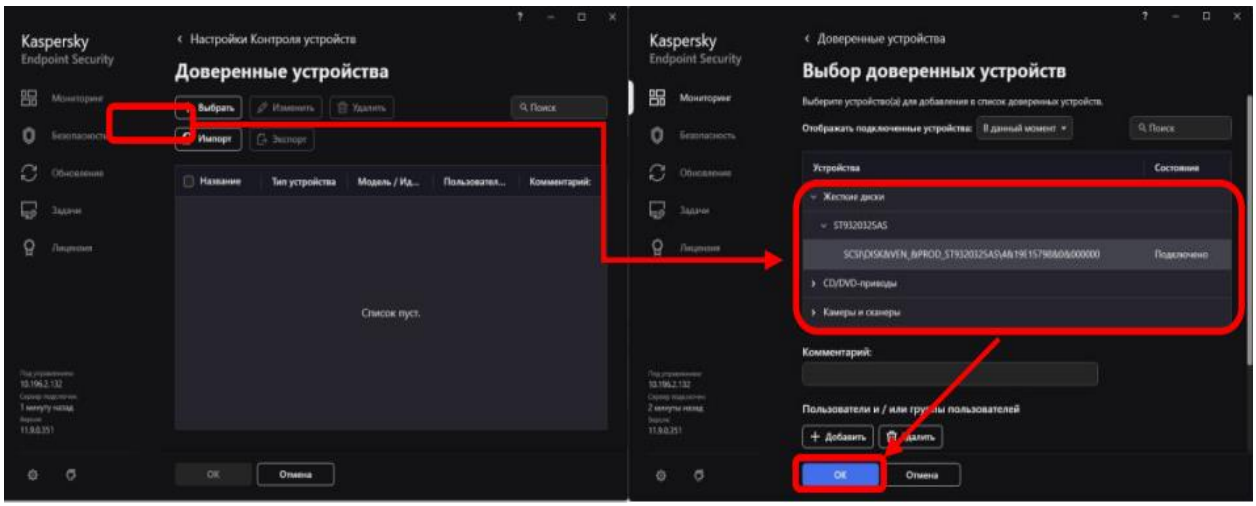

Рисунок Г.51. – Выбор доверенных устройств

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 «Веб-контроль» (см. рисунки Г.45. и Г.52.);

2) в появившемся окне активировать «Веб-Контроль» и нажать кнопку «Сохранить» (см рисунок Г.52.).

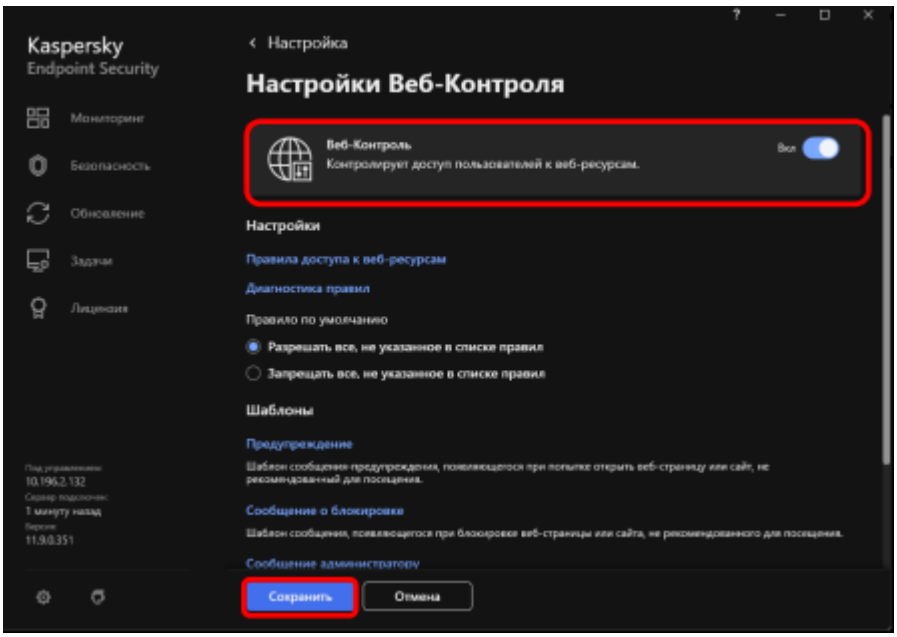

Рисунок Г.52. – Настройка компонента «Веб-контроль»

При необходимости настройки блокировки веб-ресурсов выполняются следующие шаги:

1) в разделе настроек «Контроль безопасности» выбрать меню «Веб-контроль» (см. рисунки Г.45. и Г.52.);

2) перейти в меню «Правила доступа к веб-ресурсам» (см. рисунок Г.53.);

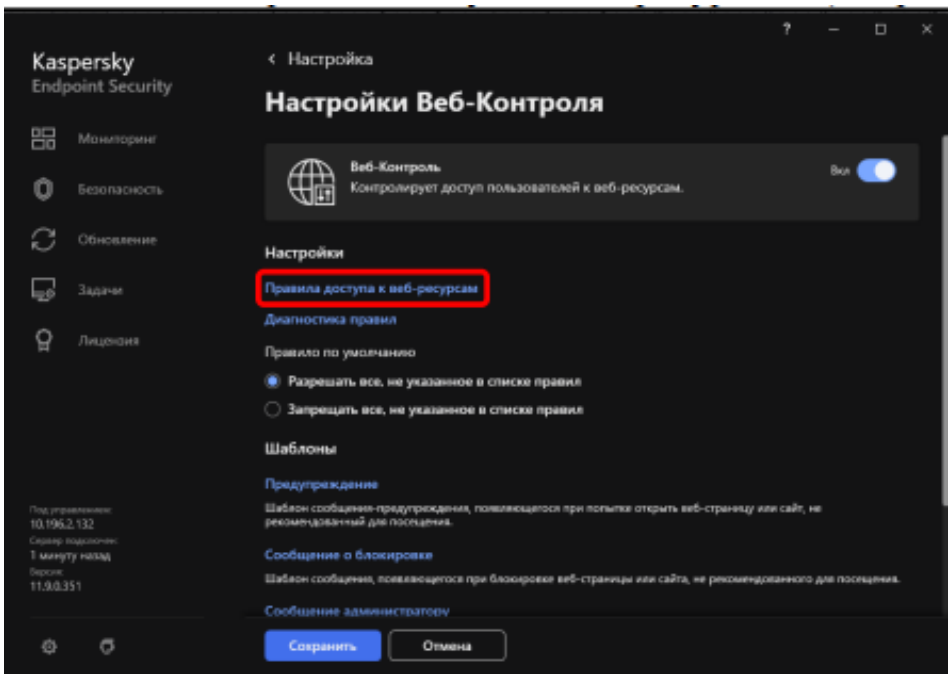

Рисунок Г.53. – Настройка правил доступа к веб-ресурсам

3) в открывшемся меню добавить новое правило, для этого нажать на кнопку «Добавить» (см. рисунок Г.54.);

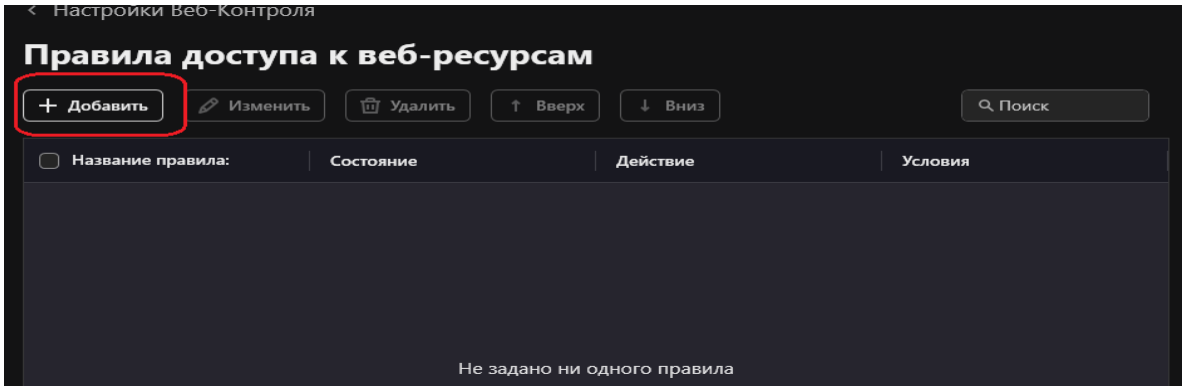

Рисунок Г.54. – Добавление нового правила доступа к веб-ресурсам

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.);

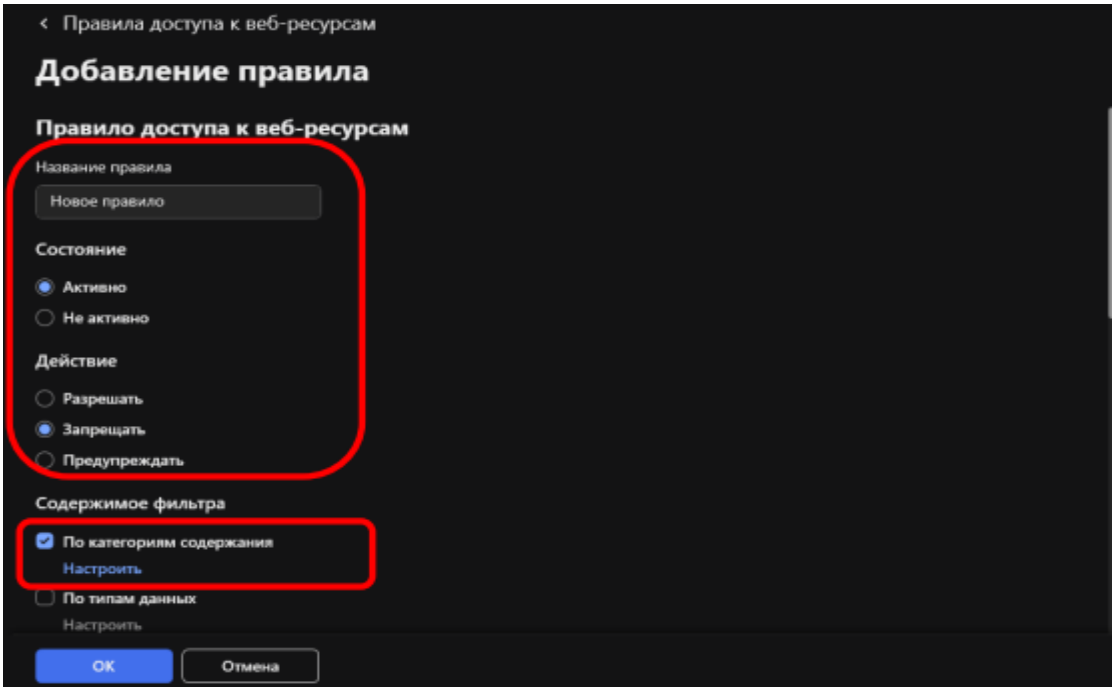

Рисунок Г.55. – Настройка правил доступа к веб-ресурсам

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.).

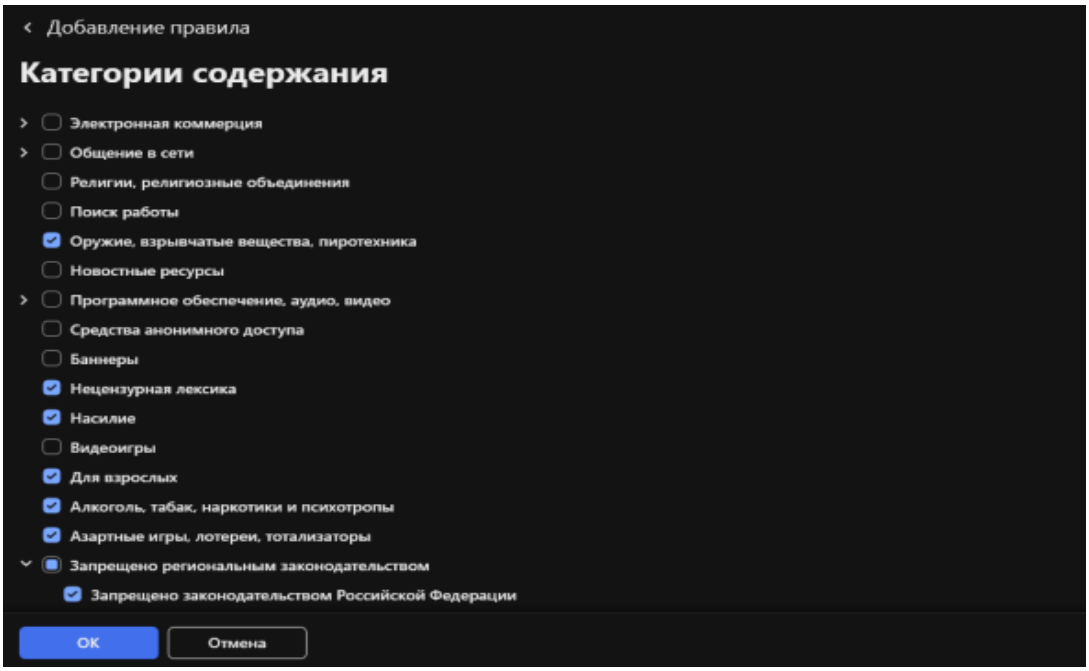

Рисунок Г.56. – Настройка категорий содержания

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.).

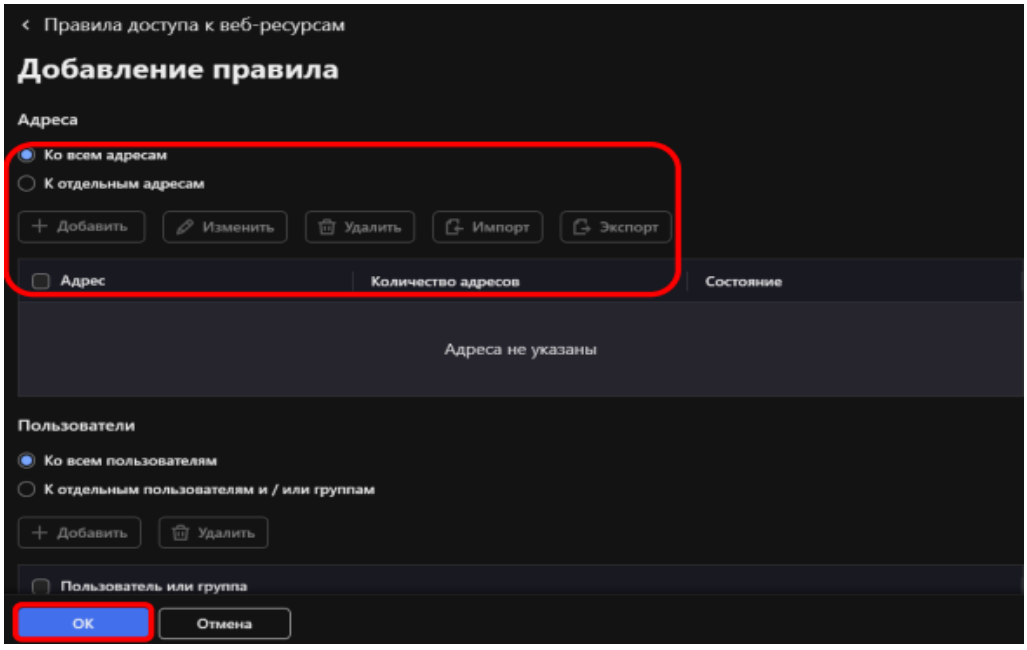

Рисунок Г.57. – Настройка категорий содержания

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.);

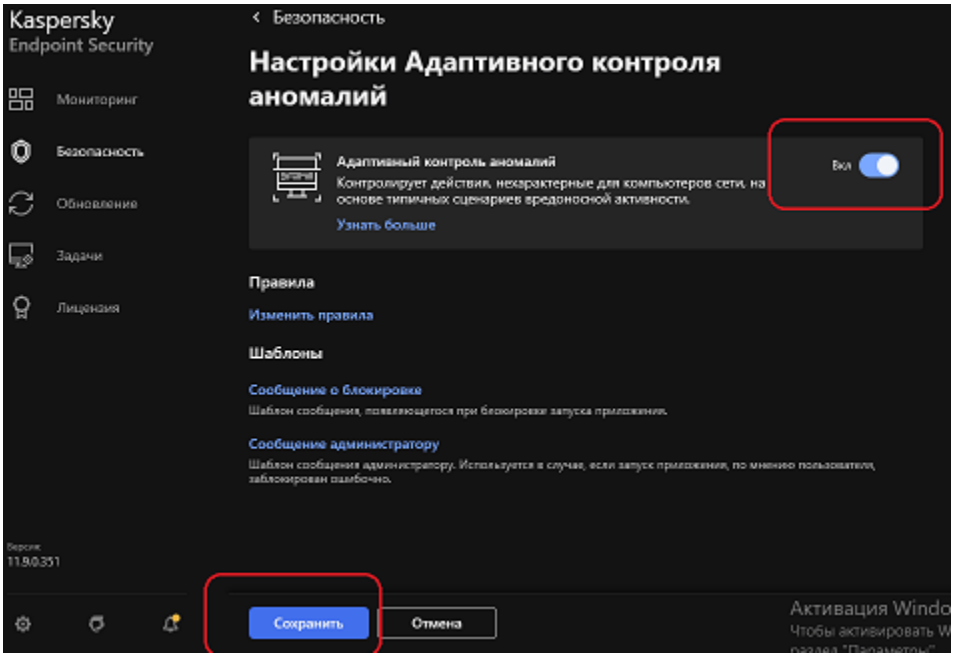

Рисунок Г.58. – Настройка компонента «Веб-контроль»

В разделе «Настройки Адаптивного контроля аномалий» нажать изменить правила. Установить чекбоксы около существующих правил, нажать «ОК»(см. рисунки Г.59. и Г.60.).

