

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет информационных
технологий и электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

Специализация -

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПРАКТИКУМ ПО КОНТРОЛЮ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Студент Авдеев Владимир Александрович

Руководитель Липилин О.В.

Нормоконтролёр Егорова Н.А.

Рецензент ведущий инженер НПП «Рубин» Сидоров М.В.

Работа допущена к защите (протокол заседания кафедры от 16.06.23 № 10)

Заведующий кафедрой С.Л. Зефирова

Работа защищена с отметкой удовлетворительно (протокол заседания ГЭК

от 28.06.23 № 10)

Секретарь ГЭК А.П. Иванов

Проверено
8.06.23 27.06.23

Пенза 2023

Содержание

Введение.....	2
1 Обзор требований нормативно-правовых документов по контролю СЗИ.....	4
2 Обзор способов контроля с использованием СЗИ.....	11
3 Разработка структуры практикума.....	19
4 Разработка лабораторного стенда для проведения практикума.....	22
5 Разработка рекомендации по проведению практикума.....	23
6 Разработка вариантов заданий для проведения практикума.....	24
7 Составление методического пособия.....	25
7.1 Создание групп пользователей.....	25
7.2 Добавление дистрибутива для установки.....	31
7.3 Установка СЗИ от НСД с использованием заданий установки.....	39
7.4 Настройка параметров сервера безопасности.....	46
7.5 Настройка групповой политики.....	58
7.6 Настройка подсистемы контроля устройств.....	78
7.7 Предоставление доступа к устройствам.....	88
7.8 Настройка прав пользователей на доступ к устройству.....	107
7.9 Утверждение аппаратной конфигурации.....	119
7.10 Настройка механизма контроля целостности.....	121
7.11 Проверка заданий контроля целостности.....	137
7.12 Настройка механизма замкнутой программной среды.....	146
7.13 Формирование замкнутой программной среды.....	148
7.14 Мониторинг в СЗИ Secret Net Studio.....	167
7.15 Анализ сообщений о тревогах, анализ событий в журналах, квितिование тревог.....	173
7.16 Группы наблюдения.....	188
7.17 Выявление изменений аппаратной конфигурации.....	190
7.18 Контроль функционирования защитных подсистем.....	193
7.19 Контроль назначения ролей эксплуатационного персонала.....	196

7.20	Контроль установки СЗИ от НСД на СВТ.....	199
7.21	Общие сведения о подсистеме регистрации событий.....	200
7.22	Управление доступом к журналам регистрации событий.....	202
7.23	Настройка регистрации событий.....	208
7.24	Работа с журналом регистрации событий.....	211
8	Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	236
	Список используемых источников.....	238
	Заключение.....	240

Введение

Актуальность темы применения средств защиты информации от несанкционированного доступа непрерывно возрастает в современном информационном обществе. Вместе с развитием информационных технологий и сетевых коммуникаций угрозы, связанные с незаконным доступом к информации, становятся все более серьезными и разнообразными. Организации, владеющие ценной информацией, сталкиваются с необходимостью обеспечения эффективного контроля и защиты своих данных.

Целью данной выпускной квалификационной работы является разработка и практическая реализация практикума по контролю применения средств защиты информации от несанкционированного доступа. Основной задачей работы является исследование существующих методов и технологий, анализ их применимости в конкретных условиях и разработка практических рекомендаций по эффективному использованию средств защиты информации.

Актуальность данного исследования обусловлена необходимостью защиты информации от угроз, связанных с несанкционированным доступом. Несанкционированный доступ к информации может привести к серьезным последствиям, таким как утечка коммерческой информации, нарушение правил конфиденциальности, финансовые потери и повреждение репутации организации. Поэтому разработка эффективных методов контроля применения средств защиты информации является важным аспектом информационной безопасности.

В рамках данного исследования будет проведен обзор существующих средств защиты информации, анализ их преимуществ и недостатков, а также определены наиболее подходящие средства и методы для применения в конкретных условиях. На основе проведенного анализа будет разработан практикум, включающий набор рекомендаций и практических руководств по контролю применения средств защиты информации от несанкционированного доступа.

Ожидается, что результаты данного исследования и разработанный практикум будут полезными для организаций, занимающихся обработкой и хранением информации, а также для специалистов в области информационной безопасности, которые заинтересованы в обеспечении эффективной защиты своих данных от несанкционированного доступа.

1 Обзор требований нормативно-правовых документов по контролю СЗИ

Целью анализа нормативных документов по контролю средств защиты информации является изучение правил и процедур контроля за использованием средств защиты информации, определение соответствия этих средств установленным стандартам и требованиям.

Основными нормативными документами являются Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральный закон от 21 июля 2014 года № 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части совершенствования правового регулирования в области защиты информации" и Закон Российской Федерации от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг"[1].

Основными стандартами ISO, связанных с контролем за применением средств защиты информации, включают ISO/IEC 27001:2013 "Информационная технология. Техника безопасности. Системы менеджмента информационной безопасности. Требования", который определяет требования к системам менеджмента информационной безопасности, а также ISO/IEC 27002:2013 "Информационная технология. Техника безопасности. Практические рекомендации по управлению информационной безопасностью", который содержит рекомендации по управлению рисками, управлению активами и другим аспектам безопасности информации [2].

Описание требований Федерального закона № 149-ФЗ.

Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации" был принят 27 июля 2006 года. Он устанавливает требования к защите информации, а также определяет основные понятия в области защиты информации.

Закон устанавливает обязательные требования к организациям, которые обрабатывают информацию. Эти требования включают защиту информации и ее конфиденциальности, создание и обеспечение безопасности информационных

систем, а также проведение аудита информационной безопасности.

В соответствии с законом организации должны разрабатывать и внедрять политику безопасности информации, включая управление доступом, управление рисками и защиту от вредоносного программного обеспечения. Организации должны также обеспечивать физическую защиту информации и принимать меры для обеспечения конфиденциальности информации [3].

Описание требований Федерального закона № 242-ФЗ.

Федеральный закон № 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части совершенствования правового регулирования в области защиты информации" был принят 21 июля 2014 года. Этот закон ужесточил требования к контролю за применением средств защиты информации.

В соответствии с законом организации должны проводить анализ угроз и уязвимостей информационных систем, разрабатывать планы мероприятий по обеспечению безопасности информации и реагированию на инциденты, а также проводить систематический мониторинг и анализ эффективности принятых мер.

Описание требований Закона Российской Федерации № 210-ФЗ.

Закон Российской Федерации № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" был принят 27 июля 2010 года. Этот закон устанавливает требования к организациям, которые обрабатывают персональные данные граждан при предоставлении государственных и муниципальных услуг.

В соответствии с законом организации должны обеспечивать безопасность персональных данных граждан, а также защиту от несанкционированного доступа к ним. Организации должны разрабатывать и внедрять меры по защите персональных данных, включая управление доступом, управление рисками и защиту от вредоносного программного обеспечения [4].

Описание требований стандартов ISO/IEC 27001 и ISO/IEC 27002.

Стандарт ISO/IEC 27001 устанавливает требования к системам управления информационной безопасностью (СУИБ), которые организации должны

применять для защиты своей информации. Он определяет процессы управления рисками и защитой информации, включая управление доступом, управление конфигурацией, управление рисками и управление инцидентами.

Стандарт ISO/IEC 27002 представляет собой руководство по реализации СУИБ, основанное на требованиях стандарта ISO/IEC 27001. Он содержит рекомендации по применению мер по защите информации, включая управление доступом, управление рисками и управление конфигурацией.

В соответствии с этими стандартами организации должны разрабатывать и внедрять систему управления информационной безопасностью, включая процессы управления рисками, мониторинга и анализа эффективности мер по защите информации, а также управления инцидентами. Организации также должны обеспечивать физическую защиту информационных систем и принимать меры для обеспечения конфиденциальности информации.

В настоящее время в области защиты информации одним из ключевых аспектов является эффективность контроля за применением средств защиты информации. Для оценки эффективности контроля существует множество методик, которые основаны на разных подходах и принципах.

Первой методикой является методика оценки уровня информационной безопасности (МОУИБ), разработанная Федеральной службой безопасности России. Данная методика позволяет оценить уровень безопасности информационной системы по 9 критериям, таким как защита от несанкционированного доступа, сохранность информации, отказоустойчивость системы и другие.

Второй методикой является методика оценки эффективности защиты информации (МОЭЗИ), разработанная Государственной корпорацией по атомной энергии «Росатом» и основанная на методике ISO/IEC 27001. Она позволяет оценить эффективность защиты информации по 12 критериям, таким как управление информационной безопасностью, управление доступом, криптографическая защита и другие.

Третьей методикой является методика оценки уровня информационной

безопасности объекта (МОУИБ-О), также разработанная Федеральной службой безопасности России. Она позволяет оценить уровень безопасности конкретного объекта по 12 критериям, таким как защита от внешних угроз, управление доступом, криптографическая защита и другие.

Четвертой методикой является методика оценки эффективности защиты информации в системе управления предприятием (МОЭЗИ-СУП), разработанная Национальным институтом стандартов и технологий США. Она основана на методике ISO/IEC 27001 и позволяет оценить эффективность защиты информации в системе управления предприятием по 14 критериям, таким как управление рисками, управление доступом, управление конфигурацией и другие.

Кроме того, существуют и другие методики оценки эффективности контроля за применением средств защиты информации, например, методика оценки уровня зрелости системы управления информационной безопасностью (МОУЗСУИБ), методика оценки информационной безопасности систем автоматизированного управления технологическими процессами (МОИБ САУ ТП) и др.

Для оценки эффективности контроля за применением средств защиты информации необходимо проводить анализ в соответствии с нормативными требованиями.

В целом, выбор методики оценки эффективности контроля за применением средств защиты информации зависит от конкретных целей и задач оценки, а также от требований нормативных документов и стандартов в области информационной безопасности. При проведении оценки необходимо учитывать как позитивные, так и негативные аспекты каждой методики, а также определять необходимые квалификации эксперта для проведения оценки в соответствии с выбранной методикой.

Для проведения анализа эффективности контроля за применением средств защиты информации на основе нормативных требований необходимо учитывать требования соответствующих законодательных и нормативных актов, таких как

Федеральный закон № 149-ФЗ, которые определяют необходимые меры по защите информации и конфиденциальности.

Одним из основных критериев эффективности контроля за применением средств защиты информации является выполнение требований по защите информации и ее конфиденциальности. Для этого необходимо проводить мероприятия по защите информации, такие как установка средств защиты информации (Антивирусов, фаерволов, средств криптографической защиты и т.д.), обеспечение безопасности хранения и передачи информации, а также обучение сотрудников правилам и процедурам работы с информацией.

Кроме того, для оценки эффективности контроля необходимо проводить регулярный аудит информационной безопасности, который позволяет выявлять уязвимости и риски в системе защиты информации, а также определять необходимость внесения изменений в существующую систему защиты.

Важным критерием является также создание и обеспечение безопасности информационных систем. Для этого необходимо проводить регулярное обновление и улучшение средств защиты информации, мониторинг состояния системы, а также установку правил доступа к информации и контроль за их соблюдением.

Проведение анализа эффективности контроля за применением средств защиты информации на основе нормативных требований позволяет оценить степень соответствия системы защиты информации требованиям законодательных и нормативных актов, а также выявить пробелы и недостатки в работе системы. Это позволяет улучшить систему защиты информации и повысить уровень ее эффективности.

На основе проведенного анализа эффективности контроля за применением средств защиты информации исходя из нормативных требований, можно выделить несколько рекомендаций для улучшения данного процесса:

- усиление обучения сотрудников по вопросам информационной безопасности, особенно в области управления паролями, защиты от фишинга и других социальных инженерных атак, а также правилам обработки и хранения

конфиденциальной информации;

- регулярная проверка соответствия информационной системы нормам и требованиям по защите информации, включая проверку наличия необходимых средств защиты, актуализации установленных правил доступа и управления информационной безопасностью;

- внедрение современных технологий защиты информации, таких как системы управления и мониторинга доступа, интеллектуальные системы обнаружения атак, средства криптографической защиты и другие;

- организация регулярных аудитов информационной безопасности для проверки соответствия контроля за применением средств защиты информации нормативным требованиям и выявления уязвимостей в системе защиты;

- создание единой информационной системы, которая позволит автоматизировать процесс контроля за применением средств защиты информации и обеспечит единый доступ к информации по всем направлениям защиты информации;

- внедрение системы непрерывного мониторинга за применением средств защиты информации, которая будет позволять оперативно выявлять и реагировать на нарушения в защите информации.

Улучшение контроля за применением средств защиты информации является важным шагом для обеспечения безопасности информационных систем и защиты конфиденциальных данных. Рекомендации, предложенные на основе анализа эффективности контроля и соответствия нормативным требованиям, помогут улучшить процесс контроля и повысить уровень защиты информации в организации.

В результате анализа нормативных документов по контролю за применением средств защиты информации были выявлены следующие основные критерии оценки эффективности контроля: защита от несанкционированного доступа, сохранность информации, отказоустойчивость системы, управление информационной безопасностью, управление доступом,

криптографическая защита и другие. Были проанализированы три методики оценки уровня информационной безопасности: МОУИБ, МОЭЗИ и МОУИБ-О, каждая из которых имеет свои особенности и позволяет оценить эффективность контроля по различным критериям.

На основе анализа были выявлены проблемы в контроле за применением средств защиты информации, такие как недостаточная оценка рисков, несоответствие требованиям безопасности при выборе и использовании средств защиты, отсутствие мониторинга и анализа защищаемой информации.

Для улучшения контроля за применением средств защиты информации были предложены следующие рекомендации: улучшение оценки рисков и выбора средств защиты, внедрение мониторинга и анализа защищаемой информации, обеспечение обучения и повышения квалификации персонала по вопросам информационной безопасности.

Таким образом, контроль за применением средств защиты информации является важным аспектом обеспечения информационной безопасности. Для повышения эффективности контроля необходимо учитывать требования нормативных документов и рекомендации по их применению.

2 Обзор способов контроля с использованием СЗИ

Контроль — это процесс установления соответствия действительного состояния объекта контроля его целям, задачам и требованиям. В контексте информационной безопасности контроль представляет собой систему мероприятий, направленных на обеспечение сохранности и конфиденциальности информации.

Средства защиты информации — это технические, программные или организационные меры, принимаемые для обеспечения безопасности информации и защиты от несанкционированного доступа, разглашения, модификации или уничтожения.

Рассмотрим способы контроля с использованием средств защиты информации.

Контроль доступа — это механизм, который используется для обеспечения безопасности информации путем управления доступом пользователей к конфиденциальной информации. Он определяет, кто может получить доступ к определенным ресурсам и какой уровень доступа будет предоставлен. Контроль доступа является важным элементом средств защиты информации и включает в себя различные методы и технологии.

Основными методами контроля доступа являются:

- аутентификация - процесс проверки подлинности пользователя. Это может быть достигнуто путем использования пароля, биометрических данных (например, отпечатков пальцев или распознавания лица) или аппаратных токенов;
- авторизация - процесс определения, какие действия пользователь может выполнять. Авторизация определяет, к каким ресурсам пользователь имеет доступ и какие операции он может выполнять с этими ресурсами;
- аудит — это процесс регистрации всех действий пользователей с системой. Он включает в себя запись событий, связанных с доступом к ресурсам, изменением конфигурации системы и других важных событий. Аудит

необходим для того, чтобы можно было отследить любые попытки несанкционированного доступа или изменения системы;

- управление правами доступа — это процесс управления правами пользователей и ресурсами. Он позволяет определить, какие пользователи имеют доступ к каким ресурсам и какие действия они могут выполнять с этими ресурсами;

- контроль доступа на основе ролей — это метод, который предоставляет доступ к ресурсам на основе роли пользователя. Роли определяют, какой уровень доступа может быть предоставлен определенным пользователям. Этот метод позволяет упростить управление доступом, так как администраторам не нужно назначать права доступа для каждого пользователя отдельно.

Контроль целостности данных – это процесс обеспечения сохранности информации и контроля за ее изменением. Он является одним из ключевых элементов защиты информации и обеспечивает целостность данных во время их передачи и хранения.

Основная цель контроля целостности данных заключается в обеспечении сохранности информации от изменений, а также в обнаружении и предотвращении несанкционированных изменений. Для этого используются различные методы, включая аппаратные и программные средства.

Среди методов контроля целостности данных можно выделить следующие:

- хэширование данных – это процесс преобразования исходных данных в хэш-код, который служит для проверки целостности данных. При изменении данных хэш-код также изменяется, что позволяет обнаружить несанкционированные изменения;

- цифровые подписи – это метод, который позволяет подтвердить авторство и целостность данных. Цифровая подпись гарантирует, что данные не были изменены после создания подписи, а также позволяет проверить подлинность автора данных;

- контроль доступа – это метод, который ограничивает доступ к данным только уполномоченным пользователям. Он позволяет предотвратить несанкционированный доступ к данным и обеспечить их сохранность;

- мониторинг системы – это метод, который позволяет отслеживать изменения в системе и обнаруживать необычную активность. Мониторинг может быть настроен на определенные события и предупреждать о любых подозрительных изменениях.

В целом, контроль целостности данных является важной составляющей защиты информации, так как позволяет обеспечить сохранность данных и защитить их от несанкционированных изменений. Однако, для эффективного контроля целостности данных необходимо использовать несколько методов, а также следить за их правильной настройкой и функционированием.

Конфиденциальность информации — это возможность предотвращения несанкционированного доступа к информации и защиты ее от разглашения. Контроль конфиденциальности информации включает в себя средства и механизмы, которые обеспечивают защиту информации в процессе ее передачи, хранения и обработки.

Средства контроля конфиденциальности информации включают в себя криптографические методы, такие как шифрование данных и аутентификацию пользователей. Шифрование данных обеспечивает защиту информации путем преобразования данных в непонятную форму, которая может быть прочитана только с помощью ключа дешифровки. Аутентификация пользователей используется для проверки подлинности пользователей и обеспечения доступа только для авторизованных пользователей.

Другими методами контроля конфиденциальности информации являются управление доступом и контроль целостности данных. Управление доступом позволяет ограничить доступ к информации только для тех пользователей, которые имеют соответствующие разрешения. Контроль целостности данных позволяет обнаруживать любые изменения в данных и предотвращать несанкционированный доступ к информации.

Одним из современных методов контроля конфиденциальности информации является использование технологий блокчейн. Блокчейн представляет собой распределенную базу данных, в которой каждый блок содержит информацию о предыдущем блоке. Это обеспечивает надежную защиту информации путем ее шифрования и распределения на множество устройств, что делает невозможным несанкционированный доступ к информации.

В целом, контроль конфиденциальности информации является необходимым элементом защиты информации в любой системе. Современные технологии обеспечивают множество способов контроля конфиденциальности, что позволяет выбирать оптимальный вариант для каждой конкретной задачи.

Контроль целостности системы – это процесс проверки и поддержания целостности компьютерной системы и ее компонентов в целом. Целостность системы является одним из основных аспектов информационной безопасности, и ее нарушение может привести к серьезным последствиям, таким как потеря данных, нарушение работы приложений и систем, а также уязвимости для злоумышленников.

Для контроля целостности системы используются различные методы и средства, такие как:

- криптографические методы: шифрование данных, цифровые подписи, хэширование;
- антивирусные программы: сканирование системы на наличие вредных программ, обновление базы данных вирусов;
- файрволы: контроль доступа к системе и сети, фильтрация сетевого трафика;
- системы контроля целостности файлов: мониторинг изменений файловой системы, анализ хеш-сумм и сравнение с предыдущими версиями файлов;
- методы мониторинга: контроль изменений в системном журнале,

проверка наличия изменений в системных файлах;

– средства управления доступом: установление правил доступа к ресурсам, аутентификация пользователей и авторизация доступа к ресурсам.

Контроль целостности системы необходим для защиты компьютерной системы от целого ряда угроз, включая вредоносные программы, несанкционированный доступ и прочие угрозы. Он должен проводиться регулярно и с использованием современных методов и средств для обеспечения эффективной защиты системы.

Контроль доступности системы – это механизмы и процессы, обеспечивающие доступность информационной системы для пользователей в соответствии с установленными требованиями и ограничениями. Контроль доступности направлен на обеспечение доступности системы в течение требуемого времени и минимизации риска прерывания доступа к информации.

Одним из основных заданий контроля доступности является предотвращение и управление проблемами, которые могут привести к недоступности системы. Это могут быть технические сбои, атаки хакеров, ошибки персонала и т.д.

Для контроля доступности используются различные методы и технологии. Одним из ключевых элементов является резервирование. В случае отказа одного из компонентов системы, другой компонент может автоматически взять на себя работу, что обеспечивает непрерывность работы системы. Резервирование может быть реализовано как на уровне оборудования, так и на уровне программного обеспечения.

Еще одним важным элементом контроля доступности является мониторинг системы. Мониторинг позволяет отслеживать работу системы и выявлять возможные проблемы, такие как перегрузки, неисправности и др. На основе данных мониторинга можно принимать меры по устранению проблем до того, как они приведут к серьезным последствиям.

Также для обеспечения доступности системы применяются средства балансировки нагрузки, которые позволяют распределять нагрузку между

несколькими серверами или устройствами, что повышает эффективность использования ресурсов и обеспечивает непрерывность работы системы.

Для контроля доступности также используются средства защиты от DDoS-атак, так как такие атаки могут привести к перегрузке сети и недоступности системы.

В целом, контроль доступности системы является важным элементом обеспечения безопасности информации и требует постоянного мониторинга и обновления технологий и методов для обеспечения надежности работы системы.

Контроль безопасности устройств является важной частью обеспечения безопасности информации. Это включает в себя контроль аппаратных средств, таких как компьютеры, мобильные устройства, роутеры и другие устройства, которые могут хранить или обрабатывать информацию. Контроль безопасности устройств помогает предотвратить несанкционированный доступ к устройствам, защитить их от вредоносных программ и других угроз безопасности.

Существует несколько способов контроля безопасности устройств:

- пароли и аутентификация. Это меры безопасности, которые позволяют убедиться в том, что пользователь является тем, за кого себя выдает. Они обеспечивают доступ к устройству только авторизованным пользователям, что защищает его от несанкционированного доступа;

- обновления и патчи. Обновления программного обеспечения устройств содержат исправления ошибок и уязвимостей, которые могут быть использованы злоумышленниками. Важно регулярно обновлять устройства и устанавливать последние версии программного обеспечения;

- контроль доступа к устройству. Контроль доступа к устройству может включать в себя различные методы, такие как физические ограничения, а также настройки безопасности на уровне программного обеспечения;

- шифрование данных. Шифрование данных помогает защитить данные, хранимые на устройстве, от несанкционированного доступа.

Шифрование можно использовать как на уровне устройства, так и на уровне файлов и папок;

- антивирусные программы. Антивирусные программы обнаруживают и удаляют вирусы и другие вредоносные программы, которые могут попасть на устройство и угрожать безопасности информации.

- фаерволы. Фаерволы помогают защитить устройство от несанкционированных сетевых подключений и атак, блокируя нежелательный трафик и проверяя входящие и исходящие соединения.

В целом, контроль безопасности устройств — это важный элемент в обеспечении безопасности информации и защите от угроз. Важно использовать несколько методов контроля безопасности, чтобы обеспечить максимальную защиту устройства и информации, которая на нем хранится.

3 Разработка структуры практикума

Структура практикума состоит из следующих этапов:

- создание групп пользователей;
- добавление дистрибутива для установки;
- установка СЗИ от НСД с использованием заданий установки;
- настройка параметров сервера безопасности;
- настройка групповой политики;
- настройка подсистемы контроля устройств;
- предоставление доступа к устройствам;
- настройка прав пользователей на доступ к устройству;
- утверждение аппаратной конфигурации;
- настройка механизма контроля целостности;
- проверка заданий контроля целостности;
- настройка механизма замкнутой программной среды;
- формирование замкнутой программной среды;
- мониторинг в СЗИ Secret Net Studio;
- анализ сообщений о тревогах, анализ событий в журналах, квитирование тревог;
- группы наблюдения;
- выявление изменений аппаратной конфигурации;
- контроль функционирования защитных подсистем;
- контроль назначения ролей эксплуатационного персонала;
- контроль установки СЗИ от НСД на СВТ;
- общие сведения о подсистеме регистрации событий;
- управление доступом к журналам регистрации событий;
- настройка регистрации событий;
- работа с журналом регистрации событий.

4 Разработка лабораторного стенда для проведения практикума

Для проведения практикума по контролю применения СЗИ от НСД был разработан лабораторный стенд. Для удобства и простоты развертывания лабораторного стенда он был реализован в виде виртуальных машин. В качестве средства виртуализации было использовано программное обеспечение Oracle VirtualBox. Данное средство виртуализации возможно использовать с операционными системами семейства Linux и Windows.

Для проведения практикума необходимо использовать несколько виртуальных машин для обеспечения сетевого взаимодействия между компонентами подсистемы СЗИ от НСД.

Первая виртуальная машина предназначена для использования в качестве сетевого сервера управления СЗИ. В качестве сетевого центра управления был выбран Сервер безопасности Secret Net Studio версии 8.8 (далее – SNS), поскольку эта версия является сертифицированной на момент разработки практикума. Требования к функционированию SNS включают наличие установленных компонентов, таких как система управления базами данных, почтовый сервер и необходимые компоненты для функционирования графической консоли управления. Исходя из требований в качестве операционной системы первой виртуальной машины была использована Windows Server 2012 R2, в состав которой входят компоненты «Центр управления Secret Net Studio версии 8.8», «Сервер безопасности Secret Net Studio», «Сервер безопасности *Kaspersky Security Center*», «Консоль управления *Kaspersky Security Center*».

Разработанная виртуальная машина имеет следующие настройки:

- тип операционной системы – Windows;
- вид операционной системы – Windows Server 2012 R2;
- разрядность операционной системы – 64 бита;
- объем виртуальной оперативной памяти – 2048 Мб;
- объем виртуального жесткого диска – 40 Гб;

- тип жесткого диска – неизменяемый;
- название устройства – SNSServ23New;
- тип виртуальной локальной сети – внутренняя сеть;
- общий сетевой ресурс виртуальной машины – \\VBOXSRV\Share.

Вторая виртуальная машина предназначена для установки клиента управления СЗИ.

Разработанная виртуальная машина имеет следующие настройки:

- тип операционной системы – Windows;
- вид операционной системы – Windows 10;
- разрядность операционной системы – 64 бита;
- объем виртуальной оперативной памяти – 2048 Мб;
- объем виртуального жесткого диска – 40 Гб;
- тип жесткого диска – неизменяемый;
- название устройства – SNS-Client 1;
- тип виртуальной локальной сети – внутренняя сеть;
- общий сетевой ресурс виртуальной машины – \\VBOXSRV\Share.

Для обеспечения взаимодействия виртуальных машин по сети используются виртуальные сетевые интерфейсы, сетевые настройки которых позволяют осуществлять взаимодействие по протоколам TCP и UDP.

Виртуальный стенд состоит из двух виртуальных машин:

SNS-Server.SNS.local – выполняет функции контроллера домена SNS.local, установлен Сервер безопасности Secret Net Studio 8.8 и Центр управления. Созданы две группы SecretNetAdmin_Domain и SecretNetAdmin_Forest. В настройках групповой политики отключены параметры проверки паролей на сложность. Для пользователей домена удален из меню раздел «Завершение работы» (выключение, выход, перезагрузка только через команды). Учетная запись Администратор с паролем P@ssw0rd

SNS-Client.SNS.local – выполняет функции защищаемого компьютера.

UML – диаграмма лабораторного стенда при проведении практикума показана на рисунке 1.

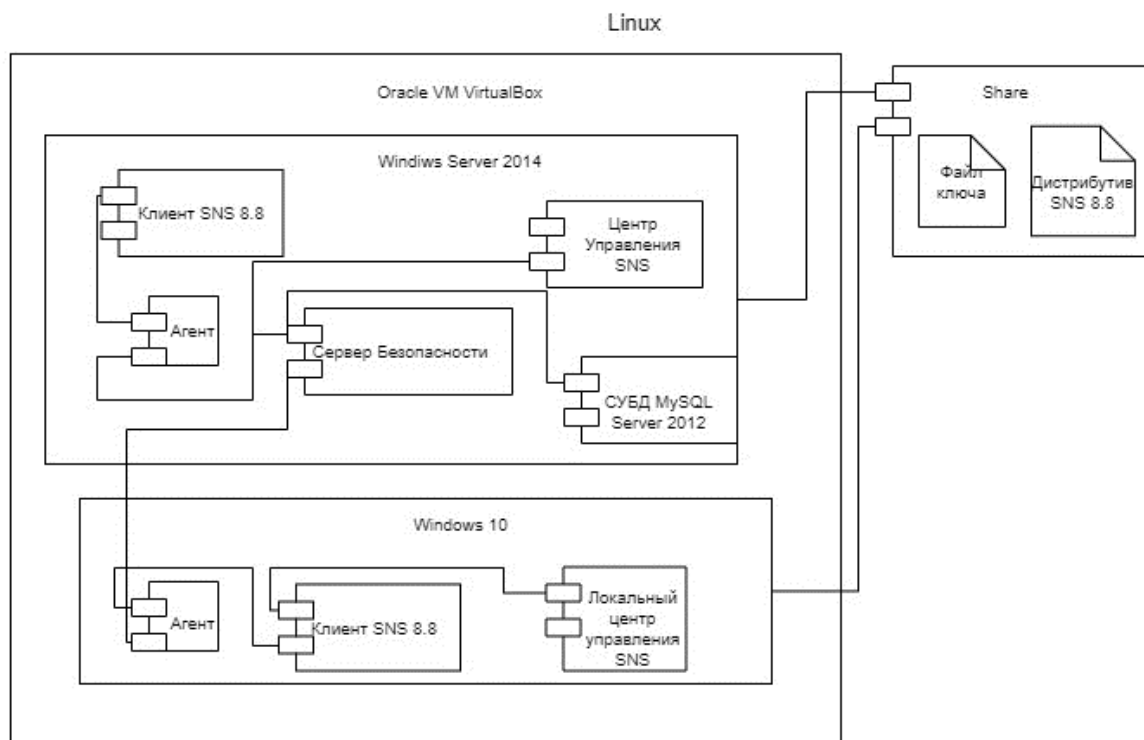


Рисунок 1 – UML диаграмма лабораторного стенда

UML – диаграмма вариантов использования лабораторного стенда при проведении практикума показана на рисунке 2.

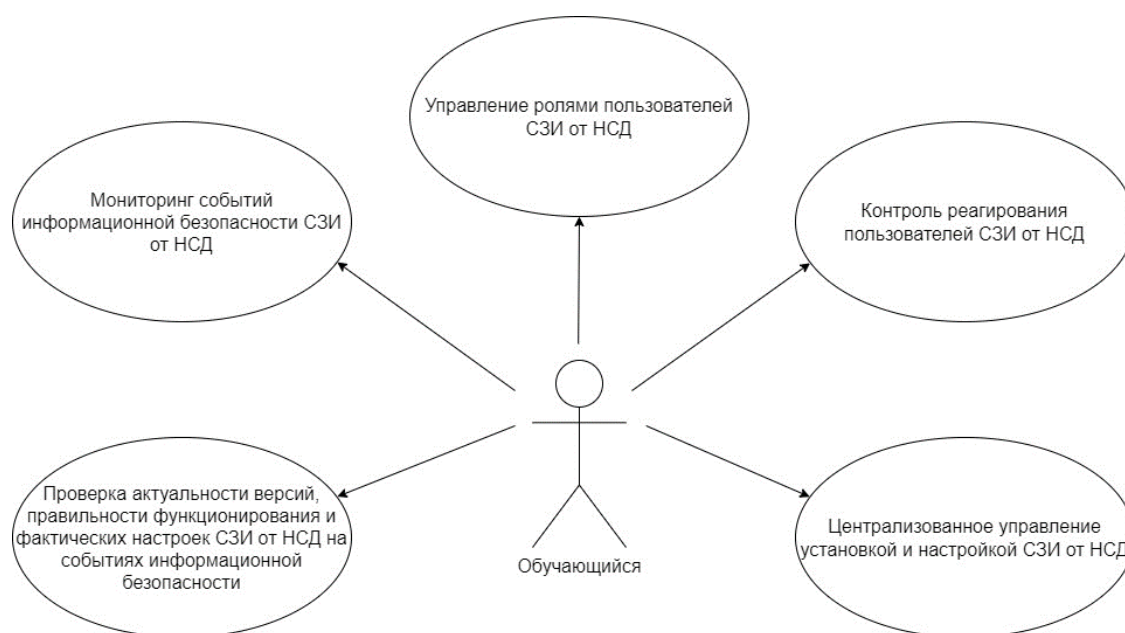


Рисунок 2 – UML-диаграмма вариантов использования лабораторного стенда при проведении практикума

5 Разработка рекомендации по проведению практикума

Разработанный лабораторный практикум можно использовать для работы студентов при очной и заочной формах обучения.

Для студентов очного отделения предполагается самостоятельное выполнение лабораторных работ в учебной аудитории под руководством преподавателя. На начальных этапах преподаватель проводит вводный инструктаж, в ходе которого студенты осмысливают сущность предстоящей работы, а также последовательность её выполнения. В течении всего занятия преподаватель наблюдает за ходом выполнения работы, консультирует студентов по возникающим вопросам, оценивает результаты их деятельности и выставляет итоговую оценку после выполнения студентом всех предусмотренных заданий. Студенты выполняют полученные задания, в случае необходимости обращаясь за помощью педагогу.

6 Разработка вариантов заданий для проведения практикума

Были разработаны варианты заданий для проведения практикума, включающие набор значений настроек СЗИ от НСД, перечень пользователей и ролей пользователей. Результат представлен в таблице 1.

Таблица 1 – Варианты заданий, перечень пользователей и ролей пользователей

Вход в систему и журнал		Время ожидания						Размер блока		Пользователи и их роли				
Максимальный период неактивности до блокировки экрана	Максимальный размер журнала системы защиты	Разрешения имен DNS	Соединения с сервером	Отправки запроса на сервер	Окончания передачи следующего блока	События для рабочей станции	Сервером ответа на контрольный запрос	Для приема данных от сервера	Для передачи данных на сервер	User1	User2	User3	User4	Администратор
5	2386	50	60	50	60	50	60	1024	1024	Пользователь с ограниченными правами доступа	Пользователь с ограниченными правами доступа	Пользователь с ограниченными правами доступа	Пользователь с ограниченными правами доступа	Администратор
6	3008	51	59	51	59	51	59	1048	1048					
7	3136	52	58	52	58	52	58	1072	1072					
8	3264	53	57	53	57	53	57	1096	1096					
9	3648	54	56	54	56	54	56	1120	1120					
10	4416	55	55	55	55	55	55	1144	1144					
11	4800	56	54	56	54	56	54	1168	1168					
12	5696	57	53	57	53	57	53	1192	1192					
13	5952	58	52	58	52	58	52	1216	1216					
14	6080	59	51	59	51	59	51	1240	1240					
15	6528	60	50	60	50	60	50	1264	1264					

7 Составление методического пособия

7.1 Создание пользователей и групп

Запустите виртуальные машины. Переключитесь к окну виртуальной машины SNS-Server. Нажмите сочетание клавиш правый Ctrl и Del. Войдите под учетной записью SNS\Администратор с паролем P@ssw0rd.

Создадим пользователей и группы, необходимые для выполнения работы.

В «Диспетчере сервера» выберите «Средства» - «Пользователи и компьютеры Active Directory» (рисунок 3).

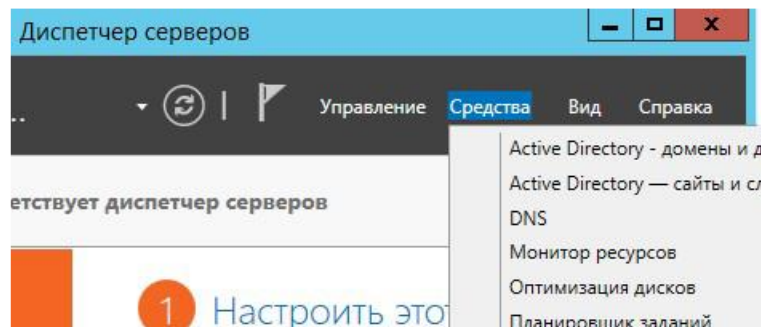


Рисунок 3 – Меню «Средства»

Выберите в дереве консоли в левой части окна узел «Users», нажмите на нем правой кнопкой мыши. В контекстном меню узла последовательно выберите пункты «Создать» - «Группа» (рисунок 4).

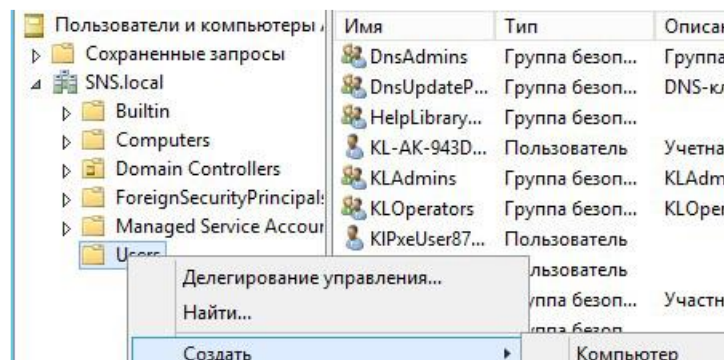


Рисунок 4 – Создание новой группы

В окне «Новый объект – Группа» в поле «Имя группы:» введите название группы SPOAdmins (рисунок 5) и нажмите ОК. Созданная группа появится в левой части окна в перечне пользователей и групп. Добавьте аналогичным образом группу Auditors. Помимо созданных групп в практической работе будут использоваться группы SecretNetAdmin_Domain и SecretNetAdmin_Forest, которые были созданы ранее перед установкой сервера безопасности.

Новый объект - Группа

Создать в: SNS.local/Users

Имя группы:
SPOAdmins

Имя группы (пред-Windows 2000):
SPOAdmins

Область действия группы

- ☐ Локальная в домене
- ☒ Глобальная
- ☐ Универсальная

Тип группы

- ☒ Группа безопасности
- ☐ Группа распространения

Рисунок 5 – Создание группы SPOAdmins

На следующем шаге создайте пользователей. Для этого в контекстном меню контейнера Users выберите последовательно пункты «Создать» - «Пользователь». В окне «Новый объект – Пользователь» в поле «Имя входа пользователя:» введите имя учетной записи user1 (рисунок 6).

Остальные поля заполните произвольно. Нажмите «Далее». На следующей вкладке задайте пользователю пароль. Снимите флаг «Требовать смены пароля при следующем входе в систему» (параметр отключен для упрощения выполнения практического задания) (рисунок 6). Нажмите «Далее». В следующей вкладке отобразится информация о создаваемом пользователе. Нажмите кнопку «Готово». Созданный пользователь появится в списке объектов контейнера Users. Аналогичным образом создайте пользователей user2 и user3.

Рисунок 6 – Создание нового пользователя

Разрешим созданным пользователям локальный вход на сервер безопасности. Нажмите клавиши Win и R, введите gpmmc.msc и нажмите Enter (рисунок 7).

Рисунок 7 – Открытие «Управление групповой политикой»

В окне «Управление групповой политикой», раскройте последовательно узлы «Лес: SNS.local – SNS.local – Domain Controllers». Выберите «Default Domain Controllers Policy», в контекстном меню выберите пункт «Изменить...» (рисунок 8).

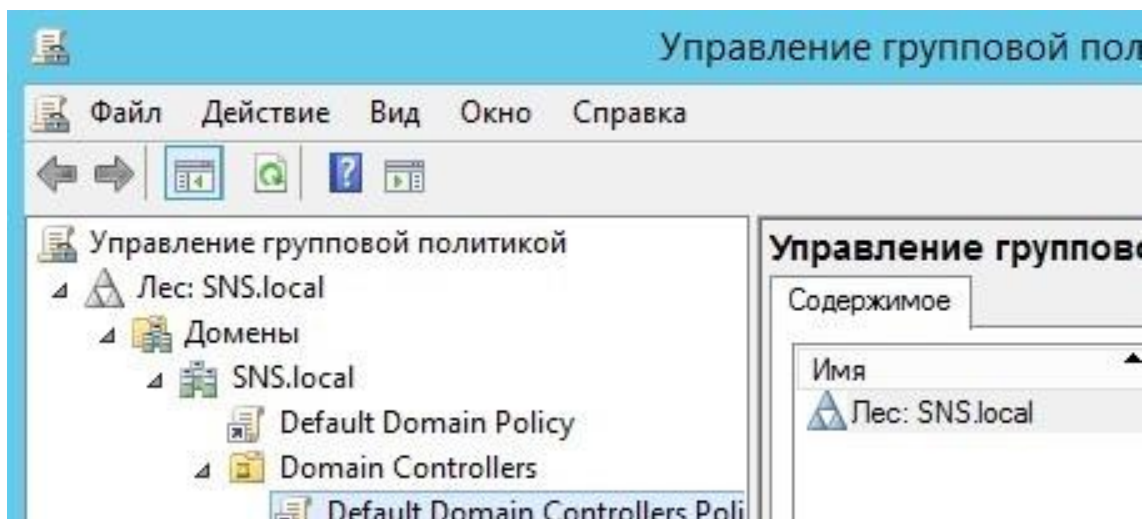


Рисунок 8 – Окно «Управление групповой политики»

Раскройте последовательно узлы «Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности – Локальные политики» и выберите узел «Назначение прав пользователей». В правой части консоли выберите политику «Локальный вход в систему» и в контекстном меню политики выберите пункт «Свойства» (рисунок 9).

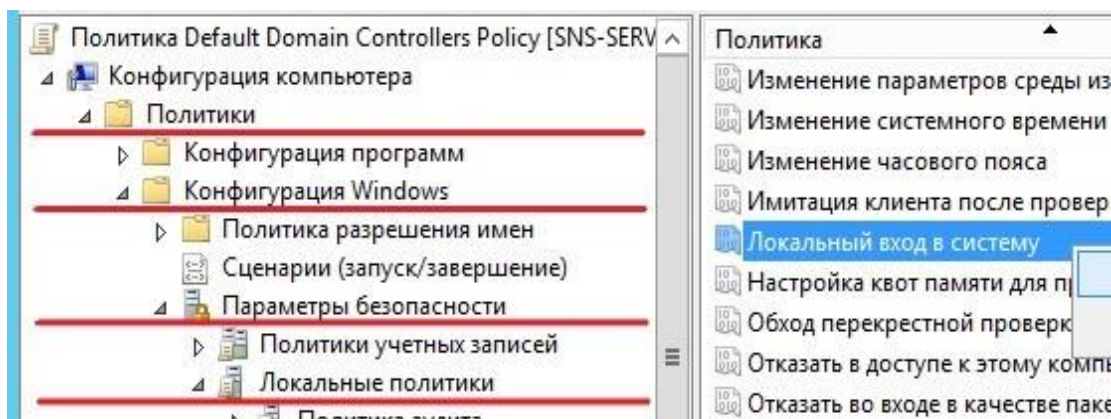


Рисунок 9 – Свойства «Назначение прав пользователей»

В окне свойств нажмите кнопку «Добавить пользователя или группу» (рисунок 10).

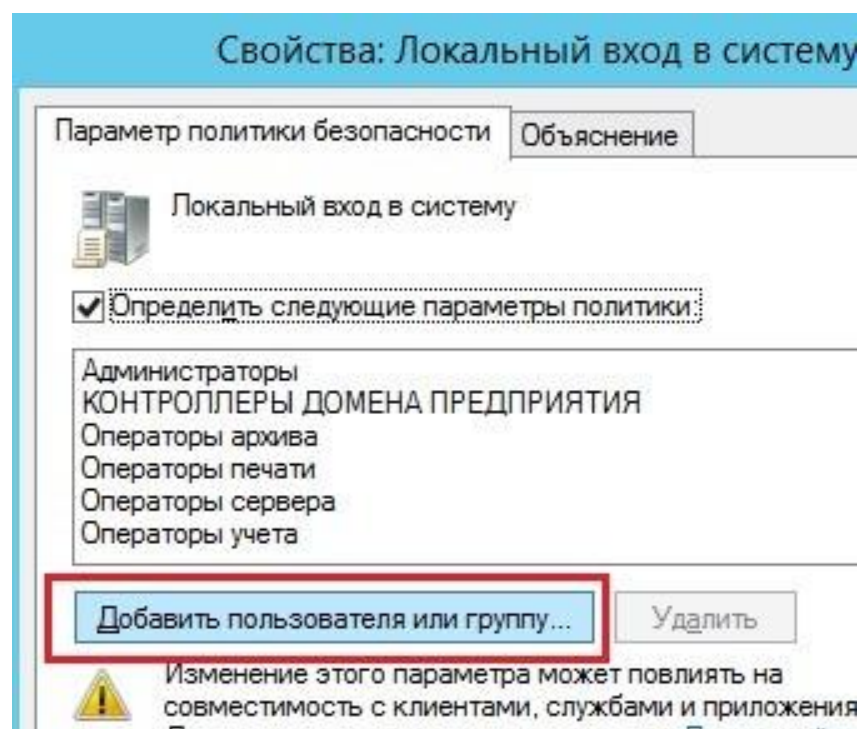


Рисунок 10 – Меню свойств

Введите имена пользователей user1; user2; user3 (разделяя имена пользователей точкой с запятой) и нажмите «ОК» (рисунок 11).

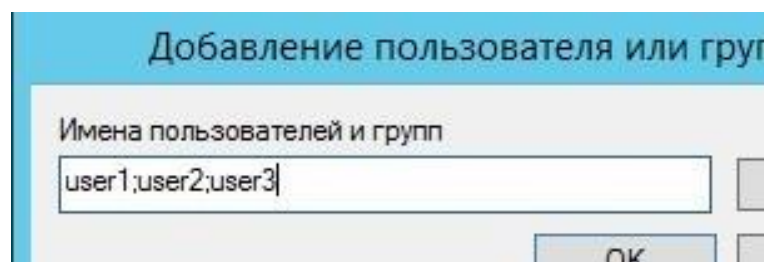


Рисунок 11 – Добавление пользователей

Пользователи добавятся в список. Нажмите кнопку «ОК» в окне свойств политики. Закройте окно Редактора и окно Управления групповыми политиками. Нажмите клавиши Win и R. Введите команду `groupdate /force` и нажмите клавишу Enter (рисунок 12). Дождитесь завершения обновления групповых политик.

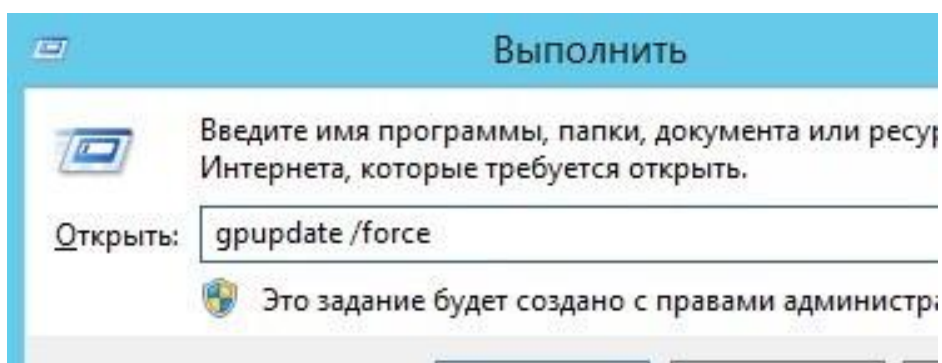


Рисунок 12 – Обновление групповых политик

7.2 Добавление дистрибутива для установки

На сервере безопасности запустите программу «Центр управления». Для этого нажмите кнопку «Пуск», нажмите круглую кнопку с пиктограммой «стрелка вниз», выберите раздел «Код безопасности», нажмите правой кнопкой на «Центр управления» и выберите в контекстном меню «Открыть расположение файла» (рисунок 13).

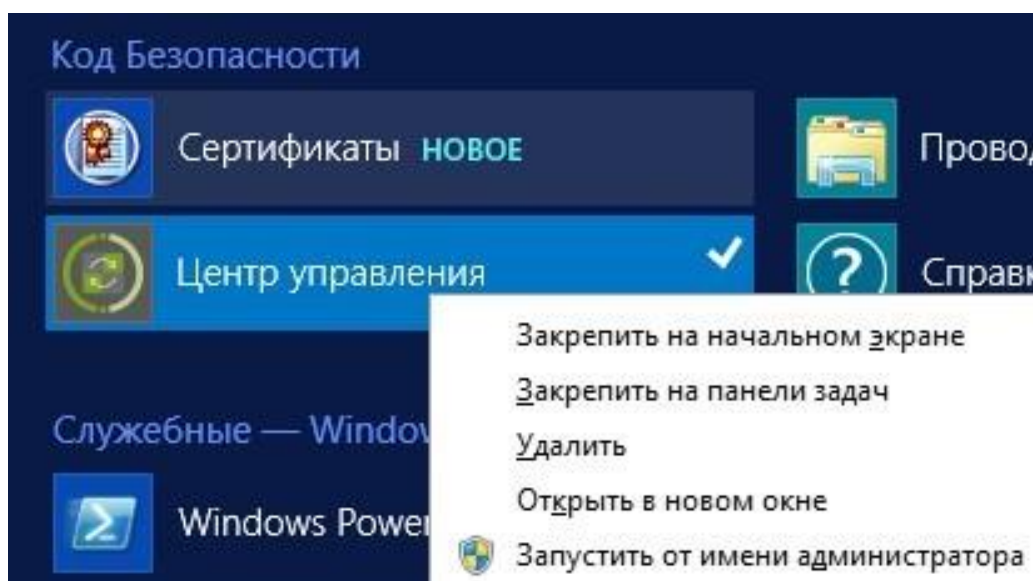


Рисунок 13 – Открытие ярлыка в папке

Зажмите левой кнопкой мыши ярлык «Центр управления» и переместите его на рабочий стол (рисунок 14). Закройте окно Проводника и запустите Центр управления.

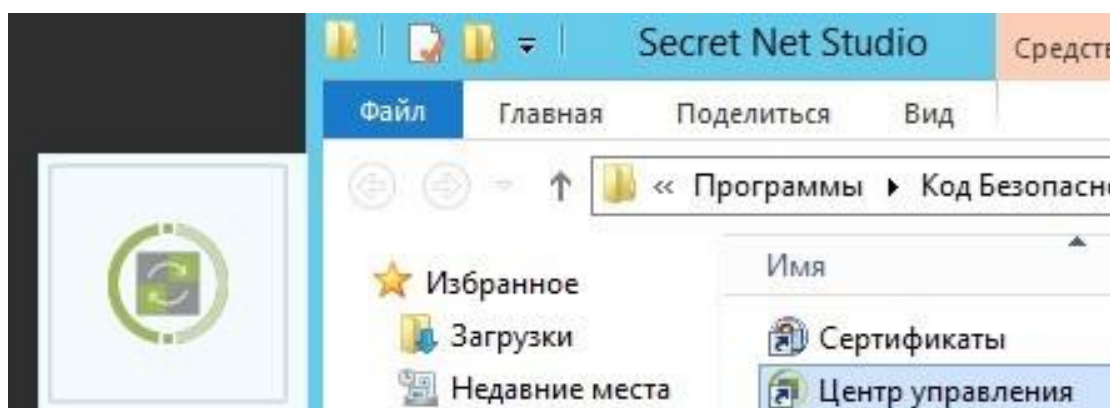


Рисунок 14 – Запуск «Центра управления»

Отобразится стартовое окно программы «Центр управления», в поле «Выберите сервер безопасности:» выберите SNS-Server.SNS.local (или введите, если название сервера не отображается) и нажмите «Подключиться» (рисунок 15).

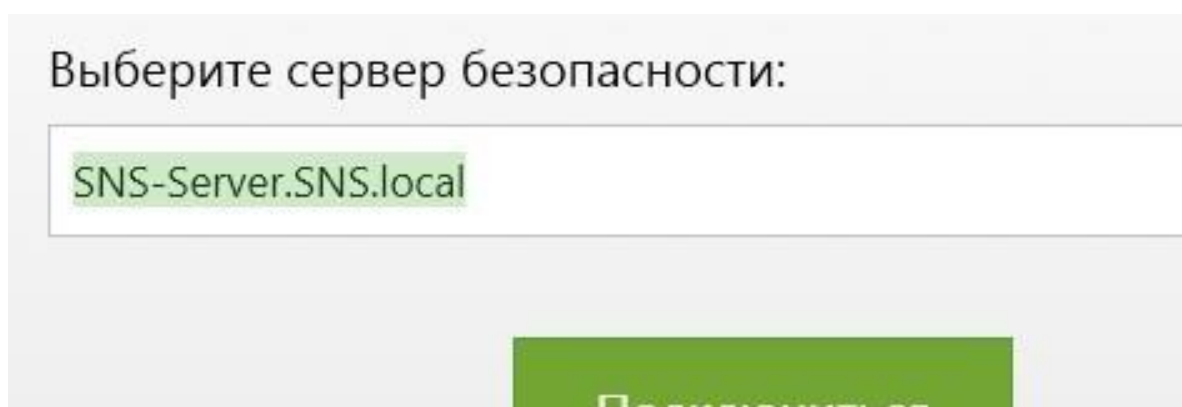


Рисунок 15 – Выбор сервера безопасности и подключение к «Центру управления»

После подключения программы «Центр управления» к серверу безопасности отобразится окно с предложением перейти к разворачиванию компонентов системы защиты. Нажмите кнопку «Начать работу» (рисунок 16).

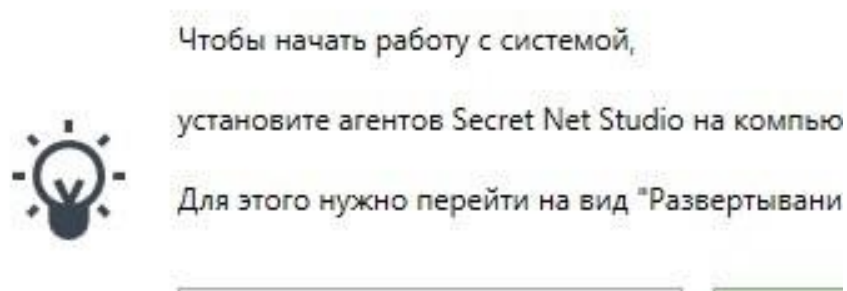


Рисунок 16 – Развертывание компонентов

В главном окне программы отобразится панель «Статистика», в которой отображается информация о тревогах различного уровня и основных ошибках.

Перейдите на панель «Компьютеры», нажав пиктограмму в левой части экрана (рисунок 17).



Рисунок 17 – Панель «Компьютеры»

На панели отображаются объекты управления, которыми управляет сервер безопасности, и их структура. Для панели «Компьютеры» предусмотрены следующие режимы отображения объектов управления:

- «Диаграмма» – режим предназначен для отображения в графическом виде сведений о структуре объектов управления (рисунок 18);
- «Таблица» – режим предназначен для вывода иерархического списка объектов управления в табличном виде, панель открывается по умолчанию в этом режиме (рисунок 18).

Переключение вида осуществляется соответствующими кнопками, выделенными на рисунке 18.

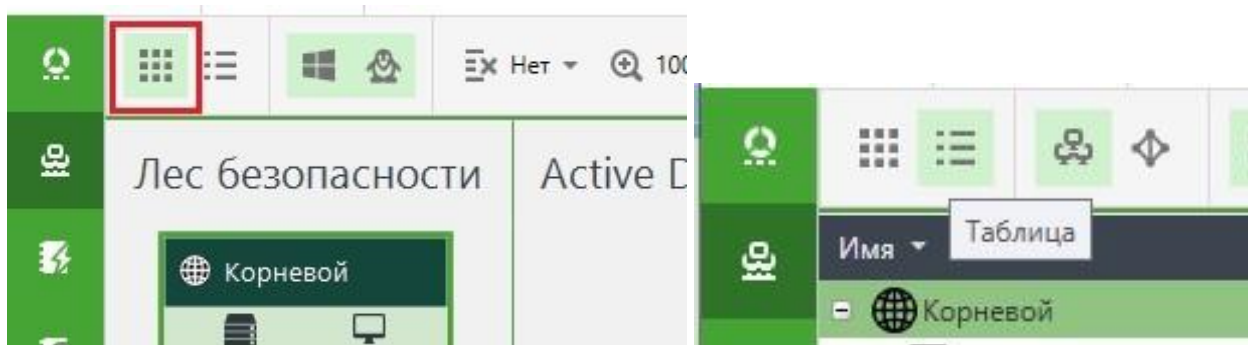


Рисунок 18 – Переключение вида панели «Компьютеры»

Перейдите на панель «Журналы тревог» (рисунок 19). В ней содержатся средства загрузки записей журнала событий тревоги.

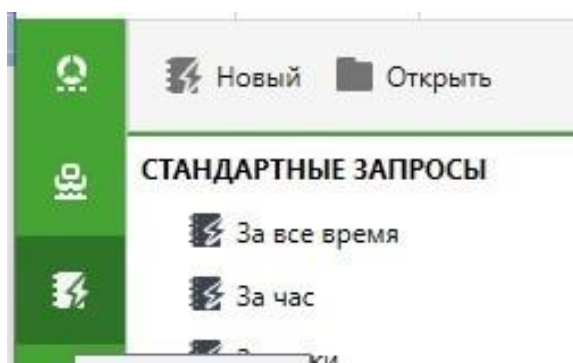


Рисунок 19 – Панель «Журнал тревог»

Перейдите на панель «Журналы станций» (рисунок 20). Панель предназначена для работы с журналами защищаемых компьютеров.

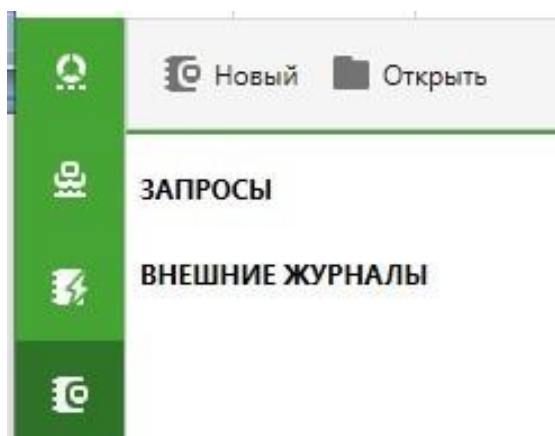


Рисунок 20 – Панель «Журнал станций»

Перейдите на следующую панель «Журналы сервера». В ней содержатся инструменты для работы с журналами сервера безопасности. Панель «Архивы» предназначена для работы архивами журналов.

Перейдите к панели «Отчеты» (рисунок 21). В ней формируются отчеты для сбора сведений о состоянии и конфигурации компонентов системы защиты на управляемых компьютерах.

Просмотрите назначение отчетов «Программы и компоненты», «Ресурсы АРМ», ПАК «Соболь» и «Электронные идентификаторы».

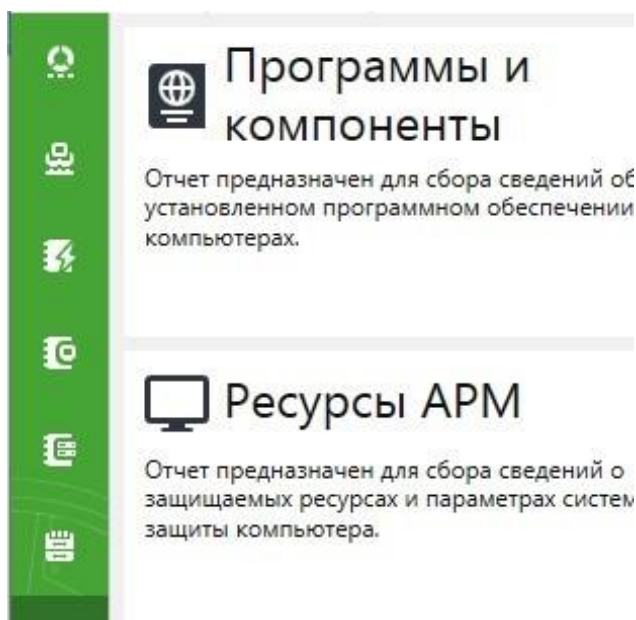


Рисунок 21 – Панель «Отчеты»

Перейдите к панели «Развертывание». Отобразится всплывающее окно с предложением добавить дистрибутив, нажмите «Продолжить» (рисунок 22).

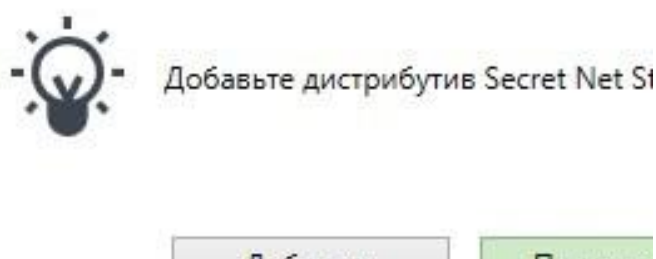


Рисунок 22 – Панель «Развертывание»

Откроется панель «Развертывание». На вкладке «Развертывание» отобразится структура управления – список компьютеров домена с параметрами системы защиты от НСД. В левой части окна отображаются названия доменов, в правой части отображается список компьютеров. В левой части окна нажмите кнопку «SNS» (рисунок 23). Список компьютеров очистится, поскольку ни на

один компьютер еще не установлено средство защиты. Нажмите кнопку «Все» для отображения полного списка устройств.

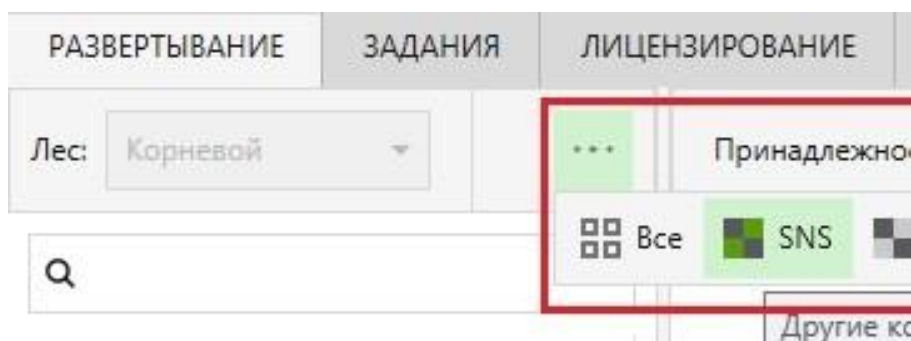


Рисунок 23 – Вкладка «Развертывание»

В правой части окна в списке выберите компьютер SNS-Client.SNS.local. Двойным нажатием левой кнопки мыши откройте окно свойств выбранного компьютера. Перечень параметров содержит пока только имя компьютера. Нажмите на кнопку с изображением стрелки для скрытия окна свойств (рисунок 24).

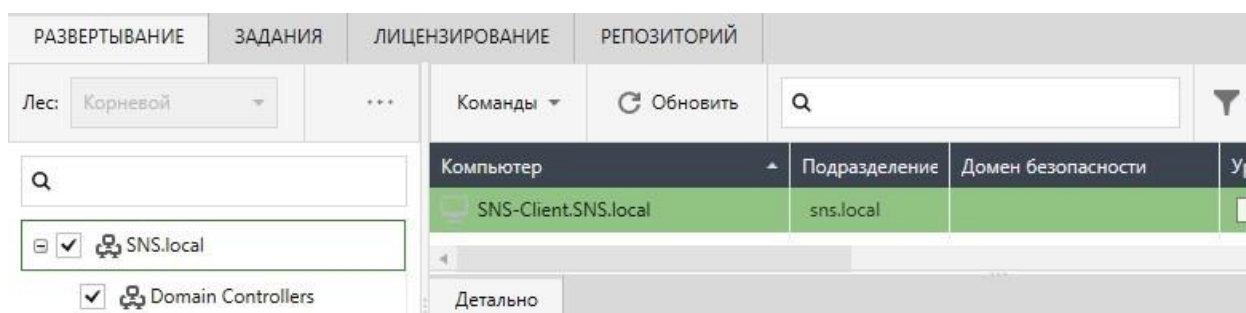


Рисунок 24 – Скрытие окна свойств

Перейдите на вкладку «Репозиторий». Нажмите кнопку «Добавить» (рисунок 25).

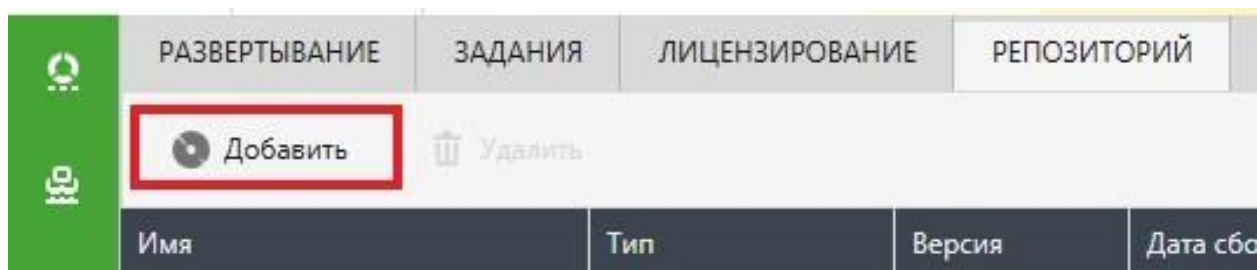


Рисунок 25 – Вкладка «репозиторий»

Откроется окно «Добавить...». Нажмите кнопку «Добавить» (рисунок 26).

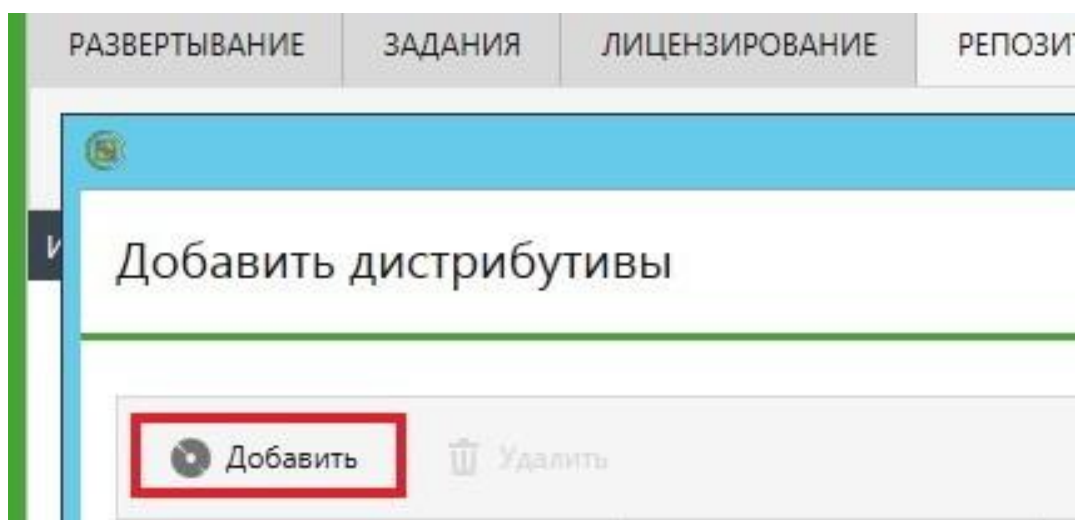


Рисунок 26 – Добавление дистрибутива

В открывшемся окне выберите каталог C:\Distrib\8_8_15891_00 и нажмите кнопку «Выбор папки» (рисунок 27).

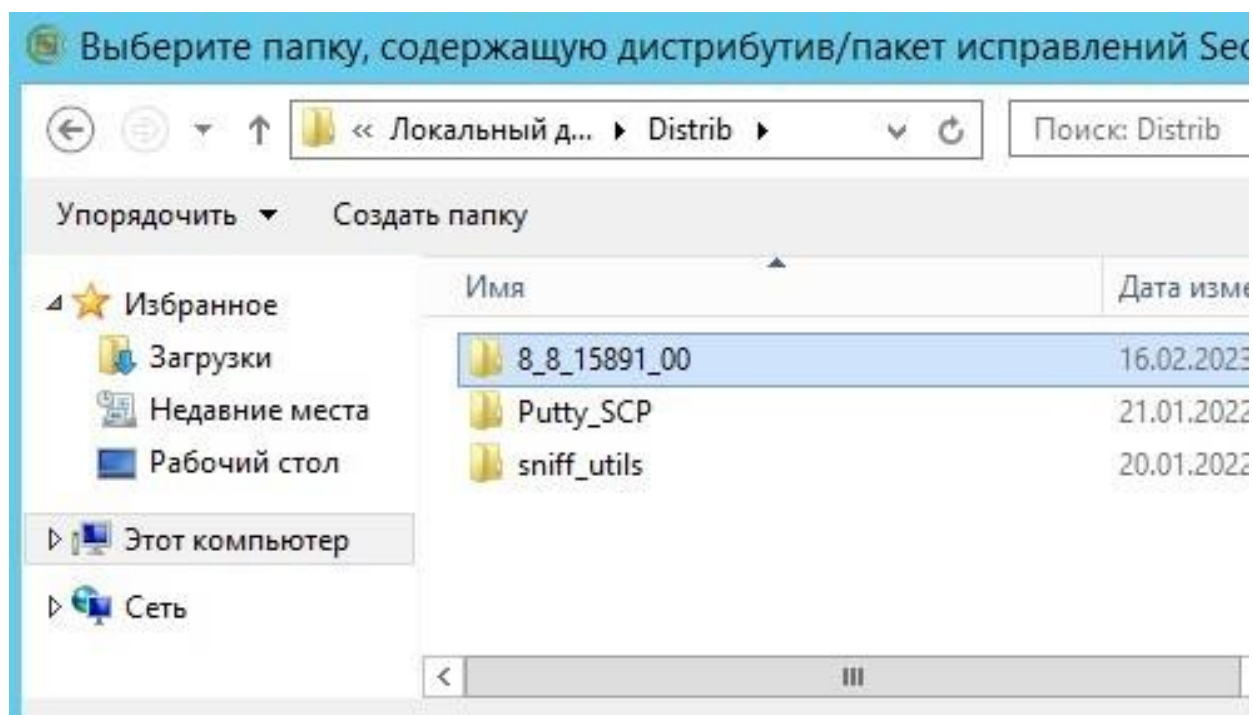


Рисунок 27 – Выбор папки, содержащую дистрибутив

В окне «Добавить» появится информация о выбранном дистрибутиве. Нажмите кнопку «Применить» (рисунок 28).

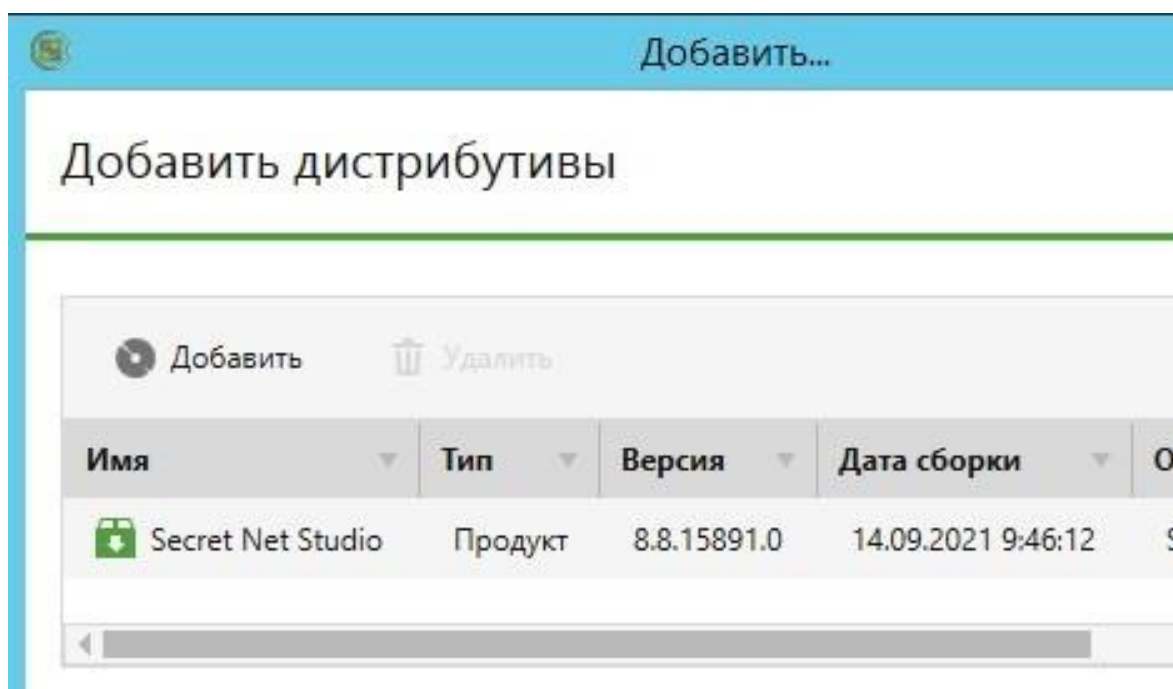


Рисунок 28 – Применение выбранного дистрибутива

Запустится процесс добавления дистрибутива на сервер (рисунок 29), который может занять некоторое время.

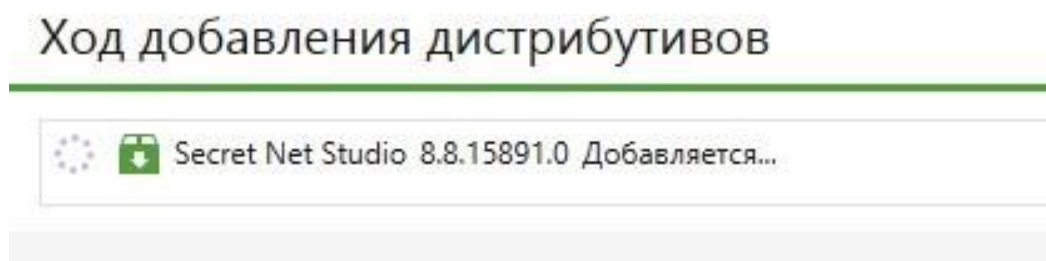


Рисунок 29 – Процесс добавления дистрибутива

После окончания добавления дистрибутива нажмите кнопку «Закрыть» (рисунок 30).

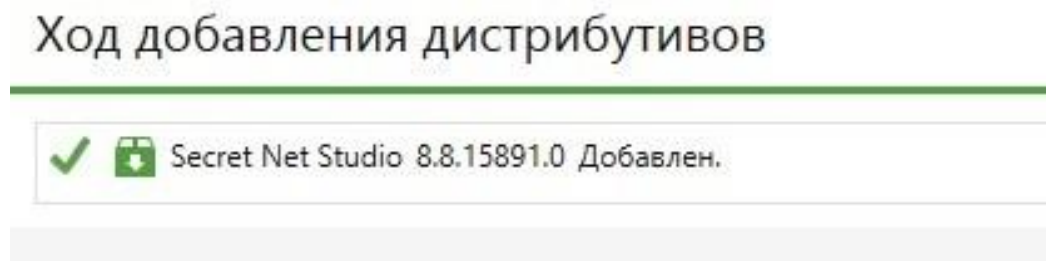


Рисунок 30 – Дистрибутив добавлен

В окне вкладки «Репозиторий» появится новый объект «Secret Net Studio». Установочный комплект хранится на сервере безопасности в каталоге C:\Program Files\Secret Net Studio\Server\Security Server\Repository. По этому пути добавился

каталог, в котором размещен установочный комплект. Права доступа к этому каталогу устанавливаются автоматически, и их не следует изменять, иначе установка станет невозможна. Перейдите на вкладку «Лицензирование». Нажмите кнопку «Добавить/Заменить» (рисунок 31).

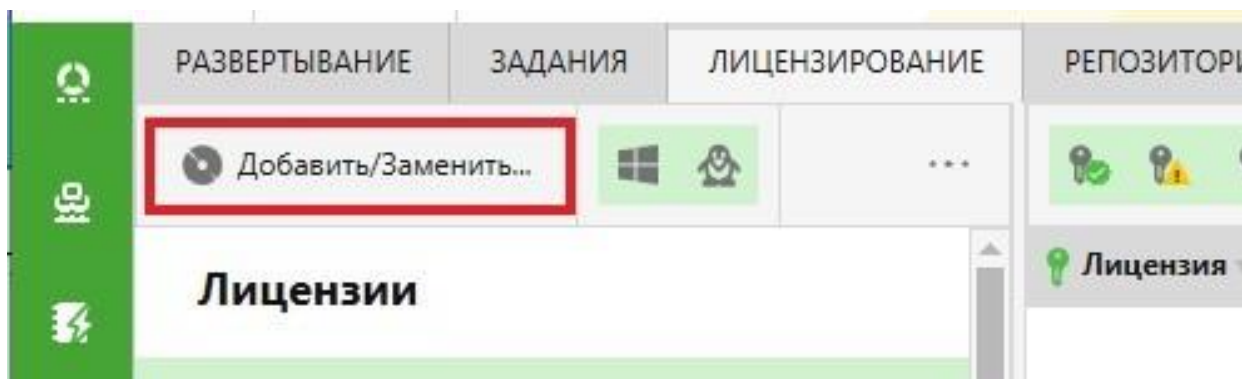


Рисунок 31 – Добавление лицензирования

В окне выбора файлов перейдите в каталог C:\Distrib\8_8_15891\Secret_Net_Studio_testbed и выберите файл лицензии (рисунок 32). Нажмите кнопку «Открыть».

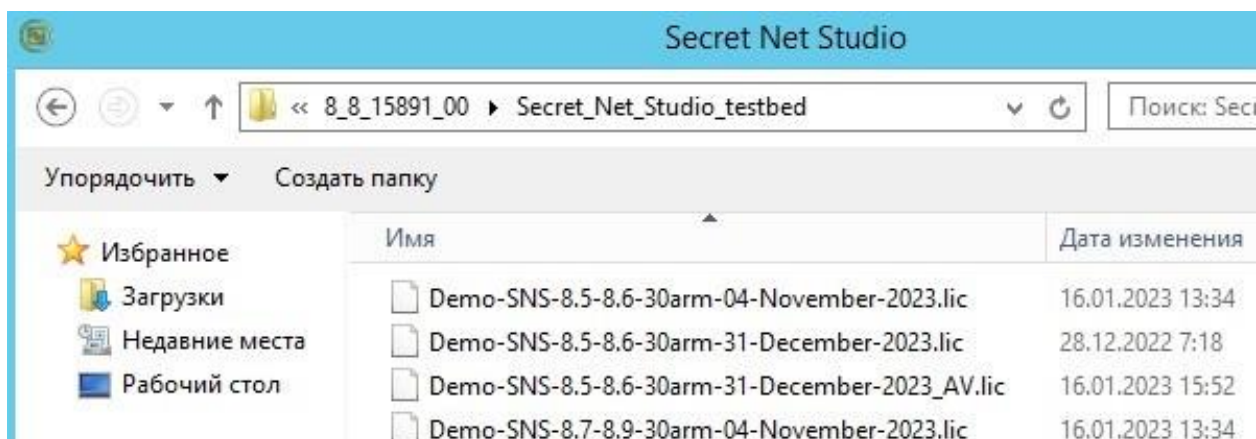


Рисунок 32 – Выбор файла лицензирования

Откроется окно с перечнем доступных лицензий, нажмите «Применить» (рисунок 33).

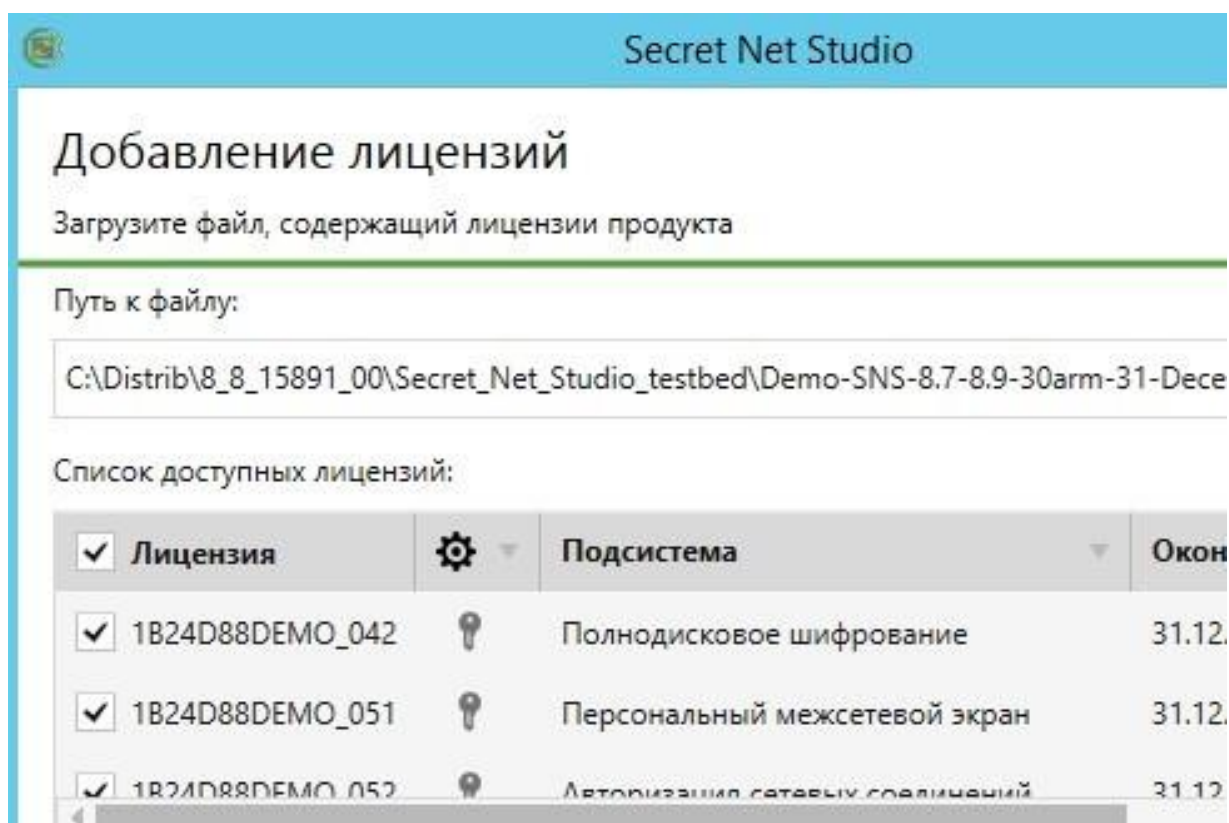


Рисунок 33 – Применение лицензирования

В списке лицензий появится информация о добавленной лицензии (рисунок 34).

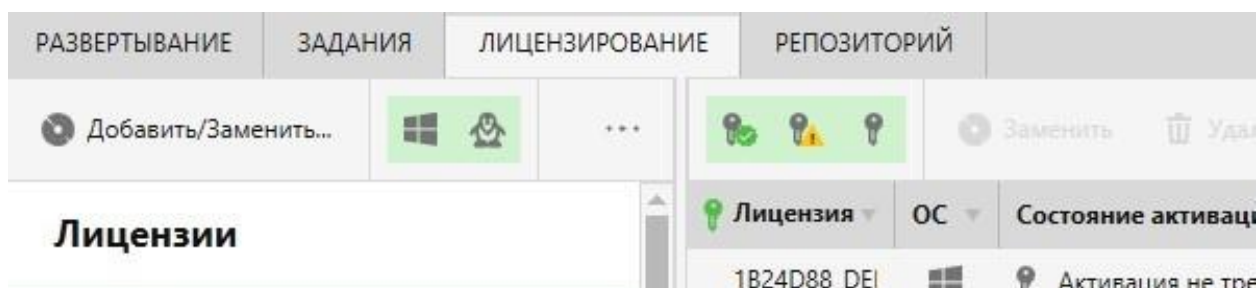


Рисунок 34 – Лицензия добавлена

7.3 Установка СЗИ от НСД с использованием заданий установки

После формирования списка устанавливаемого программного обеспечения необходимо добавить задания развертывания. Задания определяют списки компьютеров, на которых в автоматическом режиме будут выполняться действия. Перейдите на вкладку «Развертывание». Перейдите на вкладку «Развертывание». В ней отображается контроллер домена SNS-Server, на котором установлен также сервер безопасности, и рабочая станция SNS-Client.

Выберите в списке компьютер SNS-Server, нажмите правой кнопкой мыши и в контекстном меню выберите пункт «Установить ПО» (рисунок 35).

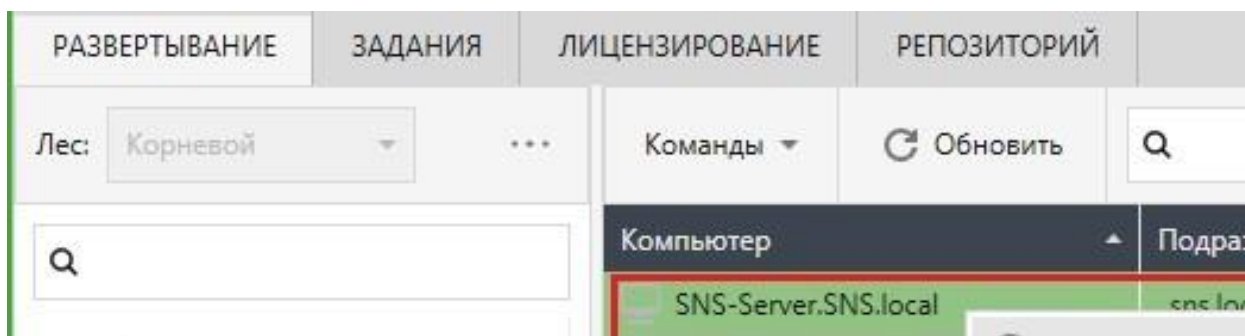


Рисунок 35 – Установка ПО на SNS-Server

В правой части окна программы «Центр управления» отобразится панель настройки задания установки «Установка дистрибутива» (рисунок 36). Название задания и сервер безопасности устанавливаются автоматически и недоступны для изменения. Параметры «Дистрибутив» и «Папка для установки» оставьте без изменения. Параметр «Время ожидания перезагрузки компьютера после установки» оставьте вариант по умолчанию «Ожидание не ограничено». В этом случае автоматическая перезагрузка выполняться не будет. Поле «Параметры» оставьте пустым.

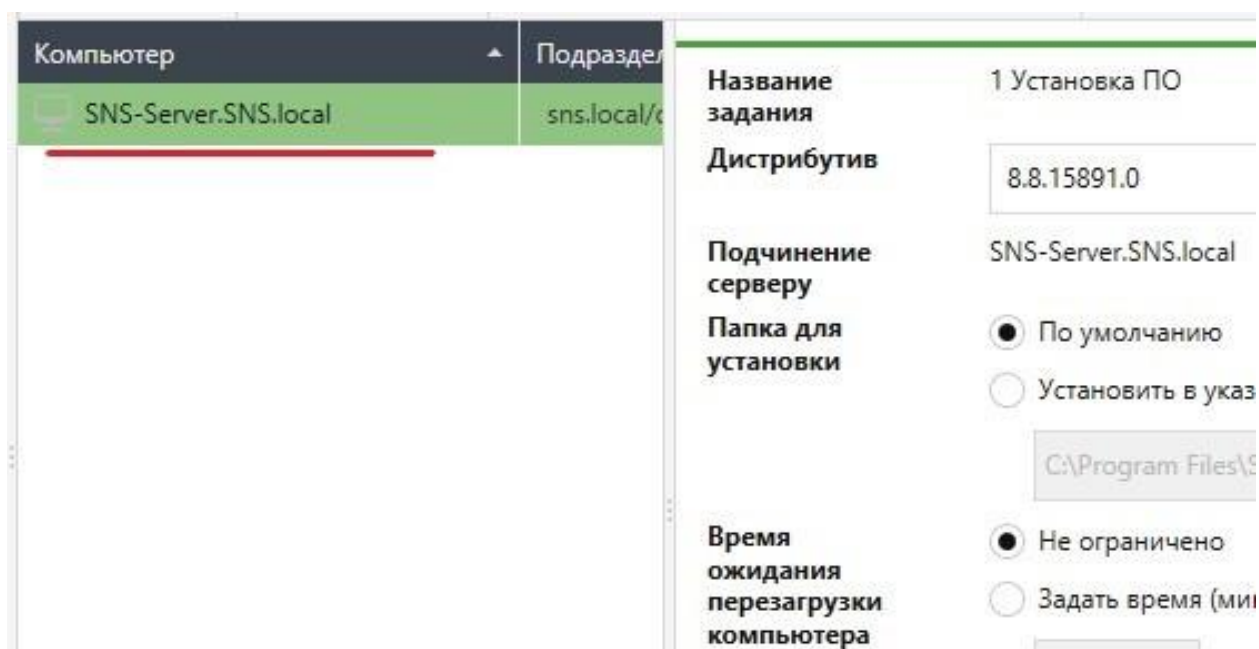


Рисунок 36 – Панель «Настройки задания установки»

В поле «Защитные подсистемы» выбираются компоненты системы защиты от НСД, которые будут устанавливаться на защищаемые компьютеры. Перечень используемых защитных механизмов приводится в Унифицированных конфигурациях. По умолчанию при формировании задания для установки отмечены все компоненты, которые входят в лицензию, что отображается пиктограммой в виде зеленого квадрата рядом с названием компонента. В списке компонентов рядом с названием компонента «Дискреционное управление доступом» нажмите на пиктограмму (рисунок 37). Пиктограмма изменит цвет на серый, под выпадающим списком появится надпись «Компонент не будет установлен» (рисунок 37).