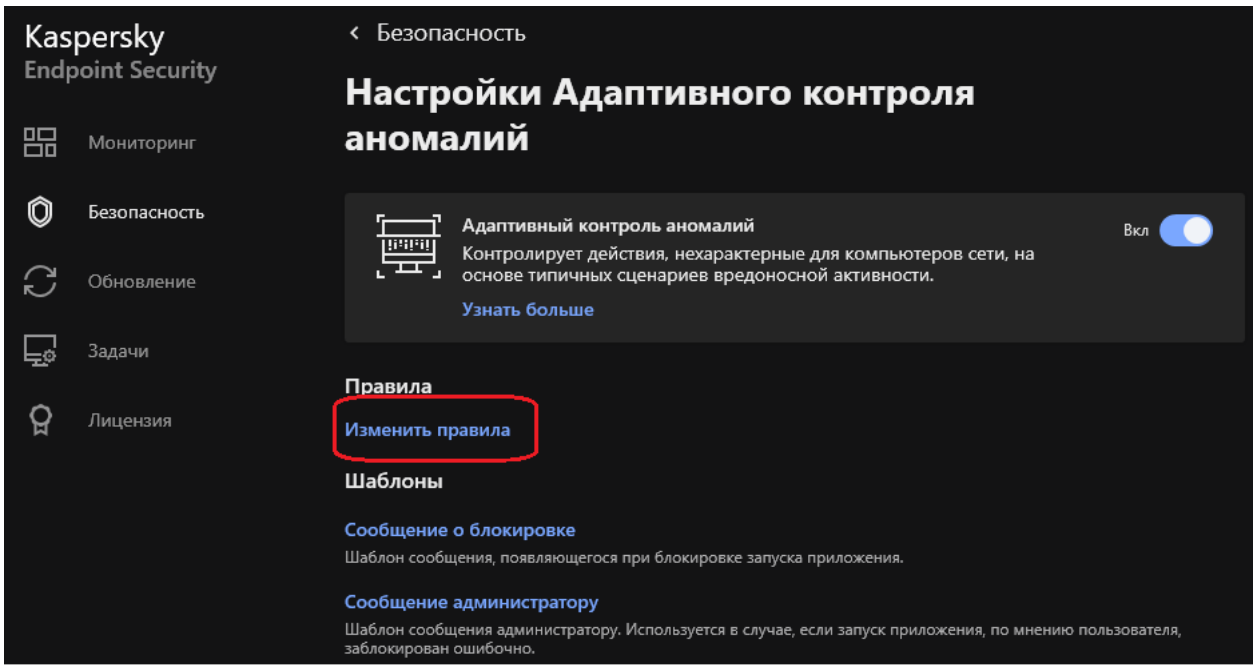

Рисунок Г.59. – Изменение правил адаптивного контроля аномалий

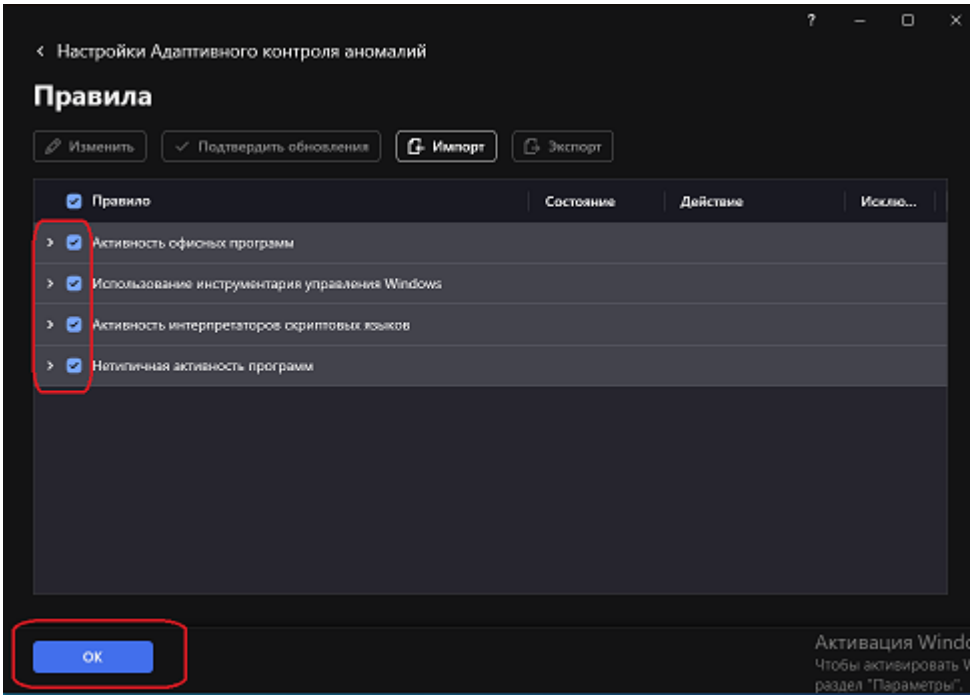

Рисунок Г.60. – Установка правил адаптивного контроля

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.).

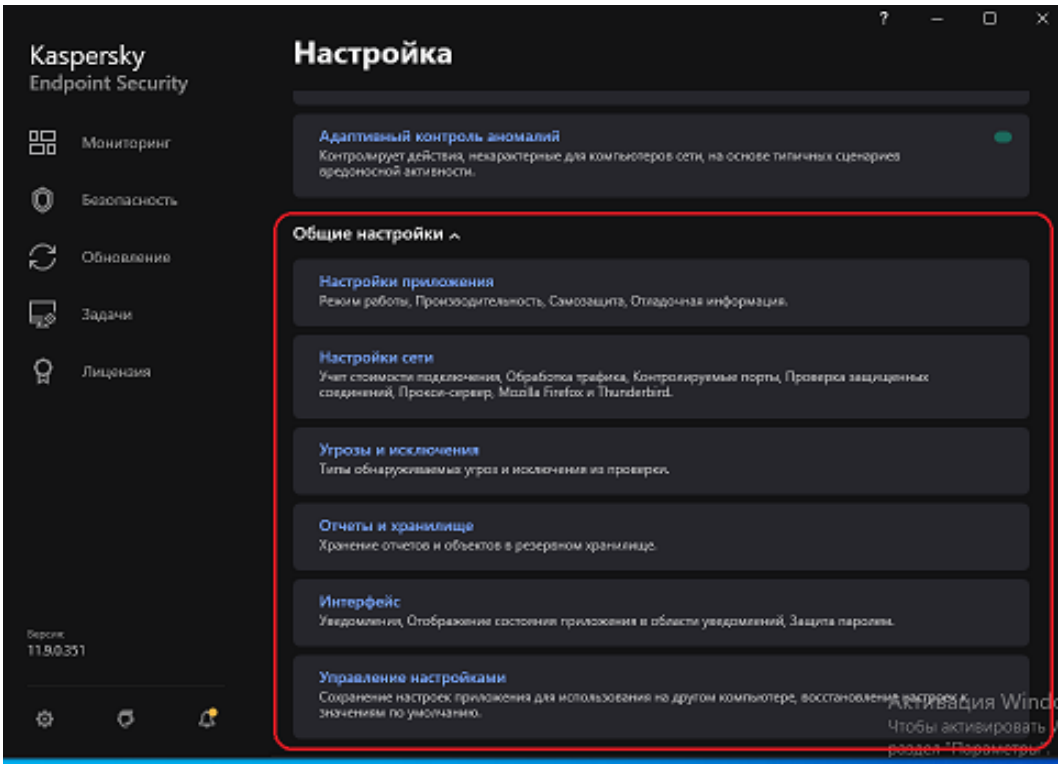

Рисунок Г.61. – Меню настроек «Общие настройки»

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.);

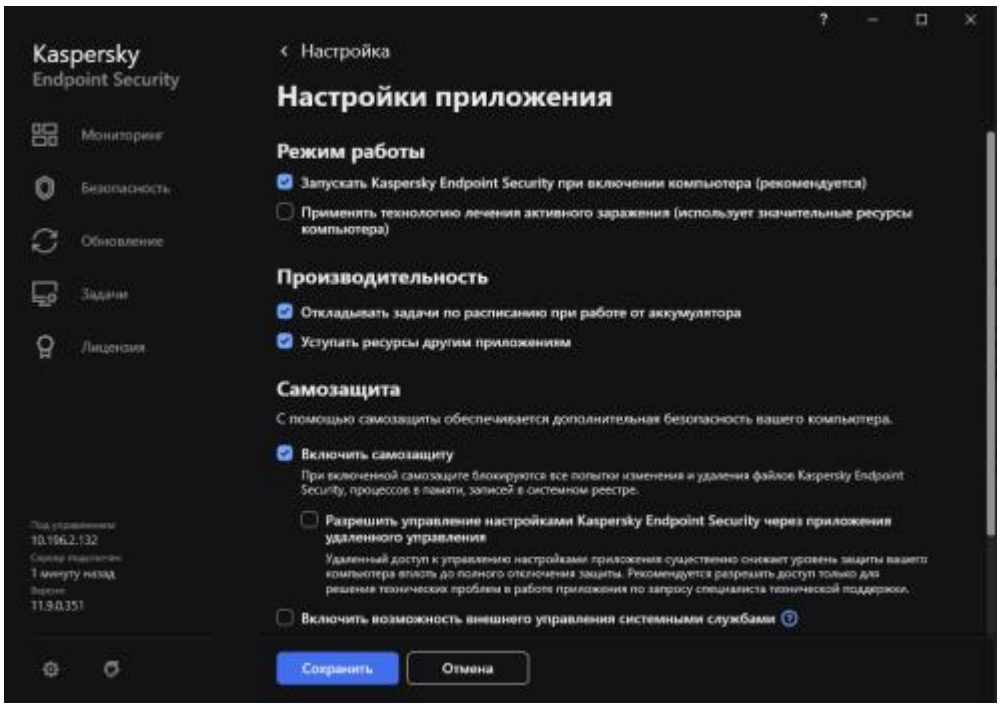

Рисунок Г.62. – Настройка компонента «Настройки приложения»

3) в поле «Отладочная информация» выключить «Запись дампов» и «Защита файлов дампов и файлов трассировки». Нажать кнопку «Сохранить» (см. рисунок Г.63.).

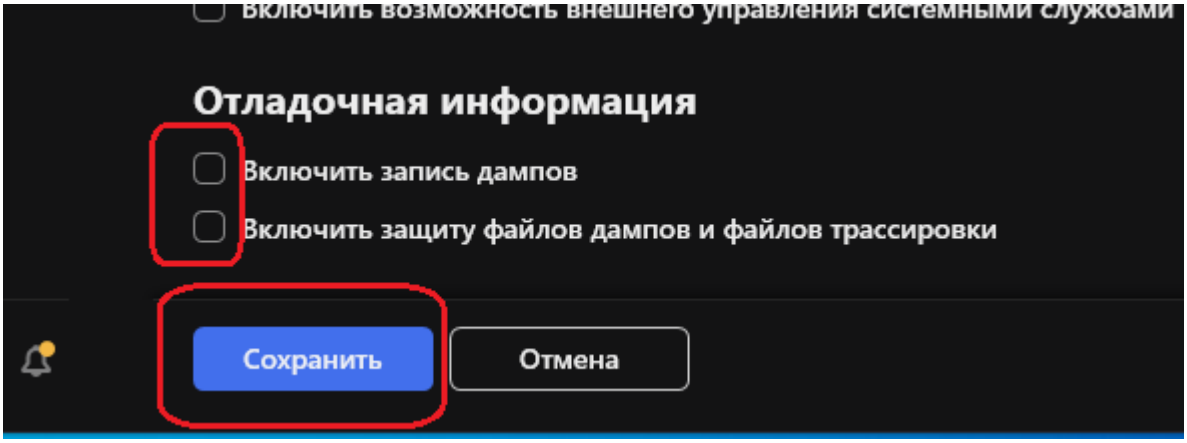

Рисунок Г.63. – Настройка компонента «Настройки приложения»

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».

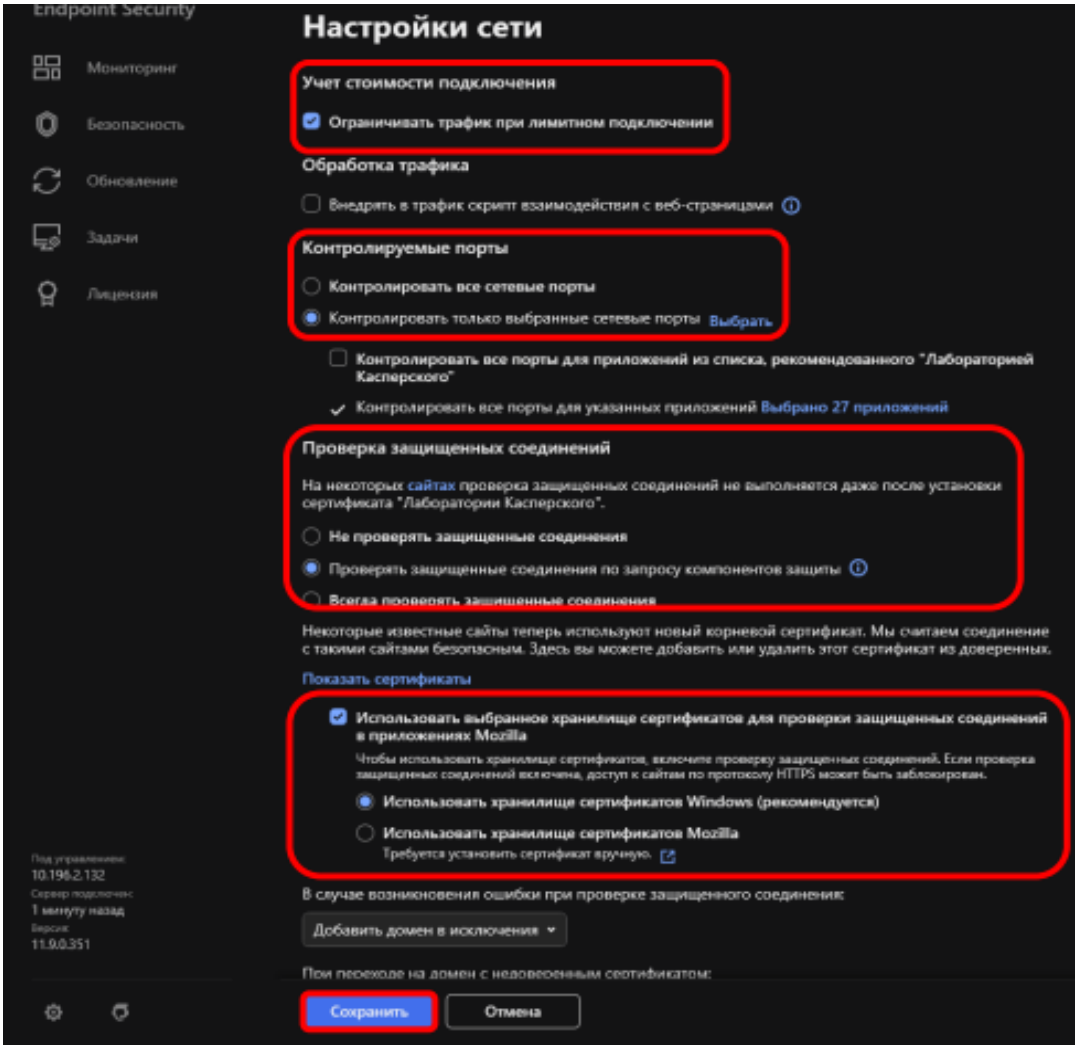

Рисунок Г.64. – Настройка компонента «Настройка сети»

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.).