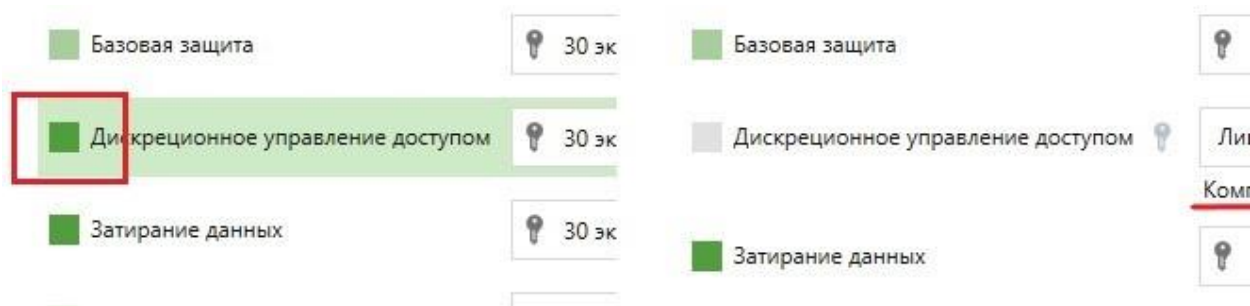


Рисунок 37 – Список компонентов

Аналогичным образом исключите установку следующих компонентов:

- замкнутая программная среда;
- полномочное управление;
- контроль печати;
- защита дисков и шифрование данных;
- персональный межсетевой экран;
- авторизация сетевых соединений;
- обнаружение вторжений;
- антивирус (должен быть отключен по умолчанию);
- доверенная среда;
- безопасная среда;
- полnodисковое шифрование.

Под списком компонентов содержится поле для выбора пакетов исправлений, входящих в установочный комплект. Исправления, являющиеся обязательными, по умолчанию выбраны для установки, необязательные исправления по умолчанию не выбраны. Для версии Secret Net Studio, выбранной для установки, пакетов исправлений нет, поэтому поле пустое. Под списком исправлений введите параметры учетной записи администратора (Администратор, пароль P@ssw0rd). Проверьте параметры задания установки и нажмите кнопку «Установить» (рисунок 38).

Рисунок 38 – Установка ПО

Перейдите на вкладку «Задания». В списке заданий отобразится задание «1 Установка ПО». Нажмите левой кнопкой мыши на задании. В правой части окна отобразится компьютер SNSServer. Двойным кликом по названию компьютера раскройте окно детальной информации (рисунок 39), в котором будет отображаться ход установки.

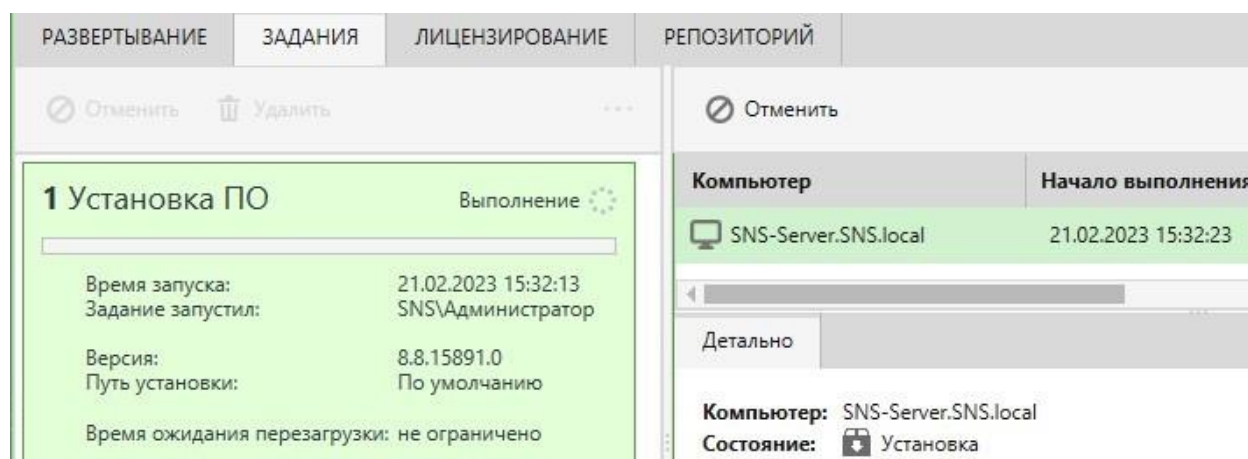


Рисунок 39 – Процесс установки ПО

После завершения установки появится всплывающее окно, с напоминанием о необходимости перезагрузки компьютера для завершения установки (рисунок 40).

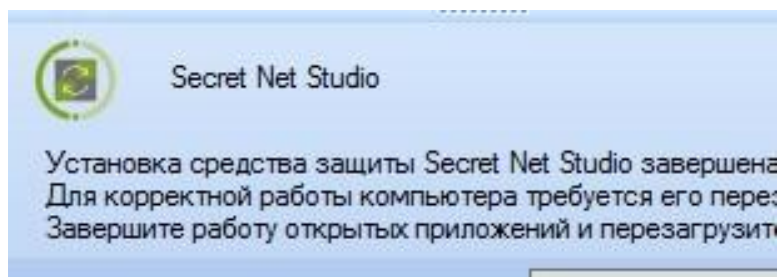


Рисунок 40 – Окно напоминания о перезагрузке

Поскольку в параметрах задания время ожидания до перезагрузки было не ограничено, то требуется перезагрузить компьютер вручную. Закройте все окна и перезагрузите компьютер SNSServer. Для этого нажмите на клавиатуре сочетание клавиш Win+R, введите команду shutdown /R /t 0 и нажмите клавишу Enter (или кнопку OK). Войдите под учетной записью Администратора. Запустите Центр управления (может занять некоторое время). Перейдите к панели «Развертывание». На вкладке «Развертывание» в левом верхнем углу нажмите кнопку с пиктограммой «...» и выберите кнопку SNS (рисунок 41). В списке компьютеров отобразится компьютер SNS-Server и краткая информация об установленной системе защиты.

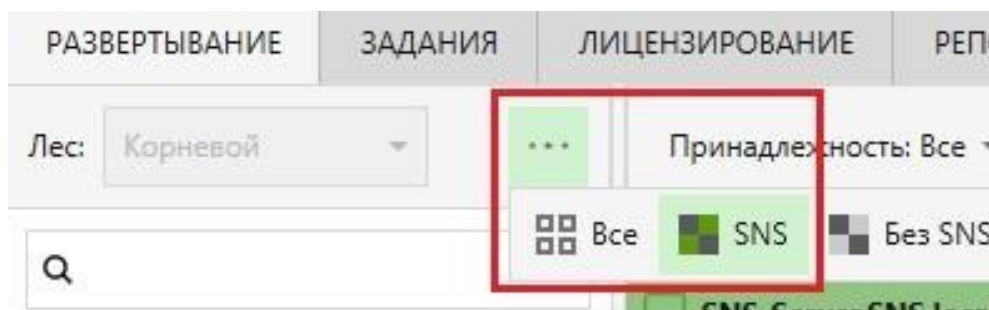


Рисунок 41 – Отображение списка устройств «SNS»

Двойным нажатием левой кнопкой мыши раскройте окно детальной информации о компьютере (рисунок 42).

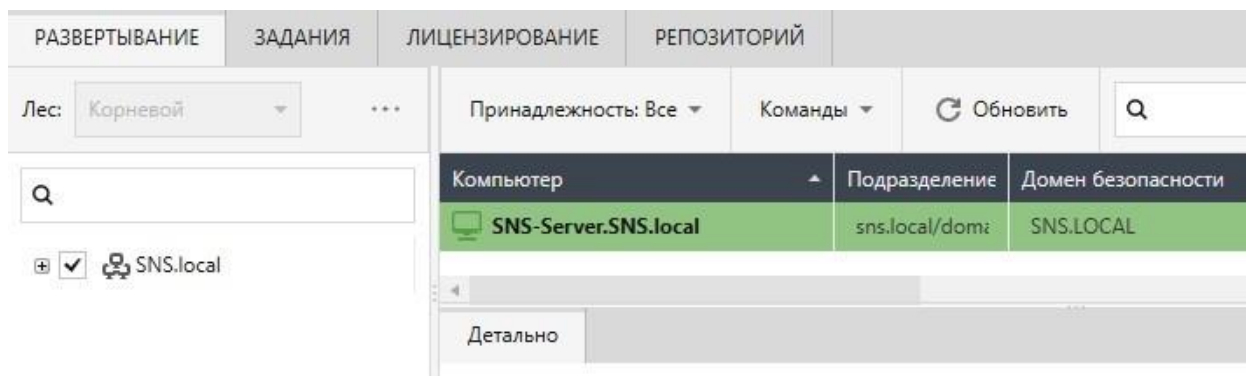


Рисунок 42 – Детальная информации о компьютере

Перейдите на вкладку «Лицензирование». В перечне лицензий в столбе «Осталось лицензий» счетчик уменьшился на единицу (рисунок 43).

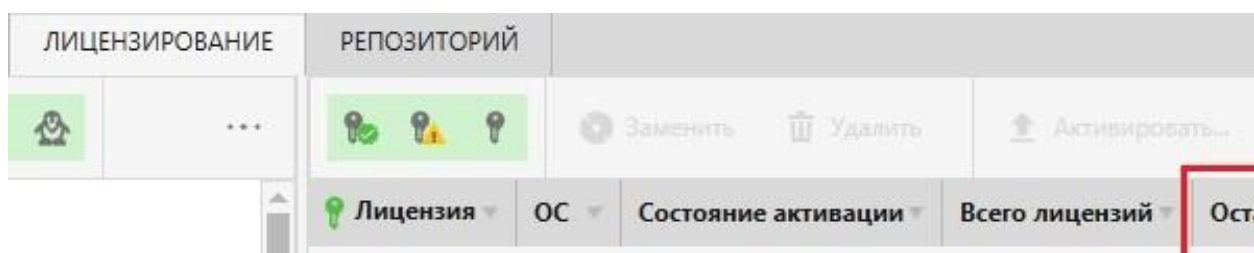


Рисунок 43 – Счетчик лицензий

Перейдите на вкладку «Развертывание», включите отображение списка устройств «Без SNS» (рисунок 44).

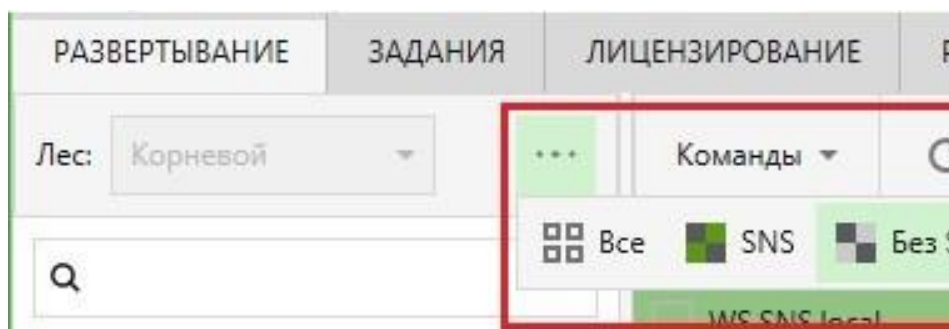


Рисунок 44 – Отображение списка устройств «Без SNS»

Сформируйте задание установки СЗИ от НСД на компьютер SNS-Client. Установите время в 1 минуту до автоматической перезагрузки после завершения установки. При формировании списка устанавливаемых компонентов исключите установку следующих (остальные компоненты должны быть выбраны для установки):

- дискреционное управление доступом;
- полномочное управление доступом;

- контроль печати;
- персональный межсетевой экран;
- авторизация сетевых соединений;
- обнаружение вторжений;
- антивирус (если не отключен по умолчанию);
- доверенная среда;
- безопасная среда;
- полнодисковое шифрование.

Запустите задание установки, отслеживайте выполнение, дождитесь завершения установки. После завершения установки и завершения перезагрузки компьютера SNS-Client, в Центре управления перейдите на вкладку «Развертывание», отобразите список компьютеров, на которых установлен Secret Net Studio. Если в списке не отображается компьютер SNS-Client, то нажмите кнопку «Обновить» (рисунок 45). Если компьютер не появился, или уровень защиты показан как минимальный – перезапустите «Центр управления».

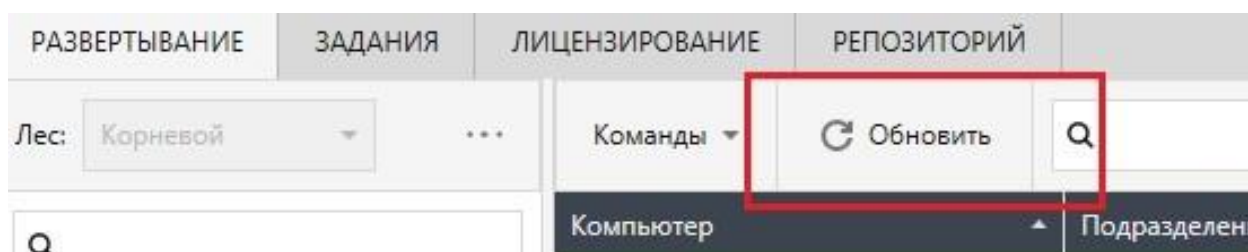


Рисунок 45 – Обновление списка компьютеров

Можно сохранить перечень компьютеров, с установленным СЗИ от НСД. Для этого выделите все компьютеры в списке (зажать кнопку Shift и выбрать левой кнопкой мыши) и в строке меню выберите пункт «Экспорт», выберите место сохранения файла (рисунок 46).

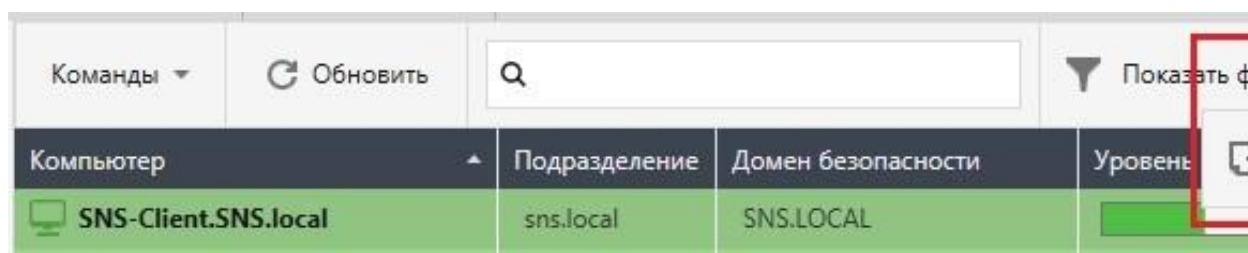


Рисунок 46 – Экспорт перечня компьютеров

В программе Центр управления перейдите к панели «Компьютеры» (рисунок 47). В окне отобразится иерархия управления. Панель открывается с видом «Диаграмма» – режимом, отображающим в графическом виде сведения о структуре оперативного управления. Нажмите на кнопку «Таблица» для смены формата отображения информации (рисунок 47).

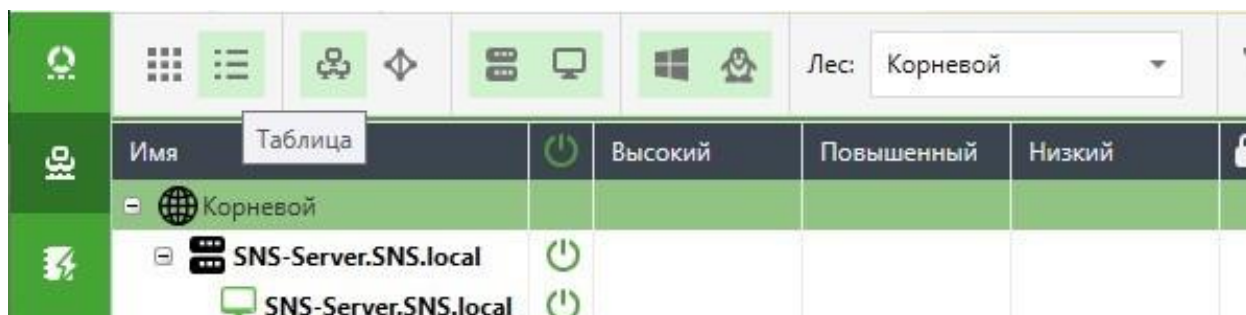


Рисунок 47 – Вид таблицы в панели «Компьютеры»

В этом режиме отображения выводится информация о состоянии компьютера (зеленый индикатор означает, что компьютер подключен), количестве тревог высокого, повышенного и низкого уровня (цифрой отображается количество), информацию о блокировке, прохождении функционального контроля, текущей сессии пользователя и т.д.

7.4 Настройка параметров сервера безопасности

Настройка параметров сервера безопасности будет осуществляться в соответствии со значениями, указанными в Унифицированных конфигурациях. В программе Центр управления перейдите к панели «Компьютеры». Включите отображение структуры в виде таблицы.

В структуре отображается Сервер безопасности, обозначенный черной пиктограммой в виде сервера, и защищаемые компьютеры, обозначенные пиктограммой в виде компьютера. Т.к. на компьютер SNS-Server был установлен и сервер безопасности, и клиент СЗИ от НСД, то имя компьютера встречается в структуре два раза – верхний (корневой узел) – это сервер безопасности, узел структуры (компьютер) – защищаемый компьютер (рисунок 48). При настройке SNS-Server как сервера безопасности, параметры будут влиять на всю структуру

системы защиты, при настройке SNS-Server как клиента – только на настройки самого компьютера.

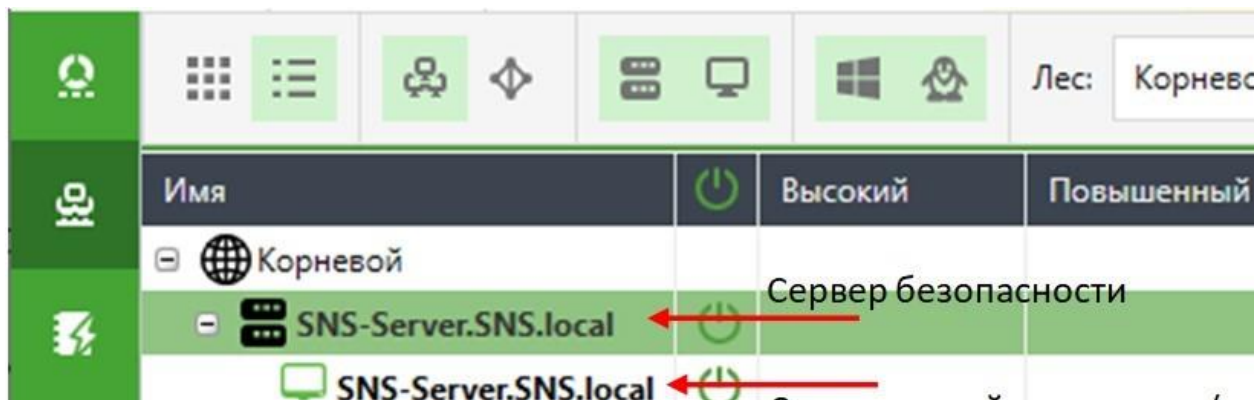


Рисунок 48 – Узел «Корневой»

Выберите сервер безопасности SNS-Server (с черной пиктограммой в виде сервера) и в его контекстном меню выберите пункт «Свойства» (рисунок 49).

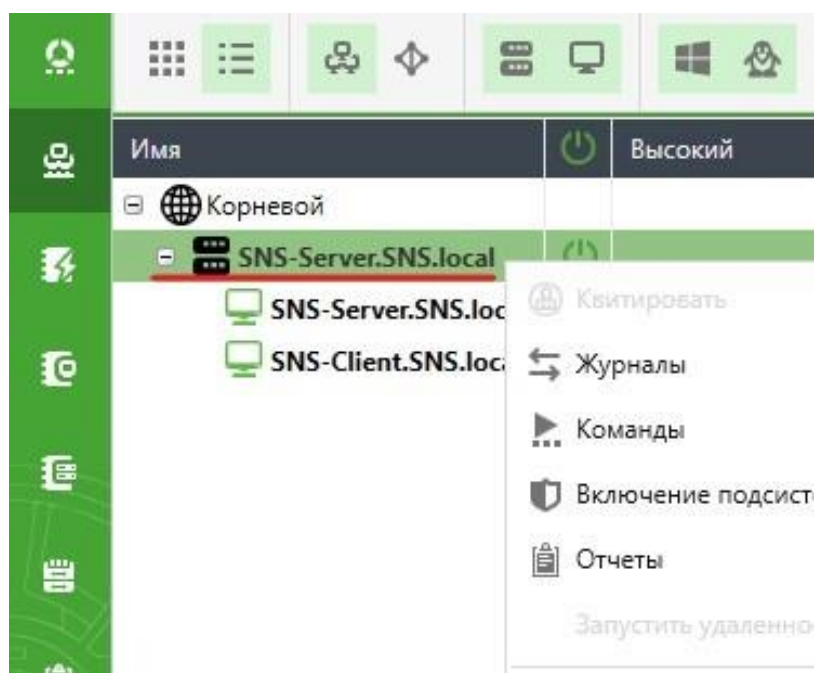


Рисунок 49 – Свойства сервера безопасности «SNS-Server»

Перейдите на вкладку «Настройки» и нажмите кнопку «Загрузить настройки» (рисунок 50).

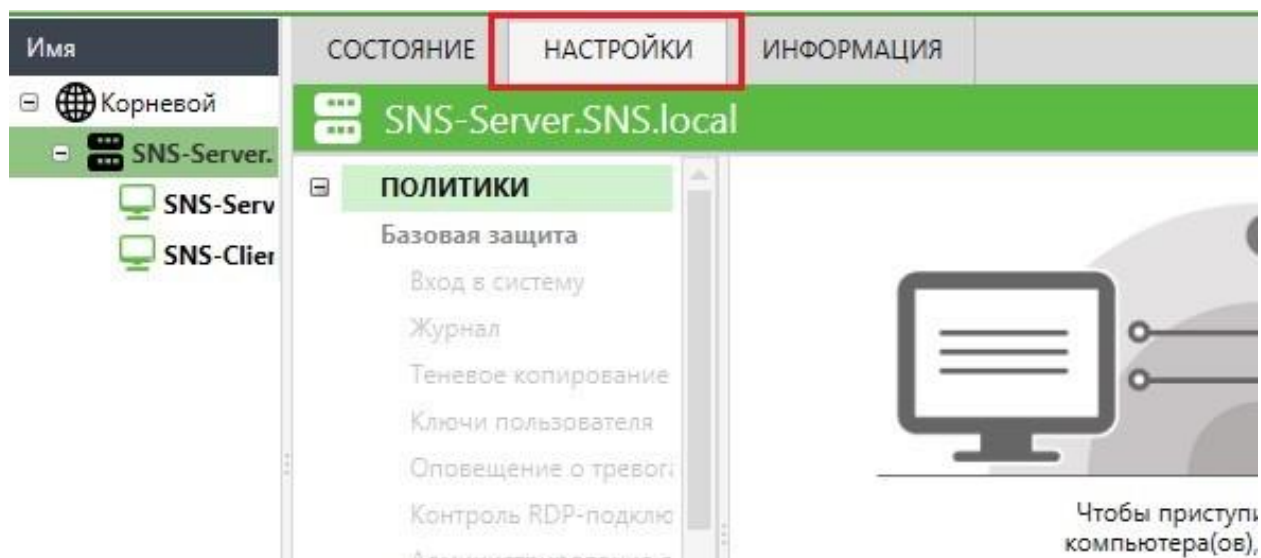


Рисунок 50 – Настройки сервера безопасности «SNS-Server»

В списке параметров сверните узел «Политики», нажав на кнопку «-» и раскройте узел «Параметры», нажав на кнопку «+» (рисунок 51).

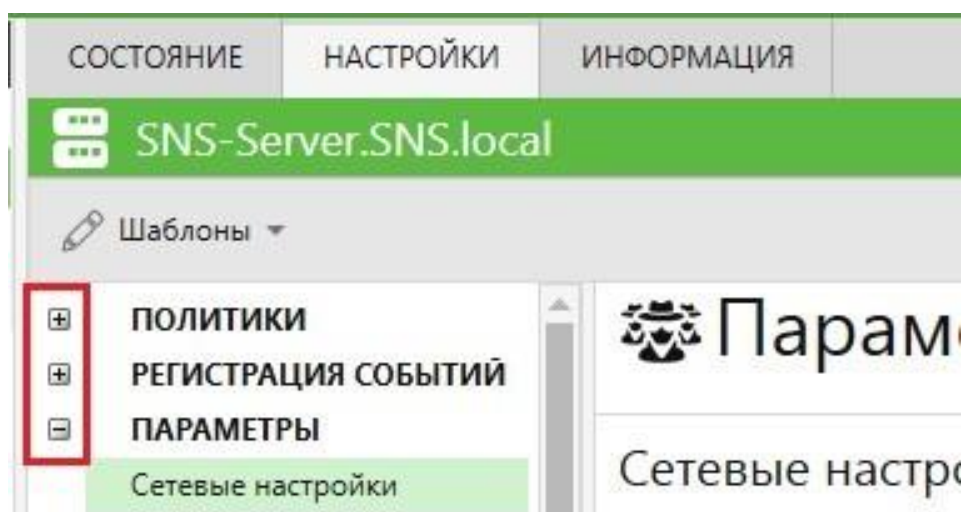


Рисунок 51 – Узел «Параметры»

В правой части окна в группе настроек «Сетевые параметры» вставьте значения из таблицы 1, согласно вашему варианту:

- время ожидания;
- разрешения имен DNS;
- соединения с сервером;
- отправки запроса на сервер;
- окончания передачи следующего блока;

- события для рабочей станции;
- сервером ответа на контрольный вопрос;
- размер блока;
- для приема данных от сервера;
- для передачи данных на сервер.

Если какие-то параметры не соответствуют указанным, исправьте эти значения. Выберите в списке настроек «Параметры» группу настроек «Сбор журналов». Установите флаг «При заполнении журнала на 80% и более. Установка параметра «При подключении агента к серверу безопасности» определяется в каждом подразделении самостоятельно, в рамках практики параметр устанавливаться не будет. В поле «Включить в сбор следующие журналы» должны быть установлены флаги у всех журналов» (рисунок 52).

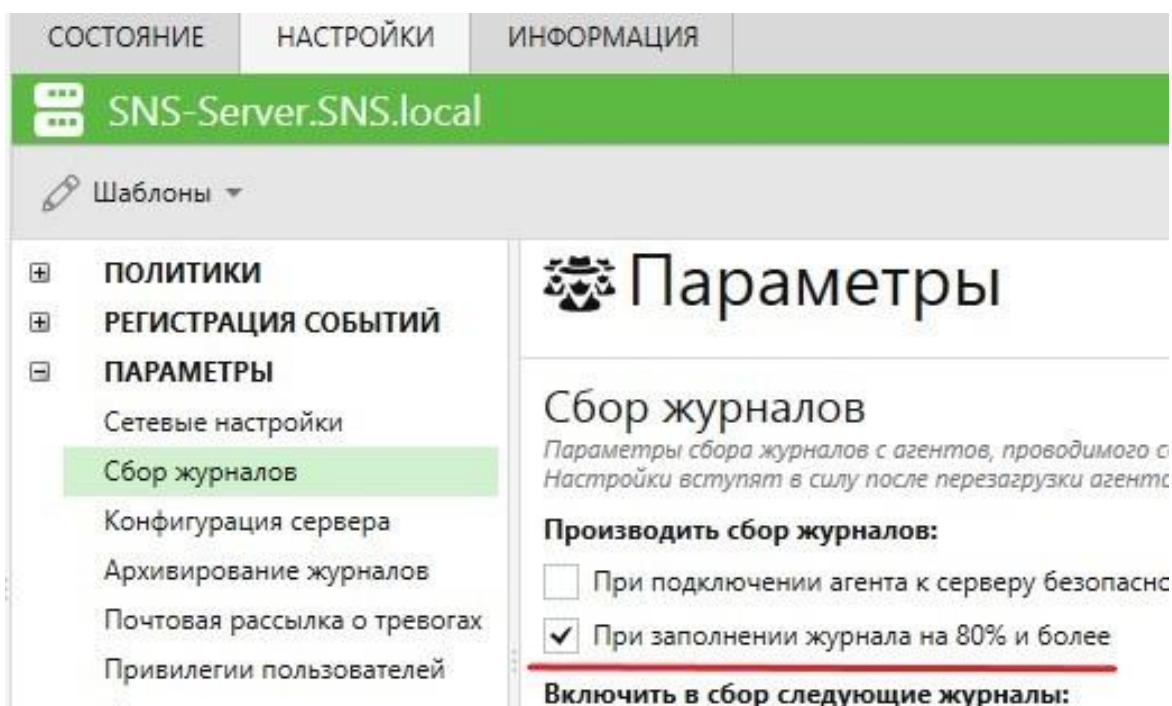


Рисунок 52 – Параметры «Сбор журналов»

Параметр «Сохранять копии журналов на защищаемом компьютере» должен быть отключен. В унифицированных конфигурациях указано, что в значении параметра «Расписание сбора журналов» периодичность определяется в каждом подразделении самостоятельно. В выпадающем списке выберите

параметр «Периодическое» и произвольно установите периодичность сбора журналов (рисунок 53).

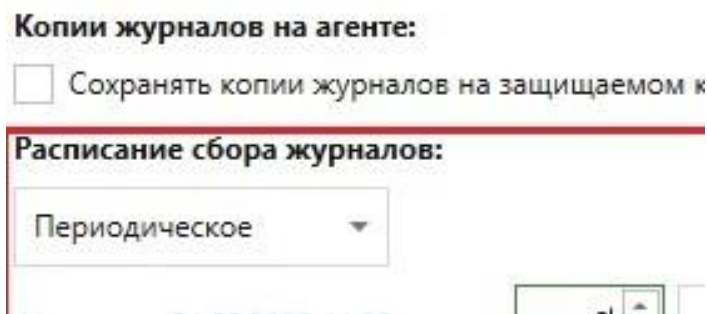


Рисунок 53 – Параметр «Расписание сбора журналов»

В группе параметров «Расположение файлов на сервере» параметры оставьте без изменения. В Унифицированных конфигурациях указано, что значения параметров «Каталог архивов» и «Каталог временных файлов» выбирается подразделением. Периодичность архивирования журналов также определяется подразделением в зависимости от объема данных и других факторов. В группе настроек «Архивирование журналов» раскройте выпадающий список и установите «Периодическое» и задайте произвольную периодичность архивирования журналов (рисунок 54).

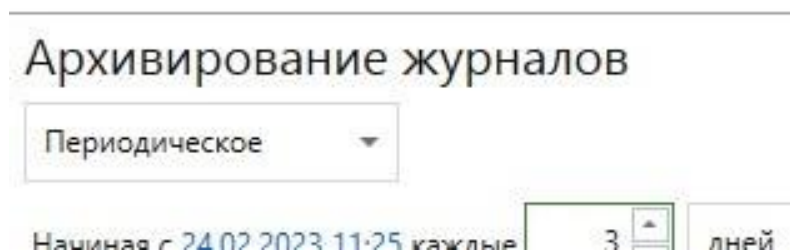


Рисунок 54 – Параметр «Архивирование журналов»

Почтовая рассылка о тревогах не используется, поэтому настройка параметров не требуется. Нажмите кнопку «Применить» для сохранения внесенных изменений. Перейдите в группу настроек «Привилегии пользователей». По умолчанию в перечне пользователей и групп есть группа «SNS\SecretNetAdmin_Domain», в которую входит пользователь Администратор, под которым сейчас выполняется настройка. В унифицированных конфигурациях указаны следующие группы пользователей: SecretNetAdmin_Forest и SecretNetAdmin_Domain с полным перечнем

привилегий, SPOAdmins и Auditors с ограниченным набором полномочий. Нажмите сочетание клавиш Win и R. Введите dsa.msc и нажмите Enter (рисунок 55).

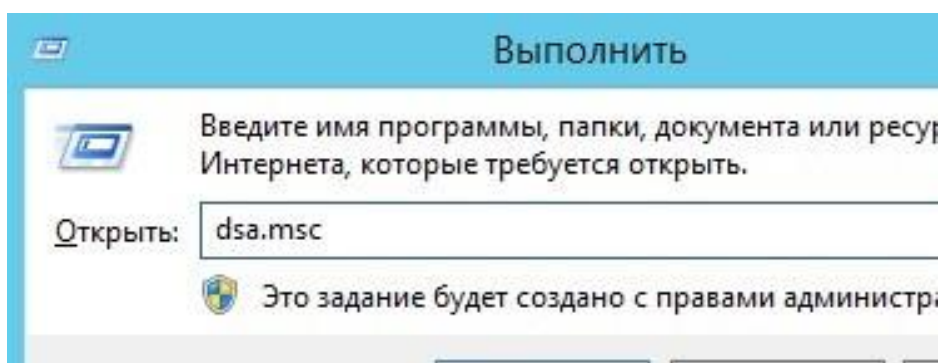


Рисунок 55 – Запуск консоли «Active Directory – Пользователи и компьютеры»

Запустится консоль «Active Directory – Пользователи и компьютеры». Перейдите в контейнер Users. Выберите группу SecretNetAdmin_Domain и в контекстном меню выберите пункт «Свойства» (рисунок 56).

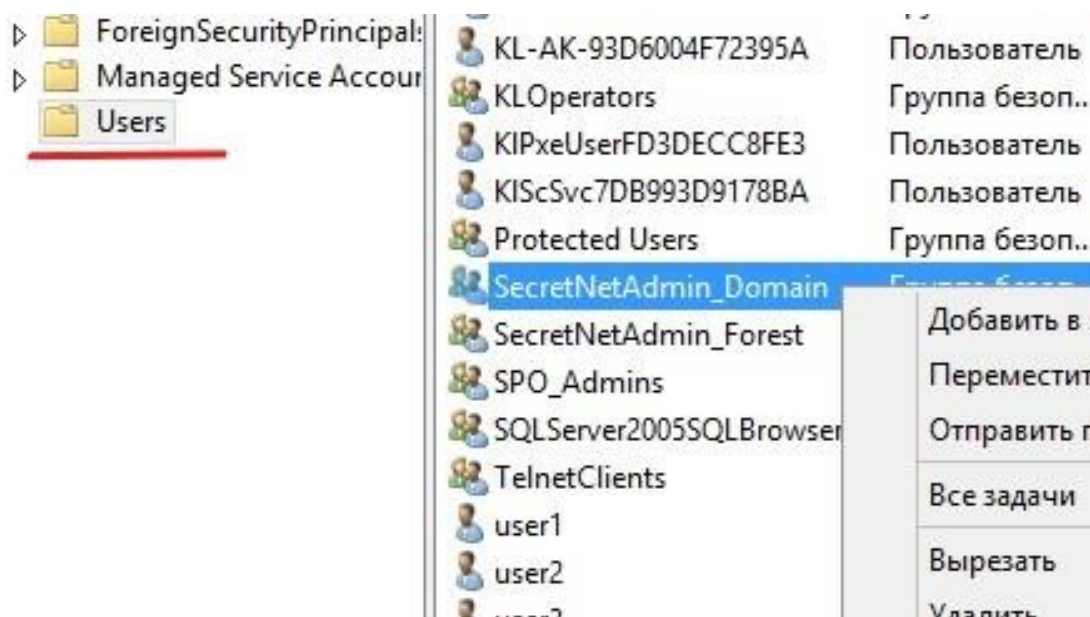


Рисунок 56 – Свойства группы «Users»

В окне свойств откройте вкладку «Члены группы», в группу включена учетная запись Администратора домена. Учетная запись была добавлена в группу перед установкой Сервера безопасности. В рамках практической работы для упрощения учетная запись администратора будет использоваться для выполнения функций администратора безопасности, но при эксплуатации, как

правило, должна быть создана отдельная учетная запись для администратора безопасности. Закройте окно свойств группы SecretNetAdmin_Domain.

Аналогично просмотрите членов группы SecretNetAdmin_Forest. Вернитесь к окну программы «Центр управления». В группе настроек «Привилегии пользователей». Под полем «Пользователи и группы» нажмите кнопку «Добавить пользователя» (рисунок 57).

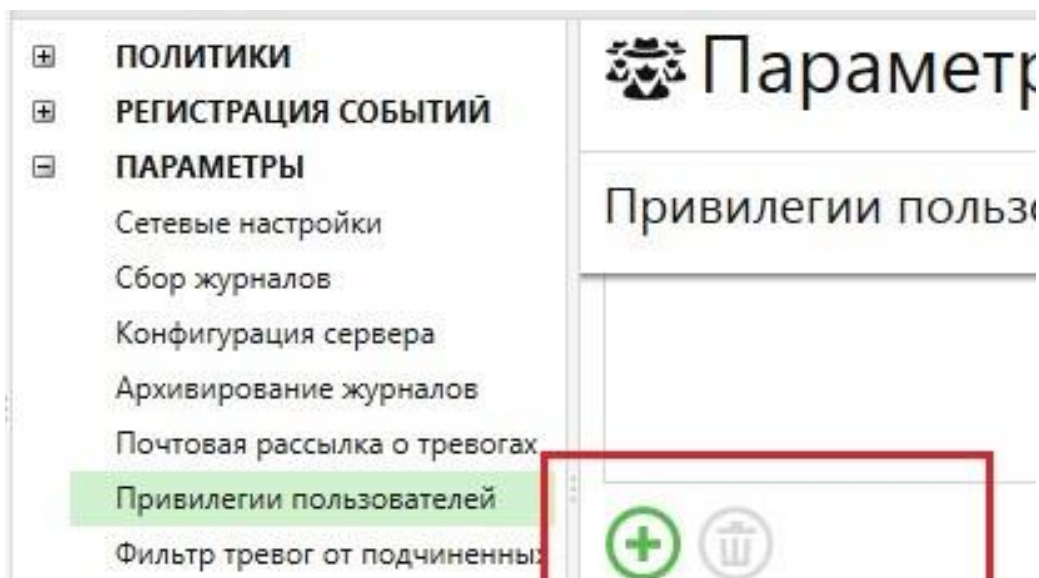


Рисунок 57 – Параметры «Привилегии пользователей»

Введите название группы «SecretNetAdmin_Forest» и нажмите кнопку «ОК» (рисунок 58).



Рисунок 58 – Выбор группы «SecretNetAdmin_Forest»

В список «Пользователи и группы» добавится группа SecretNetAdmin_Forest. Выберите эту группу в списке. Назначьте группе все

привилегии, установив все флаги в списке привилегий (рисунок 59). Нажмите кнопку «Применить» для сохранения настроек.

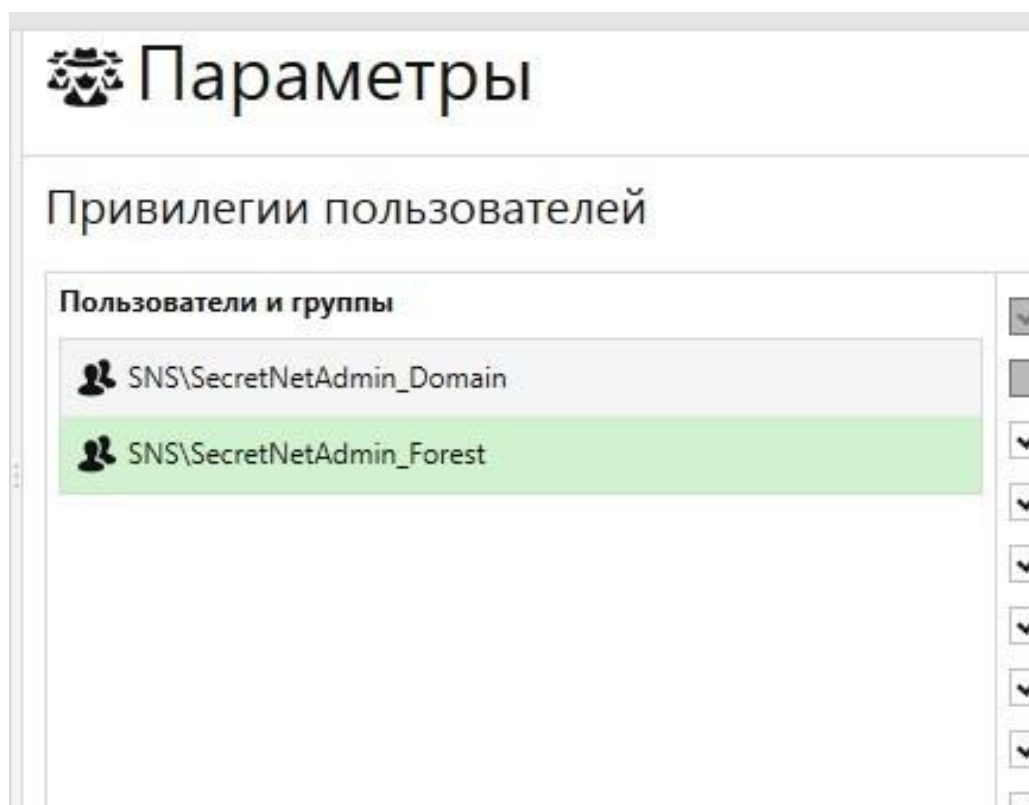


Рисунок 59 – Назначение привилегий для группы «SecretNetAdmin_Forest»

Аналогичным образом назначьте группам SPOAdmins и Auditors только следующие привилегии. Привилегии для группы SPOAdmins:

- просмотр информации;
- выполнение оперативных команд;
- сбор журналов по команде;
- загрузка СПС из файла.

Привилегии для группы Auditors:

- просмотр информации;
- выполнение оперативных команд;
- квитирование сообщений о тревогах;
- сбор журналов по команде;
- архивирование/восстановление журналов;
- загрузка СПС из файла;
- утверждение паспорта ПО;

- удаление паспорта ПО.

В группе настроек «Фильтр тревог от подчиненных серверов» в соответствии с Унифицированными конфигурациями должен быть установлен флаг «Отключить фильтр». В некоторых подразделениях возможно включение фильтра тревог при наличии согласованных настроек правил фильтрации.

Фильтр тревог от подчиненных серверов

- ☒ Не пропускать на сервер события из правил
☐ Пропускать на сервер только события из правил

Имя правила	Источник	Категория	События

Снимите флаг «Отключить фильтр» и нажмите кнопку «Добавить» (рисунок 60).

Рисунок 60 – Параметр «Фильтр тревог от подчиненных серверов»

Появится окно «Правило фильтрации». Выберите последовательно произвольные значения в выпадающих списках «Источник», «Категория» и «События» и нажмите кнопку «Применить» (рисунок 61).