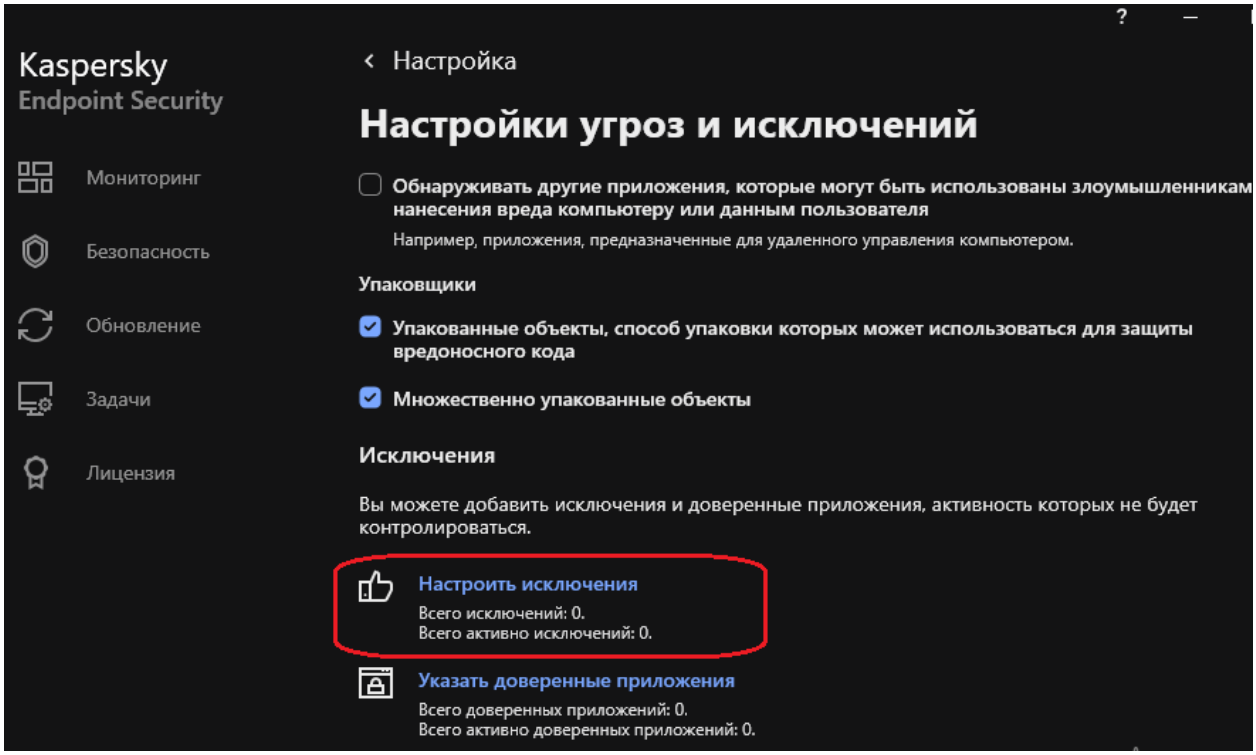

Рисунок Г.65. – Настройка компонента «Угрозы и исключения»

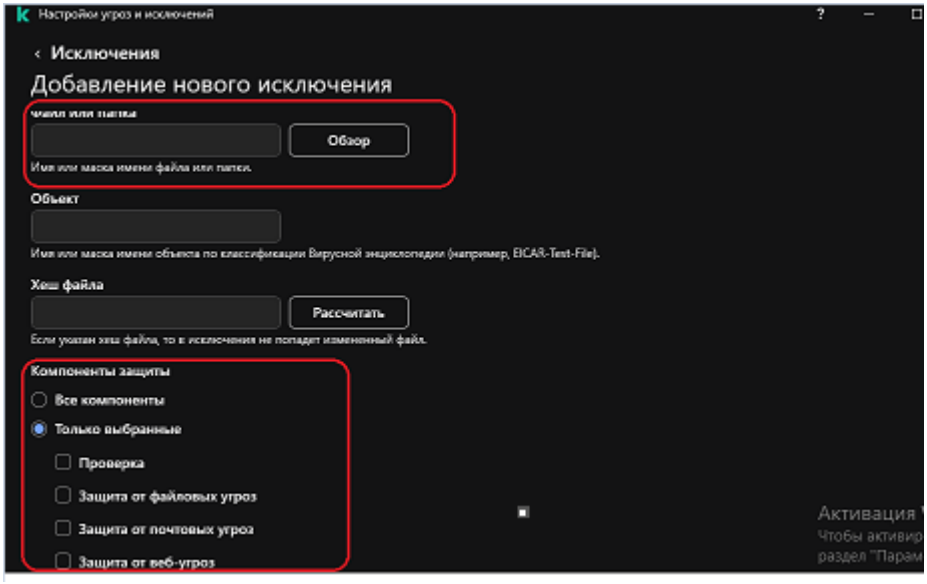

Рисунок Г.66. – Добавление исключения

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.).

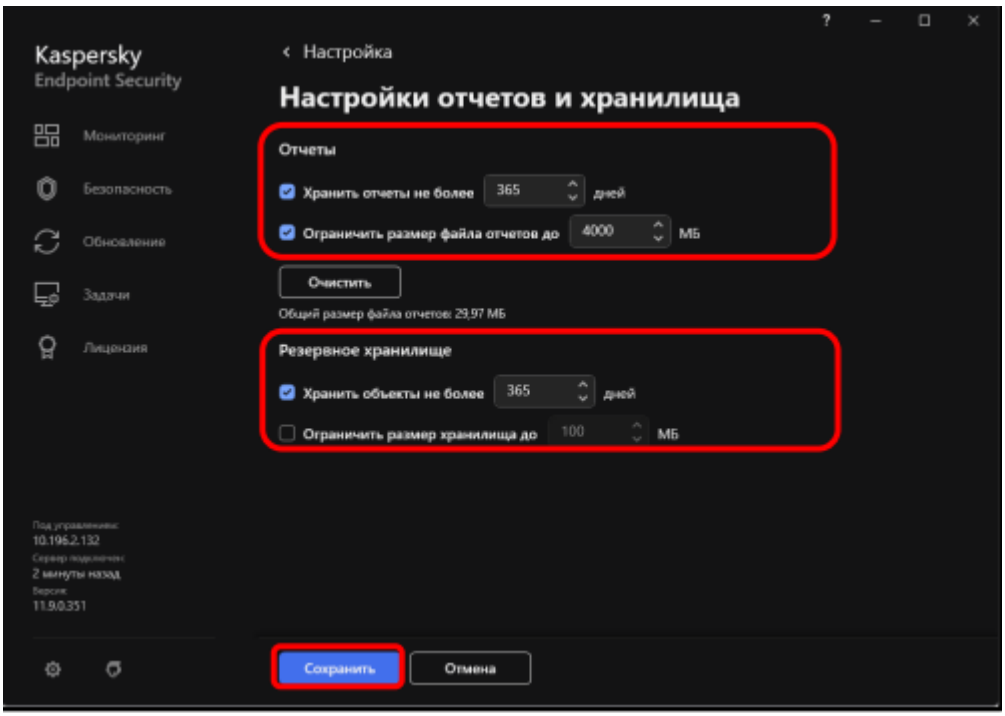

Рисунок Г.67. – Настройка компонента «Отчеты и хранения»

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.);

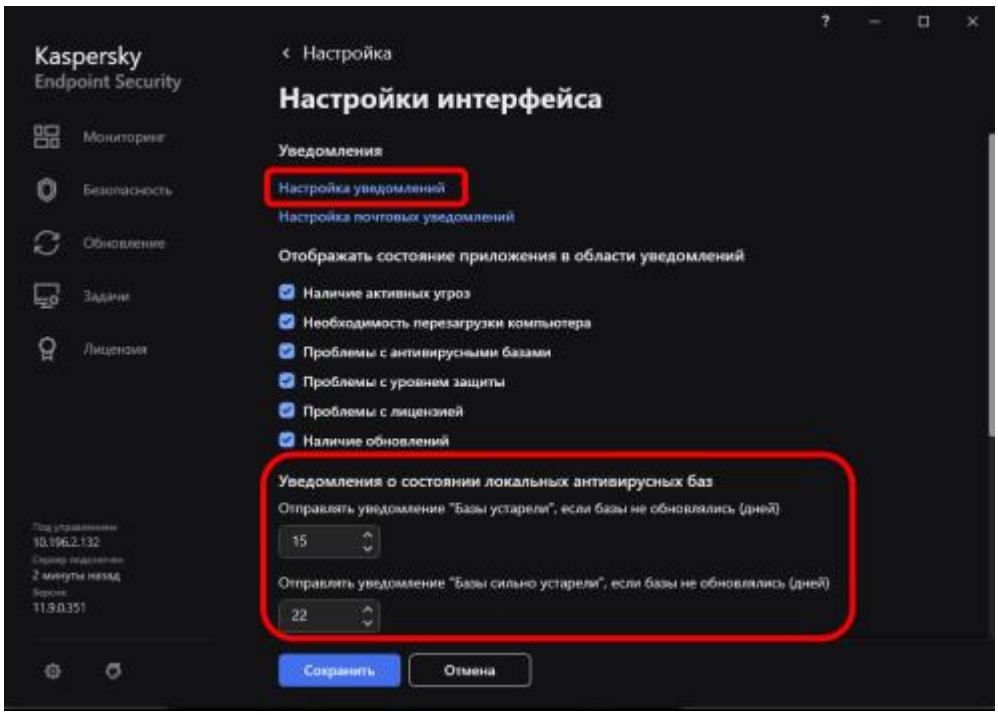

Рисунок Г.68. – Настройка компонента «Интерфейс»

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.;

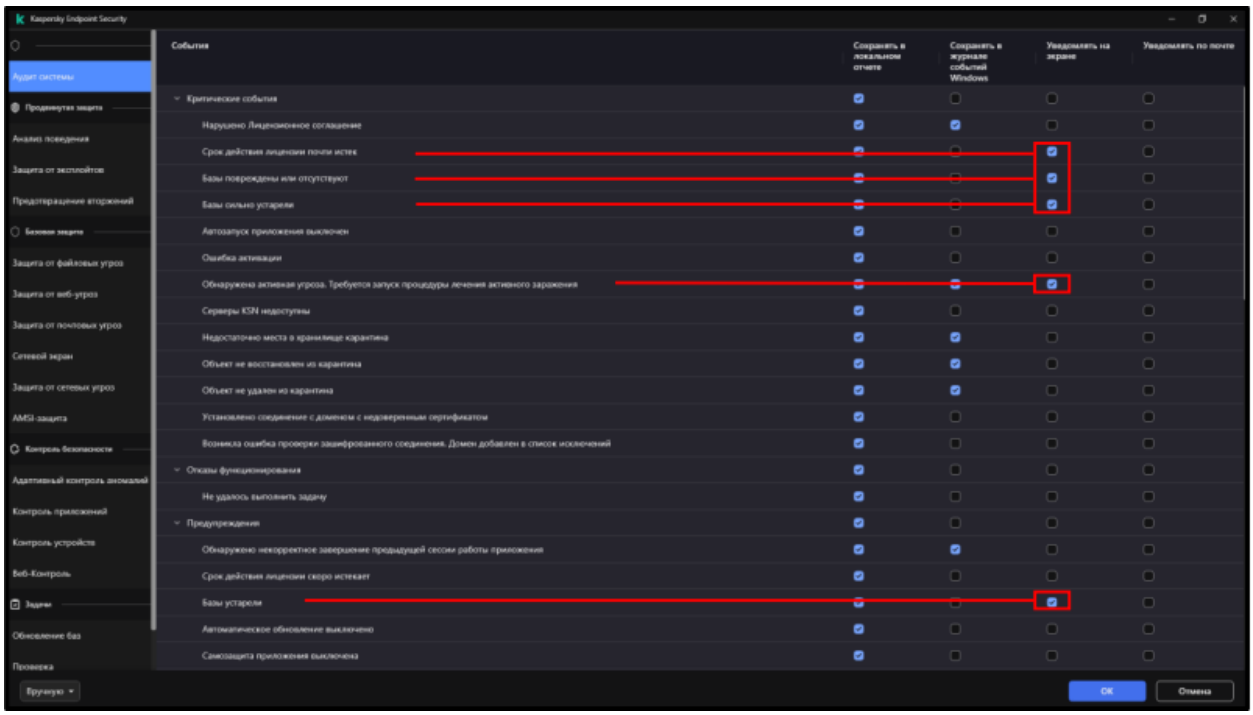

Рисунок Г.69. – Настройка уведомлений для категории «Аудит системы»

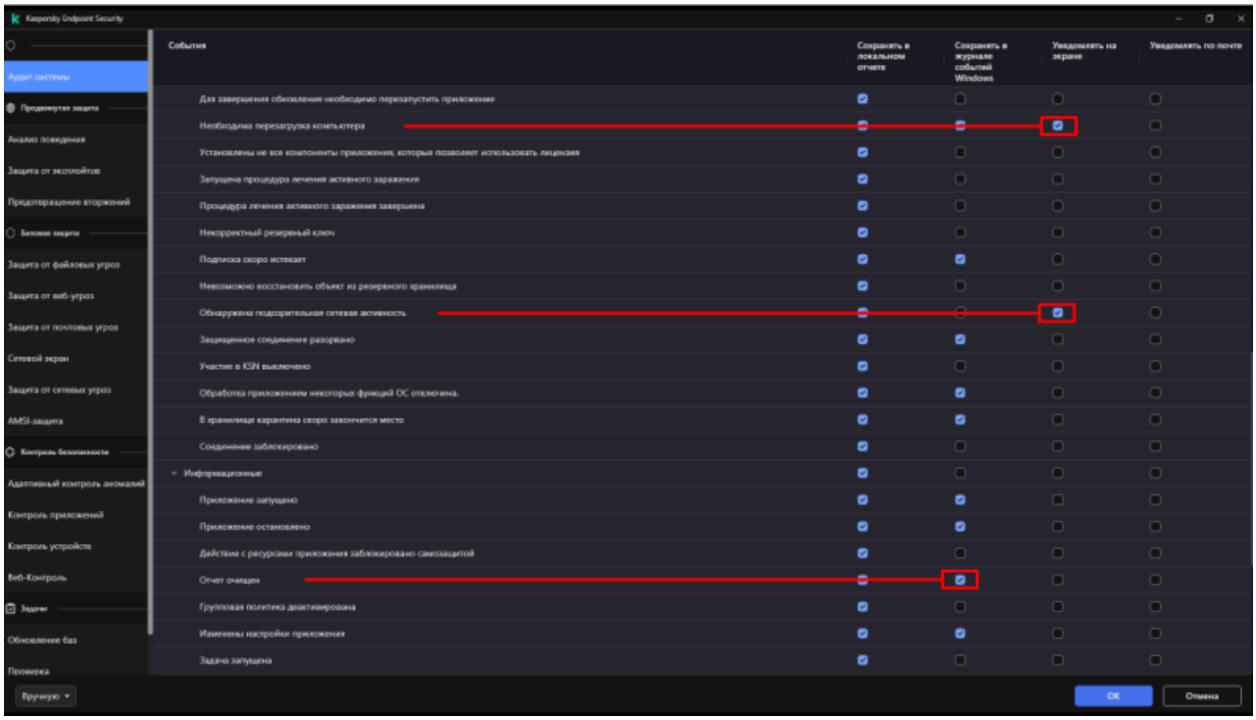

Рисунок Г.70.– Настройка уведомлений для категории «Аудит системы»

5) настроить параметры уведомлений для категории «Анализ поведения» в соответствии с рисунком Г.71.;

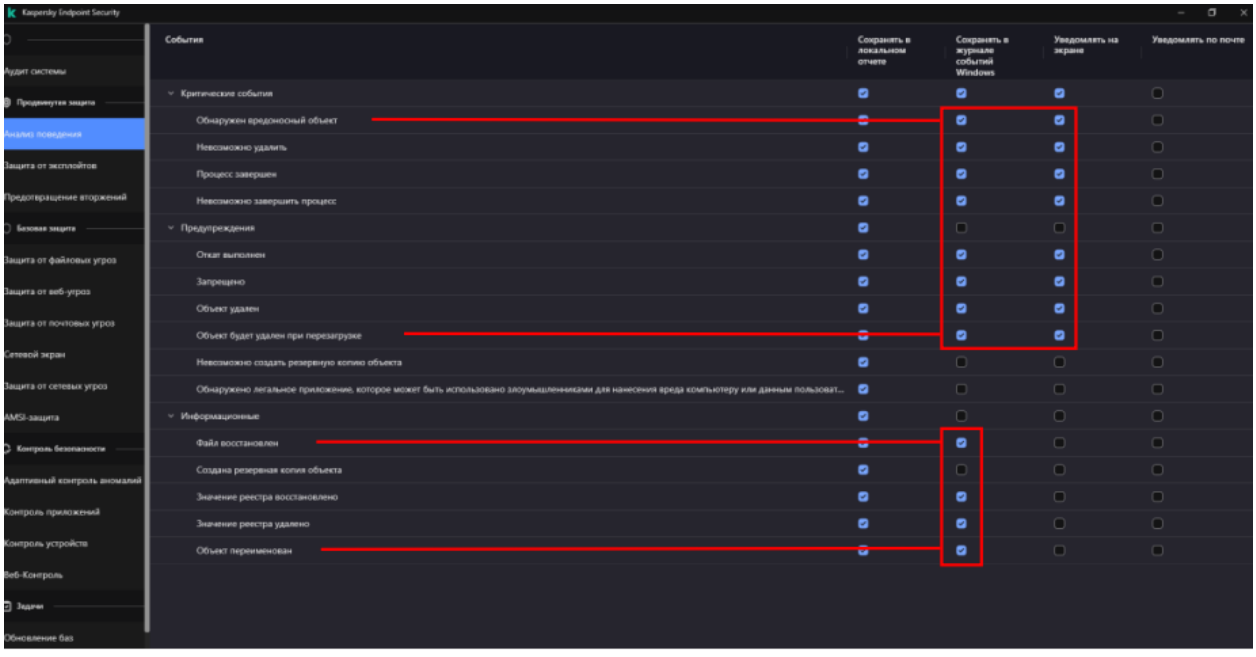

Рисунок Г.71. – Настройка уведомлений для категории «Анализ поведения»

6) настроить параметры уведомлений для категории «Защита от эксплойтов» в соответствии с рисунком Г.72.;

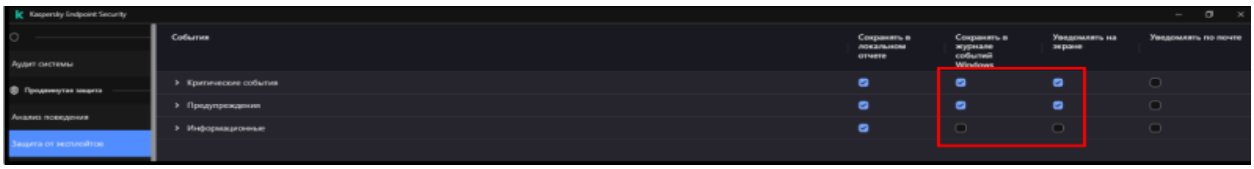

Рисунок Г.72. – Настройка уведомлений для категории «Защита от эксплойтов»

7) настроить параметры уведомлений для категории «Предотвращение вторжений» в соответствии с рисунками Г.73. и Г.74.;

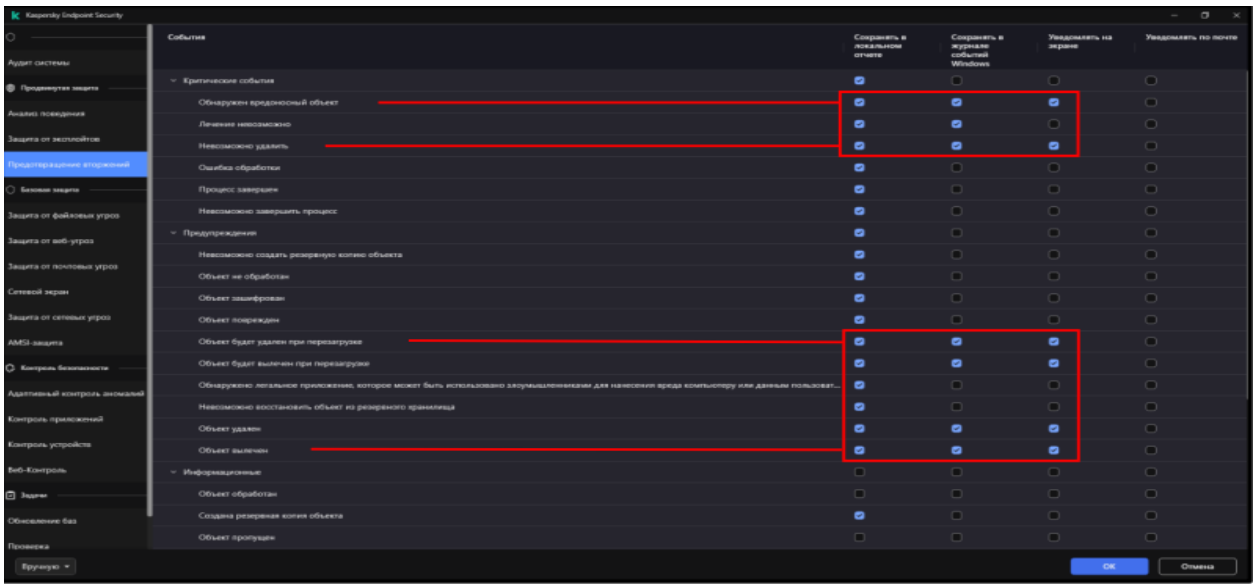

Рисунок Г.73. – Настройка уведомлений для категории «Предотвращение вторжений»

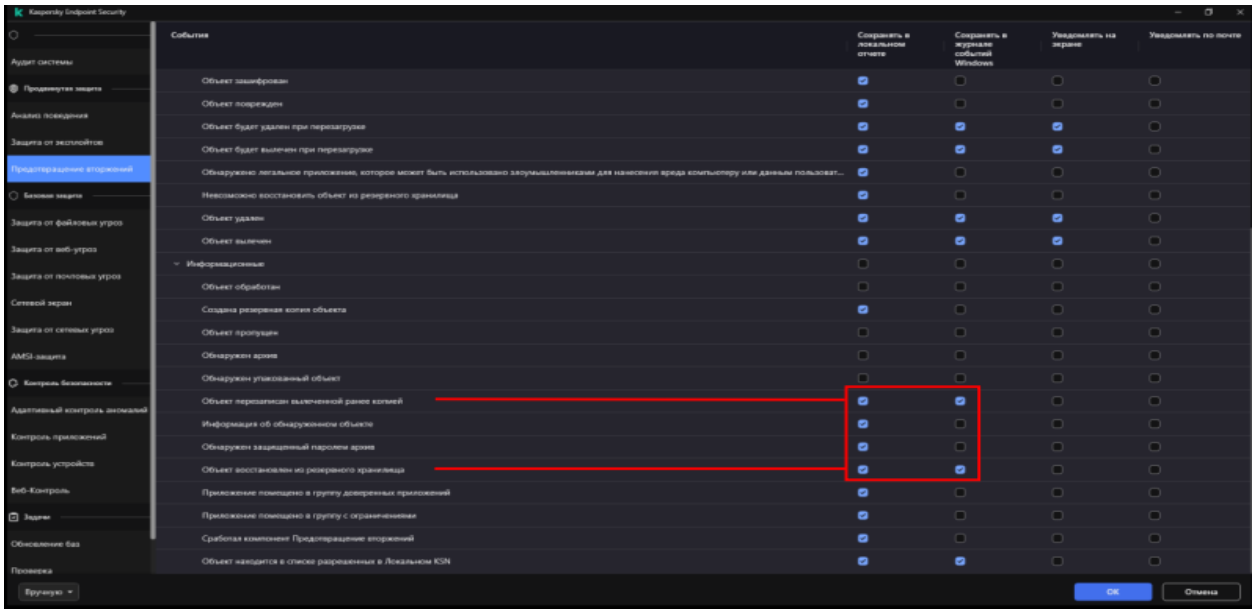

Рисунок Г.74. – Настройка уведомлений для категории «Предотвращение вторжений»

8) настроить параметры уведомлений для категории «Сетевой экран» в соответствии с рисунком Г.75.;

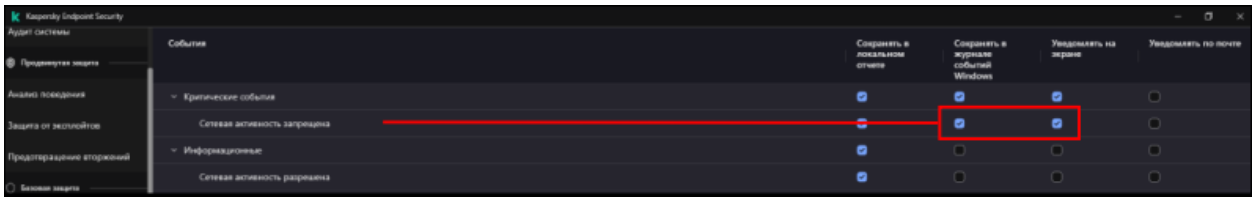

Рисунок Г.75. – Настройка уведомлений для категории «Сетевой экран»

9) настроить параметры уведомлений для категории «Защита от файловых угроз» в соответствии с рисунками Г.76. и Г.77.;

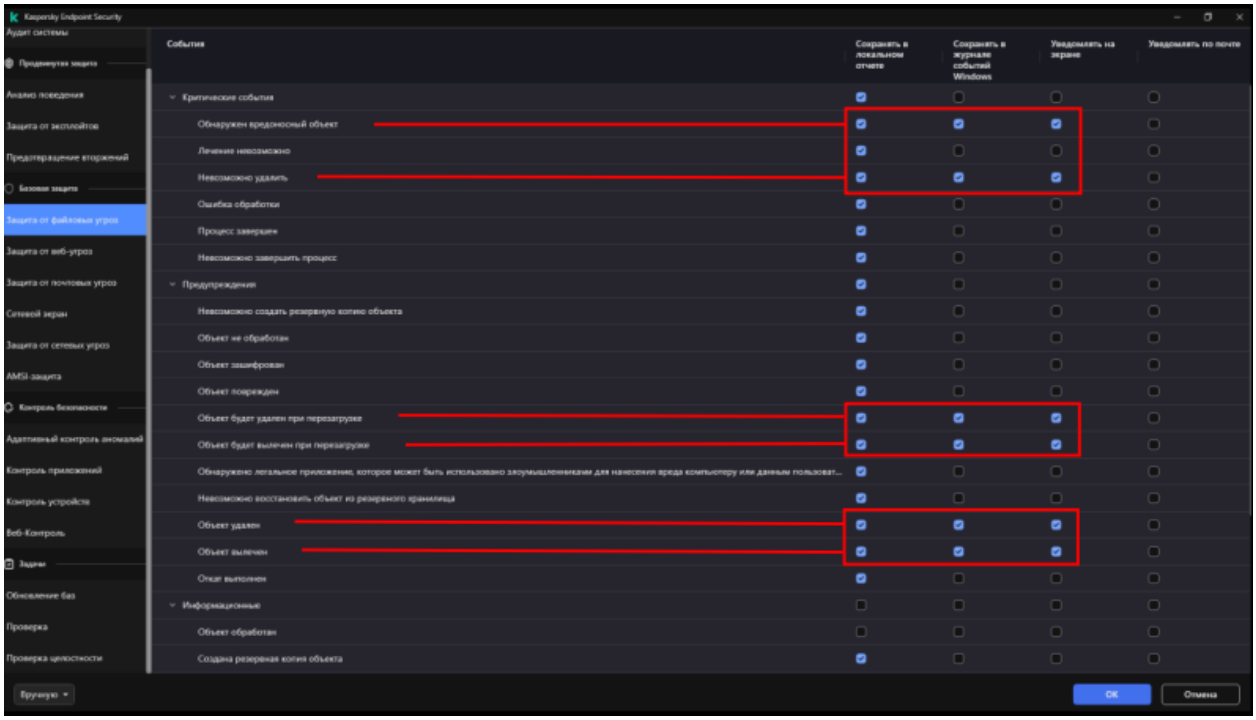

Рисунок Г.76. – Настройка уведомлений для категории «Защита от файловых угроз»

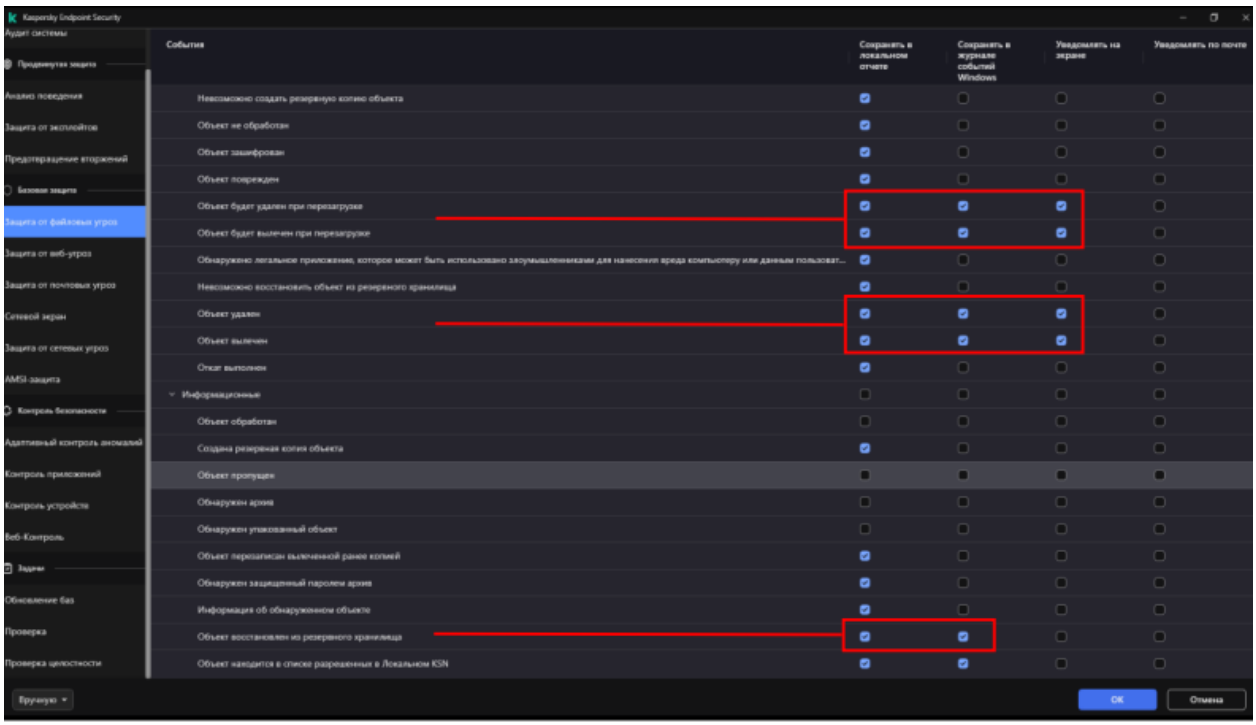

Рисунок Г.77.– Настройка уведомлений для категории «Защита от файловых угроз»

10) настроить параметры уведомлений для категории «Защита от веб-угроз» в соответствии с рисунком Г.78.;