Правило фильтрации

Правило фильтрации

Источник:

LocalProtection

Категория:

4

События:

1034

Если в списке нет необходимой категории, впишите е

Если в списке нет необходимого события, впишите еп

точку с запятой: 1045; 2045. Чтобы задать любую кате

событие, оставьте поле пустым.

Имя правила:

Правило №1

Рисунок 61 – Окно «Правило фильтрации»

Созданное правило фильтрации появится в списке правил. По умолчанию установлен флаг «Не пропускать на сервер события из правил», следовательно,

события, указанные в фильтре, не будут попадать на сервер безопасности. Если установить флаг «Пропускать на сервер только события из правил, то на сервер безопасности будут попадать только те события, которые указаны в правилах». Установите флаг «Отключить фильтр» и нажмите кнопку «Применить». В группе настроек «Аутентификация Windows» оставьте параметры без изменения. В последней группе параметров «Управление трассировкой» флаг «Включить трассировку» должен быть снят, т.к. трассировка не используется. Нажмите кнопку «Применить» для сохранения настроек. Откройте консоль «Active Directory – Пользователи и компьютеры» (dsa.msc). Перейдите в контейнер Users. Выберите группу SPOAdmin и откройте ее свойства. Добавьте пользователя user1 в группу SPOAdmin. Выберите группу Auditors, добавьте в нее пользователя user2 (рисунок 62).

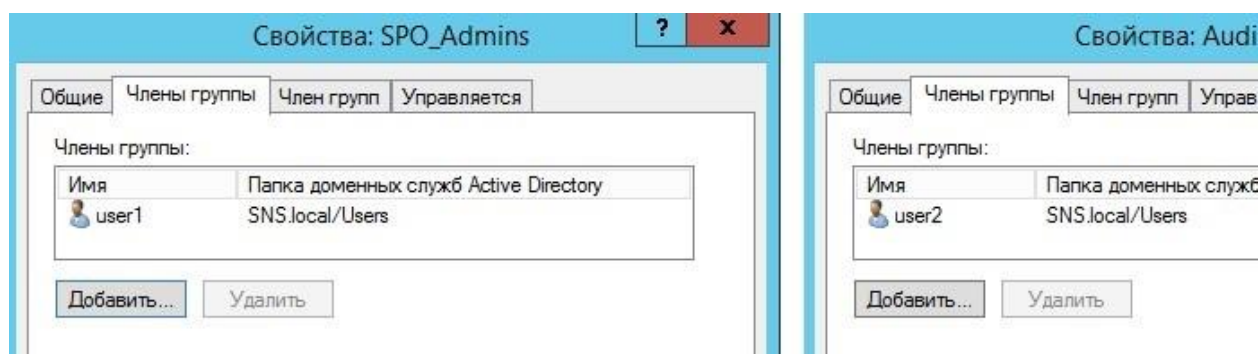


Рисунок 62 – Добавление пользователя «User1» в группу «SPOAdmin» и «User2» в группу «Auditors»

Завершите сеанс Администратора. Для этого нажмите сочетание клавиш Win + R, введите команду shutdown /L и нажмите Enter. В окне выбора пользователей выберите «Сменить пользователя» (рисунок 63). Выберите «Другой пользователь» и войдите под учетной записью пользователя SNS\user1 (рисунок 63).



Рисунок 63 – Вход под учетной записью пользователя «SNS\user1»

Запустите «Центр управления», для этого перейдите в каталог установки «Центра управления», выберите исполняемый файл Medusa.exe, создайте ярлык на рабочем столе (рисунок 64), либо запустите из каталога.

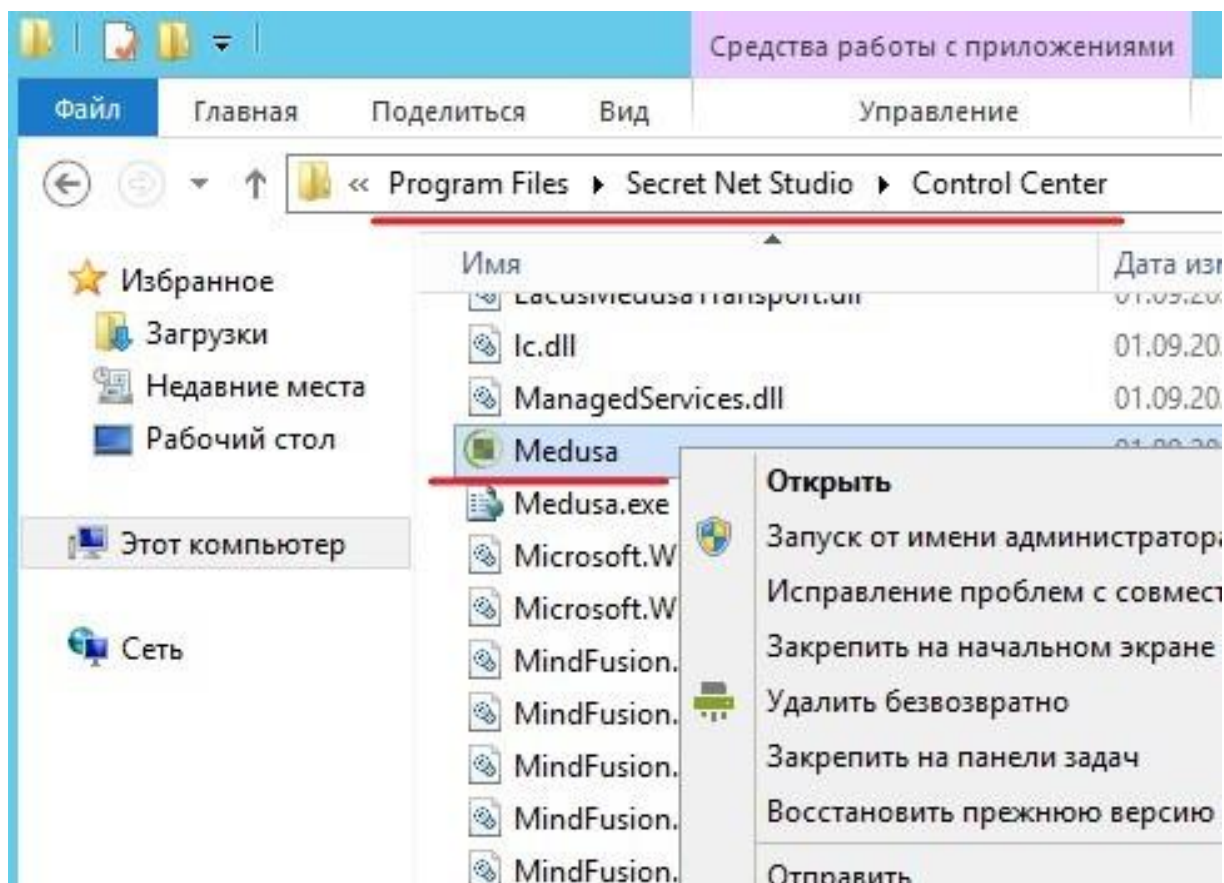


Рисунок 64 – Запуск исполняемого файла «Medusa.exe»

Нажмите на кнопку «Обновить» в окне выбора сервера безопасности, выберите сервер SNS-Server.SNS.local в окне подключения. Перейдите на панель «Компьютеры» и откройте свойства сервера безопасности SNS-Server. Перейдите на вкладку «Настройки» и нажмите кнопку «Загрузить настройки». Все настройки доступны только для просмотра (рисунок 65), т.к. пользователь user1 входит в группу SPOAdmin и на него распространяются права, установленные для группы.

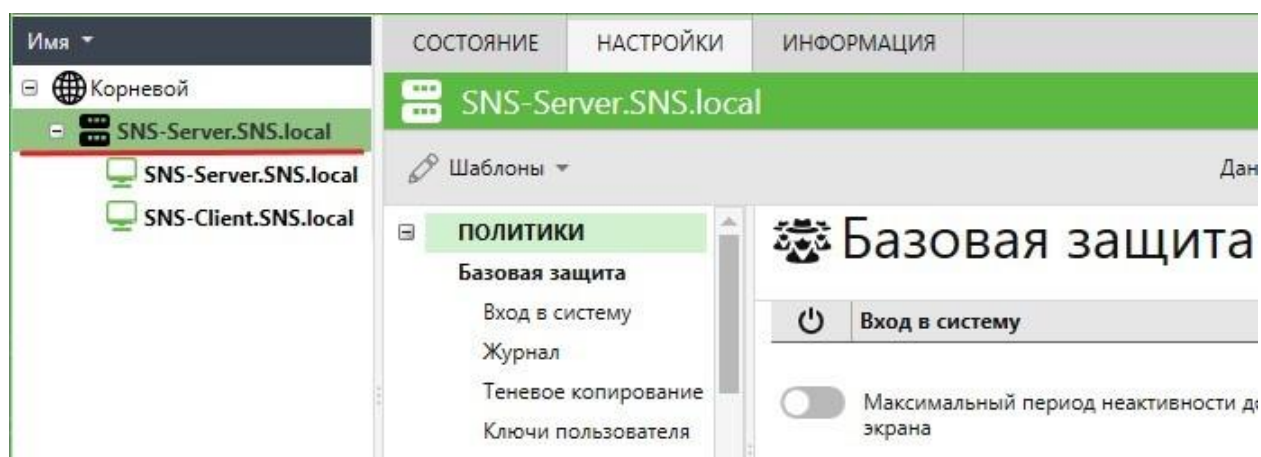


Рисунок 65 – Проверка настроек «SNS-Server»

Завершите сеанс пользователя user1. Войдите под учетной записью user2. Запустите «Центр управления» и подключитесь к серверу SNS-Server.SNS.local. Перейдите на панель «Компьютеры» и откройте свойства компьютера SNS-Server.SNS.local. Перейдите на вкладку «Настройки» и нажмите кнопку «Загрузить настройки». Все настройки также доступны только для просмотра, т.к. пользователь user2 входит в группу Auditors. Завершите сеанс пользователя user2.

7.5 Настройка групповой политики

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью SNS\Администратор. В правом нижнем углу окна программы (в трее) нажмите правой кнопкой мыши на пиктограмму SNS и выберите пункт «Управление (для администратора)» (рисунок 66).

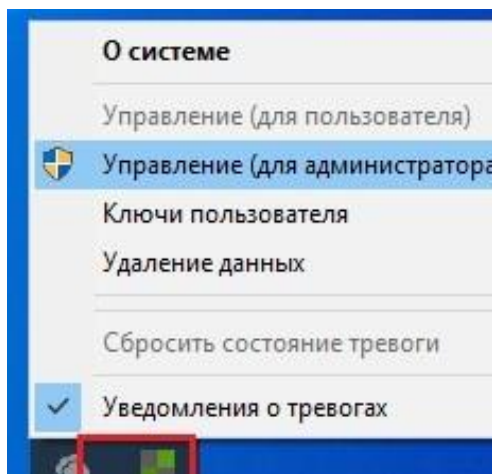


Рисунок 66 – Запуск программы «Локальный центр управления»

Запустится программа «Локальный центр управления» с правами администратора. В панели «Компьютер» на вкладке «Состояние» отображается текущая информация о состоянии средства защиты от НСД. Установленные компоненты отображаются в виде плиток темно-серого цвета, в верхнем углу плитки расположен индикатор. Зеленый цвет индикатора соответствует нормальному функционированию компонента СЗИ от НСД (рисунок 67). Компоненты, указанные в виде плиток светло-серого цвета, не установлены.

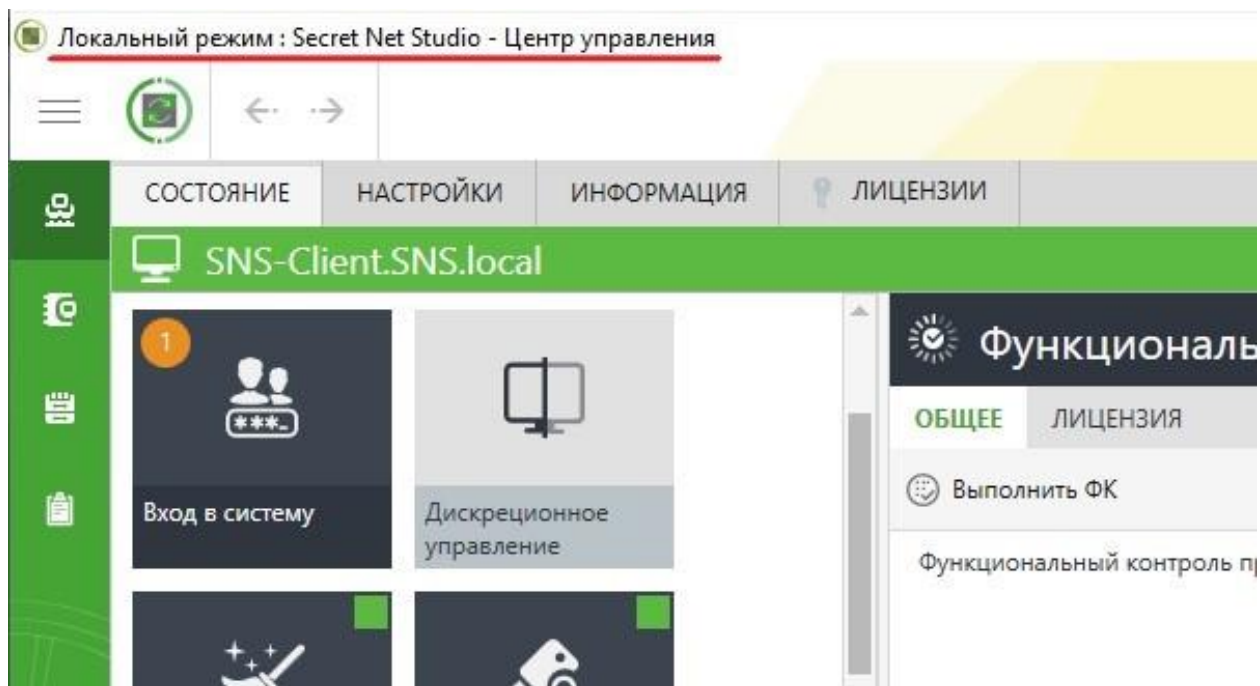


Рисунок 67 – Главное меню программы «Локальный центр управления»

Перейдите на вкладку «Настройки». Просмотрите настройки в группе параметров «Базовая защита – Журнал», определите максимальный размер журнала системы защиты (рисунок 68). Обратите внимание на значение в графе «Источник», в нем указываются сведения о политике, определяющей значение параметра. Текущее значение параметра является локальным (установленное для этого компьютера). Попробуйте изменить значение размера журнала. Установите произвольное значение и нажмите кнопку «Применить» внизу окна.

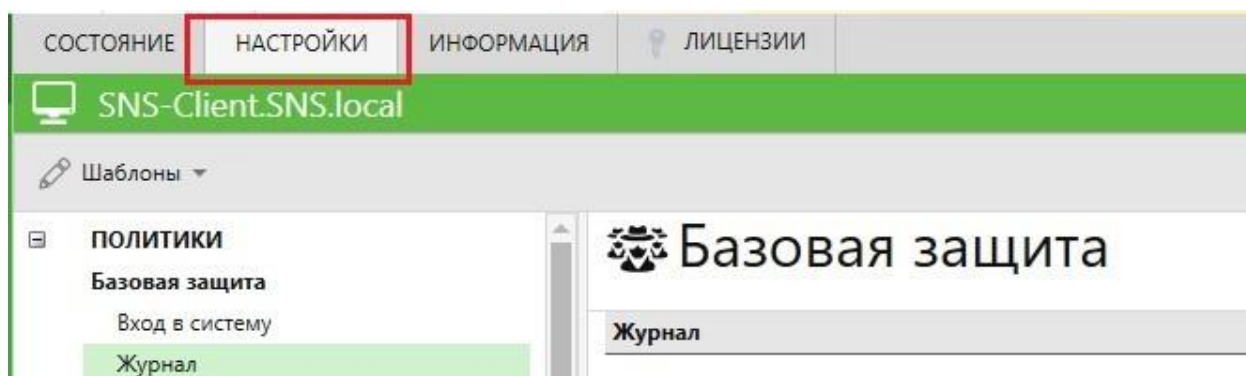


Рисунок 68 – Установка значения размера журнала

Завершите сеанс Администратора (Win + R, shutdown /L) и войдите на компьютер SNS-Client под учетной записью SNS\user1. Попробуйте запустить программу «Локальный центр управления» для администратора, окно ввода параметров учетной записи администратора (рисунок 69). Нажмите кнопку «Нет».

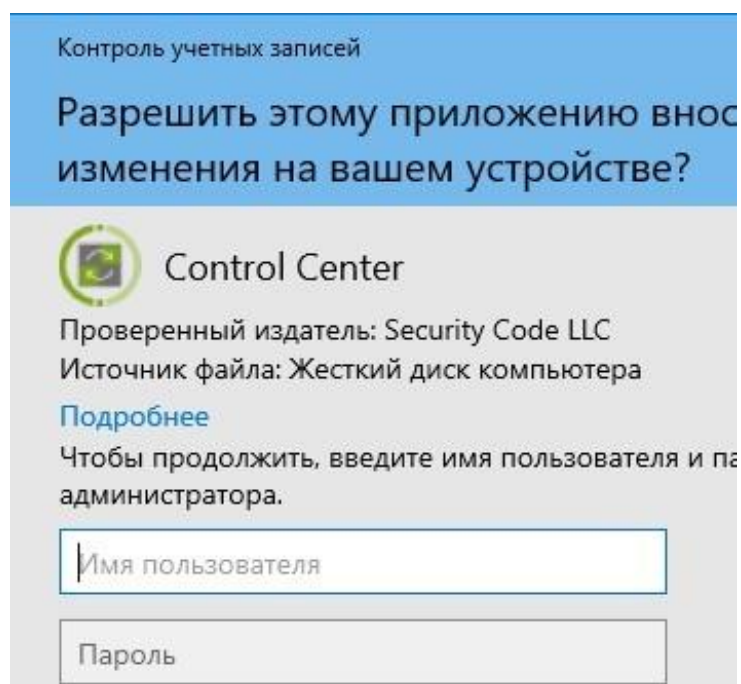


Рисунок 69 – Окно ввода параметров

Запустите «Локальный центр управления» от имени пользователя (рисунок 70).

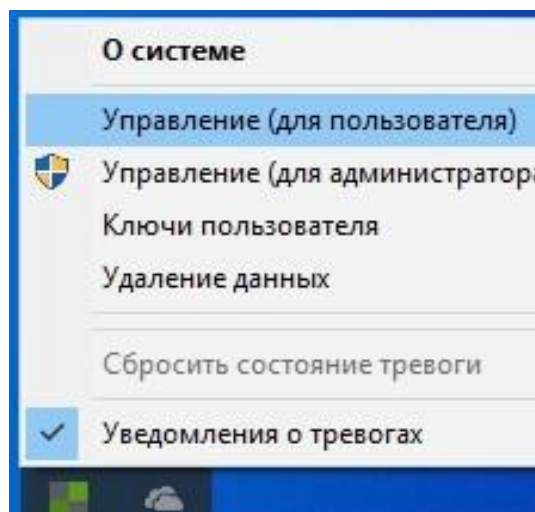


Рисунок 70 – Запуск «Локального центра управления» от имени пользователя

В программе «Локальный центр управления» перейдите на вкладку «Настройка». Все параметры доступны для просмотра, но недоступны для изменения. Перейдите на вкладку «Состояние», выберите компонент «Паспорт ПО». Кнопка «Собрать новое СПС» активна, следовательно, действие доступно для выполнения (рисунок 71).

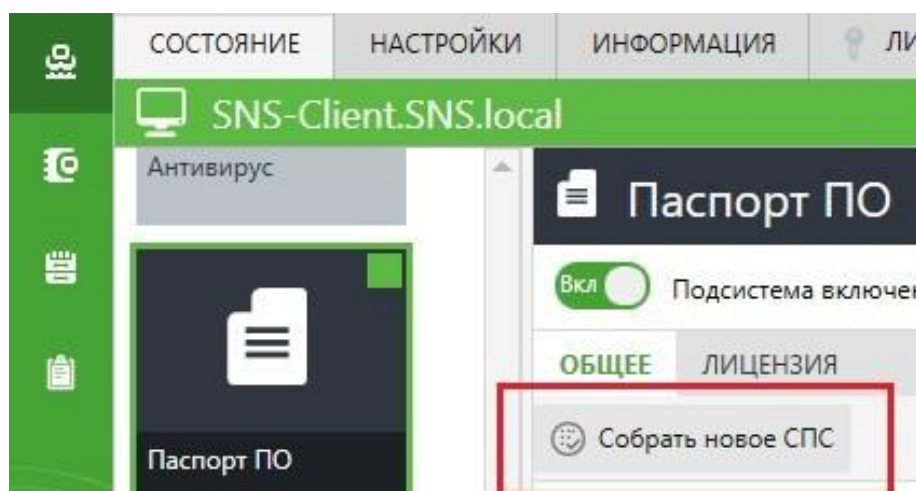


Рисунок 71 – Панель «Паспорт ПО»

Выберите компонент «Контроль устройств», нажмите на переключатель рядом с надписью «Подсистема включена» (рисунок 72). Никаких действий не произойдет, т.к. пользователю нельзя менять настройки СЗИ от НСД. Завершите сеанс пользователя user1.

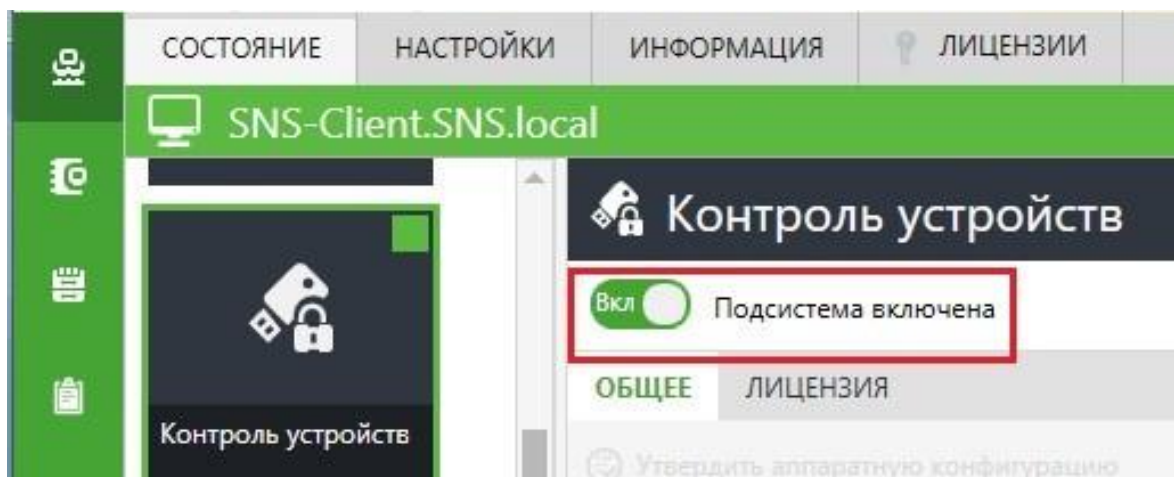


Рисунок 72 – Попытка переключения функции «Подсистема включена»

Переключитесь к окну виртуальной машины сервера безопасности SNS-Server. Войдите под учетной записью Администратора и запустите Центр управления. На панели «Компьютеры» включите отображение в виде таблицы, выберите сервер безопасности SNS-Server (с пиктограммой черного цвета) и откройте его свойства. Перейдите на вкладку «Настройки» и нажмите кнопку «Загрузить настройки» (рисунок 73).

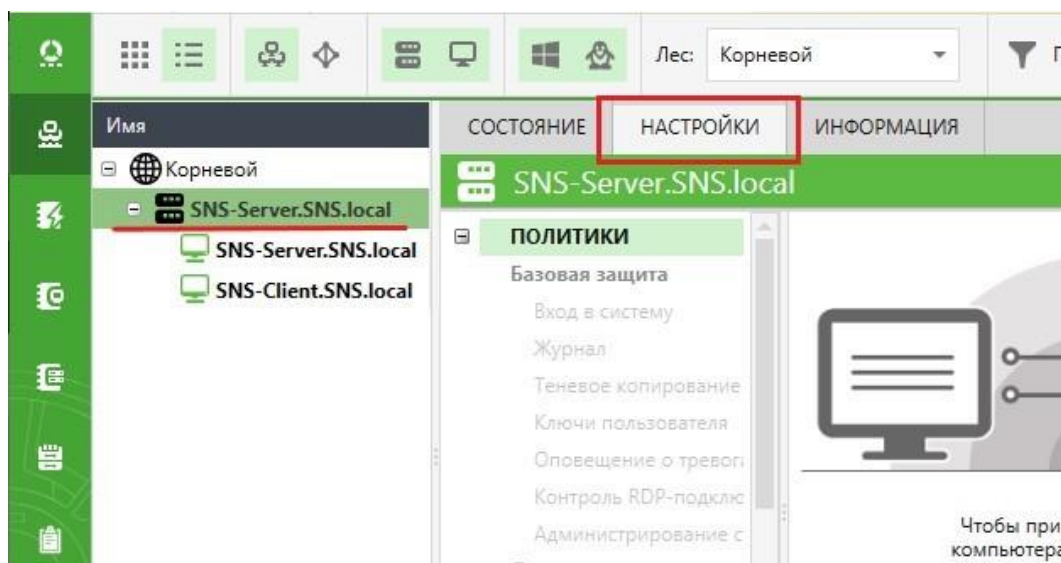


Рисунок 73 – Загрузка настроек

После установки СЗИ от НСД на всех защищаемых компьютерах применяются локальные параметры безопасности, заданные по умолчанию. Для настройки обязательных для всех компьютеров параметров необходимо выполнить настройку политики сервера безопасности. Применение параметров, заданных в разделах «Политики» и «Регистрация событий», осуществляется на компьютерах в следующей последовательности:

- параметры, заданные на компьютерах (локальные);
- параметры, заданные для доменов и организационных подразделений;
- параметры, заданные для серверов безопасности (вверх по иерархии серверов).

В практической работе существуют два уровня политик – локальные и заданные на сервере безопасности, т.к. компьютеры подчиняются непосредственно серверу безопасности SNS-Server. Таким образом, политики заданные на сервере безопасности будут иметь наивысший приоритет. Выберите в списке компьютеров SNS-Client и на вкладке «Настройки» нажмите кнопку «Загрузить настройки». В области оглавления выберите группу настроек «Базовая защита»- «Журнал» и просмотрите значение максимального размера журнала. Значение параметра соответствует тому, которое было установлено локально на компьютере SNS-Client. В графе «Источник» указано, что значение загружено из локальных параметров (рисунок 74).

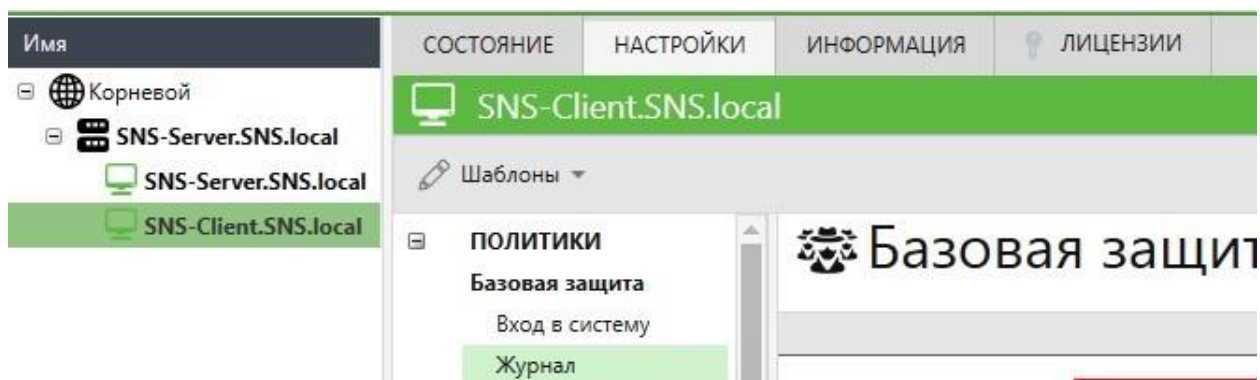


Рисунок 74 – Параметр «Журнал»

Параметры взяты из локальной политики, поскольку по умолчанию все параметры задаются локально, если политика Сервера безопасности не настроена. Для централизованной настройки параметров выполним настройку политики сервера безопасности в соответствии с Унифицированными конфигурациями.

Выберите в структуре сервер безопасности SNS-Server, в области оглавления выберите группу параметров «Базовая защита» - «Вход в систему» (рисунок 75).

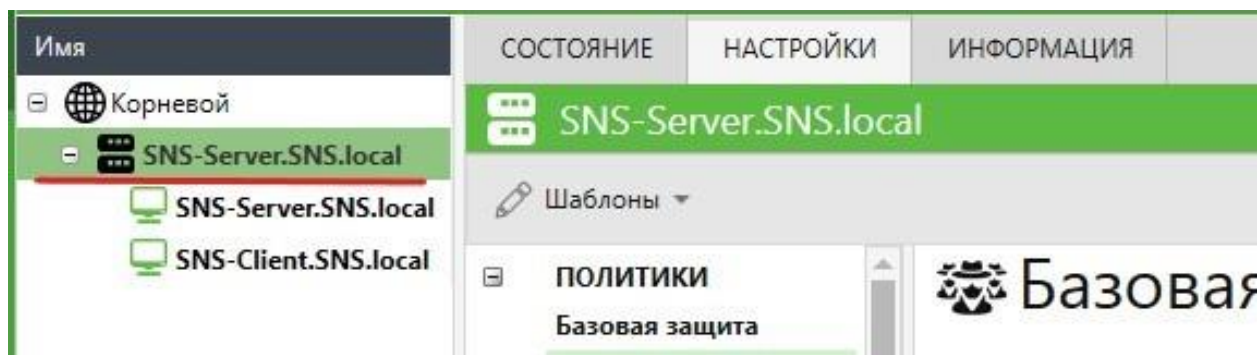


Рисунок 75 – Параметр «Вход в систему»

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к компьютеру. К механизму защиты входа относятся средства для идентификации и аутентификации пользователей, блокировки компьютера, аппаратные средства защиты от загрузки ОС со съемных носителей. В этой группе параметров осуществляется настройка параметров этих средств.

Рядом с каждым параметром (слева) расположена кнопка включения параметра. Если кнопка находится в положении «выключено» (серого цвета), то параметр политики сервера безопасности не задан, при этом значение параметра заблокировано для изменения (рисунок 76). В этом случае на защищаемых компьютерах применяется значение из локальной политики.

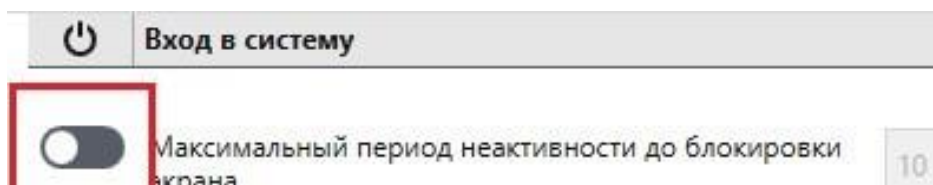


Рисунок 76 – Параметр «Максимальный период неактивности до блокировки экрана»

Нажмите на кнопку включения параметра «Максимальный период неактивности до блокировки экрана». Цвет кнопки изменится на зеленый, появится надпись «Вкл» и значение параметра станет доступным для изменения. Оставьте значение по умолчанию 10 минут, т.к. оно соответствует «Унифицированным конфигурациям» (рисунок 77). После «включения»

параметра в политике сервера безопасности и сохранения изменений в политике, параметр становится обязательным для применения на всех защищаемых компьютерах.

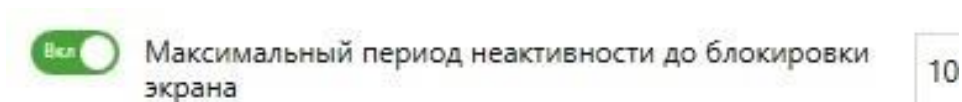


Рисунок 77 – Включение параметра

Включите все параметры в группе параметров «Вход в систему» (переведите кнопки в положение «Вкл») и нажмите кнопку «Применить» внизу области отображения параметров (рисунок 78). Теперь параметры, заданные в группе параметров «Вход в систему», будут обязательными для применения на подчиненных компьютерах.

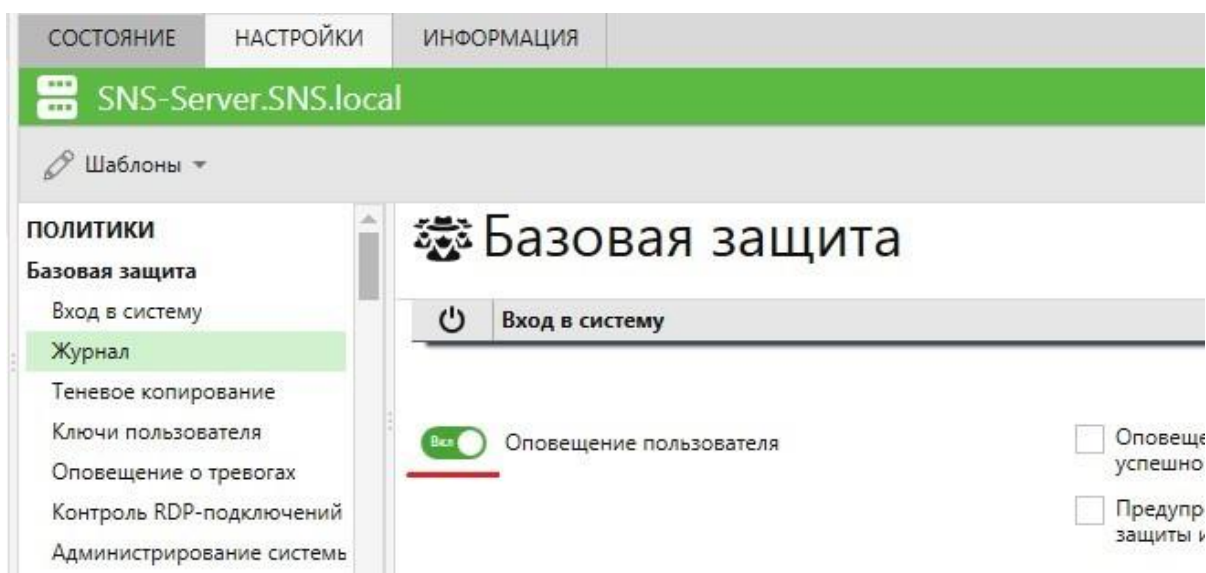


Рисунок 78 – Параметр «Вход в систему»

В левой части окна в панели «Компьютеры» в списке компьютеров выберите SNS-Client, нажмите правой кнопкой мыши на названии, в контекстном меню выберите пункт «Команды» - «Применить групповые политики» (рисунок 79).

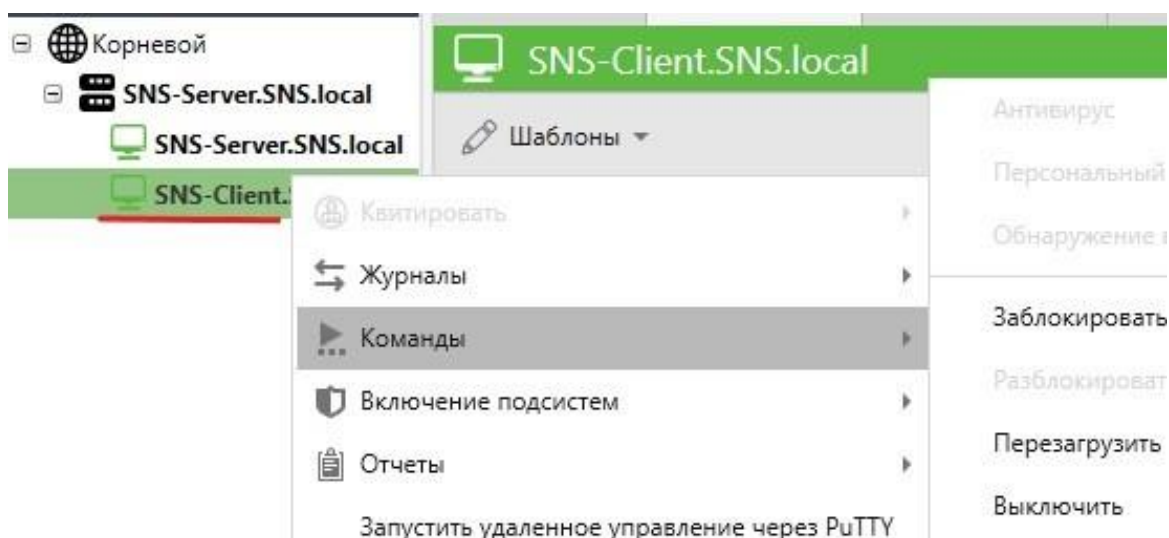


Рисунок 79 – Применение групповых политик

При выборе компьютера SNS-Client в правой части окна отобразятся его настройки. Через некоторое время после применения групповых политик параметры в группе «Вход в систему» будут заблокированы, а в графе «Источник» появится надпись SNS-Server.SNS.local (рисунок 80).



Рисунок 80 – Параметр «Вход в систему»

Выберите группу параметров «Журнал» компьютера SNS-Client. Параметры настройки журнала доступны для изменения (рисунок 81), поскольку в политике сервера безопасности были включены только настройки входа в систему, поэтому все остальные настройки берутся из локальной политики.

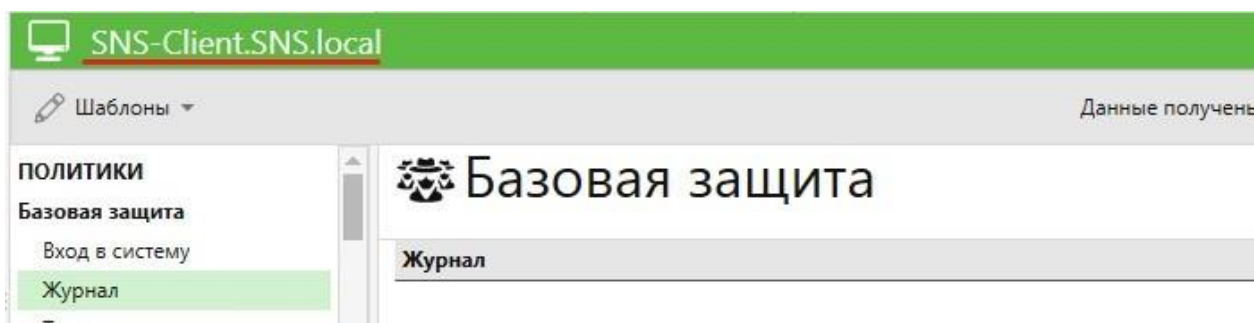


Рисунок 81 – Параметр «Журнал»

Помимо включения использования параметра в политике сервера безопасности, необходимо также выполнить настройку параметров в соответствии с Унифицированными конфигурациями. Выберите в списке компьютеров сервер безопасности SNS-Server (рисунок 82), в области оглавления снова выберите группу настроек «Базовая защита» - «Вход в систему».

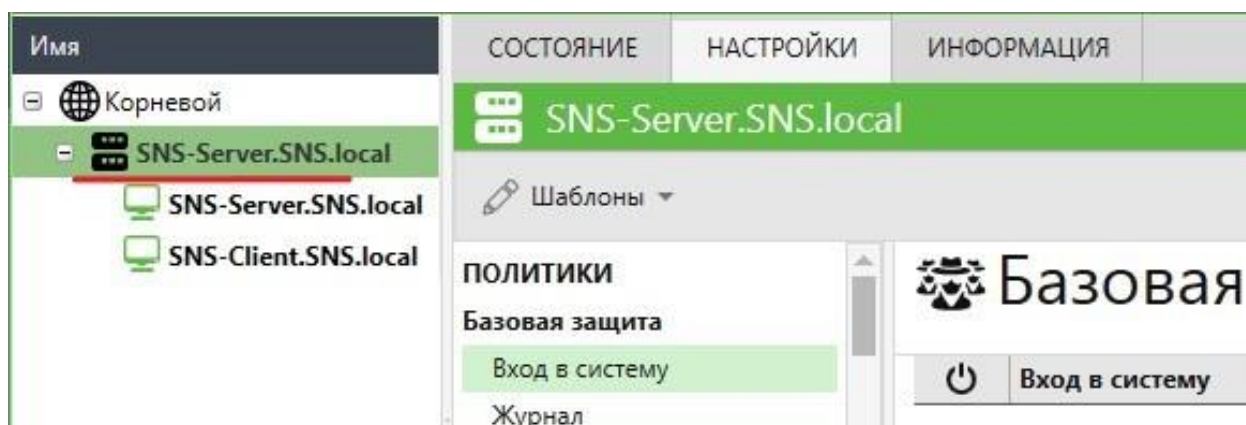


Рисунок 82 – Журнал «Вход в систему»

Вставьте значения из таблицы 1, согласно вашему варианту, в «Максимальный период неактивности до блокировки экрана».

Проверьте соответствие следующих настроек по умолчанию значениям, приведенным в Унифицированным конфигурациях:

- запрет вторичного входа в систему: отключено;
- реакция на изъятие идентификатора: не блокировать;
- количество неудачных попыток аутентификации: 0;
- разрешить интерактивный вход только доменным пользователям: отключено.

Для значения каждого параметра можно получить справочную информацию, для этого надо нажать на кнопку с обозначением «i» справа от значения параметра (рисунок 83). Также пиктограммами указывается применимость параметра для агентов соответствующих операционных систем.



Рисунок 83 – Справка значения параметра

В Унифицированных конфигурациях указано, что значение параметра «Режим идентификации пользователя» должно быть «Только по идентификатору». Но в рамках выполнения практической работы из-за ограничения виртуальной среды установите значение «По имени» (рисунок 84).

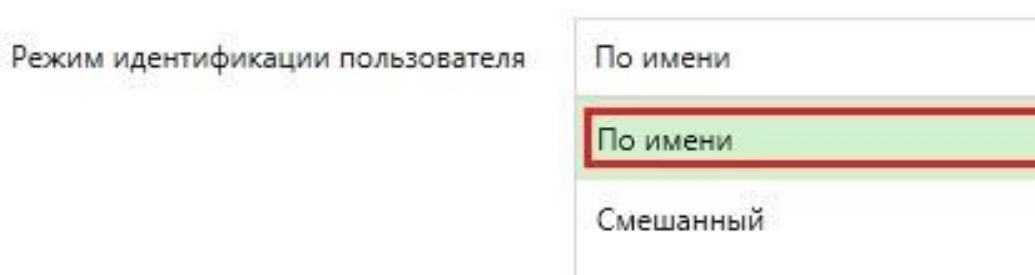


Рисунок 84 – Параметр «Режим идентификации пользователя»

Выберите в разделе «Базовая защита» следующую группу параметров «Журнал». В этой группе параметров устанавливаются общие настройки, касающиеся журналов – объем, политика перезаписи и разграничение привилегий на работу с журналами. Перечень событий, подлежащих регистрации настраивается в другом разделе политики – «Регистрация событий».

В группе параметров «Базовая защита» - «Журнал» включите использование параметров «Максимальный размер журнала» и «Политика перезаписи событий».

Для параметра «Максимальный размер журнала» в Унифицированных конфигурациях указано значение 524288 КБ, однако для выполнения практического задания большой размер журнала устанавливать нецелесообразно, поэтому установите значение 65536 Кб. Значение параметра «Политика перезаписи событий» должно быть установлено в положение «Затирать события по мере необходимости».

Параметры «Учетные записи с привилегией просмотра журнала системы защиты» и «Учетные записи с привилегией управления журналом системы защиты» будут настраиваться позднее при работе с подсистемой регистрации событий.

После установки параметров нажмите кнопку «Применить» (рисунок 85).