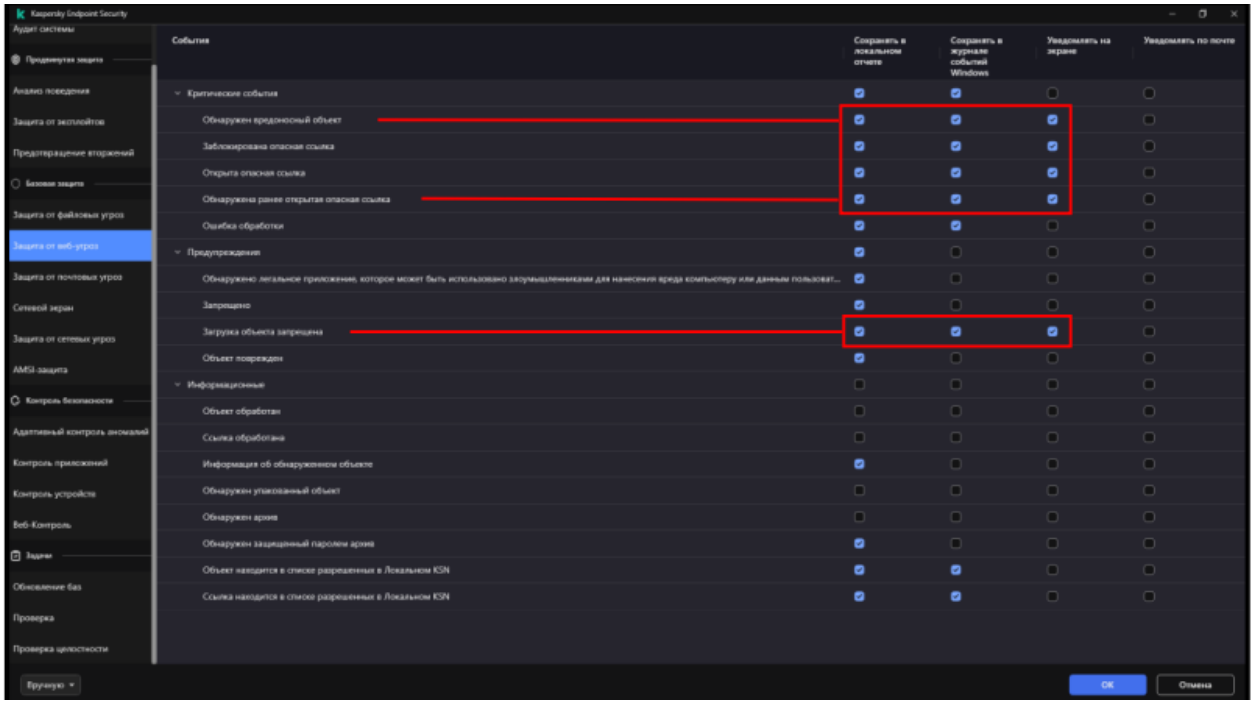

Рисунок 1 – Настройка уведомлений для категории «Защита от веб-угроз»

11) настроить параметры уведомлений для категории «Защита от сетевых угроз» в соответствии с рисунком Г.79;

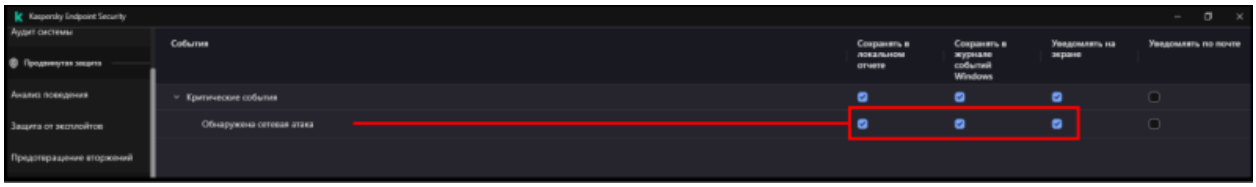

Рисунок Г.79 – Настройка уведомлений для категории «Защита от сетевых угроз»

12) настроить параметры уведомлений для категории «Защита от почтовых угроз» в соответствии с рисунком Г.80.;

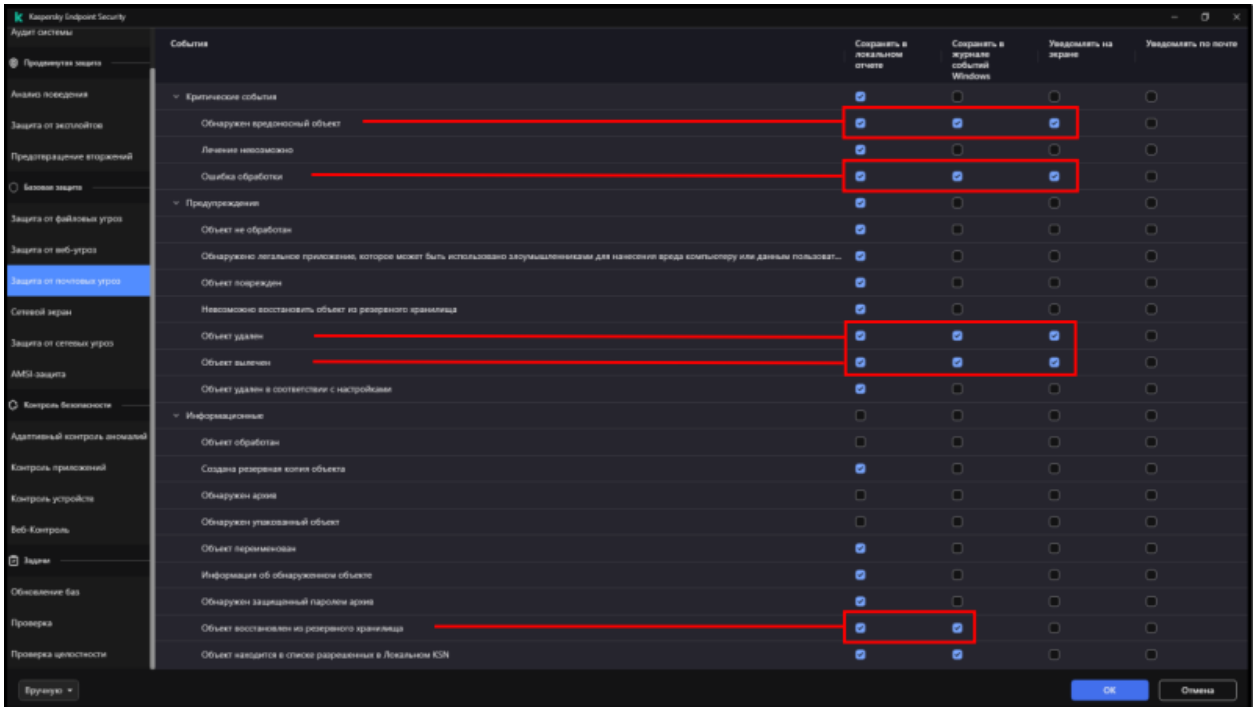

Рисунок Г.80. – Настройка уведомлений для категории «Защита от почтовых угроз»

13) настроить параметры уведомлений для категории «AMSI защита» в соответствии с рисунками Г.81. и Г.82.;

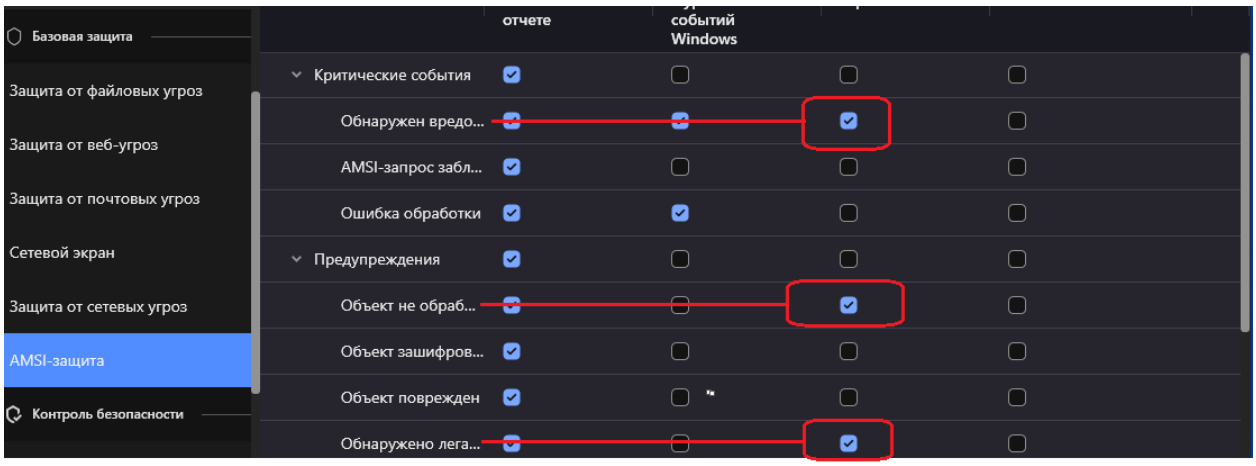

Рисунок Г.81. – Настройка уведомлений для категории «AMSI защита»

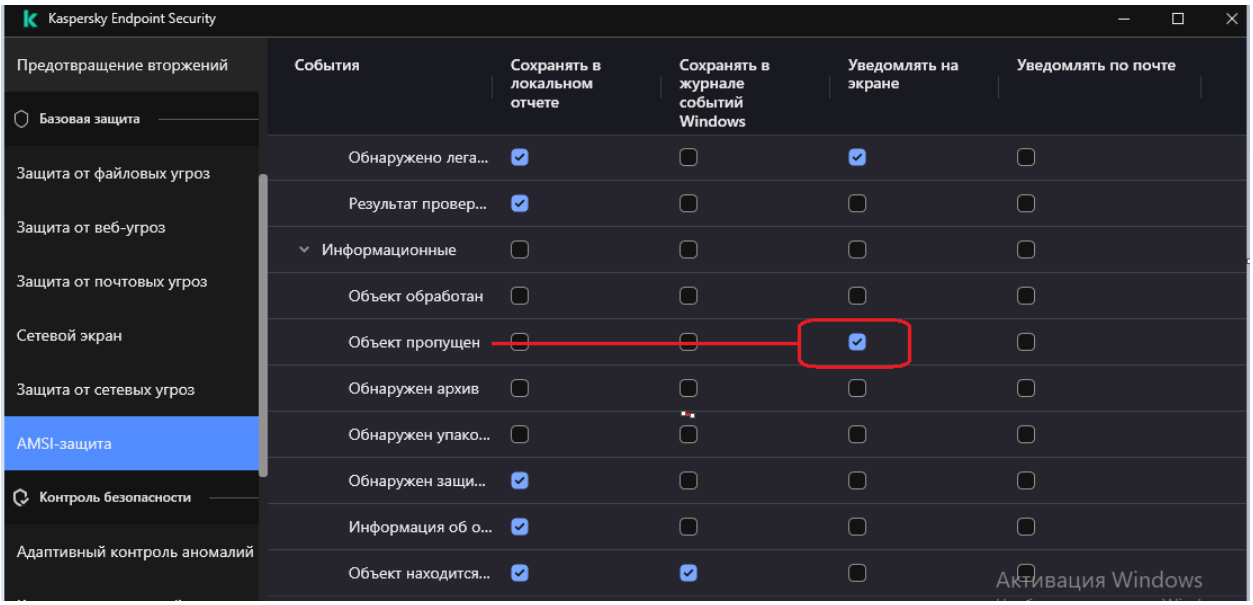

Рисунок Г.82. – Настройка уведомлений для категории «AMSI защита»

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.;

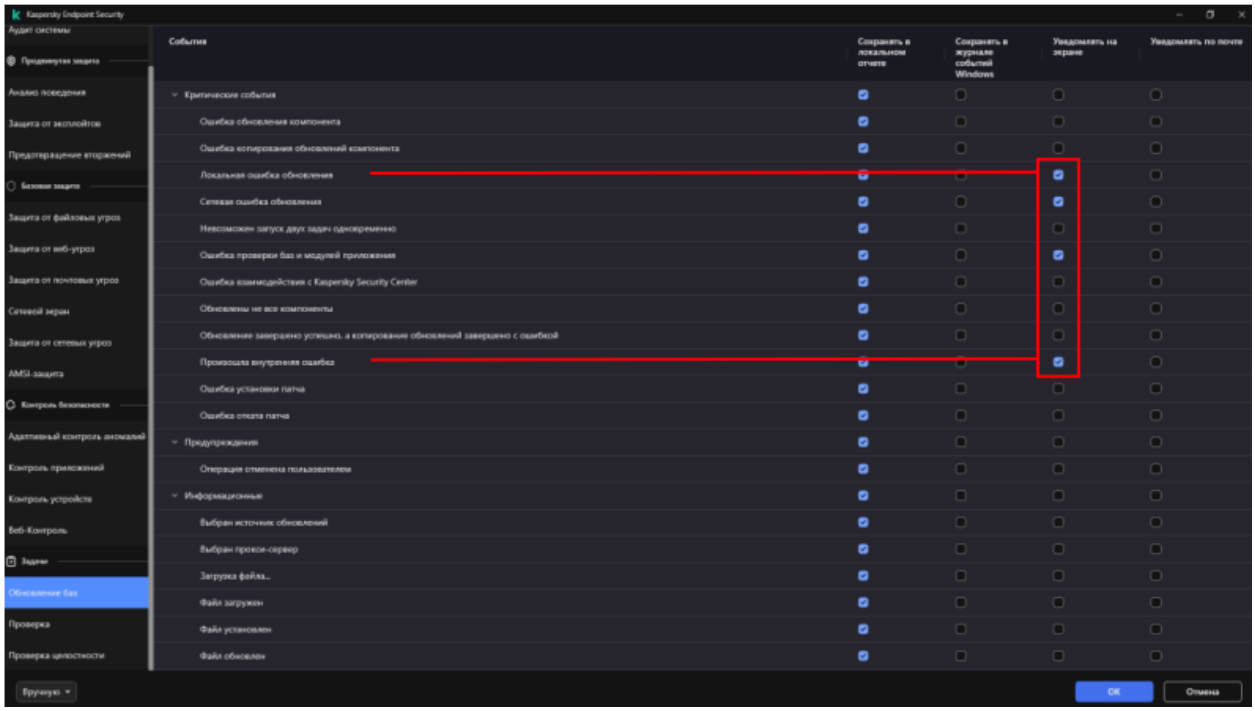

Рисунок Г.84. – Настройка уведомлений для категории «Обновление баз»

16) настроить параметры уведомлений для категории «Проверка» в соответствии с рисунком Г.85.;

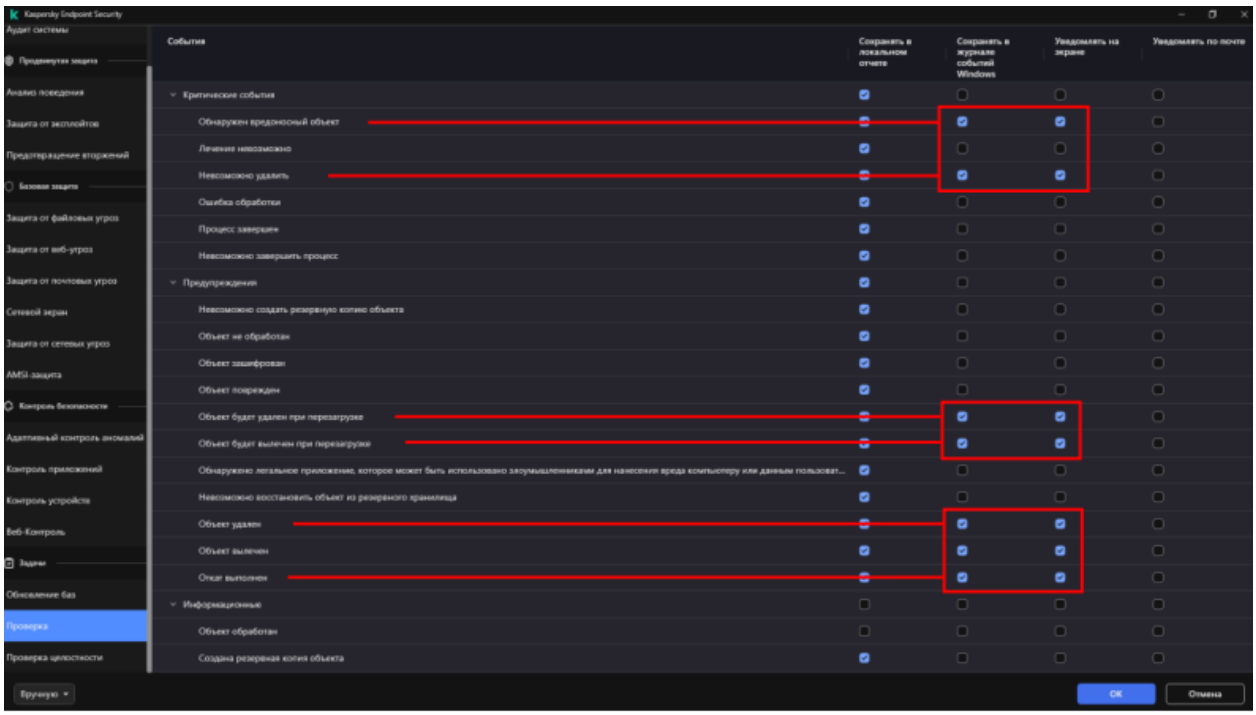

Рисунок Г.85. – Настройка уведомлений для категории «Проверка»

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.).