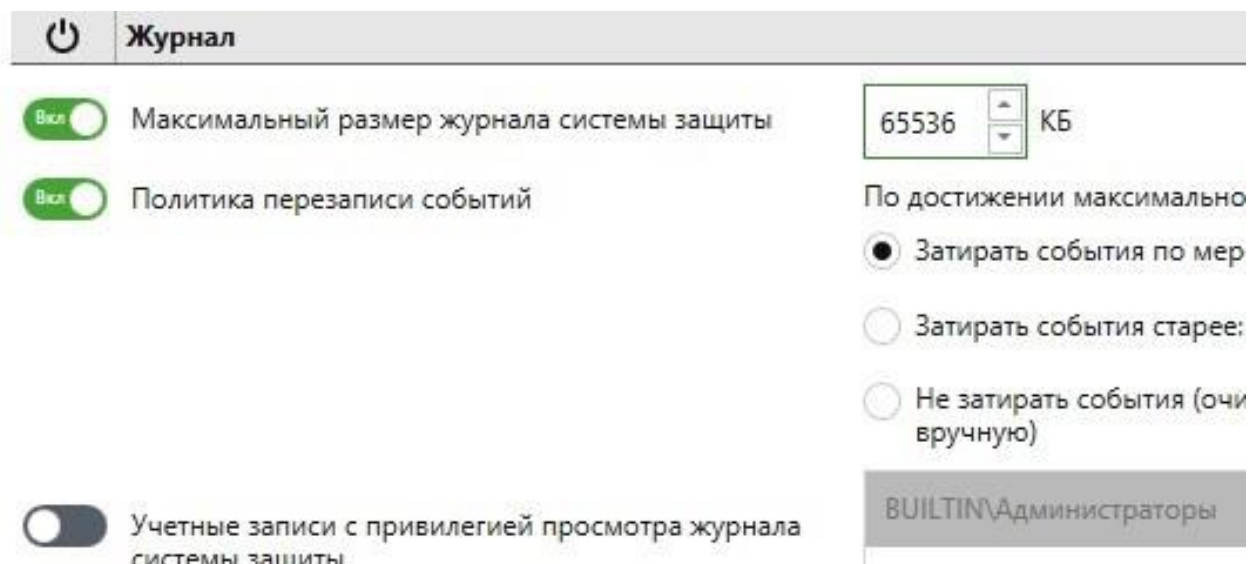


Рисунок 85 – Применение параметров

Выберите раздел «Теневое копирование». Теневое копирование используется для создания дубликатов данных, выводимых на съемные носители. В разделе «Базовая защита» настраивается только объем дискового пространства и перезапись событий. Сам механизм теневого копирования в соответствии с Унифицированными конфигурациями не используется, поэтому его настройка в политике не требуется. Непосредственно отключение теневого копирования осуществляется при настройке контроля устройств. Оставьте параметры в этом разделе без изменений.

Выберите раздел «Ключи пользователя». Включите использование всех параметров этого раздела в политике сервера безопасности. В поле «Максимальный срок действия ключа» установите значение 0 (означает, что ограничение не действует). Появится окно «Зависимые параметры» (рисунок 86). Нажмите кнопку «Применить».

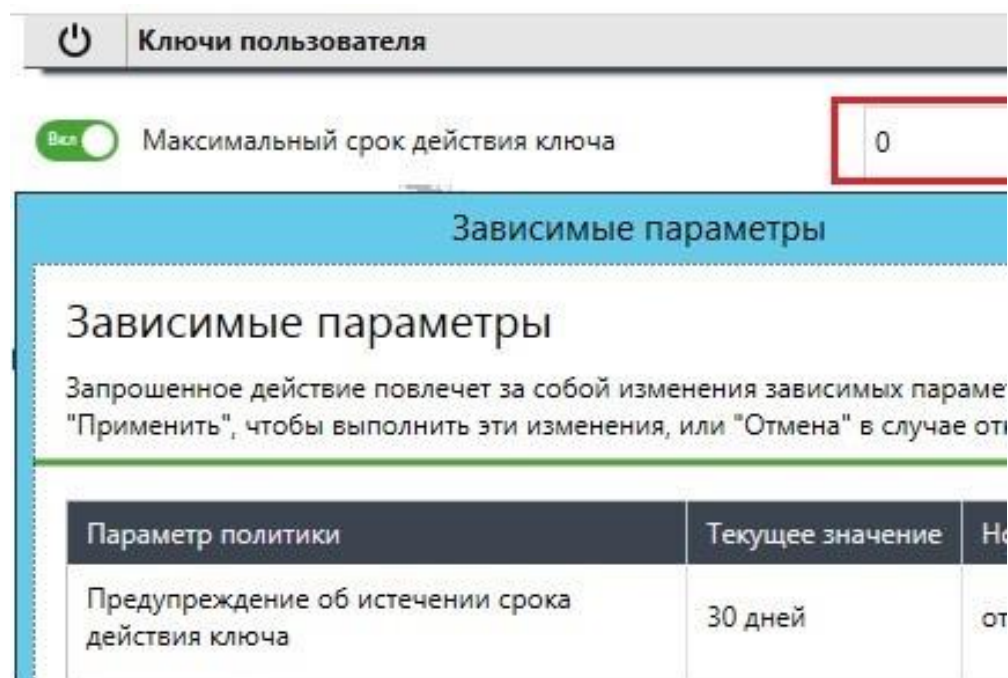


Рисунок 86 – Применение «Зависимых параметров»

Автоматически значение «Предупреждение об истечении срока действия ключа» установится в 0, рядом со значением «Максимальный срок действия ключа» появится надпись «Ключ не устаревает». Значение параметра «Минимальный срок действия ключа» установите в 0. Нажмите кнопку «Применить» для сохранения параметров политики (рисунок 87).

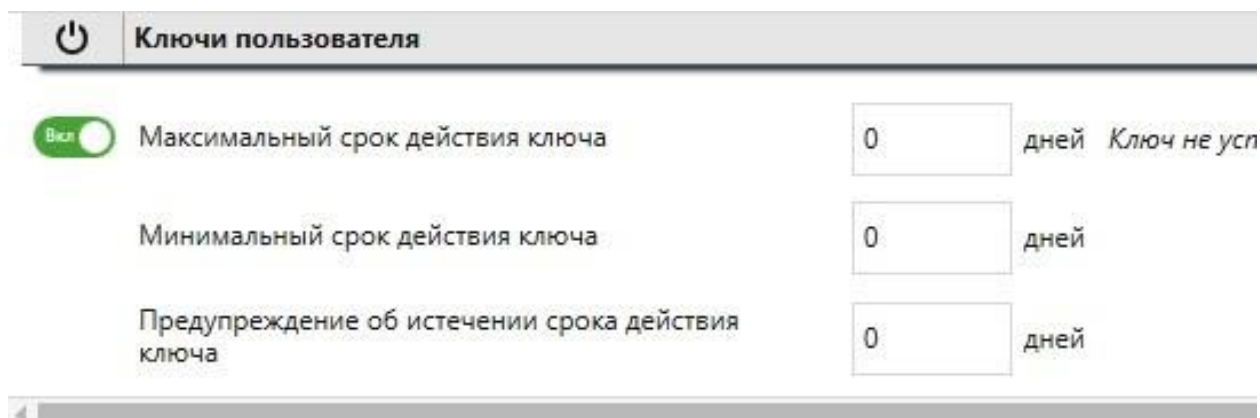


Рисунок 87 – Сохранение параметров политик

Выберите раздел «Оповещение о тревогах». Включите использование параметра «Локальное оповещение о тревогах», в выпадающем списке выберите значение параметра «Отключено». Включите использование параметра «Фильтр

тревог...» и под таблицей правил установите флаг «Отключить фильтр» (рисунок 88).

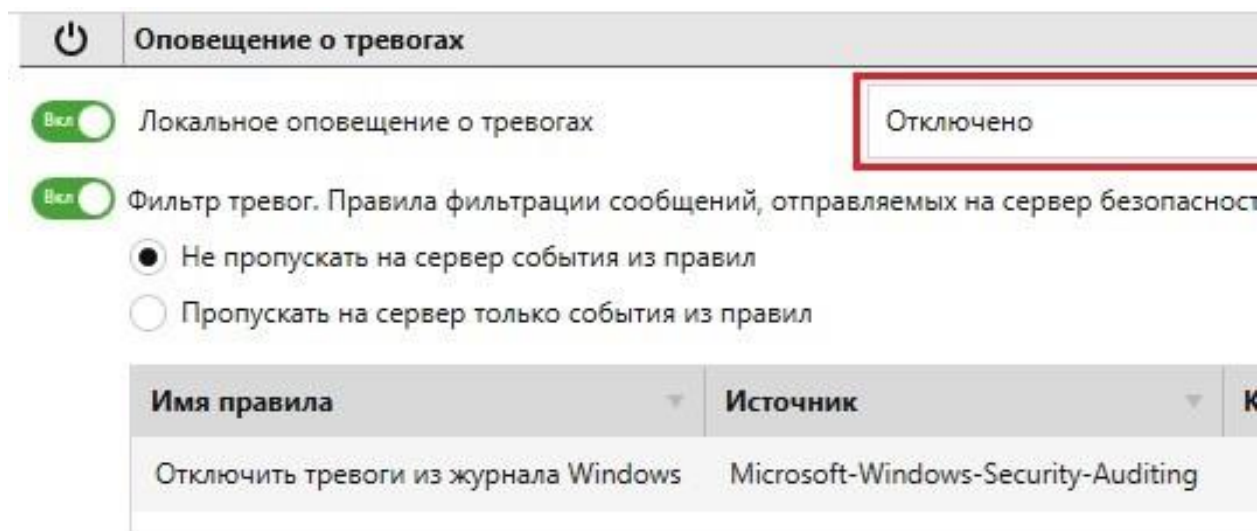


Рисунок 88 – Отключение фильтра тревог

Выберите раздел «Контроль RDP подключений», включите использование всех параметров в этой группе. Значения всех параметров должны быть установлены в значение «Определяется политиками Windows» (рисунок 89).

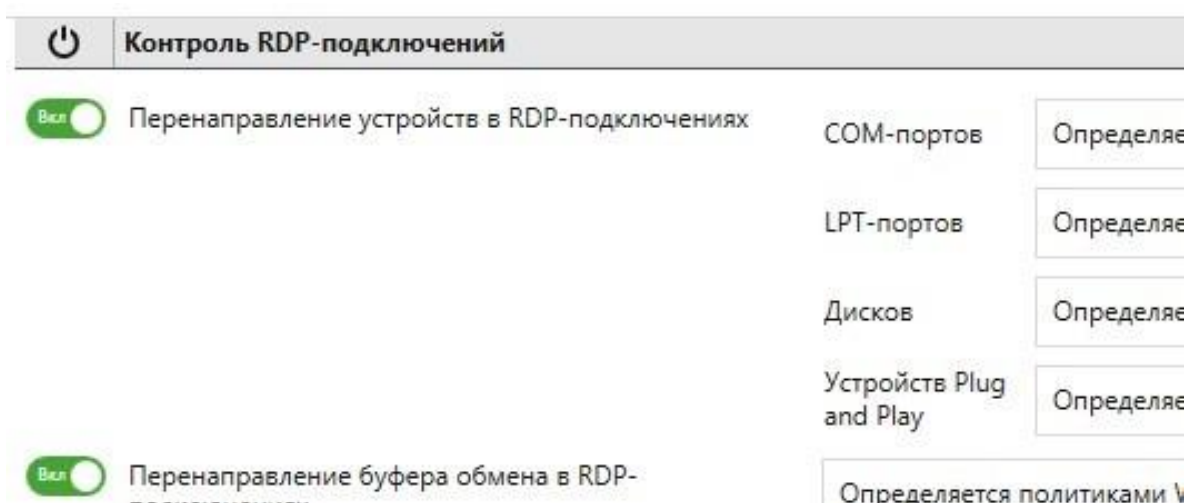


Рисунок 89 – Параметр «Контроль RDP подключений»

Перейдите к следующему разделу «Администрирование системы защиты», включите использование всех параметров. В группе параметров «Самозащита продукта» должен быть установлен флаг «Включить». Установите флаг «Включить контроль административных привилегий», после чего появится окно с информацией о необходимости установки PIN администратора. Нажмите «Да». Затем нажмите на кнопку «Изменить» в поле PIN администратора. Откроется

окно ввода и подтверждения PIN. Введите произвольный PIN (например, 123456789) и нажмите «Применить» (рисунок 90).

Рисунок 90 – Ввод нового PIN администратора

В поле «Учетные записи с привилегией управления механизмом самозащиты» нажмите кнопку «Добавить» (+) под списком групп (рисунок 91).

Рисунок 91 – Добавление учетных записей

В окне «Выбор:…» нажмите кнопку «Размещение» (рисунок 92).

Рисунок 92 – Выбор «Размещения»

В окне «Размещение» раскройте узел «Весь каталог» и выберите узел SNS.local (рисунок 93). Нажмите «ОК».

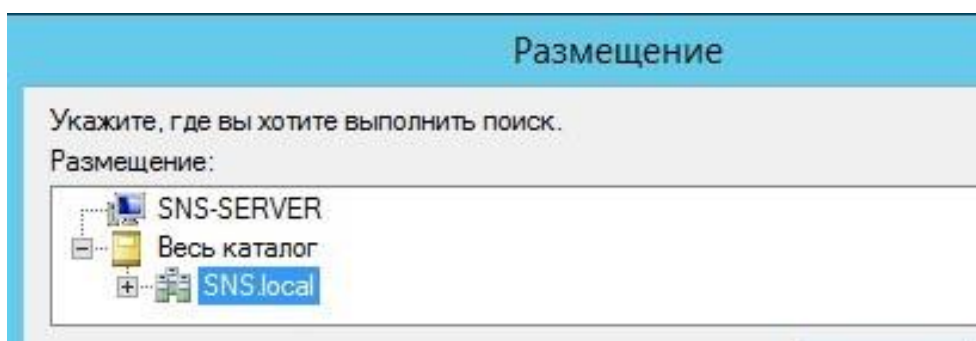


Рисунок 93 – Выбор узла «SNS.local»

В поле ввода начните вводить название группы SecretNetAdmin_Domain (несколько первых символов) и нажмите кнопку «Проверить имена». После выполнения поиска выберите имена групп SecretNetAdmin_Domain и SecretNetAdmin_Forest, нажмите «ОК» (рисунок 94) и еще раз нажмите «ОК» в окне выбора групп.

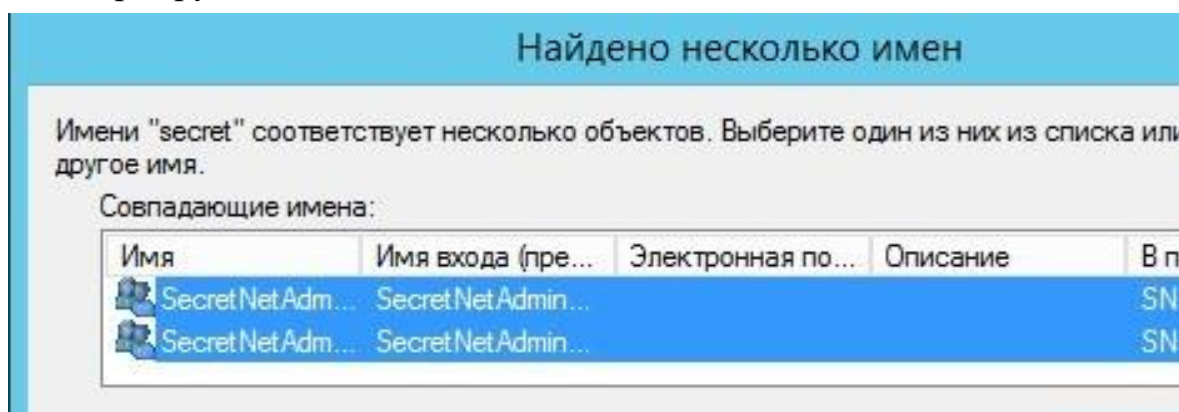


Рисунок 94 – Выбор групп

Группы добавятся в список привилегий управления механизмом самозащиты. Выберите в списке группу BUILTIN\Администраторы и нажмите кнопку «Удалить» под списком (рисунок 95). Теперь локальные администраторы, не включенные в группы управления СЗИ от НСД не смогут управлять самозащитой. Нажмите кнопку «Применить» для сохранения изменений в политике сервера безопасности.

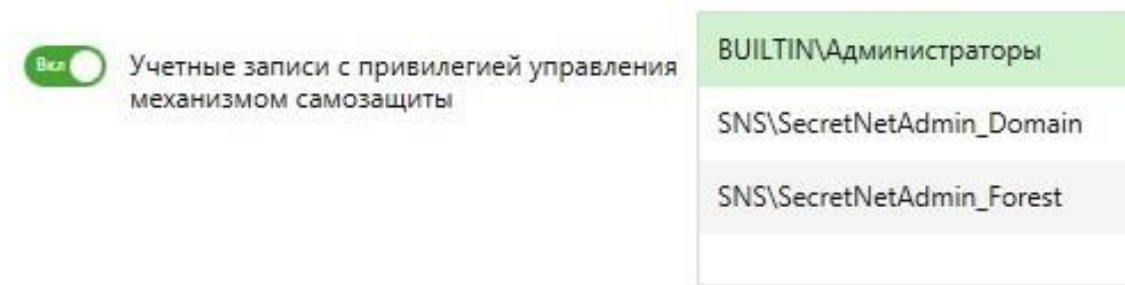


Рисунок 95 – Сохранение изменений в политике сервера безопасности

Перейдите к группе параметров «Локальная защита», в которой настраиваются параметры функционирования механизмов защиты. В соответствии с Унифицированными конфигурациями настройка параметров в разделе «Дискреционная защита» не требуется, т.к. компонент не используется.

Выберите раздел «Затирание данных», включите использование в политике всех параметры группы за исключением параметра «Список исключений», поскольку этот компонент не используется.

В унифицированных конфигурациях указано, что для параметра «Количество циклов затирания на локальных дисках» должны быть установлены следующие значения параметров:

- рабочие места пользователей: 1;
- серверы: 0.

Также указано, что на определенных разновидностях серверов и рабочих местах могут использоваться другие значения. Поскольку в политике безопасности сервера для параметра нет возможности выбора типа компьютеров, на которые будет применяться политика, то этот параметр надо будет настраивать отдельно для разных компьютеров в локальной политике. Поэтому отключите использование параметра «Количество циклов затирания на локальных дисках» в политике безопасности сервера (рисунок 96).

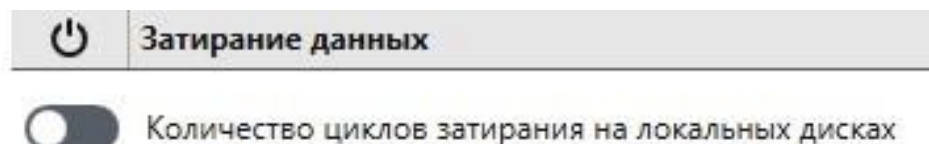


Рисунок 96 – Отключение параметра «Количество циклов затирания на локальных дисках»

Установите значения остальных параметров:

- количество циклов затирания на сменных носителях: 1;
- количество циклов затирания оперативной памяти: 0;
- количество циклов затирания по команде «удалить безвозвратно»: 2;
- количество циклов затирания при уничтожении данных на дисках: 0.

После изменения параметров нажмите кнопку «Применить».

В соответствии с Унифицированными конфигурациями настройка параметров в разделе «Полномочное управление доступом» не требуется, т.к. компонент не используется.

Выберите раздел «Замкнутая программная среда». Включите использование параметра «Учетные записи, на которые не действуют правила замкнутой программной среды» в политике сервера безопасности. Добавьте в список группы SecretNetAdmin_Forest, SecretNetAdmin_Domain и SPOAdmins и удалите группу локальных администраторов (рисунок 97). В Унифицированных конфигурациях также указана группа ModifyAdmins, не используемая в практической работе. Нажмите «Применить» для сохранения настроек.

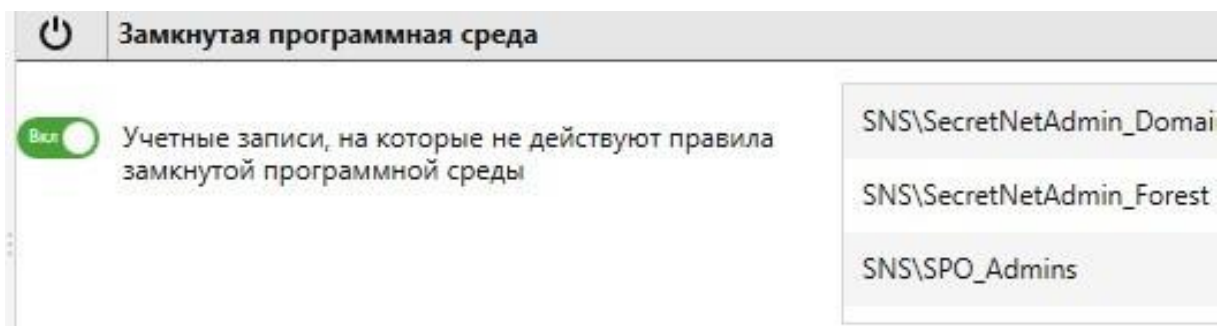


Рисунок 97 – Добавление групп в параметре «Учетные записи, на которые не действуют правила замкнутой программной среды»

Механизм «Защита диска и шифрование данных» не используется, поэтому настройка не требуется.

Компоненты раздела «Сетевая защита» не были установлены, поскольку не используются в соответствии с Унифицированными конфигурациями, поэтому их параметры недоступны для просмотра.

Настройка компонентов «Контроль печати», «Антивирус», «Обнаружение вторжений» и «Обновление» не требуется, т.к. компоненты не используются в соответствии с Унифицированными конфигурациями.

Настройка компонентов «Контроль устройств» и «Паспорт ПО», а также параметров регистрации событий будет выполняться позже.

Далее применим настройки политики сервера безопасности к компьютерам и настроим локальные параметры сервера и рабочей станции, не заданные в политике сервера безопасности. В левой части окна в списке компьютеров выберите левой кнопкой мыши компьютер SNSClient, нажмите клавишу Shift и левой кнопкой мыши выберите сервер SNS-Server. Нажмите правой кнопкой мыши на выбранной группе компьютеров и выберите в контекстном меню пункт «Команды» - «Применить групповые политики» (рисунок 98).

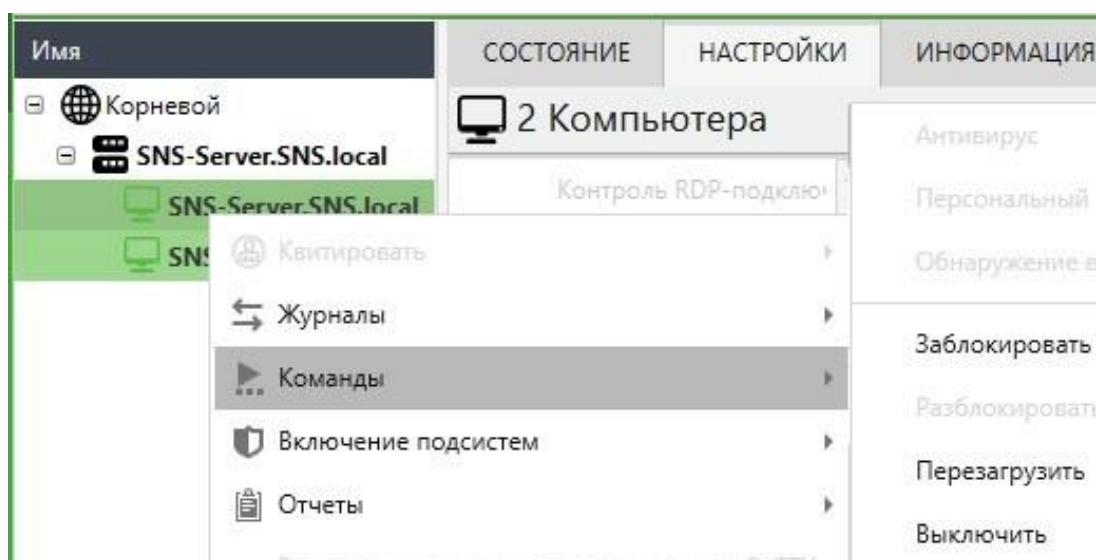


Рисунок 98 – Применение групповых политик

После обновления параметров в окне событий появится запись об изменении параметров на управляемых компьютерах (рисунок 99). Также появится уведомление о необходимости перезагрузки.

Тип	Дата и время	Событие	Оп
+	25.02.2023 11:23:38	На агенте SNS-Client.SNS.local изменились политики.	Уве
+	25.02.2023 11:23:36	На агенте SNS-Server.SNS.local изменились политики.	Уве

Рисунок 99 – Запись об изменениях параметров в окне событий

Выполните перезагрузку компьютера SNS-Client удаленно. Для этого выберите в списке компьютеров компьютер SNS-Client, в контекстном меню выберите «Команды» - «Перезагрузить» и нажмите «ОК» в окне предупреждения. Компьютер SNS-Client будет перезагружен. Для перезагрузки SNS-Server нажмите Win+R, введите команду shutdown /r /t 0 и нажмите Enter.

После перезагрузки запустите Центр управления. Перейдите к панели «Компьютеры», выберите компьютер SNS-Server, загрузите настройки. Просмотрите значения параметров в группе параметров «Базовая защита – Вход в систему». Все параметры недоступны для изменения, соответствуют параметрам, указанным в политике сервера безопасности. В графе «Источник» указан сервер безопасности SNS-Server.SNS.local (рисунок 100).



Рисунок 100 – Просмотр параметров

Просмотрите значения параметров в группе параметров «Базовая защита – Журнал». Параметры «Максимальный размер журнала» и «Политика перезаписи событий» были настроены в политике сервера безопасности и недоступны для изменения. Настройка привилегий в политике сервера не выполнялась, поэтому для этих параметров действуют настройки локальной политики (рисунок 101).

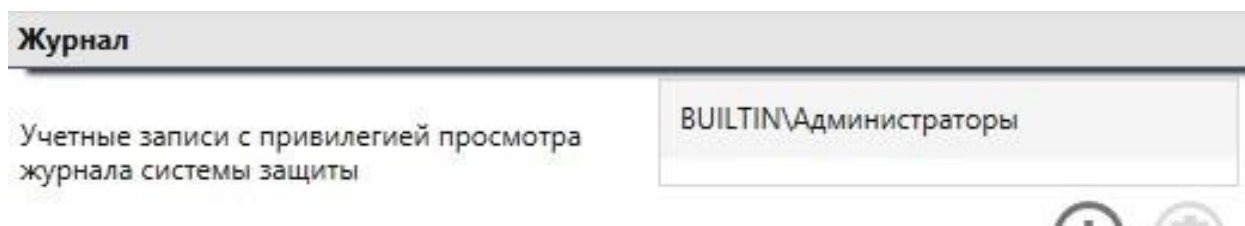


Рисунок 101 – Настройка привилегий

Выберите группу параметров «Локальная защита – Затирание данных». Установите параметр «Количество циклов затирания на локальных дисках» в значение 0 (рисунок 102).

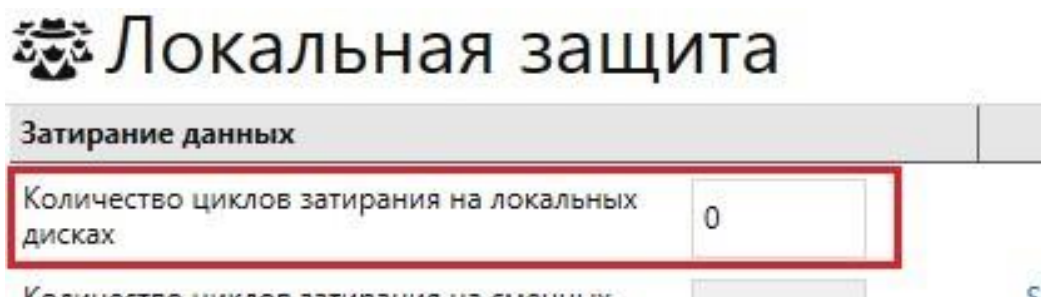


Рисунок 102 – Установка параметра «Количество циклов затирания на локальных дисках»

В списке компьютеров выберите SNS-Client, загрузите настройки. Установите значение параметра «Количество циклов затирания на локальных дисках» в 1. Нажмите кнопку «Применить». Примените групповую политику на компьютере (команда «Применить групповые политики»).

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью Администратора. Запустите «Локальный центр управления» и перейдите на вкладку «Настройки». Просмотрите значения настроек и их источник (рисунок 103).

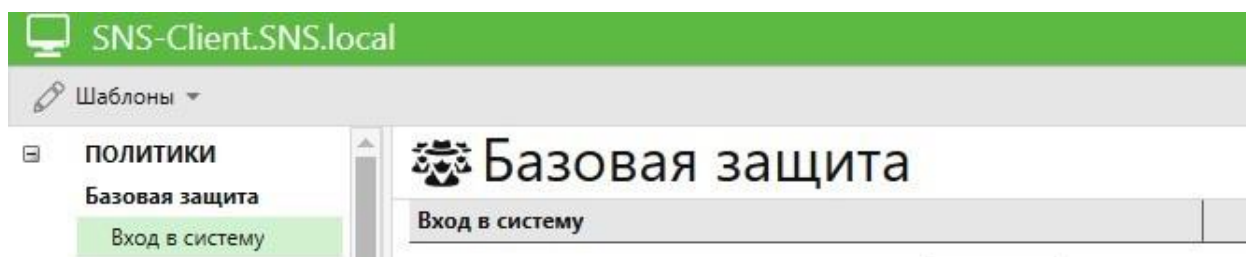


Рисунок 103 – Просмотр значений настроек и их источника

Закройте Локальный центр управления и завершите сеанс Администратора (Win+R, shutdown /L).

7.6 Настройка подсистемы контроля устройств

Настройку параметров подсистемы контроля устройств можно выполнять как для всей структуры путем редактирования политики сервера безопасности, так и для каждого отдельного защищаемого компьютера в локальной политике (с сервера или локально). На сервере безопасности целесообразно выполнить

настройку параметров, которые не зависят от конфигурации отдельного компьютера или характера выполняемых функций пользователей.

Перед настройкой подсистемы контроля устройств к компьютеру рекомендуется подключить все устройства, которые будут на нем использоваться (включая съемные носители информации).

Зарегистрируйтесь на компьютере SNS-Server под учетной записью Администратора. Запустите Центр управления. На панели «Компьютеры» откройте окно свойств сервера безопасности, перейдите на вкладку «Настройки» и нажмите кнопку «Загрузить настройки». В разделе «Политики» выберите группу настроек «Контроль устройств». Включите использование параметра «Теневое копирование» в политике сервера безопасности и выберите в выпадающем списке значение «Отключено для всех устройств» (рисунок 104).

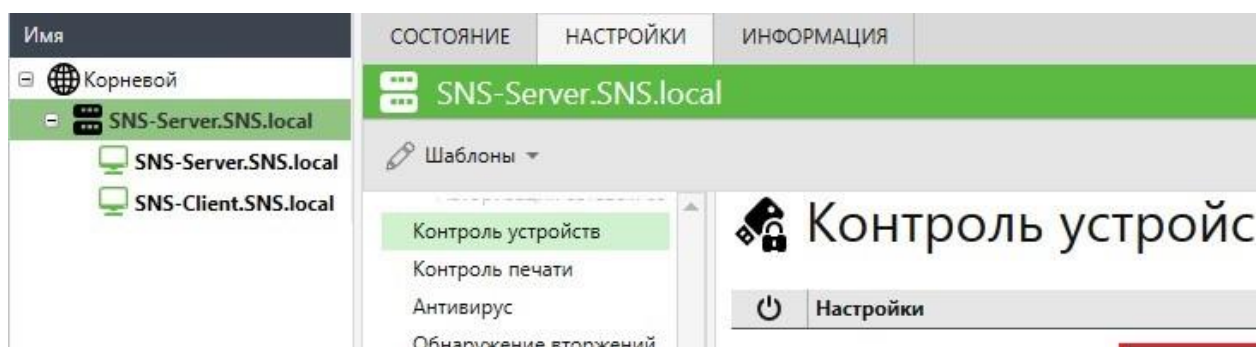


Рисунок 104 – Параметр «Теневое копирование»

В поле «Устройства» установите параметр «Политика» в положение «Включена». После этого загрузятся настройки компонента «Контроль устройств» (рисунок 105).

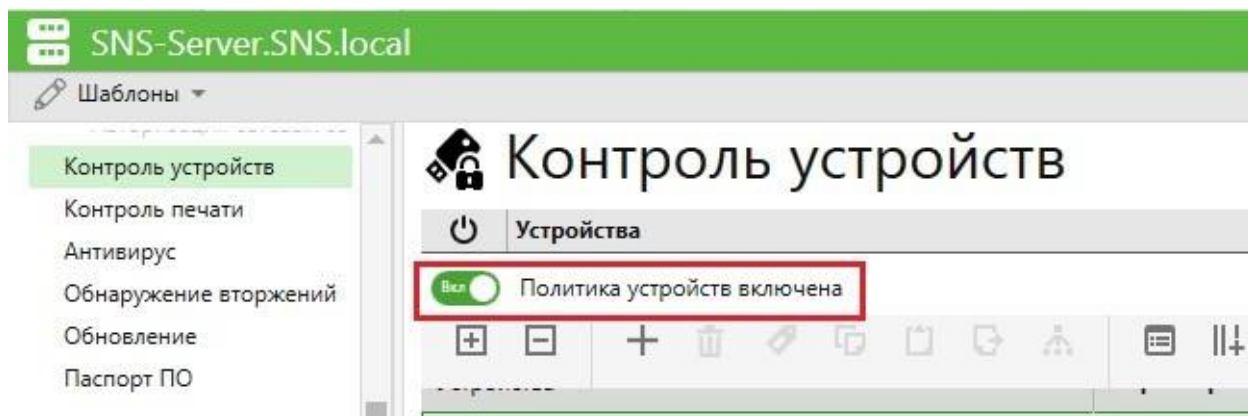


Рисунок 105 – Включение «Политики устройств»

В панели инструментов, расположенной над списком устройств, нажмите кнопку «Колонки таблицы». Откроется выпадающий список для выбора отображаемых настроек для устройства. Снимите флаг «Теневое копирование», поскольку параметр не используется (рисунок 106). Нажмите еще раз кнопку «Колонки таблицы» для скрытия списка. В списке параметров пропадет столбец «Теневое копирование».

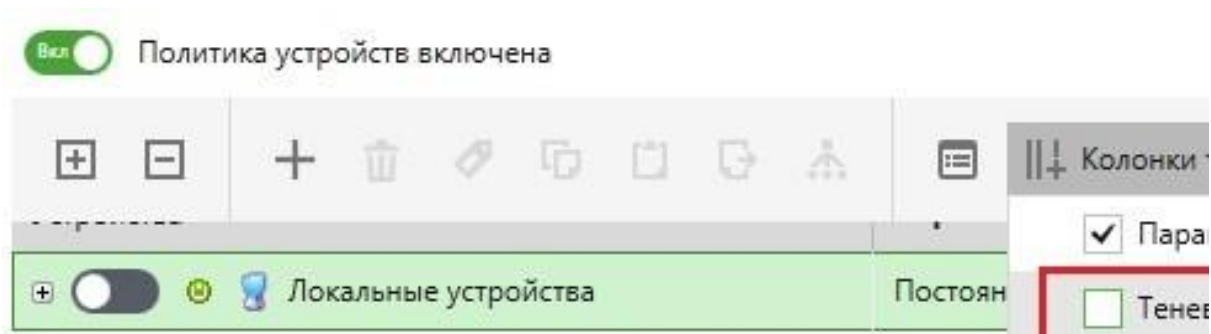


Рисунок 106 – Отключение параметра «Теневое копирование»

Выберите ниже в списке параметров группу «Локальные устройства», щелкнув один раз левой клавишей мыши по названию группы. В панели инструментов, расположенной над списком устройств, выберите команду «Показать информацию об устройстве». Отобразится информация о выбранной группе устройств (рисунок 107).

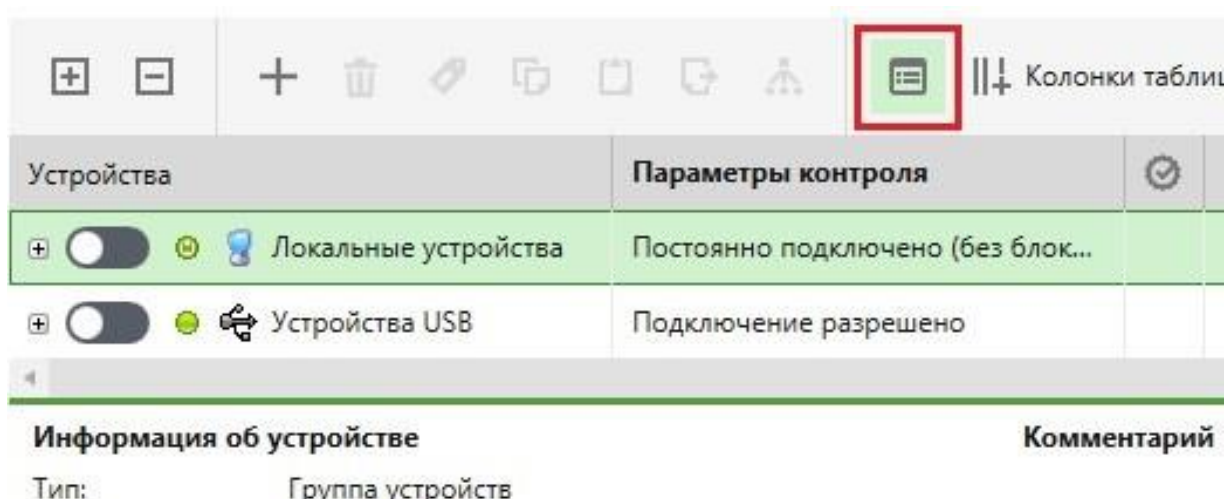


Рисунок 107 – Информация о выбранной группе устройств

В политике сервера безопасности отображается только общая информация о типах устройств и нет возможности добавления комментария. Закройте окно

информации, нажав кнопку «Показать информацию об устройстве» или кнопку «Закрыть» в окне просмотра информации.

В столбце «Параметры контроля» нажмите по пиктограмме «стрелка вниз» рядом с этим значением (рисунок 108). Будет отображено диалоговое окно настройки параметров контроля подключения группы устройств. В этом окне настраиваются параметры контроля устройства или группы устройств. Параметры контроля позволяют отключить контроль устройств, если выбран параметр «Устройство не контролируется». Контроль подключения устройства заключается в проверке постоянного подключения устройств к компьютеру, при этом устанавливается значение «Устройство постоянно подключено к компьютеру». Дополнительно можно включить блокировку компьютера в качестве реакции на отключение или замену устройств, входящих в группу локальных, установив флаг «Блокировать компьютер при изменении устройства». После просмотра параметров закройте диалоговое окно свойств, нажав левой кнопкой мыши вне окна параметров контроля.

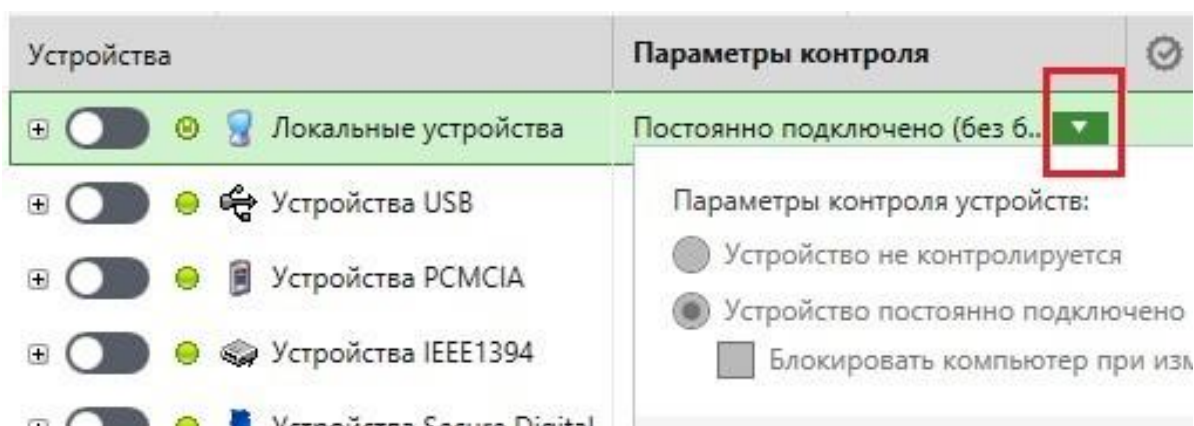


Рисунок 108 – Диалоговое окно свойств

Раскройте узел «Локальные устройства», нажав на кнопку «+». Выберите устройство «Последовательные порты». После столбца параметров контроля размещена кнопка «Разрешения» (рисунок 109). При ее нажатии открывается диалоговое окно настройки разрешений доступа к группе или классу устройств, а также к отдельным устройствам. Сейчас кнопка не активна.

Устройства	Параметры контроля
Локальные устройства	Постоянно подключено (без блок...
Последовательные п...	Наследуются (Постоянно подклоч...
Параллельные п...	Наследуются (Постоянно подклоч...

Рисунок 109 – Раскройте узел «Локальные устройства»

Выберите устройство «Сменные диски». В столбце «Параметры доступа» нажмите на пиктограмме «стрелка вниз», откроется окно параметров доступа (рисунок 110). В этом окне настраивается наследование настроек, а также параметры доступа при полномочном распределении доступа. Закройте диалоговое окно свойств, нажав левой кнопкой мыши вне окна параметров доступа.

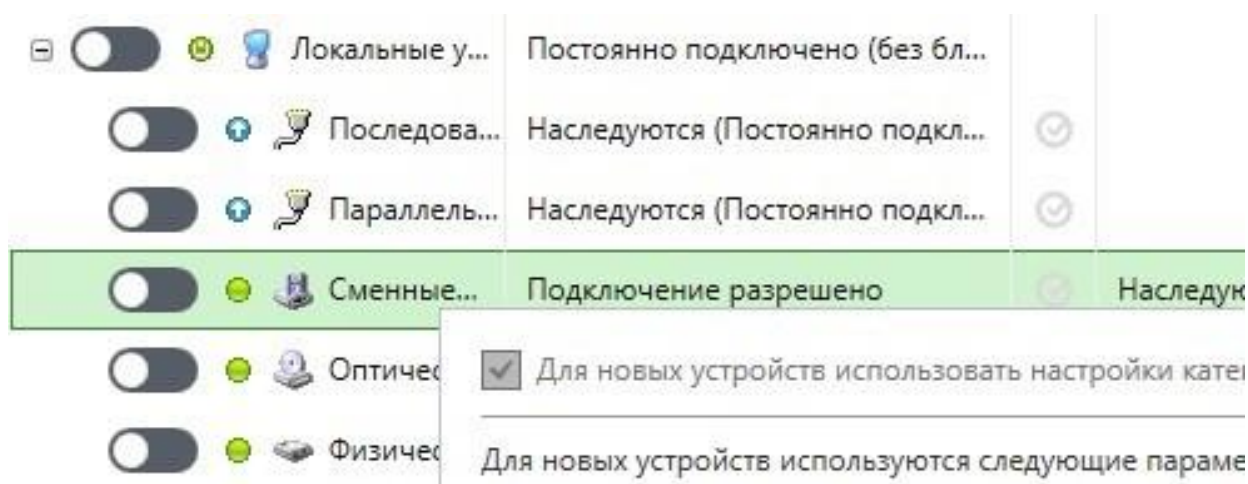


Рисунок 110 – Окно параметров доступа

Нажмите кнопку «Применить» для сохранения изменений в политике сервера безопасности.

Настройку параметров контроля в соответствии с Унифицированными конфигурациями выполним непосредственно в локальной политике защищаемого компьютера.

Выберите в списке устройств SNS-Client. Примените групповые политики к компьютеру. Дождитесь окончания применения настроек. В списке политик выберите «Контроль устройств». Факт применения настроек можно определить

по значению графы «Источник» параметра «Теневое копирование» (рисунок 111). В графе должен отобразиться источник SNS-Server.SNS.local.