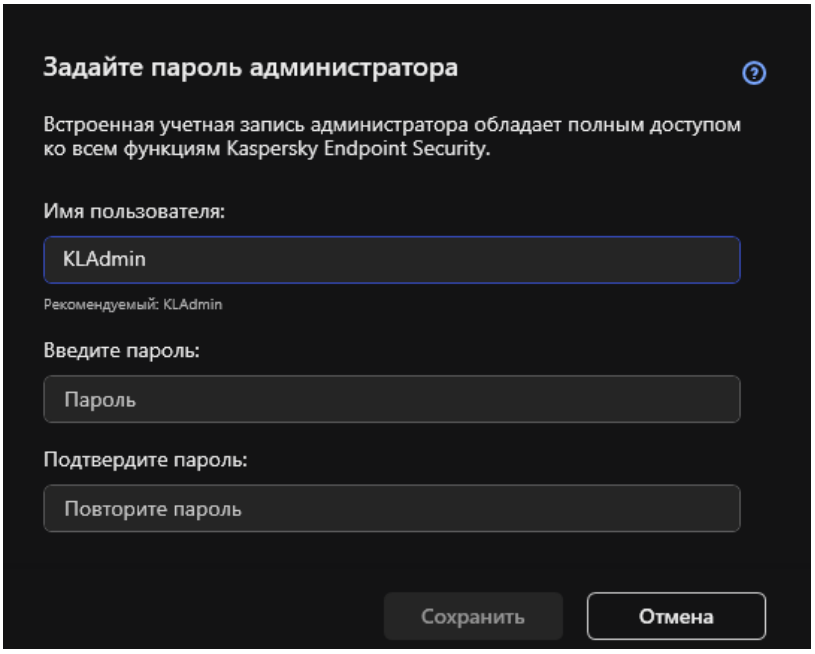

Рисунок Г.86. – Пароль для пользователя «KLAdmin»

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.).

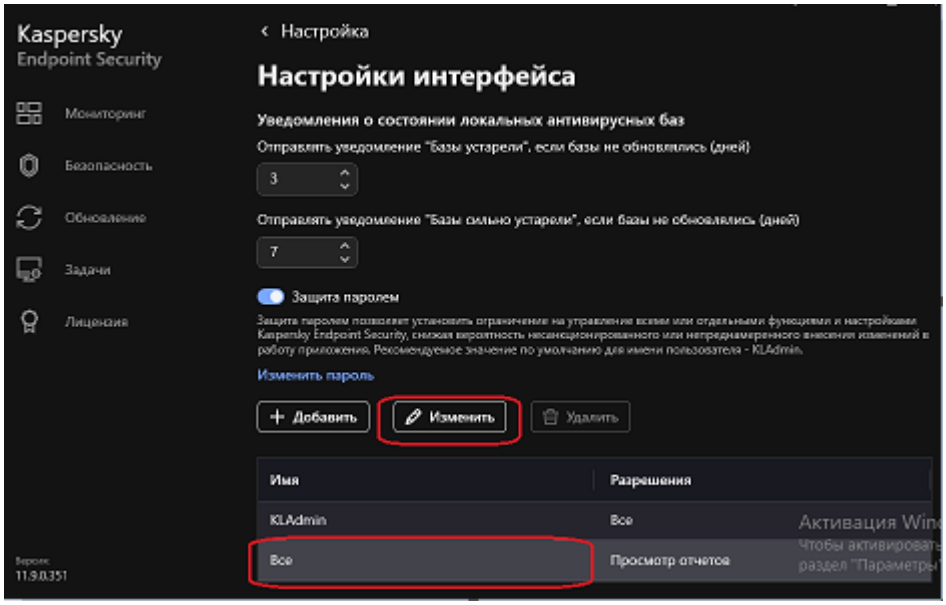

Рисунок Г.87. – Настройка прав для пользователей

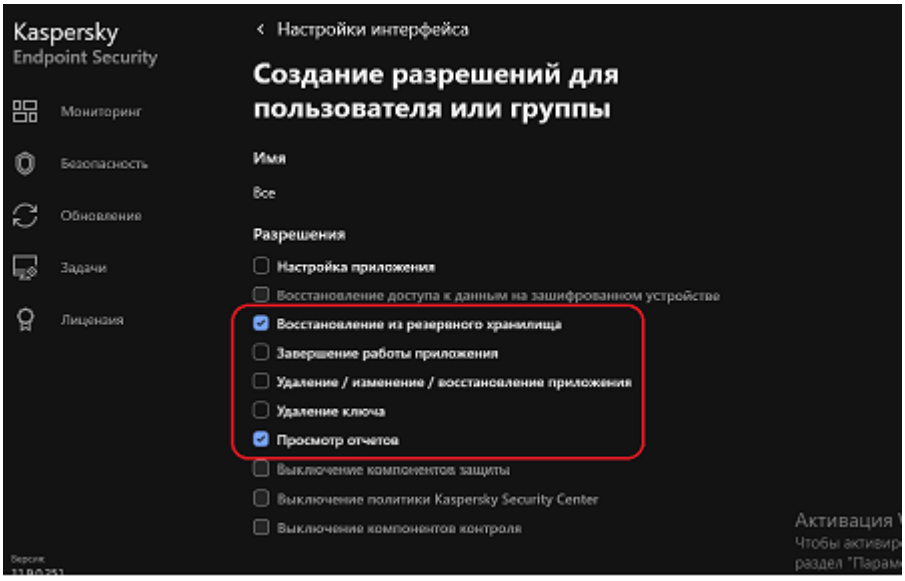

Рисунок Г.88. – Настройка прав для пользователей

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.);

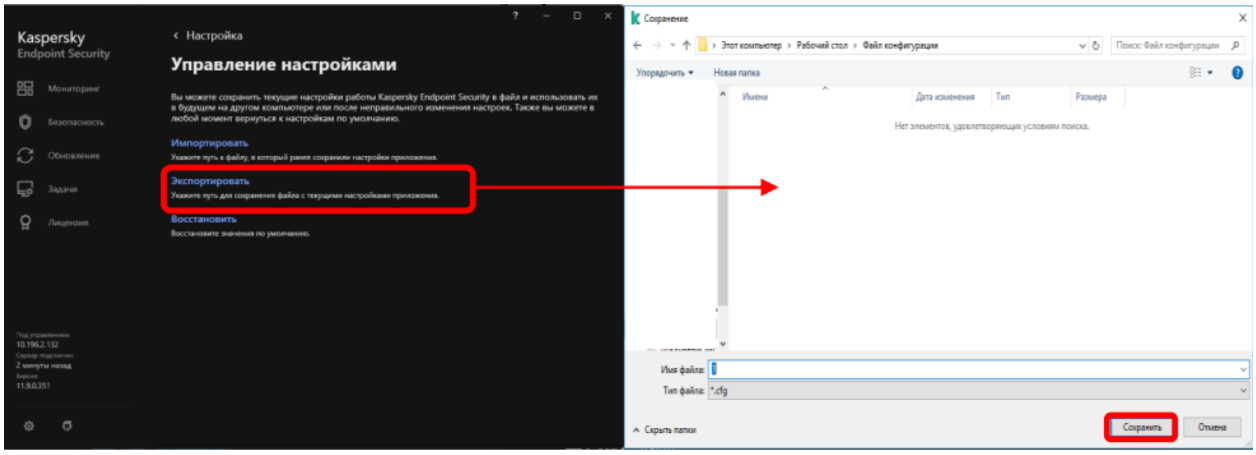

Рисунок Г.89. – Сохранение настроек конфигурации «Kaspersky Endpoint Security 11»

3) для загрузки конфигурационного файла необходимо нажать на ссылку «Импортировать», выбрать каталог с сохраненным файлом конфигурации и нажать «Открыть» (см. рисунок Г.90.);

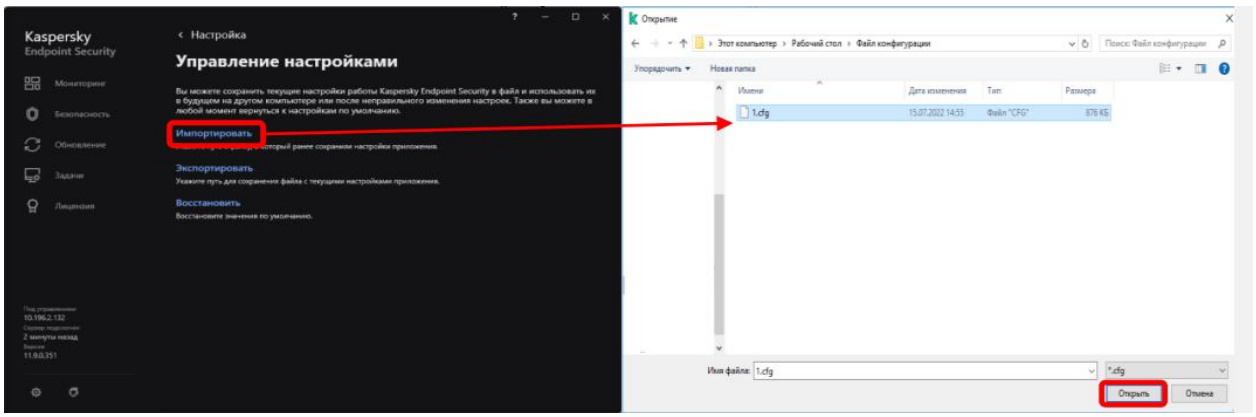

Рисунок Г.90. – Импорт конфигурации «Kaspersky Endpoint Security 11»

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.3. и Г.91.);

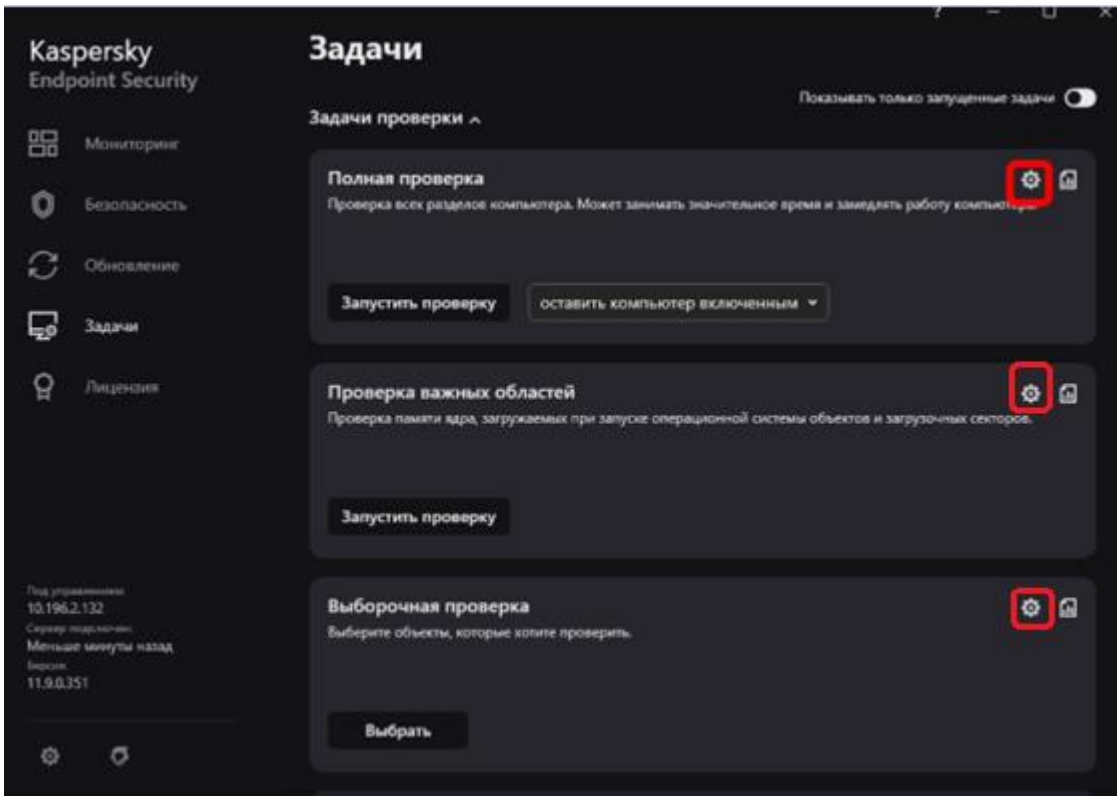

Рисунок Г.91. – Выбор задачи «Полная проверка», «Проверка важных областей», «Выборочная проверка» для настройки

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.);

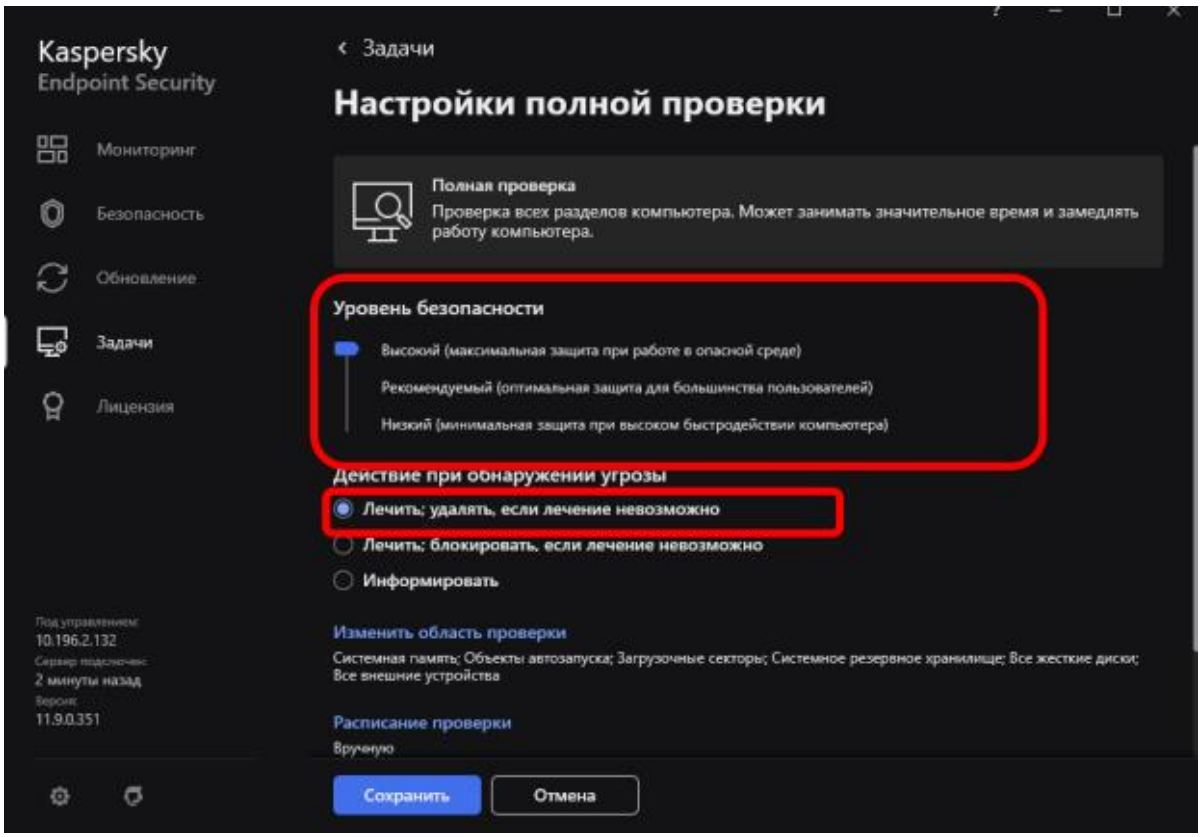

Рисунок Г.92. – Настройка задачи «Полная проверка»

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.

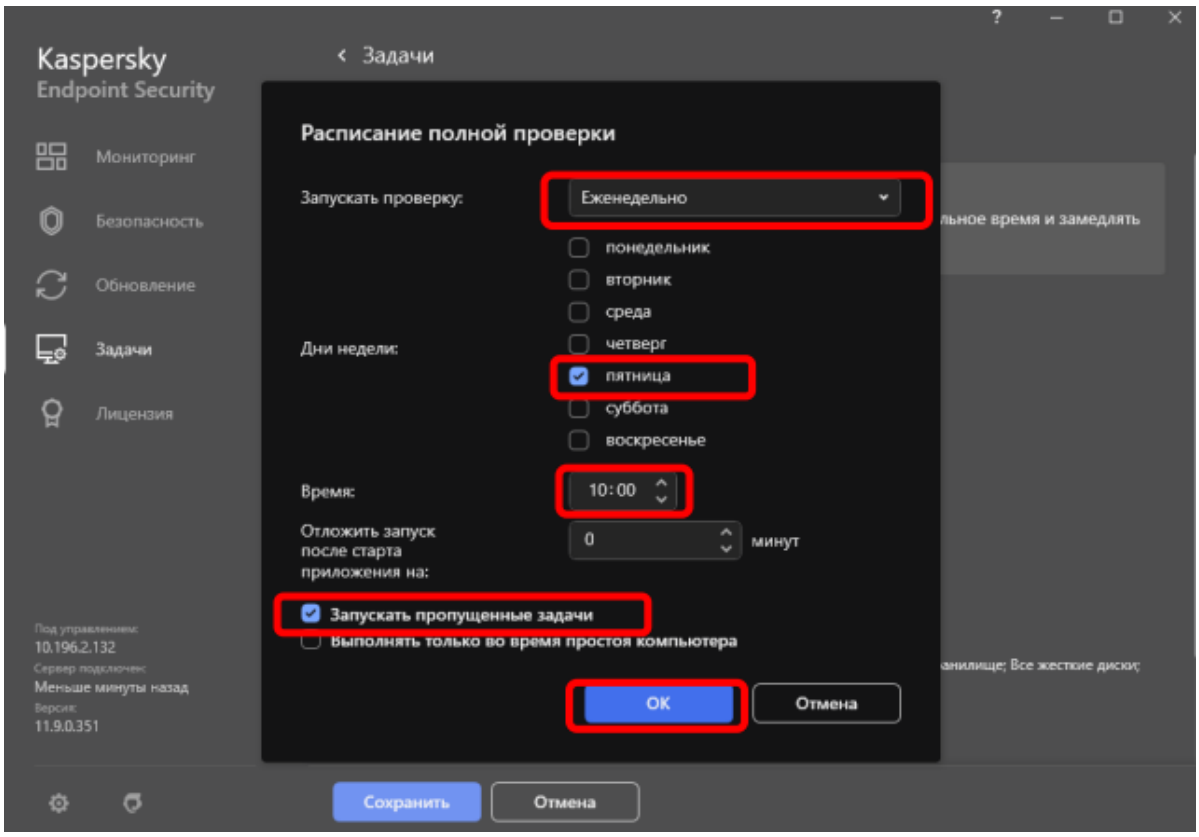

Рисунок Г.93. – Настройка режима запуска обновлений

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.);

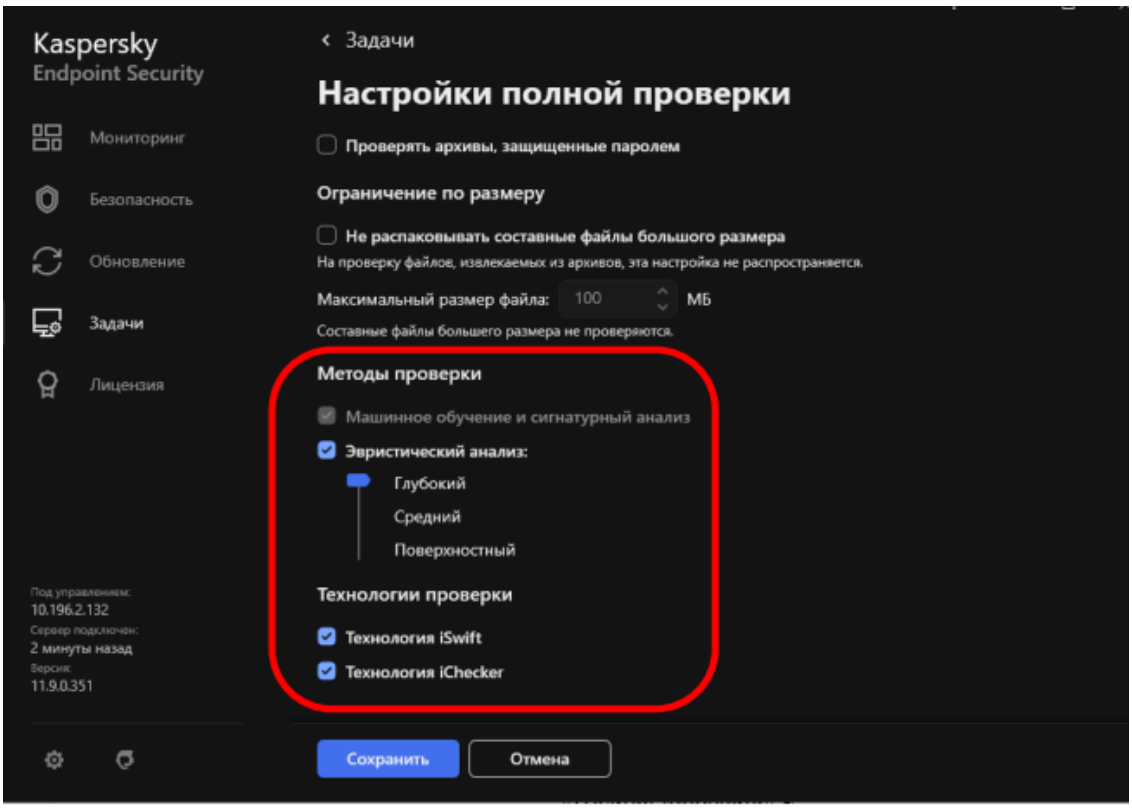

Рисунок Г.94. – Настройка дополнительных параметров задачи «Полная проверка»

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.).

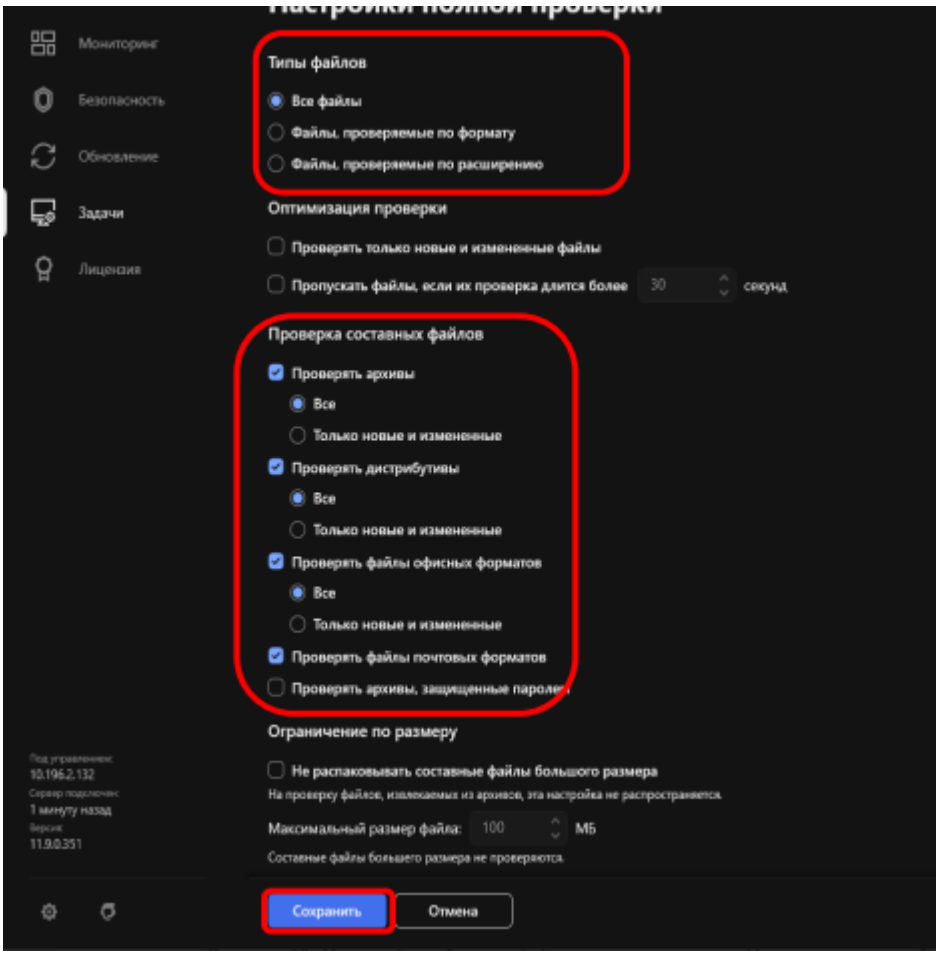

Рисунок Г.95. – Настройка области действия компонента «Полная проверка»

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.);

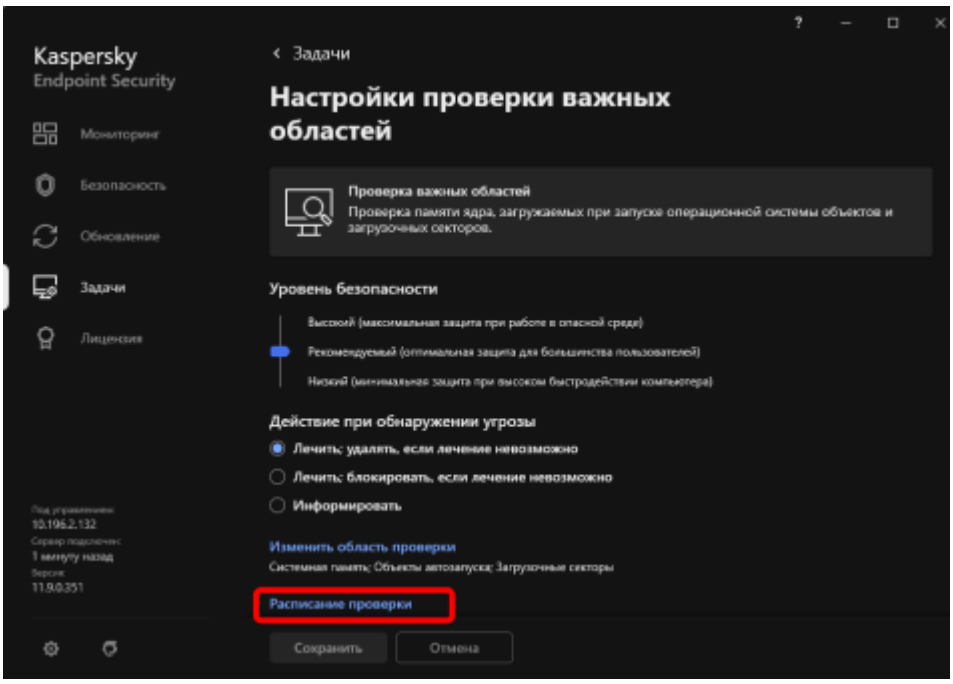

Рисунок Г.96. – Настройка задачи «Проверка важных областей»

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.);

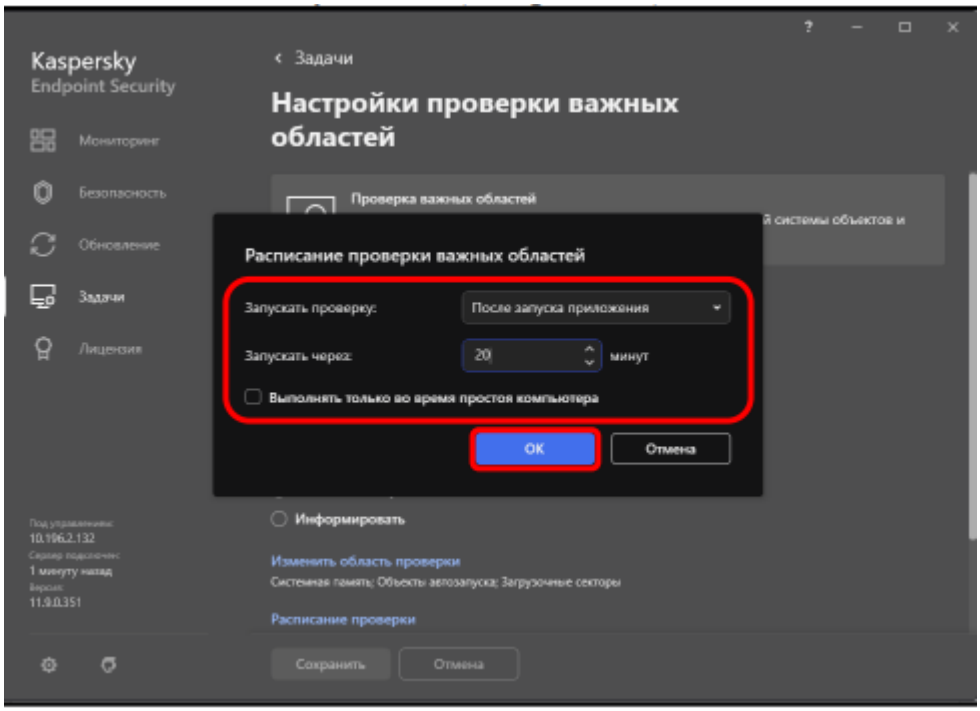

Рисунок Г.97.– Настройка режима запуска задачи «Проверка важных областей»

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.);

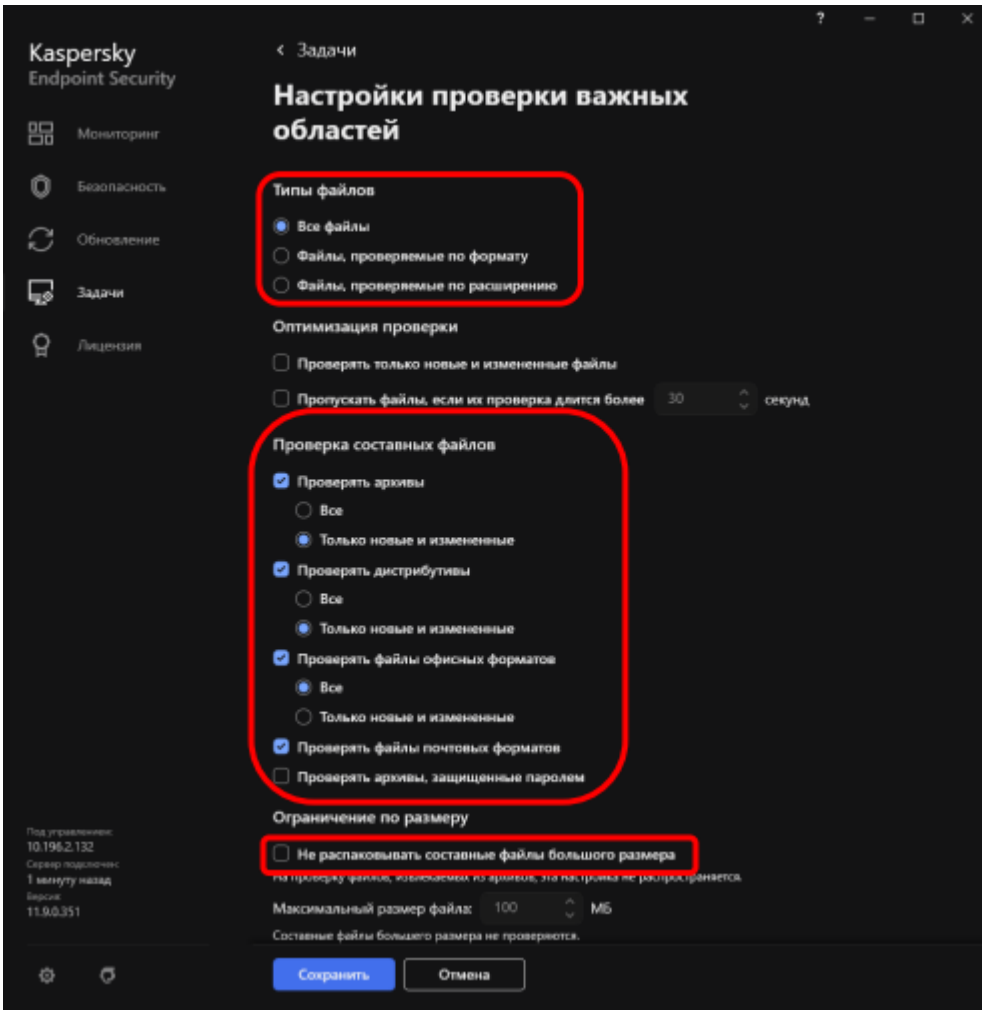

Рисунок Г.98. – Настройка области действия задачи «Проверка важных областей»

6) в пункте «Метод проверки» в зависимости от вычислительной мощности средства ВТ выбрать уровень эвристического анализа «Средний» или «Глубокий» (см. рисунок Г.99.).