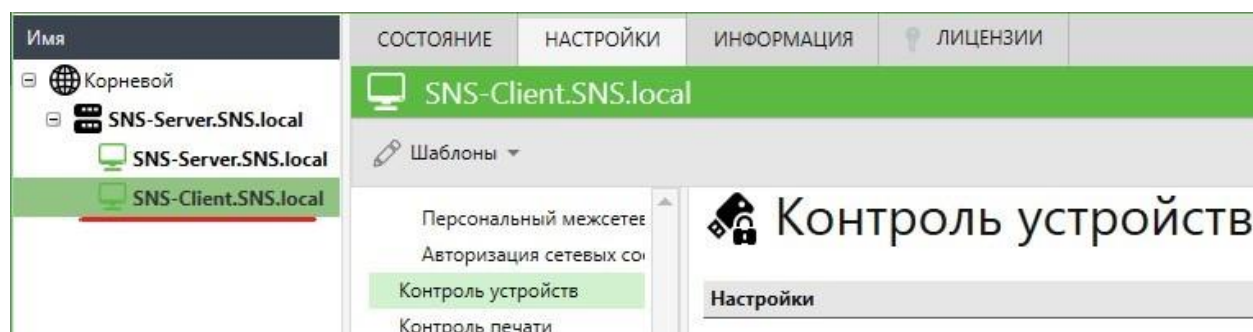


Рисунок 111 – Параметр «Контроль устройств»

В группе параметров «Устройства» выберите в списке группу устройств «Локальные устройства». Нажмите один раз левой клавишей мыши по текущему значению параметров контроля в столбце «Параметры контроля». Должен быть установлен параметр «Устройство постоянно подключено к компьютеру», флаг «Блокировать компьютер при изменении устройства» должен быть снят (рисунок 112). Закройте окно параметров контроля, нажав кнопку «Отменить».

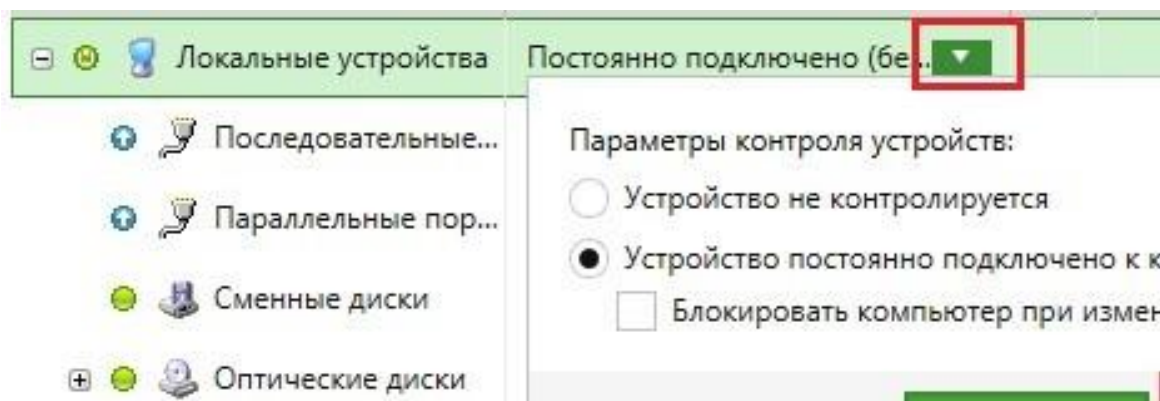


Рисунок 112 – «Параметры контроля»

Выберите в списке следующее устройство «Последовательные порты», откройте окно параметров контроля. Должен быть установлен параметр «Устройство постоянно подключено к компьютеру», флаг «Блокировать компьютер при изменении устройства» должен быть снят (рисунок 113). Снимите флаг «Наследовать настройки контроля от родительского объекта» (квадрат 1 на рисунке 113), нажмите кнопку «Применить». Затем нажмите кнопку «Разрешения» (квадрат 2 на рисунке 113).

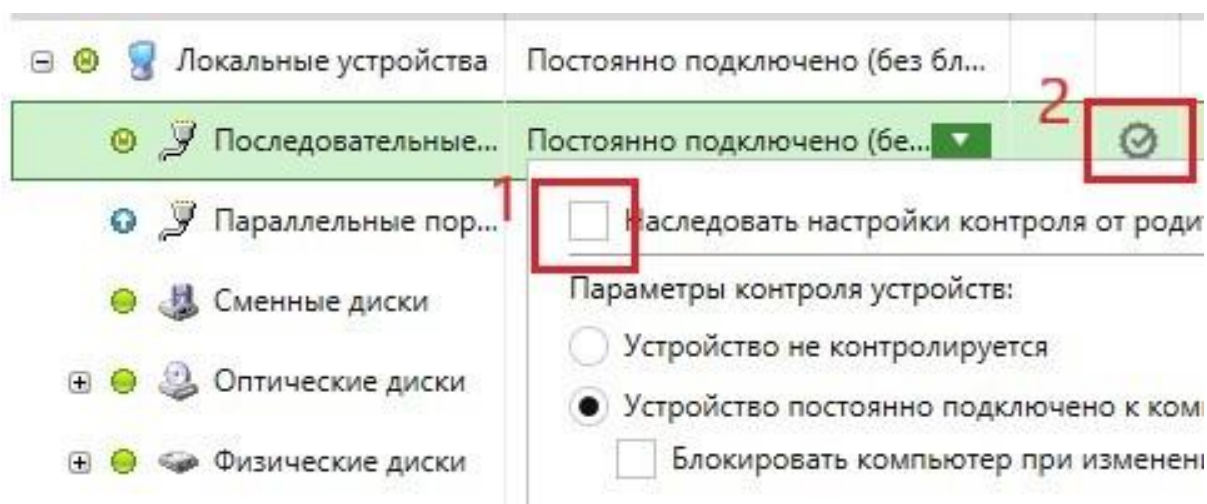


Рисунок 113 – Установка параметров контроля

Откроется окно редактирования разрешений. Выберите в списке группу «Все» и нажмите кнопку «Удалить» (рисунок 114). Нажмите кнопку «ОК» в окне разрешений.

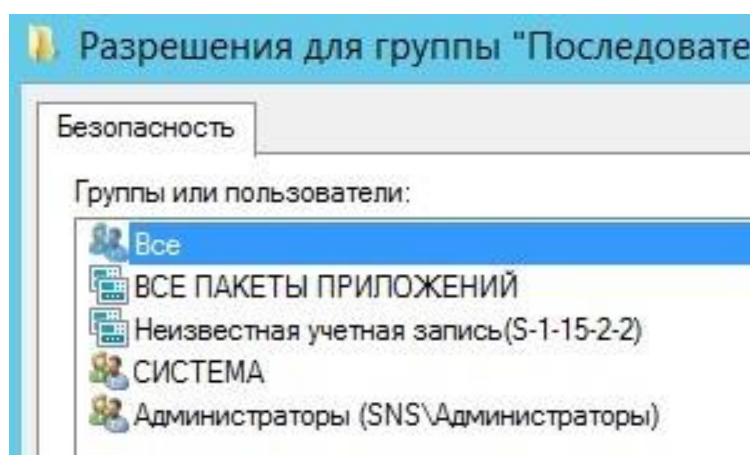


Рисунок 114 – Окно редактирования разрешений

Аналогичным образом настройте параметры устройств «Параллельные порты» и «Оптические диски» (устройство постоянно подключено к компьютеру, отключена блокировка компьютера при изменении устройства, разрешения: SYSTEM (все разрешения)). Выберите устройство «Сменные диски». В параметрах контроля установите запрет на подключение устройства (рисунок 115). Нажмите кнопку «Применить».

Для устройств «Процессоры» и «Системная плата» установите параметр контроля «Наследовать настройки контроля от родительского объекта» по аналогии с устройством «Физические диски» (если не установлено по умолчанию). Выберите устройство «Оперативная память». В параметрах контроля снимите флаг наследования параметров и установите значение «Устройство не контролируется» (рисунок 119). Нажмите «Применить».

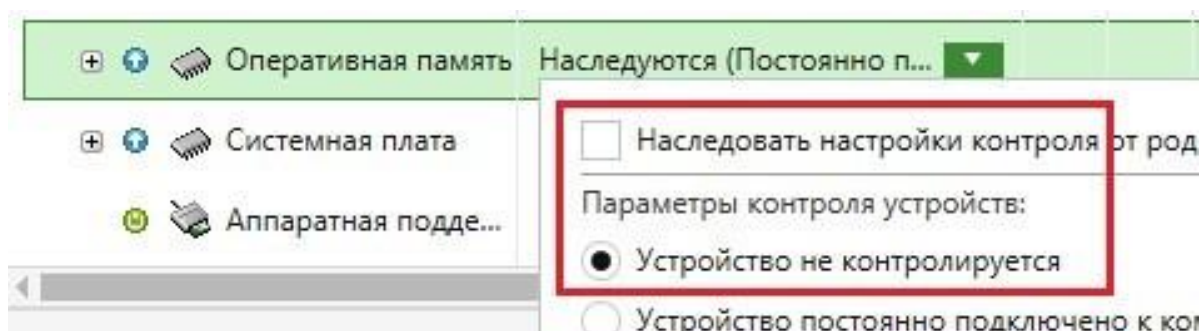


Рисунок 119 – Установка значения «Устройство не контролируется»

В списке устройств цвет индикатора рядом с названием устройства сменится на белый, что является признаком отсутствия контроля (рисунок 120).

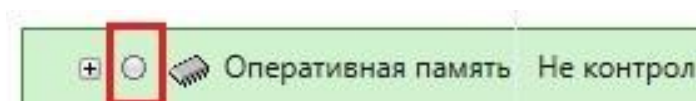


Рисунок 120 – Признак отсутствия контроля

Для устройства «Аппаратная поддержка» установите параметр контроля «Устройство постоянно подключено к компьютеру» и установите флаг «Блокировать компьютер при изменении устройства» (если значение не установлено по умолчанию).

Для устройства «Программно-реализованные диски» установите запрет на подключение. Настройка контроля устройств в группе «Локальные устройства» завершена, нажмите кнопку «Применить» для сохранения изменения настроек.

Выберите группу устройств «Устройства USB». Установите запрет на подключение группы устройств. В панели инструментов, расположенной над списком устройств, нажмите кнопку «Применить параметры контроля ко всем дочерним объектам» (рисунок 121).

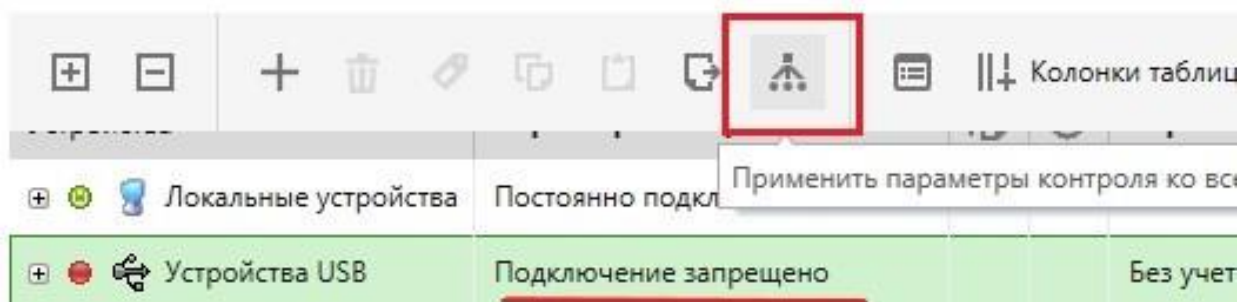


Рисунок 121 – Запрет на подключение группы устройств

Для всех устройств, входящих в группу «Устройства USB» автоматически установится параметр «Наследуется (Подключение запрещено)» (рисунок 122).

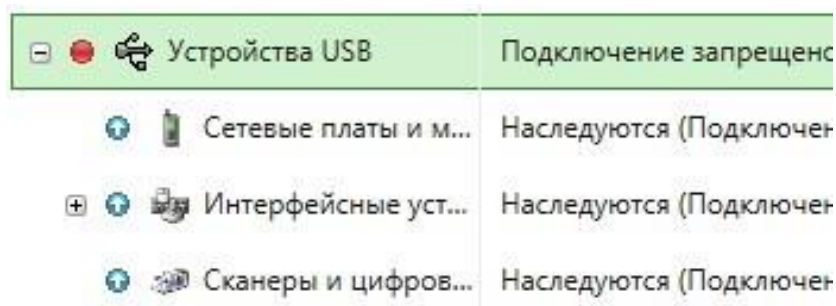


Рисунок 122 – Автоматическая установка параметра «Наследуется (Подключение запрещено)»

В группе «Устройства USB» выберите устройство «Интерфейсные устройства (мышь, клавиатура, ИБП и др.)». Откройте окно настройки параметров контроля и снимите флаг «Наследовать настройки контроля от родительского объекта» и установите переключите параметр в положение «Подключение устройства разрешено» (рисунок 123). Нажмите кнопку «Применить» в окне параметров контроля.

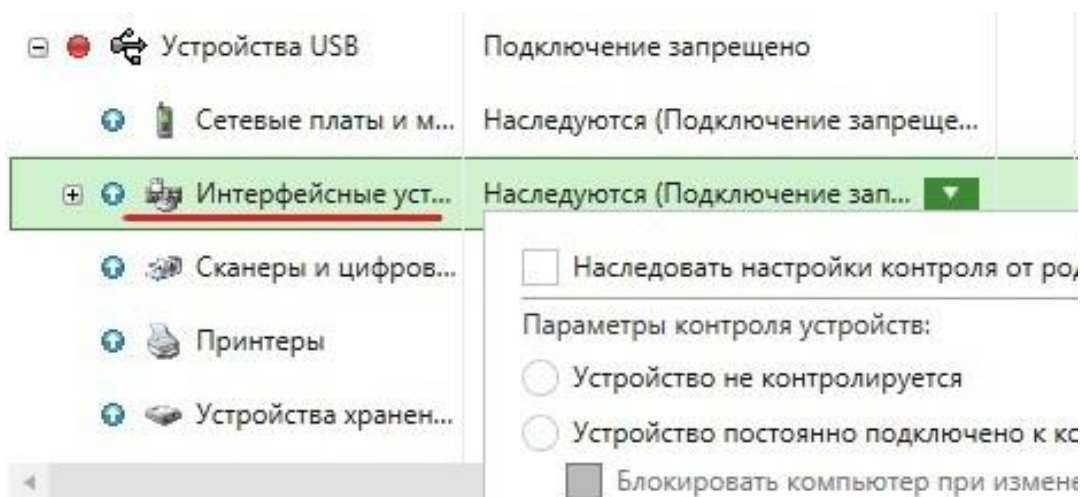


Рисунок 123 – Настройка параметров контроля

Аналогичным образом разрешите подключение устройств «Принтеры» и «Электронные идентификаторы и считыватели».

Выберите группу устройств «Устройства PCMCIA». Установите запрет подключения группы, а для всех устройств этой группы установите параметр «Наследовать настройки контроля от родительского объекта». Сохраните изменение настроек, нажав кнопку «Применить».

Выберите группу устройств «Устройства IEEE1394». Установите запрет подключения группы, а для всех устройств этой группы установите параметр «Наследовать настройки контроля от родительского объекта». Сохраните изменение настроек, нажав кнопку «Применить».

Аналогично настройте группу устройств «Устройства Secure Digital». Сохраните изменение настроек, нажав кнопку «Применить».

Выберите группу устройств «Сеть». Установите запрет подключения группы. Выберите устройство «Соединение Ethernet». Снимите наследование значения параметра и установите разрешение подключения устройства. Для остальных устройств параметры должны наследоваться (рисунок 124). Сохраните изменение настроек, нажав кнопку «Применить».

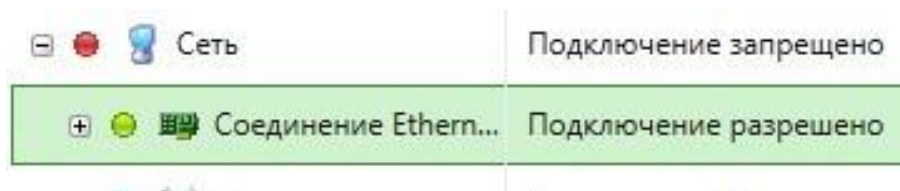


Рисунок 124 – Установка разрешения подключения устройства

После сохранения настроек примените групповые политики к компьютеру SNS-Client (через команду).

7.7 Предоставление доступа к устройствам

Переключитесь к окну виртуальной машины SNS-Client. Зарегистрируйтесь под учетной записью пользователя user3 (пользователь входит в группу Пользователи домена).

Подключите к виртуальной машине флеш-накопитель. Для этого в меню окна виртуальной машины выберите «Устройства – USB» и выберите устройство

с именем, содержащим слова Storage, drive, disk и т.п. (не mouse и keyboard) (рисунок 125).

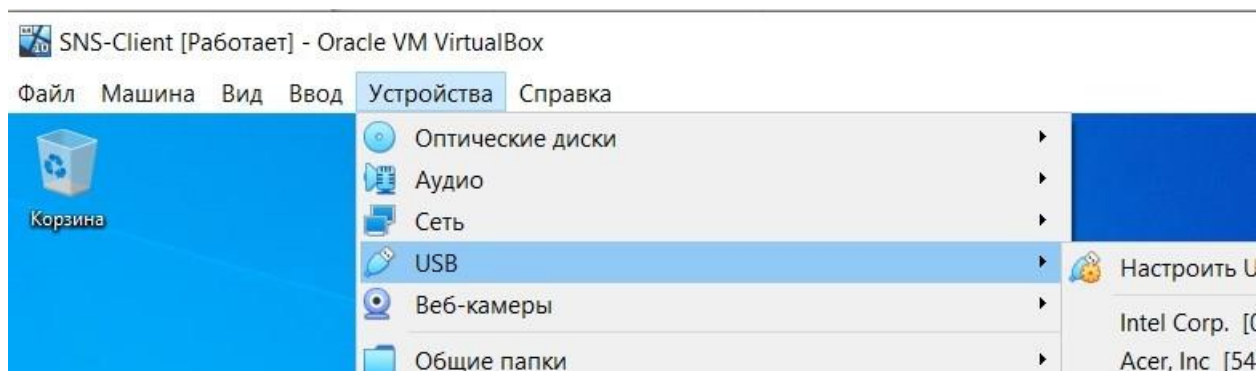


Рисунок 125 – Подключение флеш-накопителя

Откройте программу «Проводник», откройте папку «Компьютер». Флеш-накопитель не отображается в программе «Проводник». Отключите флеш-накопитель от виртуальной машины (аналогично подключению).

Переключитесь к окну виртуальной машины сервера безопасности SNS-Server. На панели «Компьютеры» пиктограмма компьютера SNS-Client поменяет цвет на красный. Перейдите на вкладку «Состояние». В списке компонентов в раздел «Тревоги» станет красного цвета, внизу окна в списке событий появится отображение события тревоги. Раскройте описание события, нажав на «+» в графе «Тип» (рисунок 126).

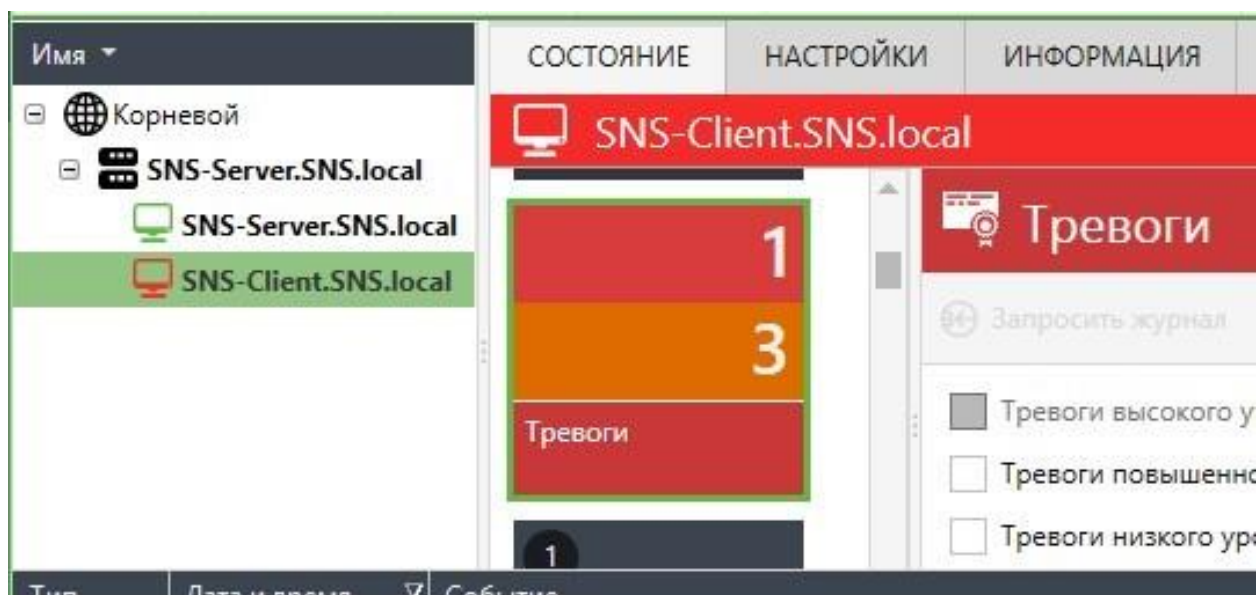
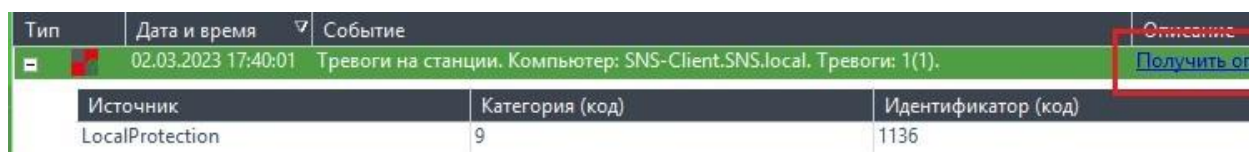


Рисунок 126 – Панель «Компьютеры»

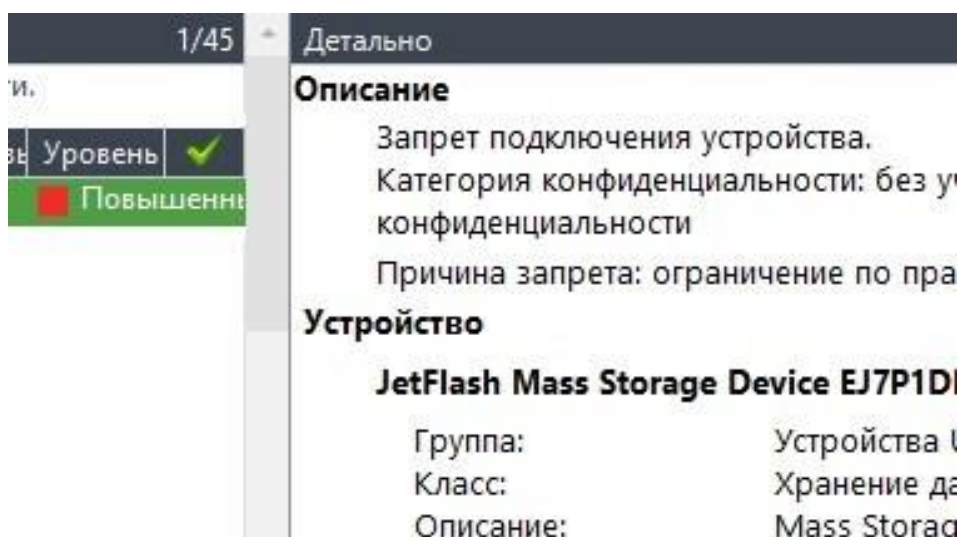
Описание события содержит код и идентификатор кода. Нажмите на строку «Получить описание тревоги» (рисунок 127).



Тип	Дата и время	Событие	Описание
	02.03.2023 17:40:01	Тревоги на станции. Компьютер: SNS-Client.SNS.local. Тревоги: 1(1).	Получить описание
Источник	Категория (код)	Идентификатор (код)	
LocalProtection	9	1136	

Рисунок 127 – Описание события

Раскроется таблица с подробностями описания события, включая имя компьютера, на котором произошло событие. Нажмите двойным кликом левой кнопки мыши на названии события. Справа откроется детальное описание события (рисунок 128).



1/45 - Детально	
Описание	
Запрет подключения устройства.	
Категория конфиденциальности: без учета конфиденциальности	
Причина запрета: ограничение по правам	
Устройство	
JetFlash Mass Storage Device EJ7P1D1	
Группа:	Устройства хранения данных
Класс:	Хранение данных
Описание:	Mass Storage Device

Рисунок 128 – Детальное описание события

Из описания события понятно, что причиной тревоги стало подключение флеш-накопителя, причем на защищаемом компьютере отображения события не произошло (в соответствии с настройками).

В программе «Центр управления» откройте настройки компьютера SNS-Client. Выберите группу параметров «Контроль устройств», в списке устройств выберите «Устройства USB» - «Устройства хранения» (рисунок 129).

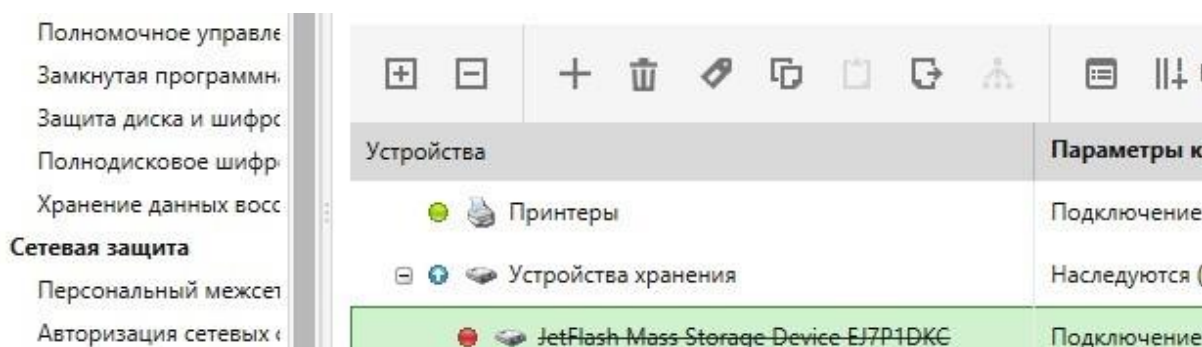


Рисунок 129 – Выбор устройства

В списке устройств хранения отобразится название подключенного флеш-накопителя с индикатором красного цвета, обозначающим запрет подключения устройства. Название устройства будет зачеркнуто. Это связано с настройками контроля устройств — подключение группы «Устройства USB» запрещено, а настройки группы «Устройства хранения» наследуются от этой группы. Выберите флеш-накопитель и нажмите кнопку «Показать информацию об устройстве». В окне отобразится детальная информация об устройстве, включающая серийный номер и название устройства, которые указываются в заявке на использование накопителя.

Откройте блокнот (Win + R, notepad) и запишите описание, производитель и серийный номер устройства. Сохраните файл.

Перейдите к окну виртуальной машины SNS-Client. Завершите сеанс пользователя user3 и войдите под учетной записью Администратора. Подключите флеш-накопитель. Запустите консоль «Управление компьютером», для этого нажмите кнопки Win и R, введите compmgmt.msc и нажмите Enter. Выберите слева раздел «Диспетчер устройств», в правой области консоли раскройте узел «Контроллеры USB», выберите «Запоминающее устройство для USB», нажмите правой кнопкой мыши и в контекстном меню выберите пункт «Свойства» (рисунок 130).

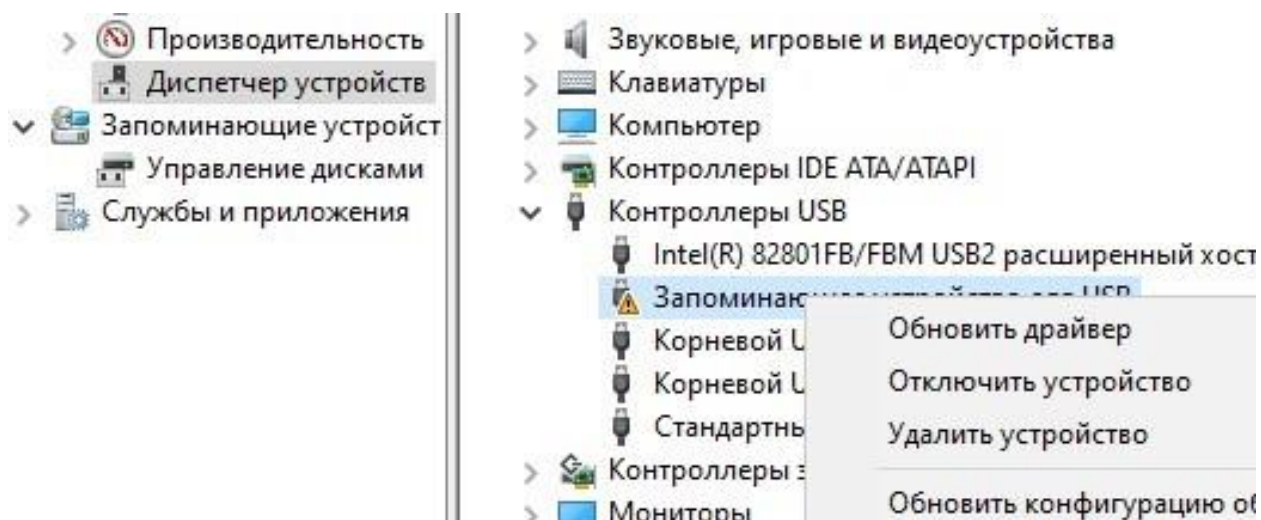


Рисунок 130 – Выбор свойства «Запоминающее устройство для USB»

В окне свойств устройства перейдите на вкладку «Сведения», в выпадающем списке «Свойство» выберите «ИД оборудования» (рисунок 131). Значения можно скопировать, выбрав в поле «Значение» строку, нажать правой кнопкой мыши и выбрать пункт «Копировать». Скопируйте значение параметра «ИД оборудования».

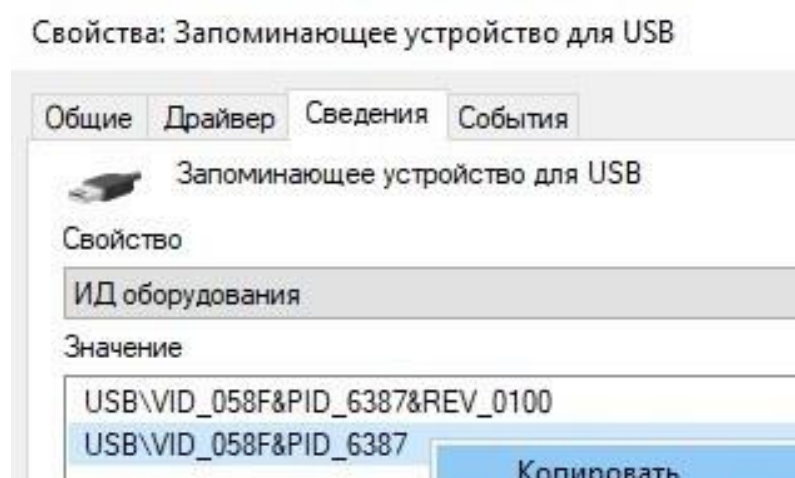


Рисунок 131 – Свойства «Запоминающее устройство для USB»

Запустите программу «Блокнот». Вставьте скопированное значение в файл. Сохраните файл в общей папке виртуальной машины (Сеть\VBOXSRV и далее). Закройте окно свойств устройства и консоль «Управление компьютером», отключите флеш-накопитель.

Переключитесь к окну виртуальной машины сервера безопасности SNS-Server, вернитесь к параметрам компьютера SNS-Client. Выберите флеш-накопитель в списке устройств. Раскройте окно настроек параметров контроля.

Установите параметр «Подключение устройства разрешено» и нажмите «Применить» (рисунок 132).

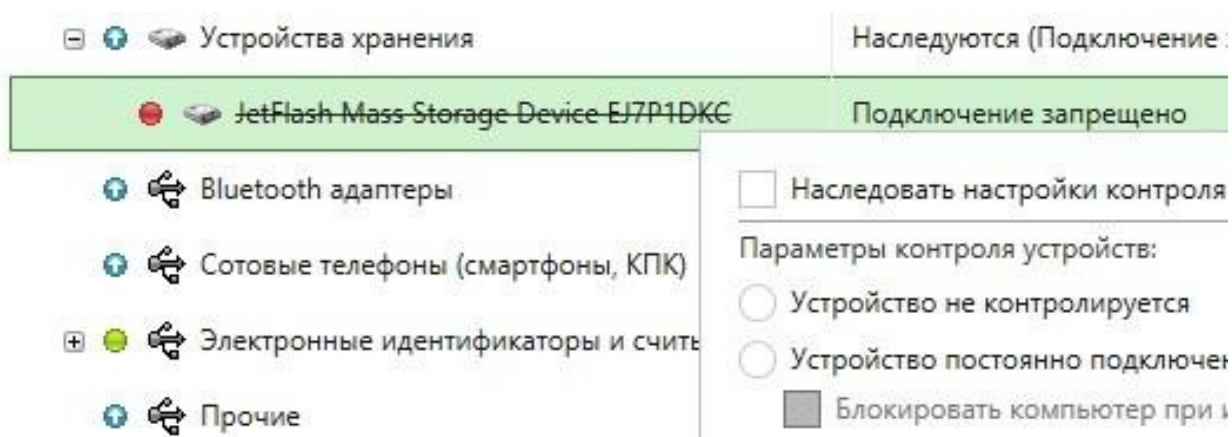


Рисунок 132 – Установка параметра «Подключение устройства разрешено»

Теперь применение на компьютере именно этого флеш-накопителя будет разрешено. Нажмите кнопку «Применить» внизу окна программы для сохранения изменения настроек. Цвет индикатора рядом с устройством сменится на зеленый, название устройства останется зачеркнутым, т.к. флеш-накопитель отключен от компьютера. Примените групповые политики на устройстве SNS-Client.

Переключитесь к окну виртуальной машины SNS-Client. Подключите к виртуальной машине флеш-накопитель. Появится окно выбора действия при подключении съемного носителя. Откройте содержимое накопителя в программе «Проводник». Переключитесь к окну виртуальной машины сервера безопасности DC-SNS. В списке устройств с флеш-накопителя исчезло зачеркивание, это означает, что устройство подключено к компьютеру.

Переключитесь к окну виртуальной машины SNS-Client. Завершите сеанс Администратора и войдите под учетной записью user3. Откройте содержимое флеш-накопителя в программе «Проводник». Попробуйте создать на флеш-накопителе файл, удалить файл, скопировать файл на накопитель. Все действия доступны. Завершите сеанс пользователя user3. Флеш-накопитель доступен для работы всем пользователям компьютера SNS-Client. Отключите флеш-накопитель от виртуальной машины.

Переключитесь к окну виртуальной машины сервера безопасности SNS-Server. Запустите программу «Проводник». Откройте на общем сетевом ресурсе виртуальных машин файл, содержащий параметры флеш-накопителя. Скопируйте файл на рабочий стол сервера безопасности. В программе Центр управления на панели «Компьютеры» откройте свойства компьютера SNS-Server (рисунок 133). Загрузите настройки.

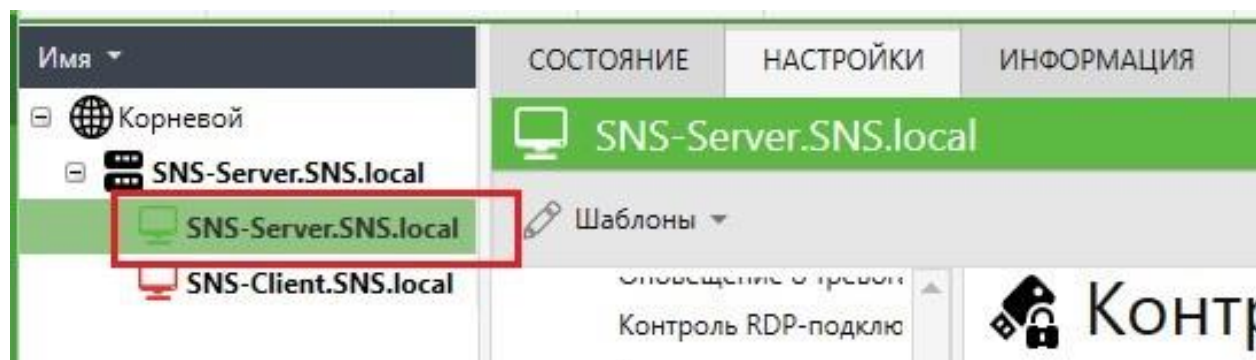


Рисунок 133 – Загрузка настроек

Выберите раздел настроек «Контроль устройств». В списке устройств в группе «Устройства USB» выберите «Устройства хранения». Откройте окно параметров контроля, снимите флаг «Наследовать настройки контроля от родительского объекта», установите переключатель в положение «Подключение устройства запрещено» и нажмите кнопку «Применить» (рисунок 134). Нажмите кнопку «Применить» для сохранения настроек. Примените к компьютеру SNS-Server команду «Применить групповую политику».

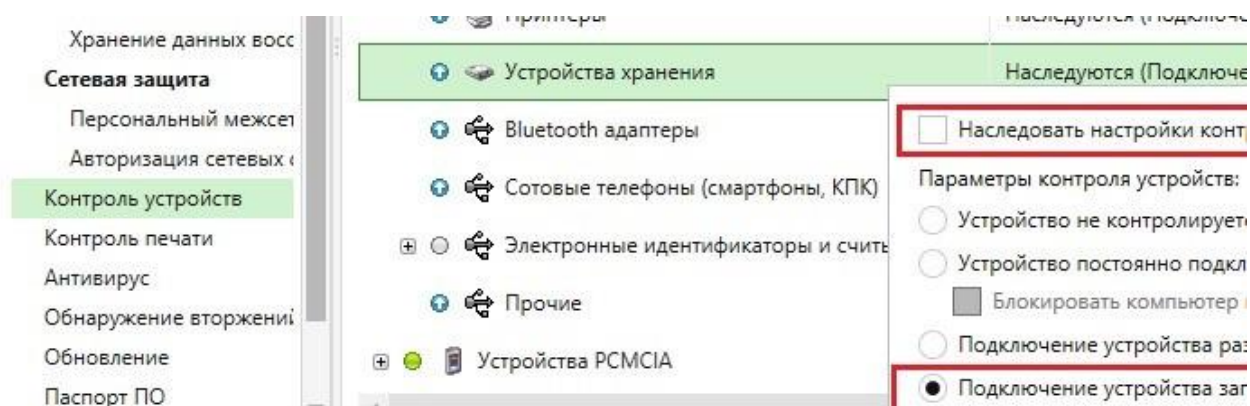


Рисунок 134 – Применение групповой политики

Теперь на компьютере SNS-Server запрещено подключение флеш-накопителей. Добавьте вручную устройство, разрешенное для подключения по информации об устройстве. Выберите в настройках компьютера SNS-Server

«Устройства хранения». Рядом с названием группы помещен индикатор красного цвета, означающий запрет подключения. В панели инструментов, расположенной над списком устройств, нажмите кнопку «Добавить устройство» с пиктограммой в виде «+» (рисунок 135).

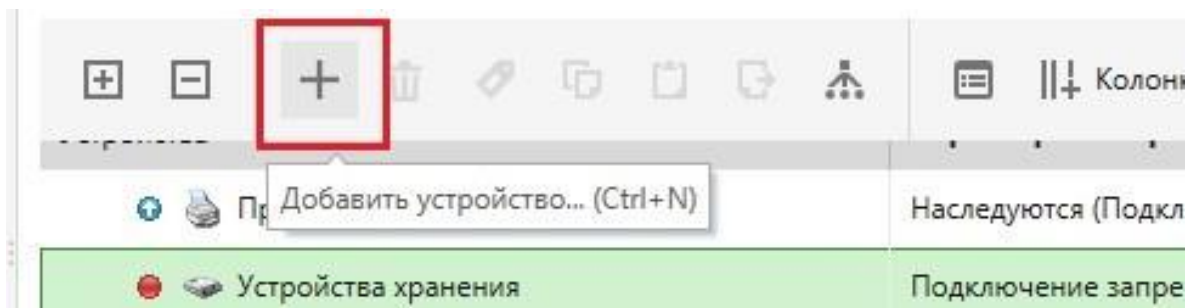


Рисунок 135 – Добавление устройства

В окне «Режим работы» установите переключатель в положение «Добавить устройства по идентификаторам» и нажмите кнопку «Далее» (рисунок 136).

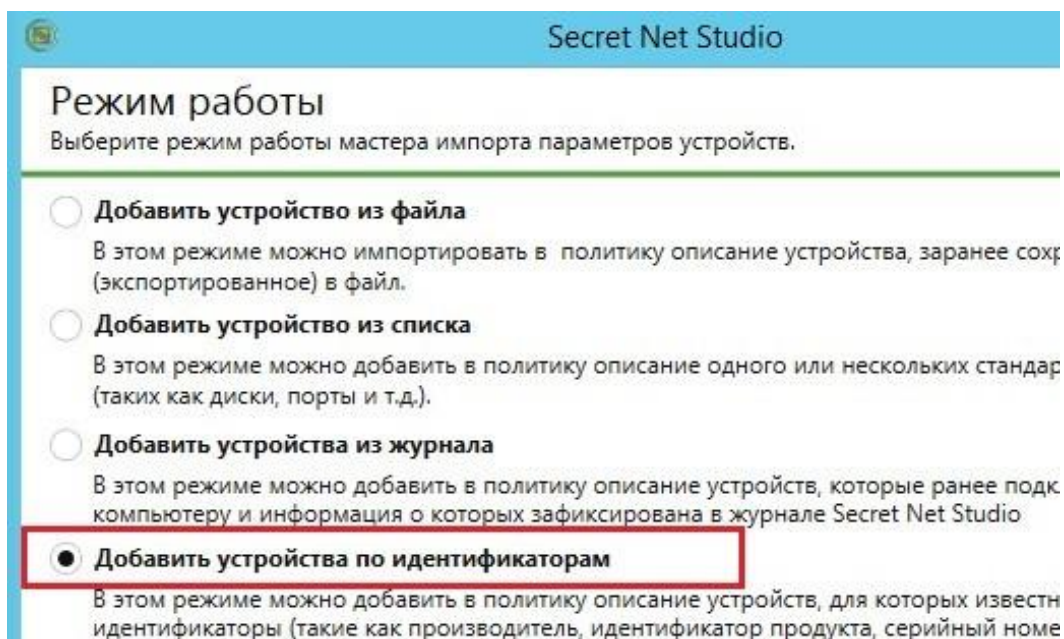


Рисунок 136 – Добавление устройства по идентификаторам

В следующем окне нажмите кнопку «Добавить устройство...» и в выпадающем списке выберите «Добавить устройство вручную» (рисунок 137).

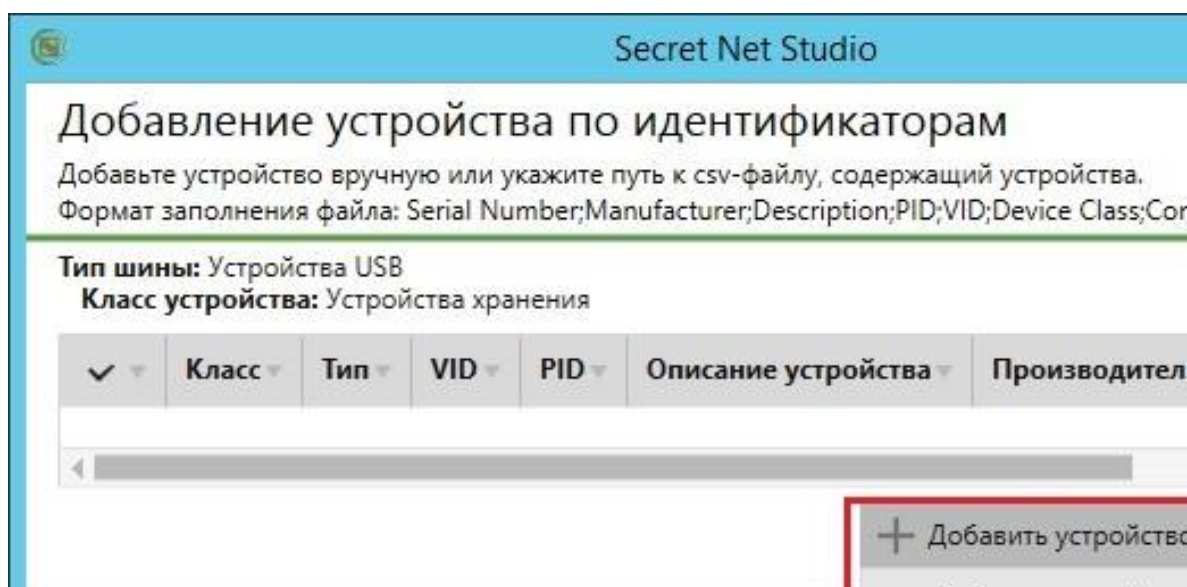


Рисунок 137 – Добавление устройства вручную

Откроется окно для ввода параметров устройства. По умолчанию в поле «Тип» установлено значение «Модель устройств». Для добавления устройств одной модели необходимо указать параметры VID (Vendor Identifier, идентификатор производителя) PID (Product Identifier, идентификатор продукта, модели устройства) и описание устройства. Откройте текстовый файл с параметрами usb устройства, созданный ранее. Скопируйте значения из файла в поля ввода (рисунок 138) и нажмите кнопку «Добавить».

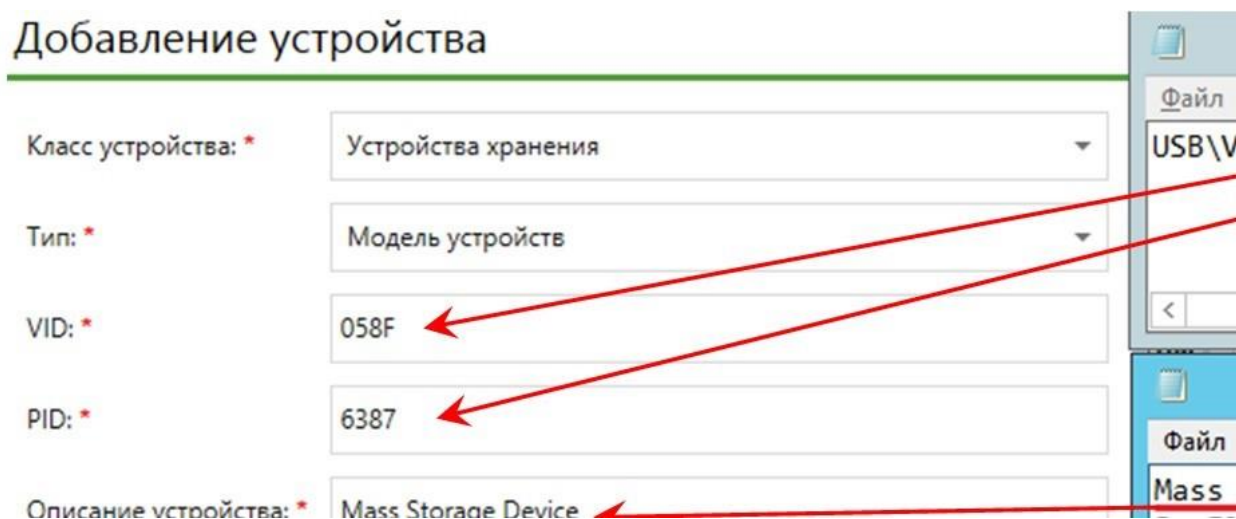


Рисунок 138 – Ввод данных из текстового файла

В окне «Добавление устройства по идентификатору» появится новое устройство. Выберите это устройство в списке и нажмите кнопку «Добавить» (рисунок 139).

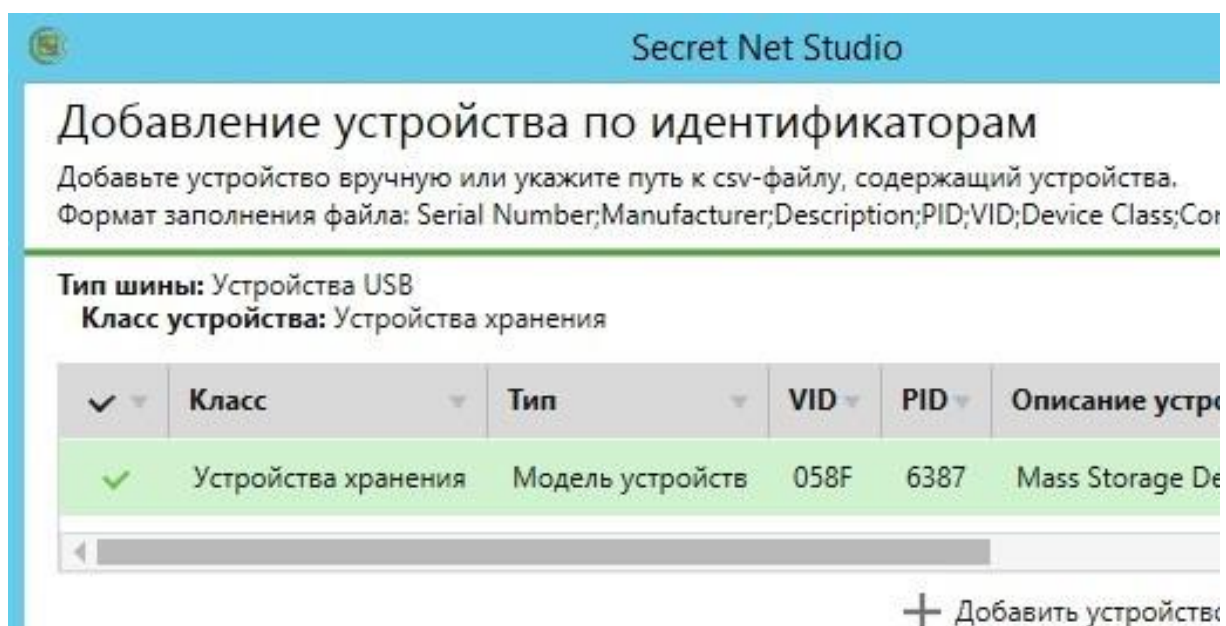


Рисунок 139 – Выбор нового устройства

В списке устройств в группе «Устройства хранения» добавится устройство (рисунок 140).



Рисунок 140 – Устройство добавлено

Параметры контроля устройства наследуются из параметров верхней группы устройств. Откройте параметры контроля добавленного устройства, снимите флаг наследования и разрешите подключение устройства. Нажмите «Применить» для сохранения настроек. Обратите внимание, что после применения настроек к устройству установится разрешение подключения на все «Устройства хранения» (рисунок 141).



Рисунок 141 – Применение настроек к устройству

Для группы «Устройства хранения» снова установите запрет на подключение, нажмите «Применить» для сохранения настроек и примените к компьютеру SNS-Server групповую политику.

Подключите флеш-накопитель в виртуальной машине SNS-Server. Дождитесь окончания установки драйвера и подготовки устройства к работе. Появится окно с выбором действия. Откройте содержимое флеш-накопителя в программе «Проводник». Попробуйте создать на флеш-накопителе файл, удалить файл, скопировать файл на накопитель. Все действия доступны. Перейдите к окну программы «Центр управления», в настройках компьютера SNS-Server в разделе «Контроль устройств» просмотрите «Устройства хранения». Подключенный флеш-накопитель отобразился в подгруппе ранее добавленного по идентификатору устройства (рисунок 142).



Рисунок 142 – Отображение флеш-накопителя

Это произошло потому, что была добавлена модель устройства по VID и PID, т.е. добавлена серия устройств с одинаковыми параметрами. В этом случае возможным станет подключение устройств одной серии, у которых будет одинаковое значение VID и PID. Для добавления конкретного устройства необходимо в окне, приведенном на рисунке выбрать тип «Устройство» и указать дополнительные данные, включая серийный номер. Выполним добавление конкретного устройства. Выберите подключенное устройство в списке и нажмите кнопку «Показать информацию об устройстве» (рисунок 143).

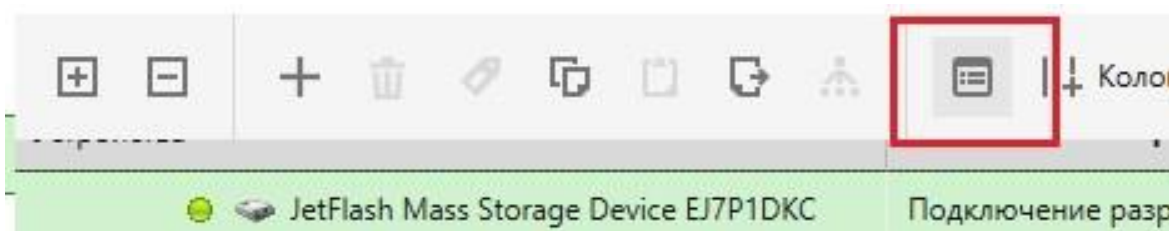


Рисунок 143 – Выбор свойства «Показать информацию об устройстве»

В окне информации об устройстве отображается серийный номер устройства, перепишите его в текстовый файл (если не записывали ранее или подключили другое устройство), в котором записана информация о накопителе (рисунок 144).



Рисунок 144 – Информация об устройстве

Закройте окно информации еще раз нажав на кнопку «Показать информацию об устройстве». Отключите флеш-накопитель от виртуальной машины SNS-Server. Удалите из группы «Устройства хранения» ранее добавленную серию устройств и само устройство (рисунок 145). Примените настройки для сохранения изменений.

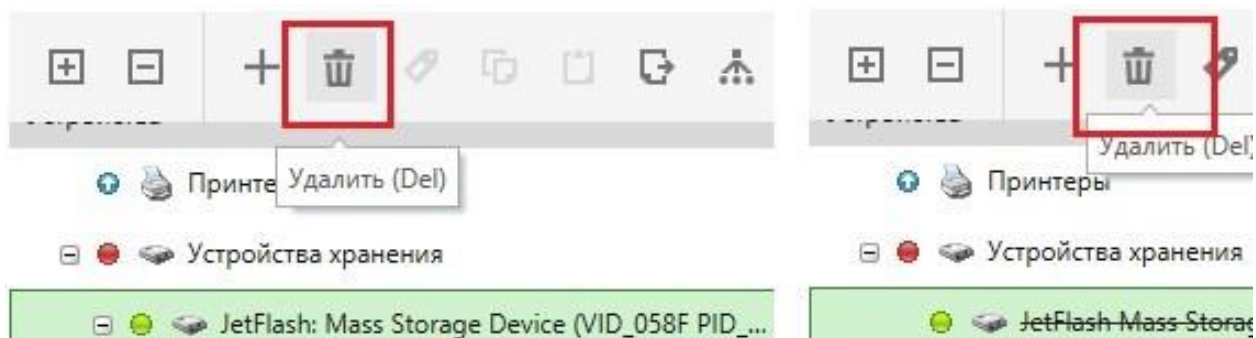


Рисунок 145 – Удаление ранее добавленной серии устройства и самого устройства

Выберите группу «Устройства хранения» и нажмите кнопку «Добавить устройство», затем выберите «Добавить устройства по идентификаторам» и «Добавить устройство вручную». В окне «Добавление устройства» в поле «Тип» выберите «Устройство» (рисунок 146). Откройте текстовый файл с параметрами флеш-накопителя и заполните обязательные поля окна. Нажмите кнопку «Добавить».

Secret Net Studio	
Добавление устройства	
Класс устройства: *	Устройства хранения
Тип: *	Устройство
VID: *	058F
PID: *	6387
Описание устройства: *	Mass Storage Device
Производитель: *	JetFlash
Серийный номер: *	EJ7P1DKC
Комментарий:	

Рисунок 146 – Заполнение обязательных полей

Выберите устройство в списке и добавьте в список контролируемых устройств. Устройство появится в списке. Автоматически установится запрет на подключение, унаследованный с группы устройств «Устройства хранения». Разрешите подключение устройства, примените настройки. Конфигурация контроля устройств должна выглядеть следующим образом (рисунок 147).

		Устройства хранения	Подключени
		JetFlash Mass Storage Device EJ7P1DKC	Подключени

Рисунок 147 – Разрешение подключения устройства

Подключите флеш-накопитель к виртуальной машине SNS-Server. После подключения в списке устройств пропадет зачеркивание с названия устройства.

Станут доступны все действия с устройством (чтение, создание, изменение, удаление файлов). Отключите флеш-накопитель от виртуальной машины SNS-Server. Выберите флеш-накопитель в перечне устройств, нажмите правой кнопкой мыши и выберите пункт «Сохранить» (рисунок 148).

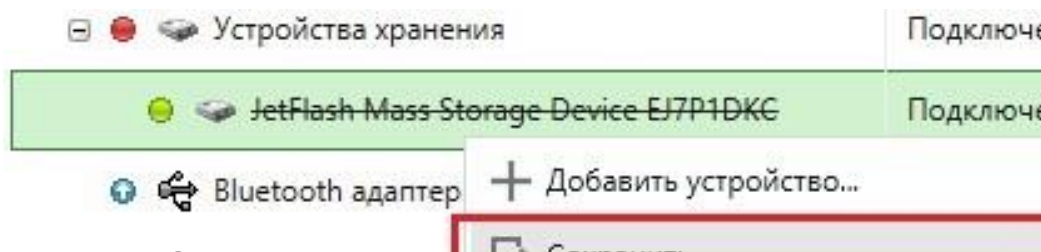


Рисунок 148 – Сохранение устройства

В окне «Сохранить устройства» укажите путь сохранения и название файла, в списке устройств должно быть отмечено выбранное устройство (рисунок 149). Нажмите «Сохранить».

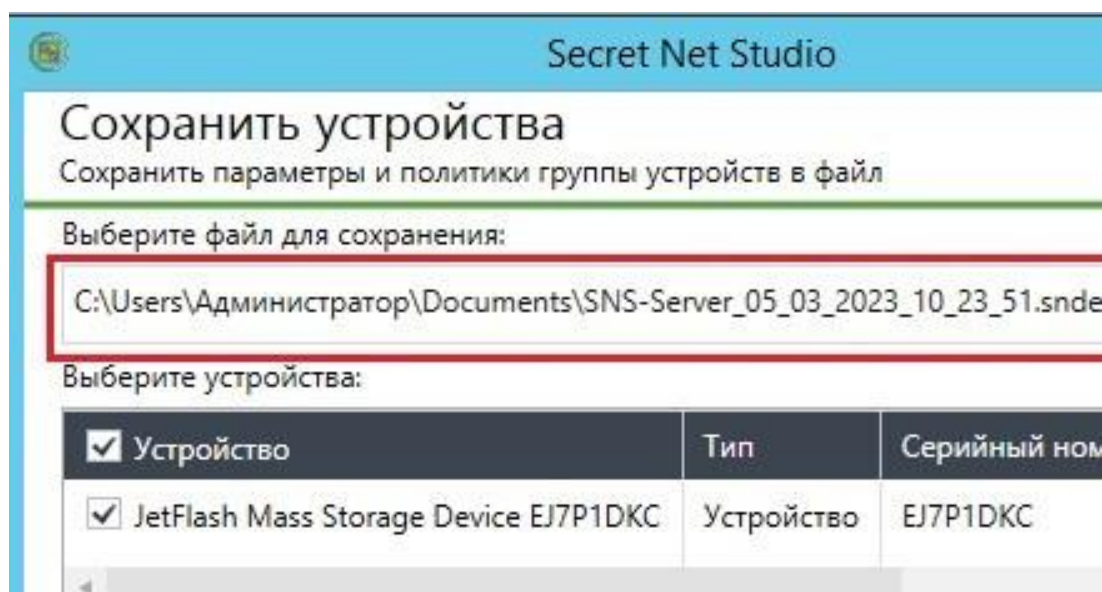


Рисунок 149 – Путь сохранения устройства

В указанном месте будет создан файл с расширением sndev, содержащий параметры флеш-накопителя (VID, PID, серийный номер и т.д.). Удалите флеш-накопитель из списка устройств. Примените настройки. Подключите флеш-накопитель к виртуальной машине SNS-Server. Подключение будет запрещено, появится сигнал тревоги (рисунок 150).

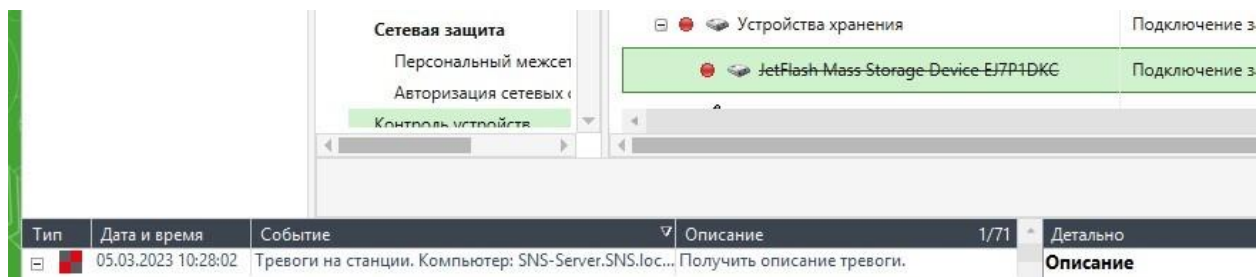


Рисунок 150 – Появление сигнала устройства

Выберите группу «Устройства хранения» и нажмите кнопку «Добавить устройство» (рисунок 151).

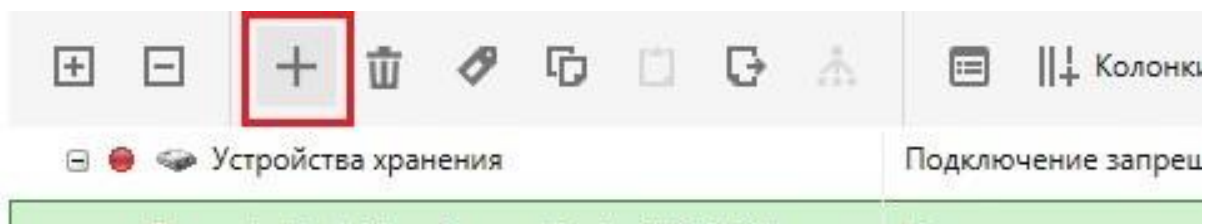


Рисунок 151 – Добавление устройства в группе «Устройства хранения»

В окне «Режим работы» выберите пункт «Добавить устройство из файла» (рисунок 152) и нажмите кнопку «Далее».

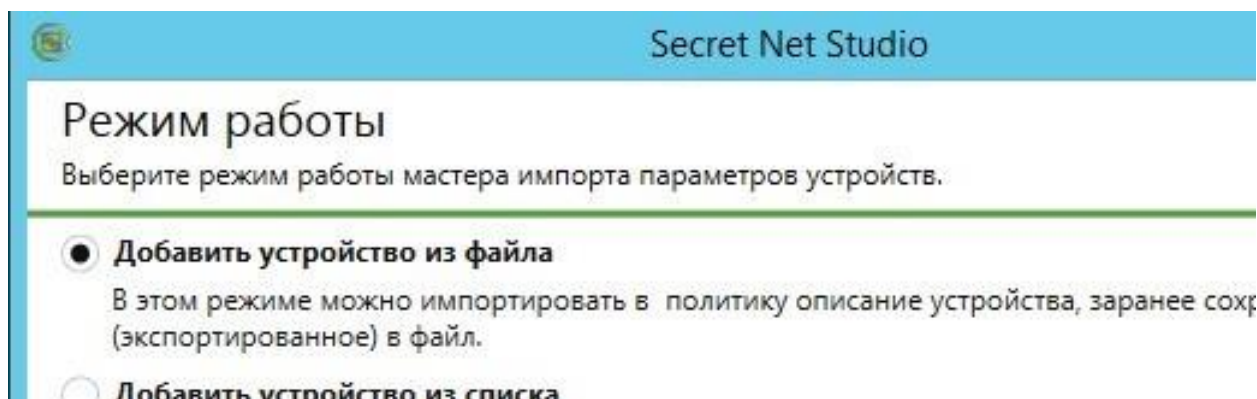


Рисунок 152 – Добавление устройства из файла

В окне «Импорт параметров устройства из файла» в поле выбора файла нажмите кнопку «...», выберите ранее созданный файл и нажмите «Открыть» (рисунок 153). Устройство добавится в список. Выберите его в списке и нажмите кнопку «Добавить».

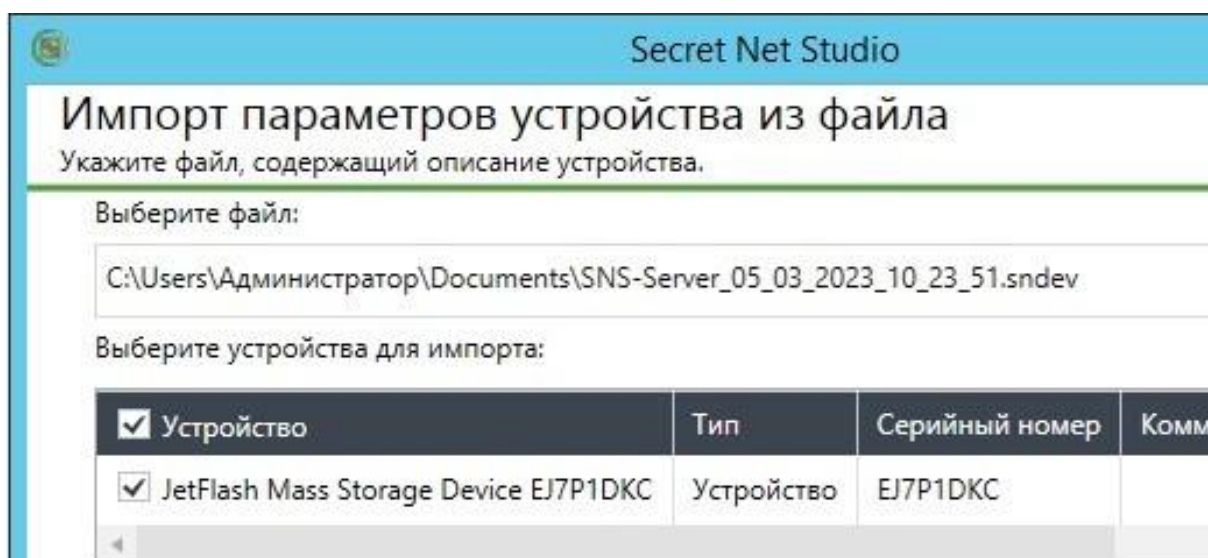


Рисунок 153 – Импорт параметров устройства из файла

Появится предупреждение о совпадении устройств в политике. Нажмите кнопку «Заменить» для изменения настроек устройства (рисунок 154).

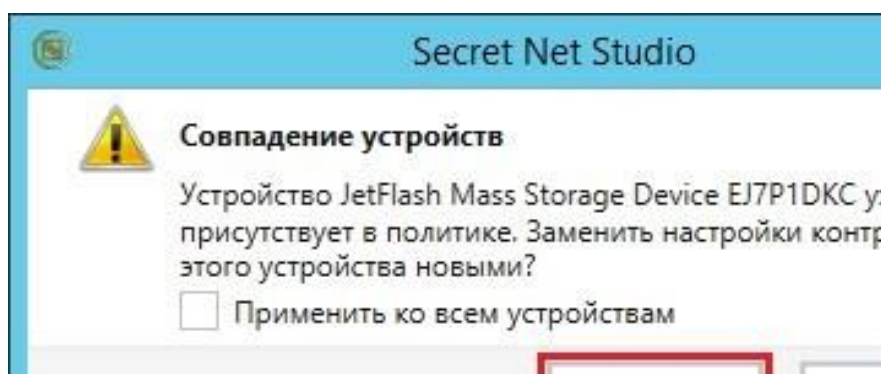


Рисунок 154 – Предупреждение о совпадении устройств в политике

Обратите внимание, что автоматически параметры контроля установятся в значение «Подключение разрешено», поскольку файл описания содержит также информацию о разрешениях на устройство (рисунок 155). Нажмите кнопку «Применить» для сохранения настроек.



Рисунок 155 – Сохранение настроек

Несмотря на то, что устройство в текущий момент времени подключено к компьютеру и его использование разрешено, оно отмечено как неподключенное (зачеркнуто). Для использования устройства его надо переподключить.

Отключите флеш-накопитель от виртуальной машины и подключите снова. Теперь устройство доступно для работы. Файлы с конфигурацией устройства можно использовать также для добавления устройств в политики других компьютеров. Отключите флеш-накопитель от виртуальной машины.

Рассмотрим способ добавления устройства в список через журналы.

Переключитесь к окну виртуальной машины SNS-Client, войдите под учетной записью Администратора и запустите программу «Локальный центр управления». Откройте панель «Журналы» (1) (рисунок 156) и в поле «Запросы» двойным кликом на запросе «Все тревоги» загрузите журнал тревог.

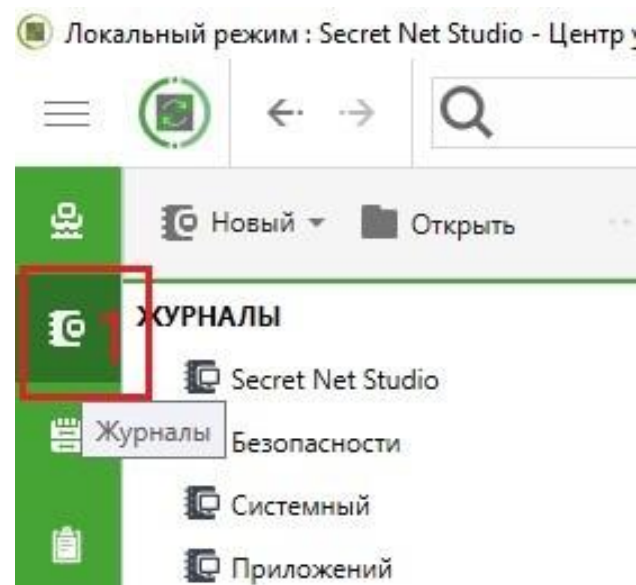


Рисунок 156 – Журнал тревог

Загрузится выборка тревог на компьютере SNS-Client, среди которых будет запись о запрете подключения устройства. Нажмите кнопку «Экспорт журнала» в правой панели окна (рисунок 157).

	Дата ▾	Журнал	Событие	Категор...	Источник
	05.03.2023...	Безопасности	Учетной записи не удалос...	Logon	Microsoft-...
	02.03.2023...	Безопасности	Учетной записи не удалос...	Logon	Microsoft-...
	02.03.2023...	Secret Net St...	Запрет подключения устр...	Разграниче...	LocalProtec...
	02.03.2023...	Secret Net St...	Запрет подключения устр...	Разграниче...	LocalProtec...

Рисунок 157 – Экспорт журнала

В поле «Путь к файлу» (рисунок 158) нажмите на кнопку «...», в адресной строке введите \\VBOXSRV\Share (общая сетевая папка виртуальных машин), нажмите Enter и введите название сохраняемого файла. Нажмите кнопку «Сохранить». Затем нажмите кнопку «Экспорт». Журнал тревог будет экспортирован на сетевую папку. Закройте окно программы «Локальный центр управления» и завершите сеанс Администратора на компьютере SNS-Client.

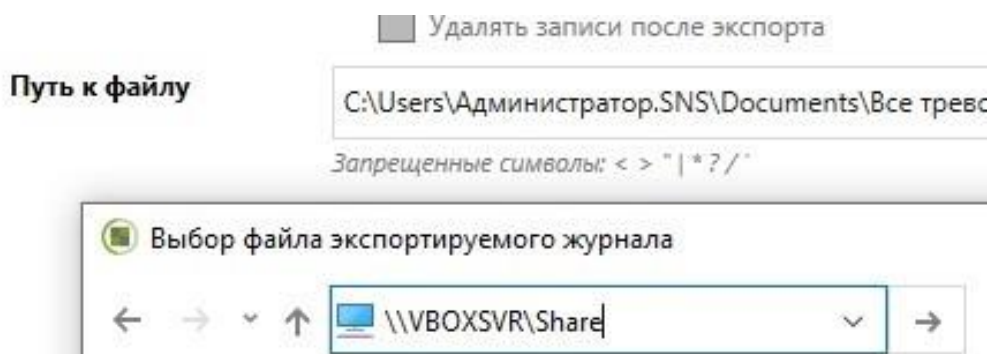


Рисунок 158 – Выбор пути сохранения журнала

Переключитесь к окну виртуальной машины SNS-Server. В программе «Центр управления» в свойствах компьютера SNS-Server в разделе «Контроль устройств» выберите флеш-накопитель и удалите из списка устройств (рисунок 159).

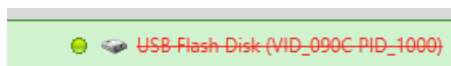


Рисунок 159 – Удаление флеш-накопителя

Сохраните изменение. Группа «Устройства хранения» должна выглядеть следующим образом (рисунок 160).

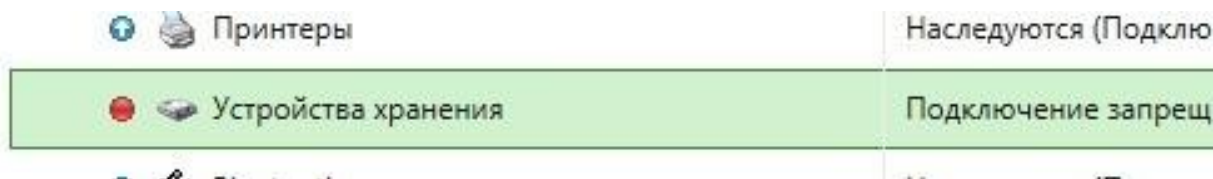


Рисунок 160 – Группа «Устройства хранения»

Выберите «Устройства хранения» и нажмите кнопку «Добавить устройство». В окне «Режим работы» установите переключатель в параметр «Добавить устройства из журнала» и нажмите кнопку «Далее» (рисунок 161).

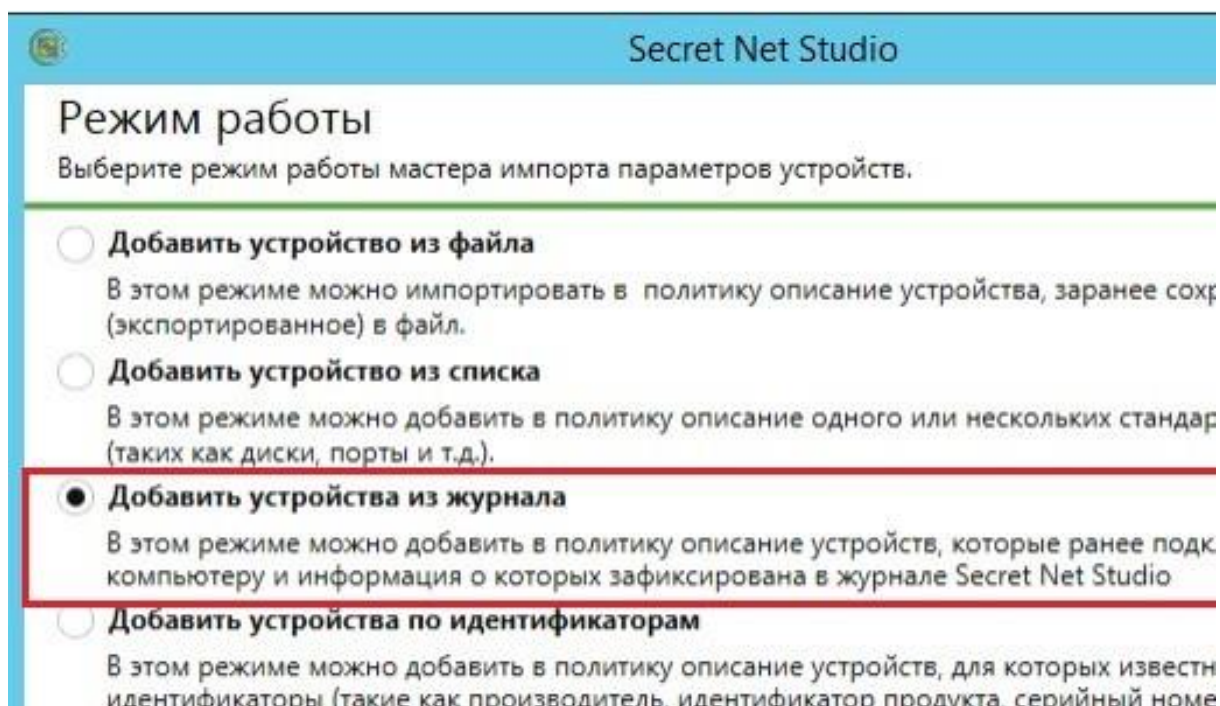


Рисунок 161 – Добавление устройства из журнала

В следующем окне нажмите кнопку «...», откройте файл с сохраненным журналом и нажмите кнопку «Открыть» (рисунок 162). В списке отобразятся устройства, подключение которых было идентифицировано как тревога. Выберите флеш-накопитель и нажмите кнопку «Добавить».

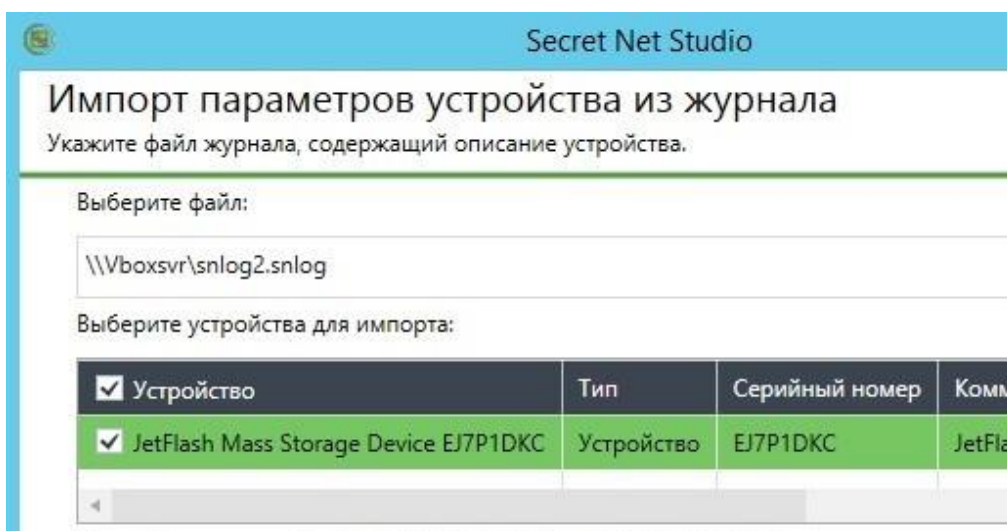


Рисунок 162 – Импорт параметров устройства из журнала

Устройство добавится в список устройств, для него автоматически в соответствии с параметрами наследования будет установлен запрет подключения. Установите разрешение подключения флеш-накопителя к

компьютеру SNS-Server и сохраните изменения в настройках, нажав кнопку «Применить».

7.8 Настройка прав пользователей на доступ к устройству

В программе «Центр управления» на панели «Компьютеры» выберите компьютер SNSServer и откройте окно свойств. В разделе настроек выберите «Контроль устройств». Выберите группу устройств «Устройства USB» - «Устройства хранения». В списке устройств должен отображаться флеш-накопитель, добавленный ранее. Подключение устройства должно быть разрешено. Настройка прав пользователей на доступ к устройству осуществляется в окне «Разрешения». Выберите в списке флеш-накопитель и нажмите кнопку «Разрешения» (рисунок 163).



Рисунок 163 – Настройка прав пользователей на доступ к устройству

Откроется окно «Разрешения для группы <название устройства>», в котором можно разграничить права доступа к устройству для групп и отдельных пользователей. Нажмите кнопку «Добавить» (рисунок 164). Откроется окно выбора субъектов доступа. Введите в поле ввода имя пользователя user3 и нажмите кнопку «Проверить имена». После проверки имени пользователя нажмите кнопку «ОК» в окне выбора.

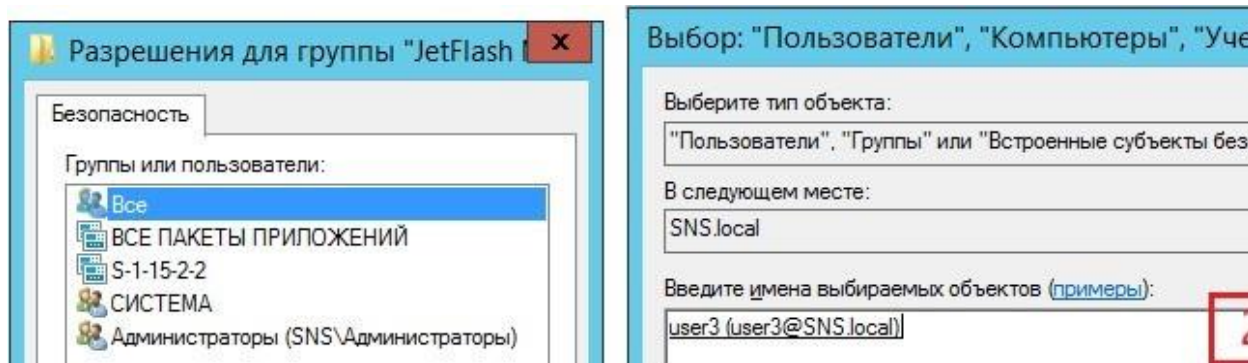


Рисунок 164 – Добавление «user3»

Пользователь user3 добавится в список субъектов безопасности. По умолчанию для него будет установлено только разрешение на использование устройства (рисунок 165).

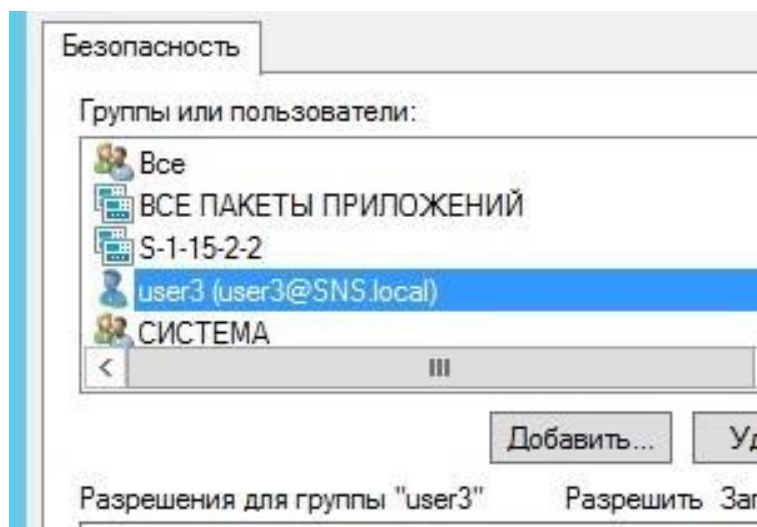


Рисунок 165 – Список субъектов безопасности

Выберите в списке субъектов группу «Все». Снимите флаг «Разрешить» в разрешении «Запись» (рисунок 166). Нажмите кнопку «ОК».

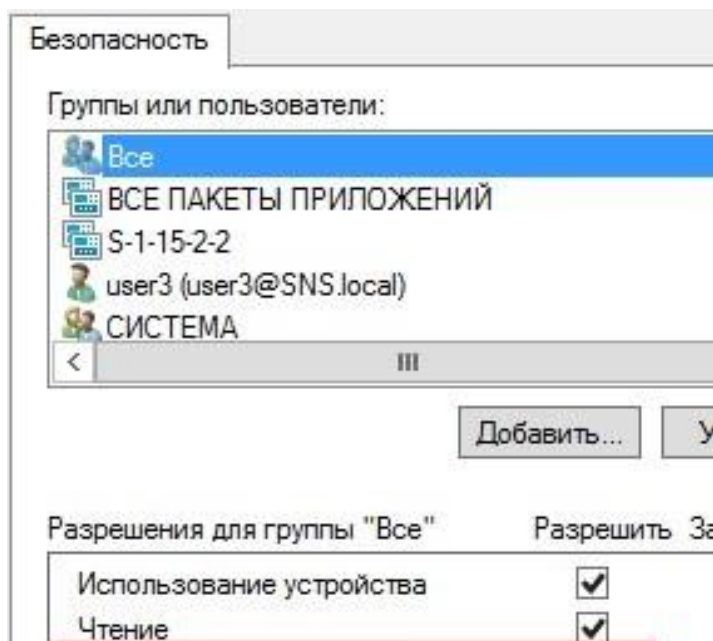


Рисунок 166 – Настройка прав «user3»

В окне программы «Центр управления» нажмите кнопку «Применить» для сохранения настроек. Завершите сеанс Администратора на компьютере SNS-Server (нажмите Win и R, введите shutdown /L и нажмите Enter).

Войдите под учетной SNS\user3 на компьютер SNS-Server. Подключите флеш-накопитель к виртуальной машине. Откройте содержимое флеш-накопителя в программе «Проводник». Попробуйте открыть документ на флеш-накопителе. Чтение с накопителя должно быть разрешено. Попробуйте создать на флеш-накопителе файл или изменить существующий — операция будет запрещена. Это связано с тем, что к пользователю user3 применяются настройки группы «Все», для которой снято разрешение на запись. Завершите сеанс пользователя user3 и войдите под учетной записью Администратора.

Запустите «Центр управления», выберите компьютер SNS-Server, откройте настройки, в разделе «Контроль устройств» выберите флеш-накопитель и нажмите кнопку «Разрешения». Выберите группу «Все» и нажмите кнопку «Удалить» (рисунок 167). Нажмите кнопку «ОК» в окне разрешений и кнопку «Применить» для сохранения настроек.

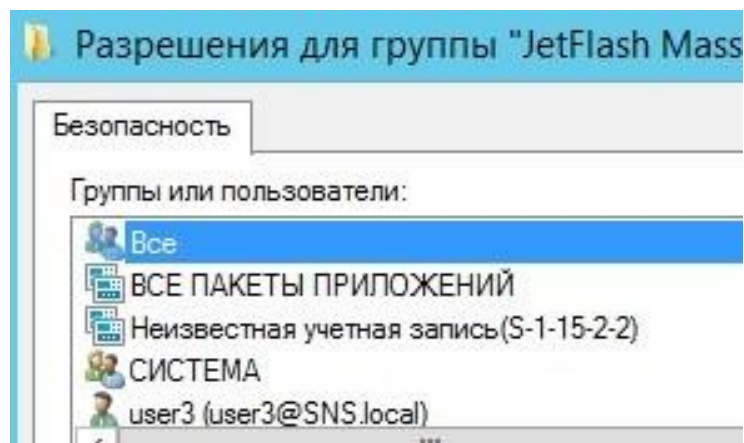


Рисунок 167 – Удаление группы «Все»

Завершите сеанс Администратора, войдите под учетной записью user3. Запустите программу «Проводник». Флеш-накопитель будет отображаться в списке доступных дисков (рисунок 168), но при попытке получения доступа появится сообщение об отказе в доступе. После удаления группы «Все» у пользователя user3 осталось только явно заданное разрешение на использование, но нет прав на чтение, запись и выполнение.

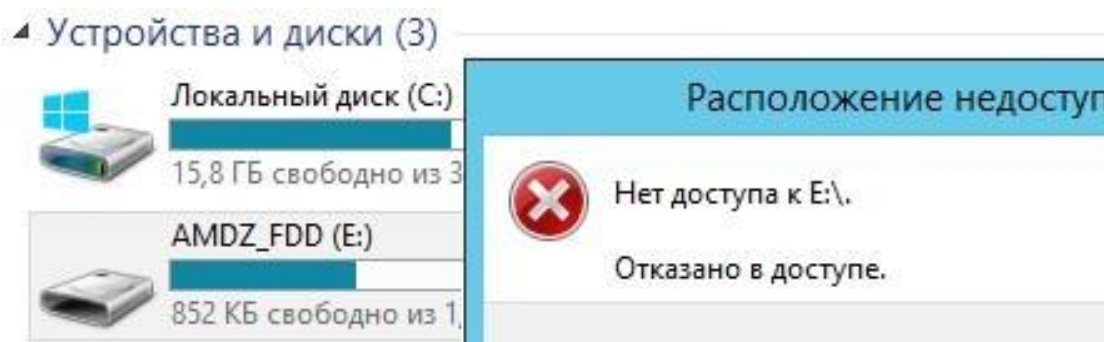


Рисунок 168 – Отказ в доступе

Завершите сеанс пользователя user3, войдите под учетной записью Администратора. Откройте окно разрешений флеш-накопителя. Добавьте следующие учетные записи и группы и установите для них следующие разрешения и запреты:

- user1: разрешить использование, чтение, запись, выполнение;
- user2: разрешить использование, выполнение;
- SPOAdmins: разрешить Использование, чтение, выполнение.