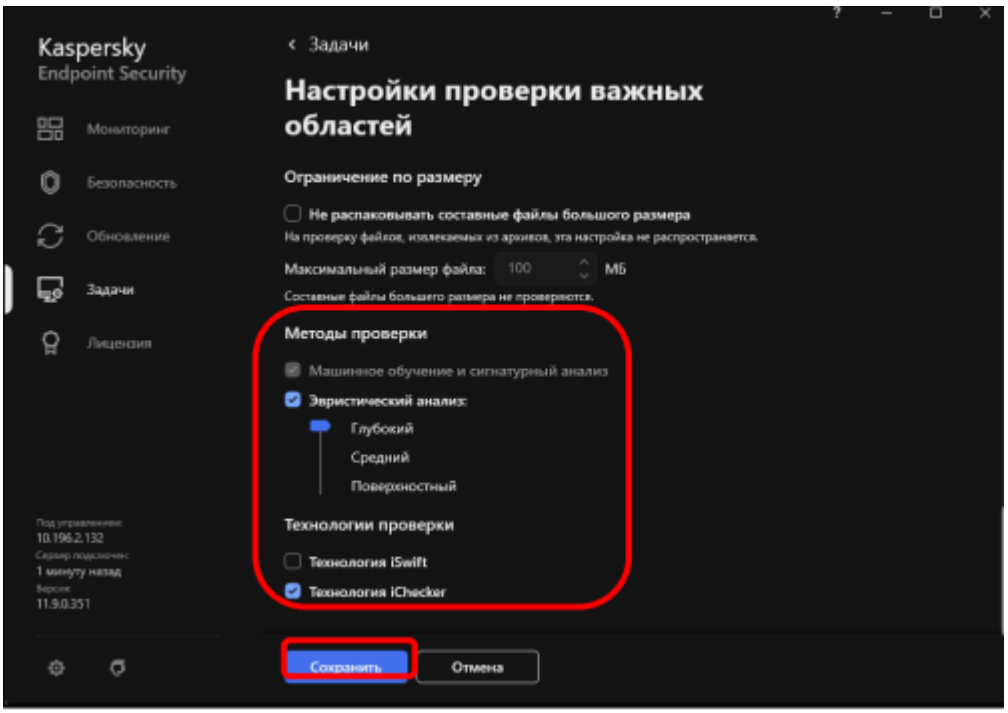

Рисунок Г.99. – Настройка дополнительных параметров компонента «Проверка важных областей»

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:

1) в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Проверка съемных дисков» (см. рисунки Г.3. и Г.100.);

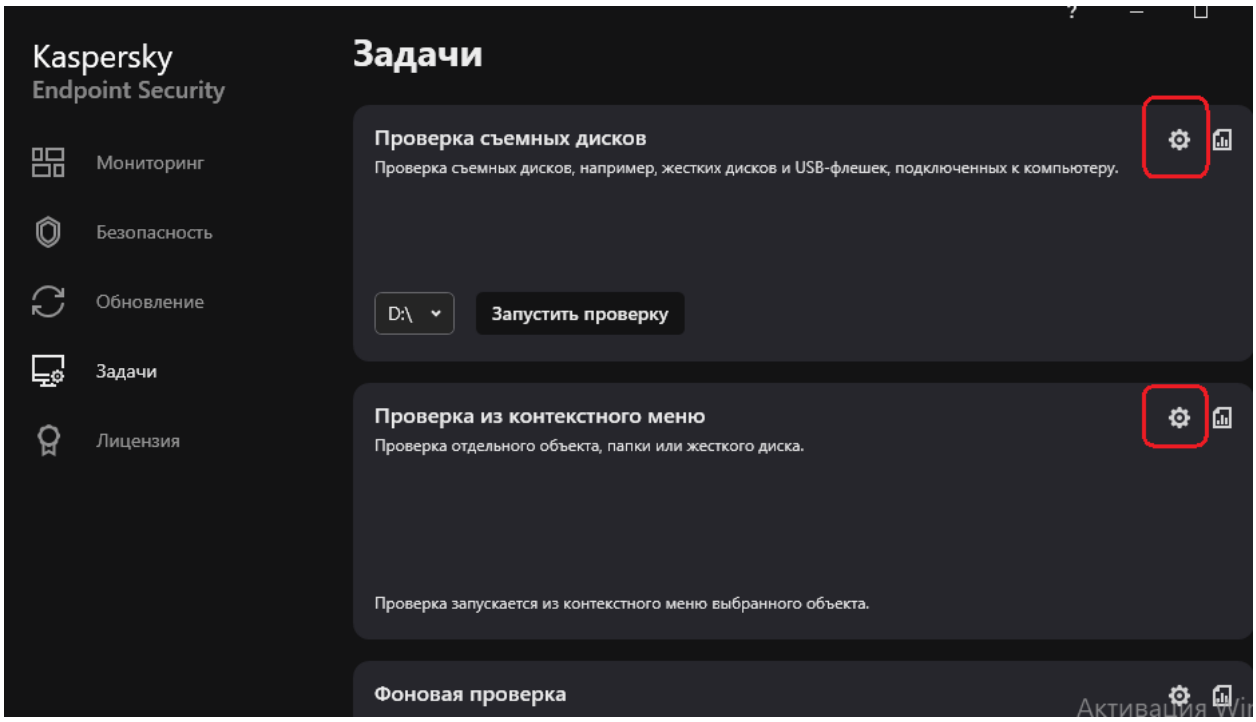

Рисунок Г.100. – Выбор задачи «Проверка съемных дисков», «Проверка из контекстного меню» для настройки.

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.).

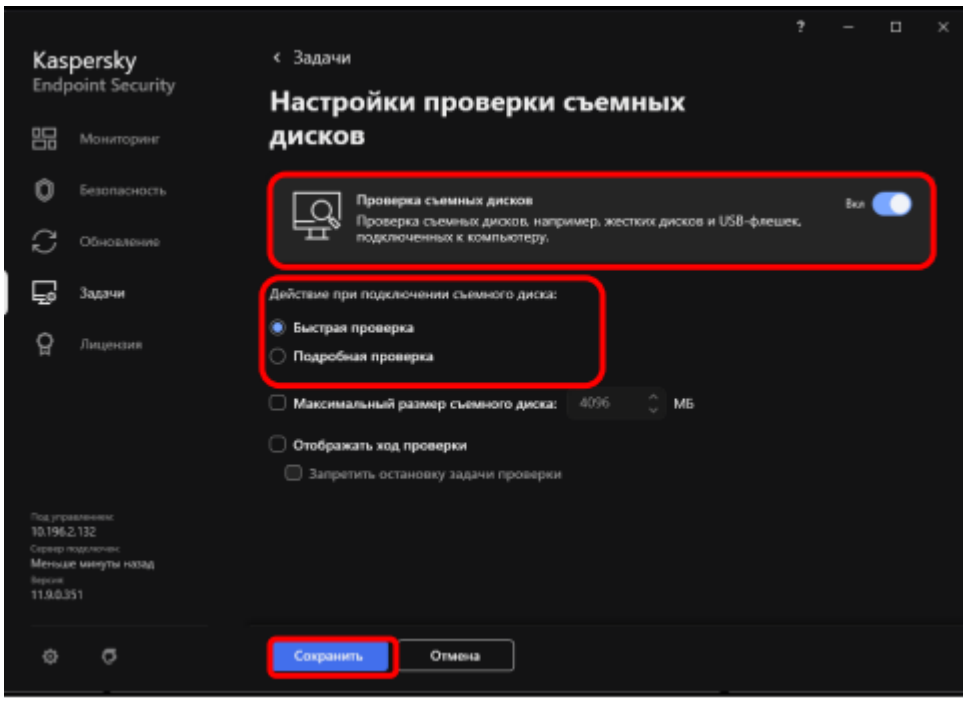

Рисунок Г.101. – Настройка проверки съемных дисков

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:

1) в главном окне САВЗ выбрать меню «Задачи» и нажать на значок шестеренки напротив задачи «Проверка из контекстного меню» (см. рисунки Г.3. и Г.100.);

2) настроить параметры проверки аналогично параметрам выборочной проверки и нажать «Сохранить» (см. рисунок Г.102.).

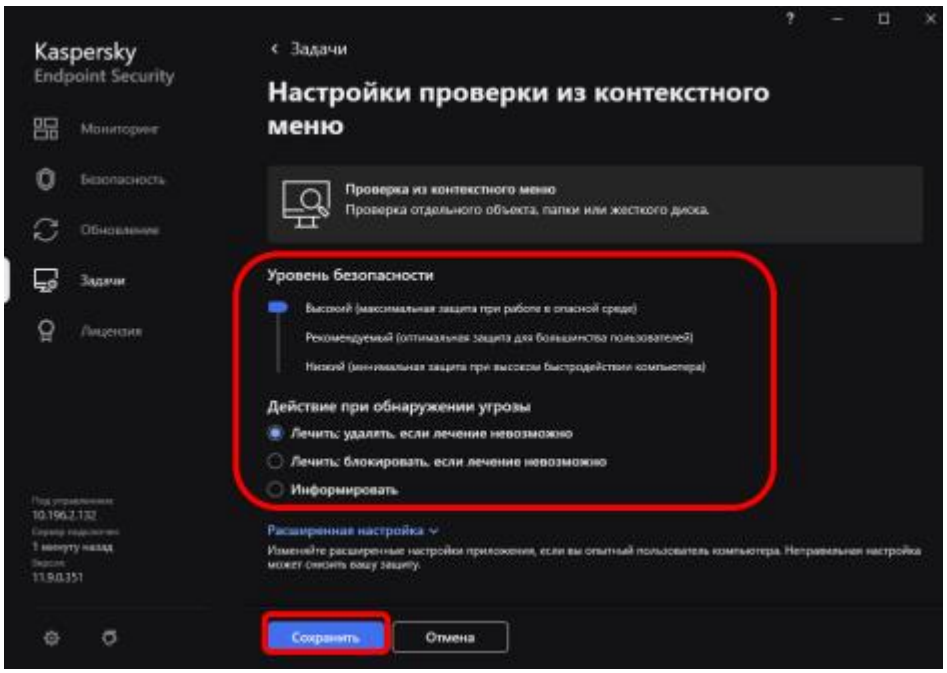

Рисунок Г.102. – Настройка проверки из контекстного меню

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:

1) в главном окне САВЗ выбрать пункт «Задачи» и нажать на значок шестеренки напротив задачи «Проверка целостности» (см. рисунки Г.3. и Г.103.);

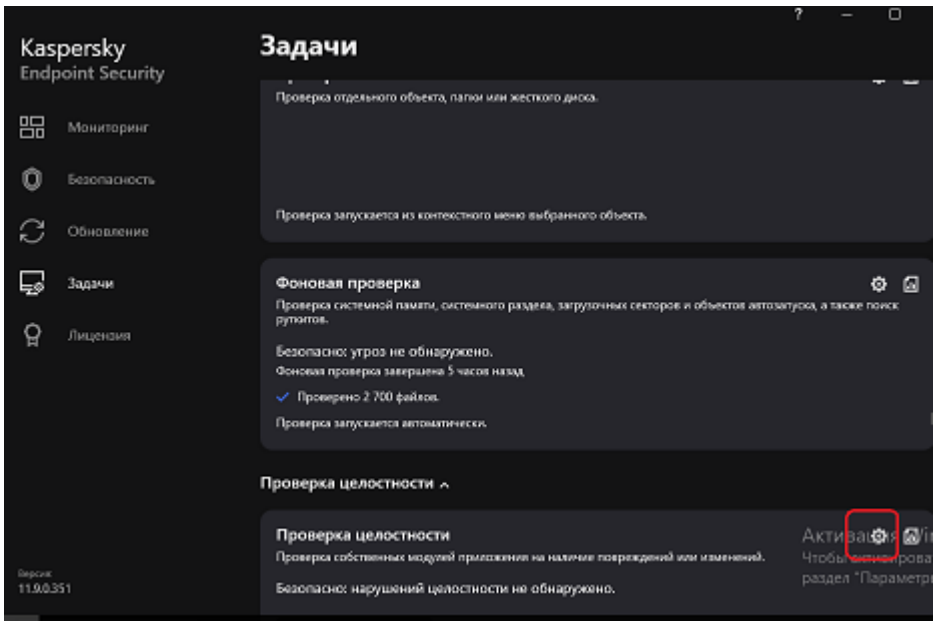

Рисунок Г.103. – Выбор задачи «Проверка целостности» для настройки.

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.).

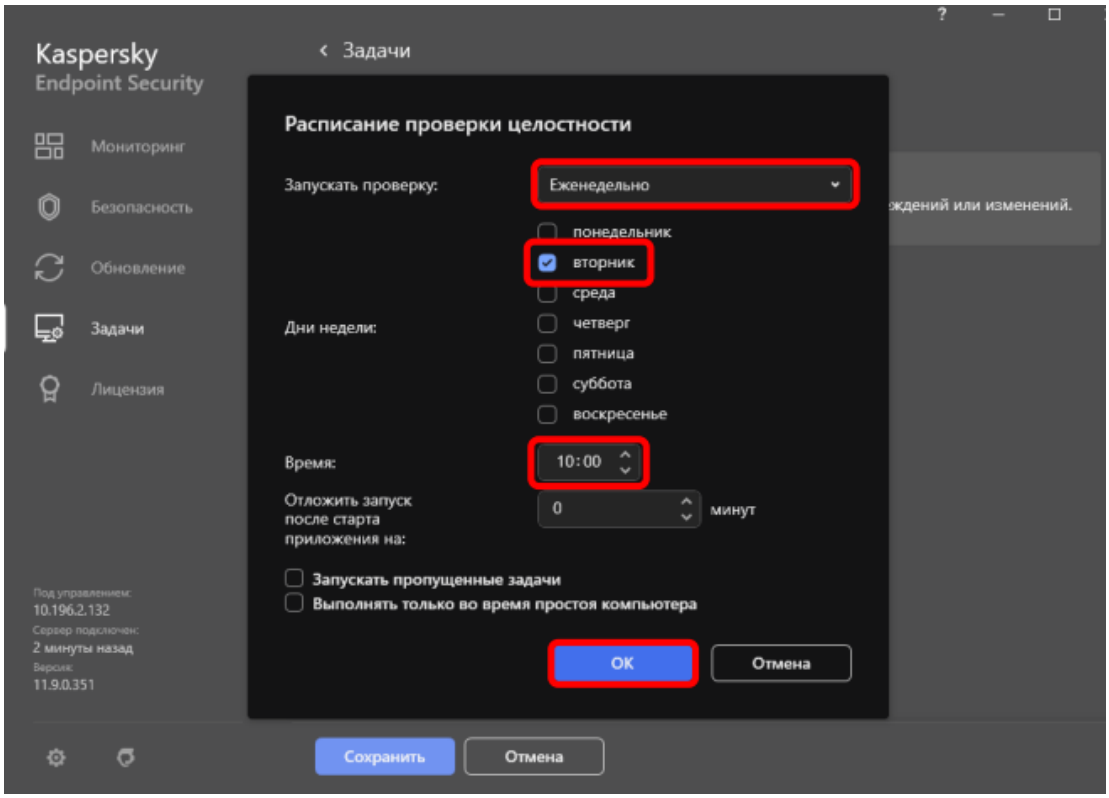

Рисунок Г.104. – Настройка расписания запуска контроля целостности