Запретить запись;

- Auditors: разрешить использование, чтение, запись, выполнение.

Сохраните изменения в настройках SNS-Server, нажав кнопку «Применить». Завершите сеанс Администратора. Войдите на компьютер SNS-Server под учетной записью user1.

Пользователю явно заданы все разрешения. В программе «Проводник» откройте флеш-накопитель. Попробуйте открыть документ на флеш-накопителе. Чтение с накопителя должно быть разрешено. Попробуйте создать на флеш-накопителе файл или изменить существующий — операция будет запрещена. Это связано с тем, что user1 является членом группы SPOAdmins, для которой установлен явный запрет на запись. Запреты имеют преимущество перед разрешениями.

Завершите сеанс пользователя user1 и войдите под учетной записью user2. Пользователю user2 явно указаны разрешения только на использование и выполнение. В программе «Проводник» откройте флеш-накопитель. Содержимое флеш-накопителя будет доступно. Попробуйте открыть

произвольный файл, создать новый файл, изменить содержимое существующего – все операции будут доступны. Это связано с тем, что пользователь user2 является членом группы Auditors, для которой установлены все разрешения. В этом случае эффективные права пользователя складываются из разрешений самого пользователя и разрешений группы. Отключите флеш-накопитель от виртуальной машины SNS-Server. Завершите сеанс user2.

Войдите под учетной записью Администратора. В программе «Центр управления» в списке устройств выберите флеш-накопитель. Нажмите кнопку «Сохранить...» (рисунок 169).

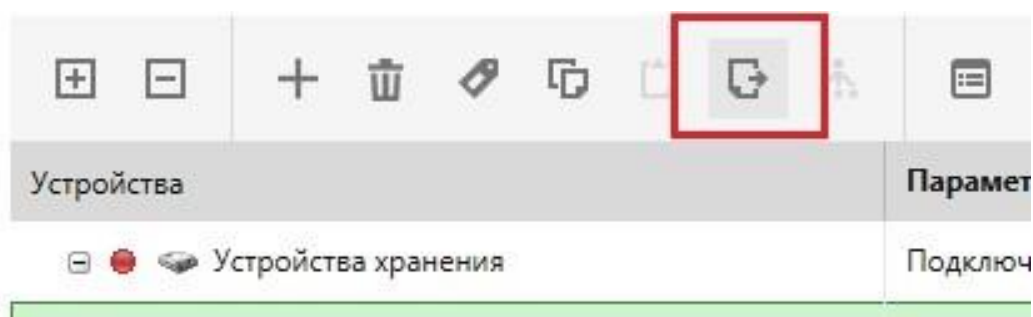


Рисунок 169 – Сохранение флеш-накопителя

Укажите путь сохранения файла конфигурации устройства, название файла и нажмите кнопку «Сохранить».

В панели «Компьютеры» выберите SNS-Client, перейдите на вкладку «Настройки», загрузите настройки и перейдите к разделу «Контроль устройств» (рисунок 170).

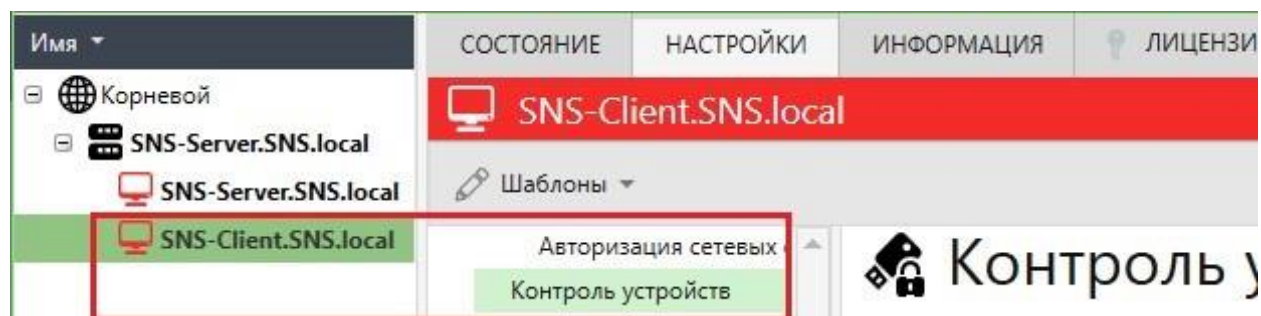


Рисунок 170 – Параметр «Контроль устройств»

Выберите в списке устройств «Устройства хранения». В списке содержится запись об флеш-накопителе. Нажмите кнопку «Разрешения» для этого устройства (рисунок 171).

Устройства	Параметры контрол
Устройства хранения	Наследуются (Подключ
JetFlash Mass Storage Device E17P1DKC	Подключение разреш

Рисунок 171 – Устройства хранения

В окне разрешений присутствуют права по умолчанию (рисунок 172). Изменение прав пользователей, выполненное ранее для SNS-Server, не применяется к SNS-Client, поскольку изменения вносились в локальную политику компьютера. Закройте окно разрешений.

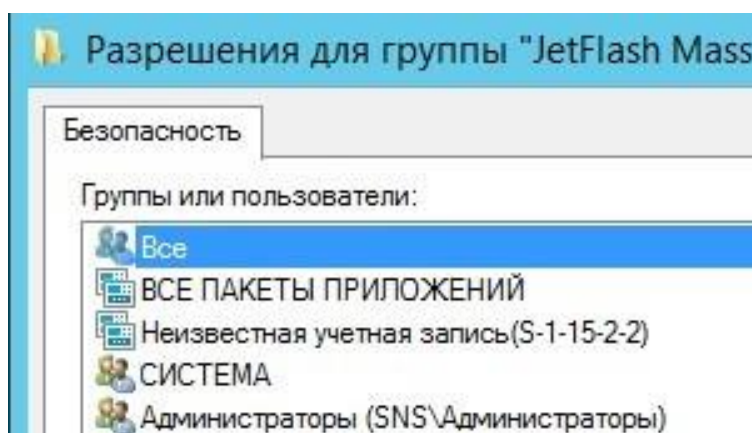


Рисунок 172 – Окно разрешений

Выберите группу «Устройства хранения» и нажмите кнопку «Добавить устройство» (рисунок 173).

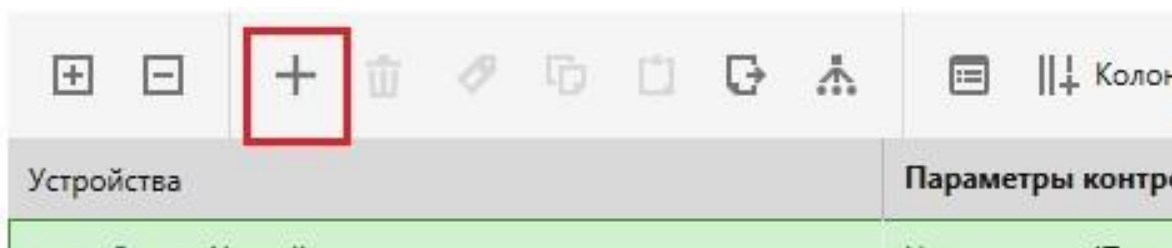


Рисунок 173 – Добавление устройства в группе «Устройства хранения» из файла описания устройства

Добавьте устройство из файла описания устройства, созданного на сервере SNS-Server для флеш-накопителя (после назначения прав пользователей). В окне с предупреждением о совпадении устройств нажмите кнопку «Заменить».

Нажмите кнопку «Применить» для сохранения изменений в политике компьютера SNSClient.

После применения настроек нажмите кнопку «Разрешения». В списке пользователей и групп появятся учетные записи, указанные при настройке разрешений для компьютера SNSServer.

Таким образом, файл описания устройства помимо параметров контроля устройства также содержит сведения о разрешениях пользователей на доступ к устройствам. Закройте окно разрешений.

В строке меню выберите пункт «Команды», в списке команд выберите «Применить групповые политики» для синхронизации настроек компьютера SNS-Client.

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью SNS\user1. Подключите флеш-накопитель к виртуальной машине. Попробуйте открыть, создать или изменить существующий на флеш-накопителе файл. Определите разрешенные и запрещенные действия. Они соответствуют разрешениям, загруженным из файла конфигурации. Завершите сеанс пользователя.

Войдите под учетной записью пользователя SNS\user2. Проверьте возможные действия с флеш-накопителем. Отключите накопитель от виртуальной машины и завершите сеанс пользователя.

Переключитесь к окну виртуальной машины SNS-Server. В программе «Центр управления» должны быть открыты настройки компьютер SNS-Client. В окне настроек нажмите кнопку «Шаблоны» и в списке выберите пункт «Создать по настройкам объекта управления» (рисунок 174).

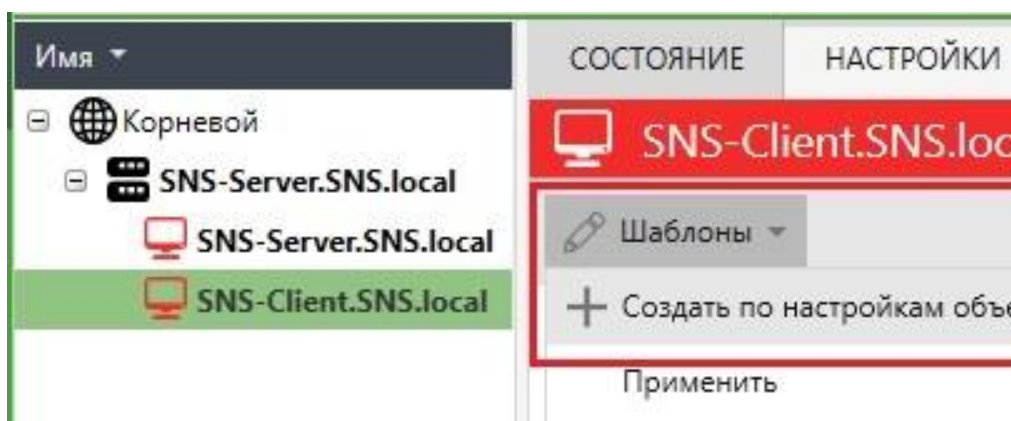


Рисунок 174 – Создание шаблона

В рабочей области отобразится окно «Создание шаблона». В списке параметров снимите флаг в узле «Политики» (рисунок 175). Автоматически будут сняты все флаги с этих разделов политики.

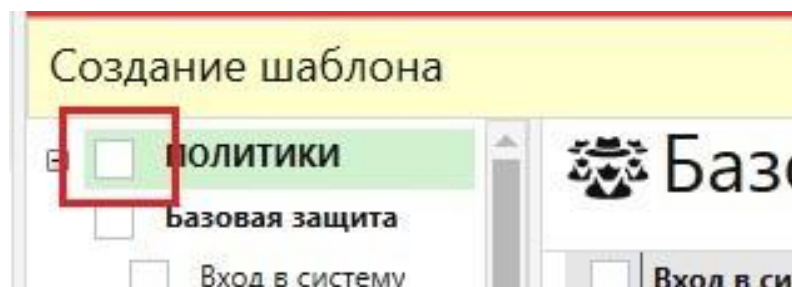


Рисунок 175 – Окно «Создание шаблона»

Пролистайте список и установите флаг «Контроль устройств» (рисунок 176).

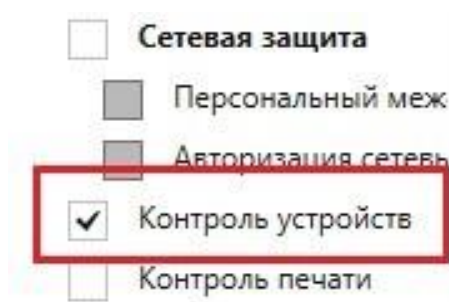


Рисунок 176 – Установка флага «Контроль устройств»

Внизу списка снимите флаги группы настроек «Регистрация событий» и «Параметры». Таким образом, в шаблон будут включены только параметры подсистемы контроля устройств. Нажмите кнопку «Сохранить». В открывшемся окне введите название создаваемого шаблона, комментарий и укажите место сохранения и название файла шаблона (рисунок 177). Нажмите кнопку «Сохранить».

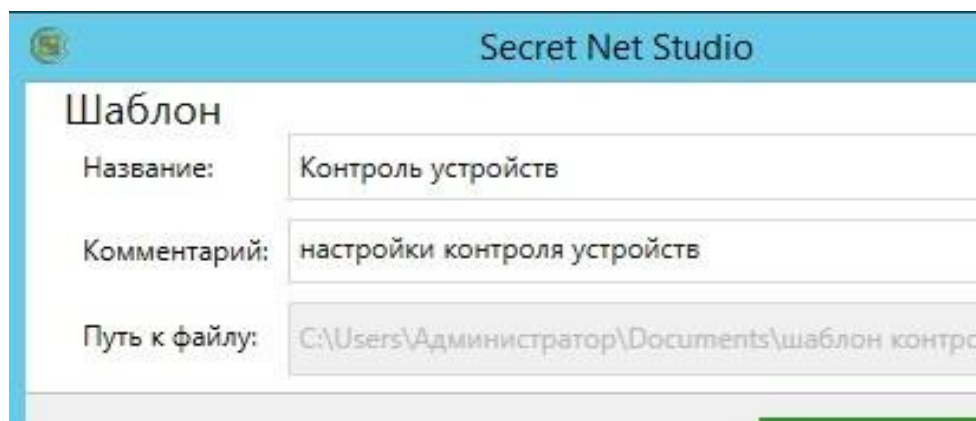


Рисунок 177 – Сохранение шаблона

В программе «Центр управления» в списке компьютеров выберите узел, соответствующий серверу безопасности, на вкладке «Настройки» загрузите настройки политики сервера безопасности (рисунок 178).

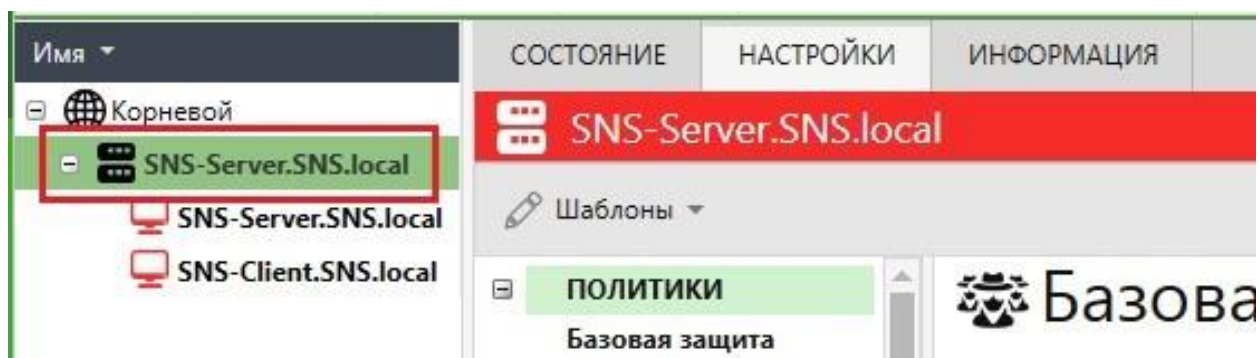


Рисунок 178 – Загрузка политик сервера безопасности

Нажмите кнопку «Шаблоны», раскройте пункт «Применить» и выберите пункт «Открыть из файла» (рисунок 179).

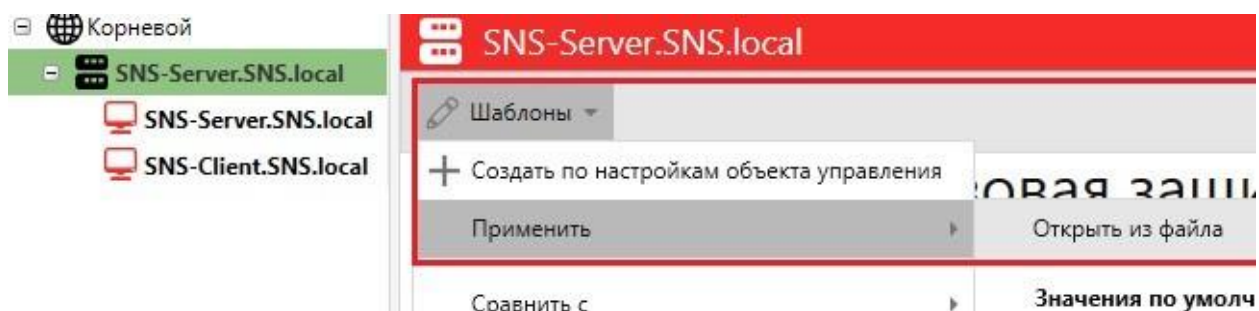


Рисунок 179 – Применение шаблона

В окне «Открыть» выберите шаблон настроек контроля устройств, созданный на предыдущем шаге, и нажмите кнопку «Открыть».

В рабочей области отобразится окно «Содержимое шаблона - <название шаблона>». В списке параметров будет установлен флаг только для группы параметров «Контроль устройств». Нажмите на название группы параметров «Контроль устройств», настройки этой группы будут доступны для выбора.

Выберите в группе «Локальные устройства» подгруппу «Физические диски». В ней содержится описание устройства «VBOX HARDDISK...». Раскройте окно параметров контроля этого устройства (рисунок 180).

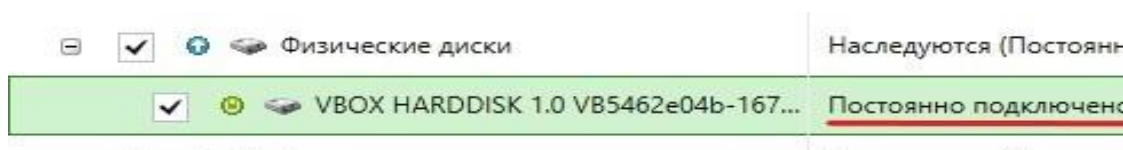


Рисунок 180 – Подгруппа «Физические диски»

В настройках параметров контроля указано, что устройство постоянно должно быть подключено и выполняется блокировка при его изменении. Это устройство содержится в конфигурации компьютера SNS-Client и не присутствует на других компьютерах. Если применить шаблон без корректировки к политике сервера безопасности, то на других компьютерах жесткий диск пропишется в конфигурацию и при выполнении контроля устройств произойдет блокировка. Поэтому из шаблона следует исключить такие устройства.

Исключение устройств из применяемого шаблона выполняется путем снятия флага рядом с названием устройства. Снимите флаг рядом с жестким диском, процессором, системной платой и памятью (рисунок 181) в группе «Локальные устройства».

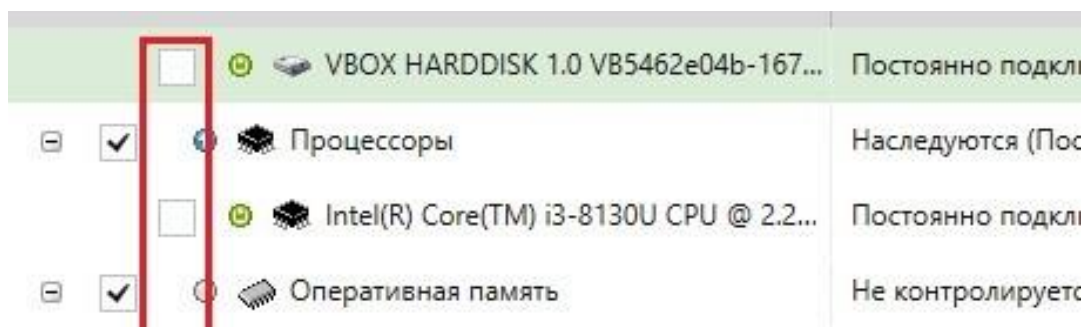


Рисунок 181 – Группа «Локальные устройства»

Затем выберите группу «Устройства USB» - «Интерфейсные устройства» и снимите флаги с устройств этой группы (рисунок 182).

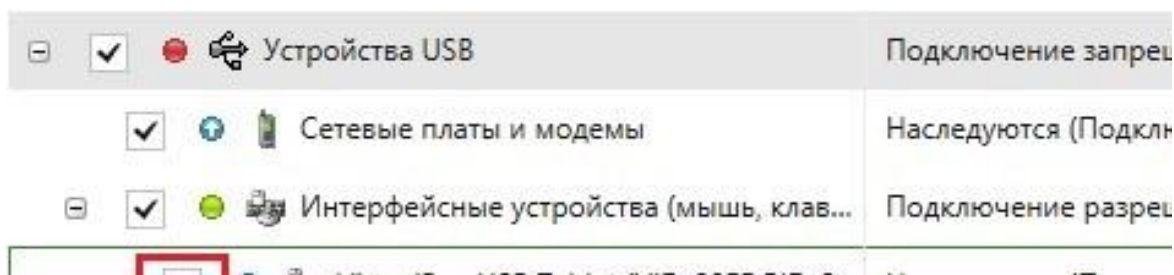


Рисунок 182 – Группа «Интерфейсные устройства»

Затем выберите группу устройств «Сеть» - «Соединение Ethernet» и снимите флаг у сетевого адаптера (рисунок 183).



Рисунок 183 – Группа «Соединение Ethernet»

Если не отключить в шаблоне интерфейсные устройства и адаптер, то блокировки компьютера не произойдет, поскольку подключение этих устройств разрешено, и блокировка отключена. Они исключаются из шаблона для того, чтобы в политике сервера безопасности не было записи о конкретных устройствах (с их уникальными серийными именами). Нажмите кнопку «Применить шаблон» (рисунок 184). В окне подтверждения нажмите «Да».



Рисунок 184 – Применение шаблона

В окне «Применение политик для группового объекта ОУ» должен быть установлен переключатель «Не менять» (рисунок 185). Нажмите кнопку «Применить».

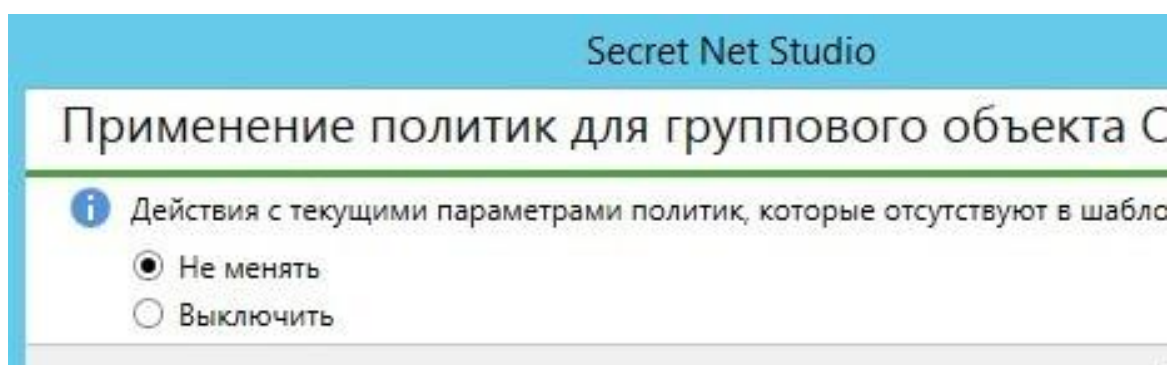


Рисунок 185 – Применение политик для группового объекта ОУ

После применения шаблона настроек выберите в списке группу параметров «Контроль устройств», просмотрите значения параметров и включение этих значений в политику сервера безопасности. Обратите внимание, что среди всех групп есть только флеш-накопитель, явно указанный в политике

сервера безопасности (рисунок 186). Это означает, что подключение флеш-накопителя будет разрешено на всех устройствах, подчиненных серверу безопасности.

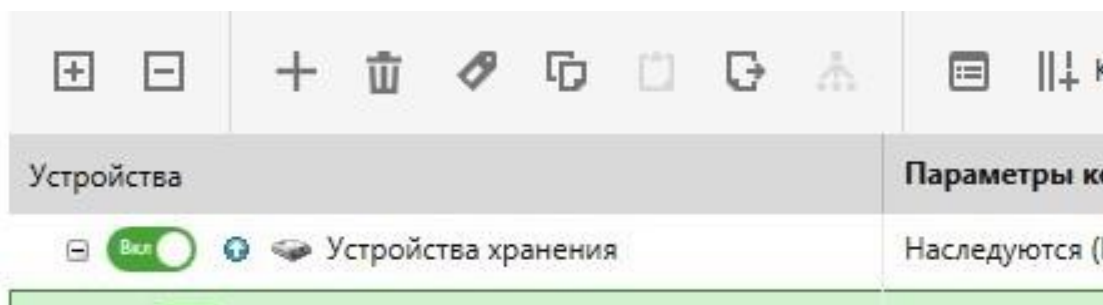


Рисунок 186 – Значения параметров политики сервера безопасности

В списке компьютеров выберите компьютер SNS-Server (рисунок 187). Примените к компьютеру групповые политики («Команды» - «Применить групповые политики»).



Рисунок 187 – Компьютер «SNS-Server»

После применения групповых политик откройте параметры контроля устройств. В качестве источника параметров будет указан SNS-Server.SNS.local (рисунок 188).

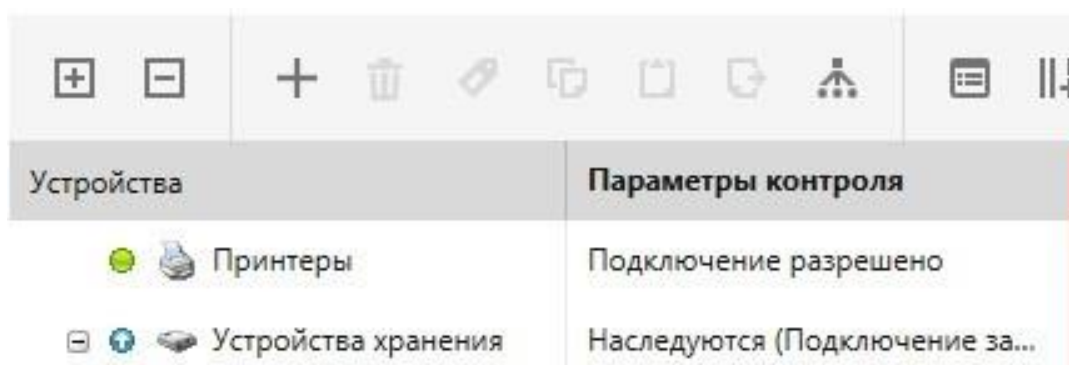


Рисунок 188 – Параметры контроля устройств

Примените групповые политики на компьютере SNS-Client.

7.9 Утверждение аппаратной конфигурации

На компьютере SNS-Server запустите консоль «Управление компьютером» (Win и R, compmgmt.msc). Выберите раздел «Диспетчер устройств». В правой области окна программы раскройте узел «DVD и CD-ROM дисководы», выберите «VBOX CD-ROM», нажмите правой кнопкой мыши и выберите пункт «Отключить» (рисунок 189). Нажмите «Да» в окне подтверждения.

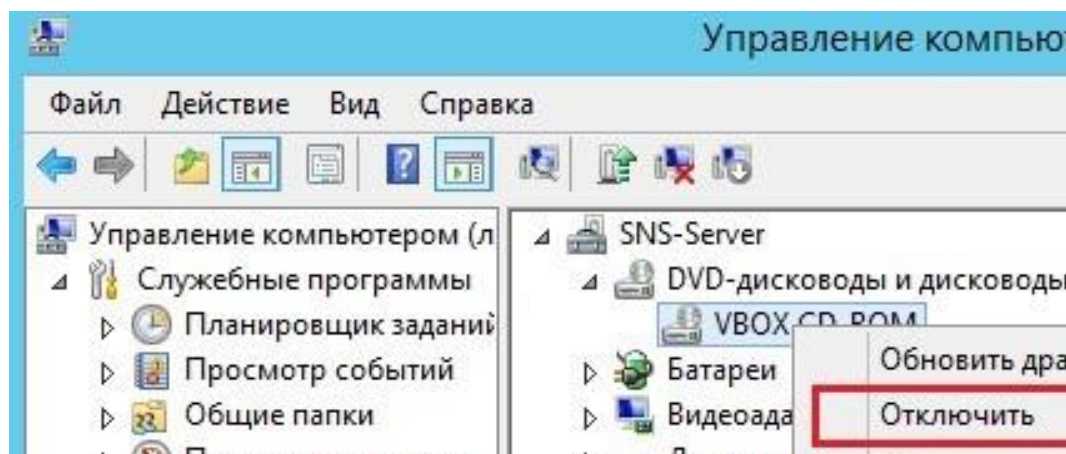


Рисунок 189 – Отключение «VBOX CD-ROM»

Произойдет блокировка компьютера из-за отключения устройства, для которого установлен параметр контроля «Постоянно подключено (с блокировкой)» (рисунок 190).

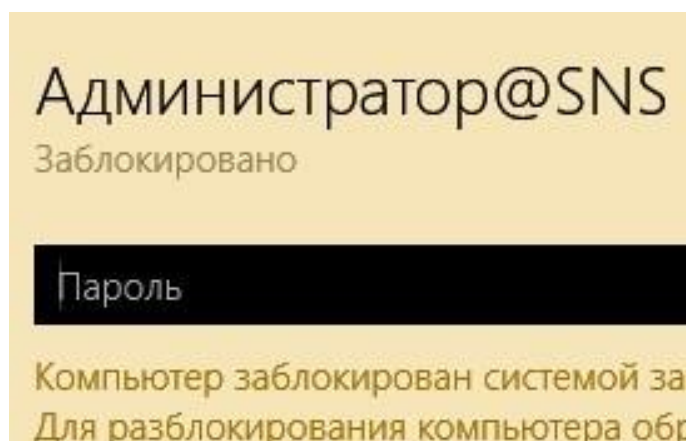


Рисунок 190 – Блокировка компьютера

Войдите под учетной записью Администратора. Появится окно предупреждения о блокировке компьютера с указанием причины. Нажмите «Да», чтобы снять блокировку (рисунок 191).

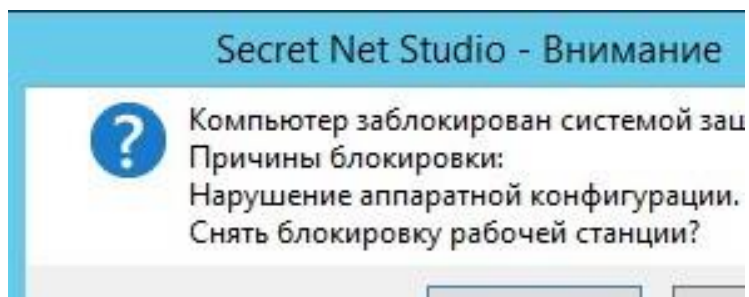


Рисунок 191 – Окно предупреждения о блокировке компьютера

В программе «Центр управления» выберите компьютер SNS-Server (прямоугольник 1 на рисунке 192) (рисунок 192). Перейдите на вкладку «Состояние» (прямоугольник 2 на рисунке 192). Нажмите на пиктограмму компонента «Контроль устройств» (квадрат 3 на рисунке 192). Пиктограмма будет синего цвета, что сигнализирует о событии изменения конфигурации. В окне справа отобразится информация об изменении в аппаратной конфигурации. Изменения аппаратной конфигурации отслеживаются СЗИ от НСД для устройств с включенным режимом контроля «Устройство постоянно подключено к компьютеру». Для внесения изменений в конфигурацию устройства надо утвердить новую аппаратную конфигурацию. Нажмите кнопку «Утвердить аппаратную конфигурацию» (прямоугольник 4 на рисунке 192) и нажмите «Да» в окне подтверждения.

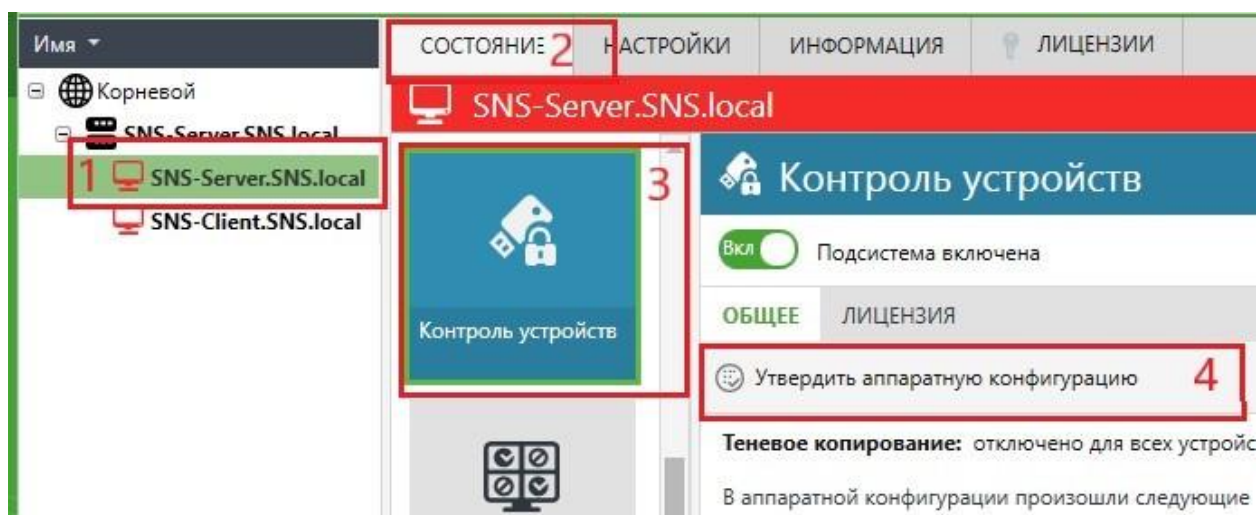


Рисунок 192 – Центр управления

7.10 Настройка механизма контроля целостности

Механизм контроля целостности (КИЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма

основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон.

Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

Унифицированные конфигурации содержат описание основных задач контроля целостности ресурсов системного реестра, ресурсов компьютера и специализированного программного обеспечения.

В рамках выполнения практической работы будут рассмотрены основные действия по настройке и проверке механизма контроля целостности. Задания контроля целостности в соответствии с унифицированными конфигурациями формироваться не будут, поскольку требуют больших затрат времени.

Подготовьте ресурсы для выполнения практической работы.

Запустите файл `sns_md.bat` (Win и R, набрать `cmd` и нажать Enter, с диска C:/ перенести файл в командную строку, нажать Enter). На диске C: будет создан каталог `Resource` с вложенной структурой каталогов и файлов. В реестр будут добавлены два ключа. Настройка модели данных для контроля целостности выполняется в программе «Контроль программ и данных (централизованный режим)». Для работы с программой предусмотрены следующие режимы:

- локальный режим работы — используется для редактирования локальной модели данных на компьютере;
- централизованный режим работы — используется для редактирования централизованной модели данных с описаниями объектов, контролируемых на защищаемых компьютерах. Централизованная модель данных применяется на клиентах в сетевом режиме функционирования совместно с локальными моделями, если они заданы. При этом приоритет имеют параметры централизованной модели.

При централизованном управлении, если в системе присутствуют компьютеры с версиями ОС различной разрядности, формируются две модели данных — для компьютеров с 32- разрядными ОС и для компьютеров с 64- разрядными ОС. Администратор с помощью программы может редактировать только одну централизованную модель данных, разрядность которой совпадает с разрядностью версии ОС Windows компьютера администратора. Поэтому при необходимости редактирования централизованной модели другой разрядности администратору следует использовать компьютер с версией ОС той же разрядности.

На компьютере SNS-Client войдите под учетной записью Администратора. Запустите программу «Контроль программ и данных (централизованный режим)» (Пуск – Код безопасности – Контроль программ и данных). После ввода PIN запустится окно программы. В поле «Субъекты управления» отображаются две структуры: «Структура x86» и «Структура x64», соответствующие компьютерам с разными типами архитектуры операционной системы (рисунок 193).

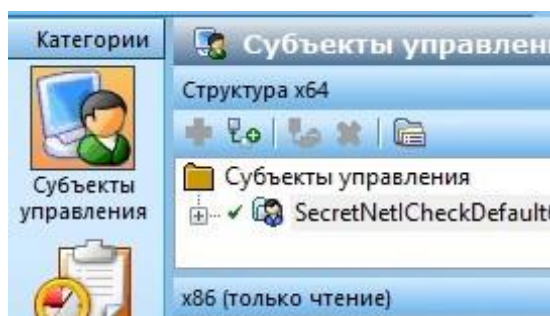


Рисунок 193 – Контроль программ и данных (централизованный режим)

Структура x86 доступна только для чтения, поскольку операционная система, установленная на компьютере SNS-Client, имеет архитектуру x64. Редактировать структуру x86 можно в аналогичной программе на компьютере с соответствующей разрядностью операционной системы. Для структуры x64 доступно редактирование (кнопки «добавить» и «удалить»), для структуры x86 на этом компьютере редактирование невозможно.

Выберите в окне «Субъекты управления» в структуре x64 субъект управления SecretNetIChcehDefault64. В правой части окна отобразятся задания,

назначенные этому субъекту управления, созданные автоматически при установке СЗИ от НСД. Нажмите правой кнопкой мыши на названии субъекта (или клавишу Enter, либо выберите в строке меню название субъекта) и в контекстном меню выберите пункт «Свойства» (рисунок 194).

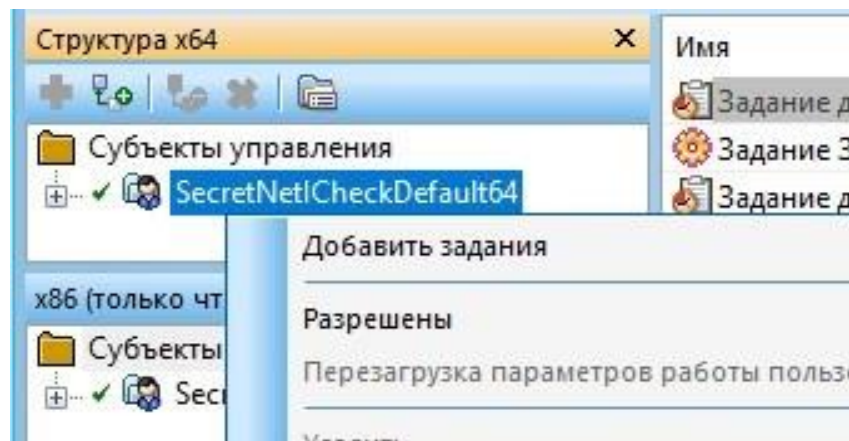


Рисунок 194 – Свойства «Субъектов управления»

Перейдите на вкладку «Режимы». На этой вкладке задается режим функционирования замкнутой программной среды. Настройки выполняются в соответствии с Унифицированными конфигурациями. Настройка режимов целесообразна после полного создания модели данных, поэтому на этой вкладке настройки выполнять не будем. Перейдите к вкладке «Синхронизация». В соответствии с Унифицированными конфигурациями установите следующие значения параметров (рисунок 195):

- при загрузке ОС: отключено;
- при входе: отключено;
- после входа: включено.

Значение последнего параметра «Периодически» определяется в каждом ТУ самостоятельно, поэтому в соответствии с Унифицированными конфигурациями флаг должен быть установлен и настроен, но в рамках выполнения практического занятия периодическая синхронизация выполняться не будет, поэтому флаг должен быть снят. Нажмите кнопку «ОК» для применения параметров.

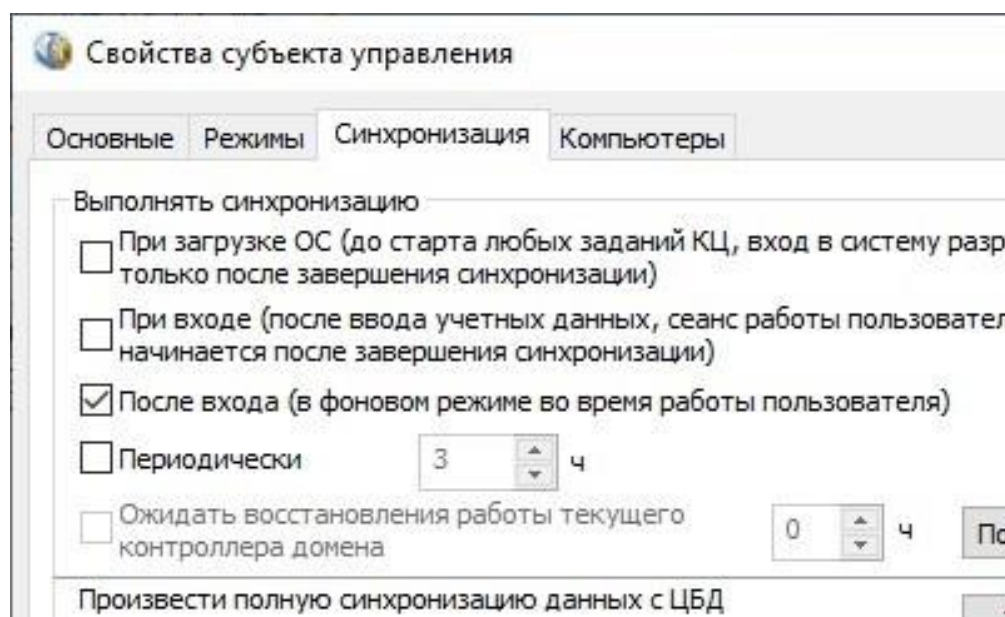


Рисунок 195 – Свойства субъекта управления

Выполните подготовку задач контроля целостности. Выберите категорию «Задачи», затем в поле «Структура» нажмите кнопку «Добавить новый» (рисунок 196).

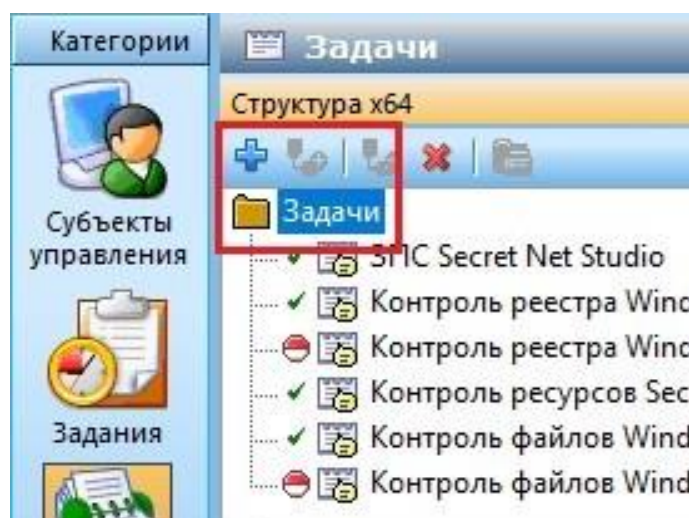


Рисунок 196 – Подготовка задач

Введите название задачи и описание, нажмите кнопку «ОК» (рисунок 197).

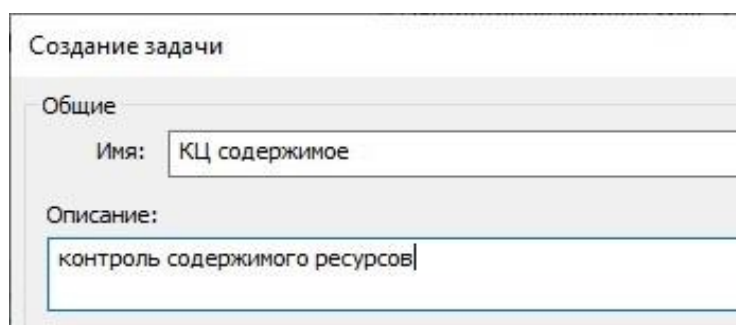


Рисунок 197 – Подготовка задачи

Нажмите правой клавишей мыши в окне структуры на имени созданной задачи. В контекстном меню выберите пункт «Добавить группы» и в выпадающем меню выберите пункт «Новую группу вручную» (рисунок 198).

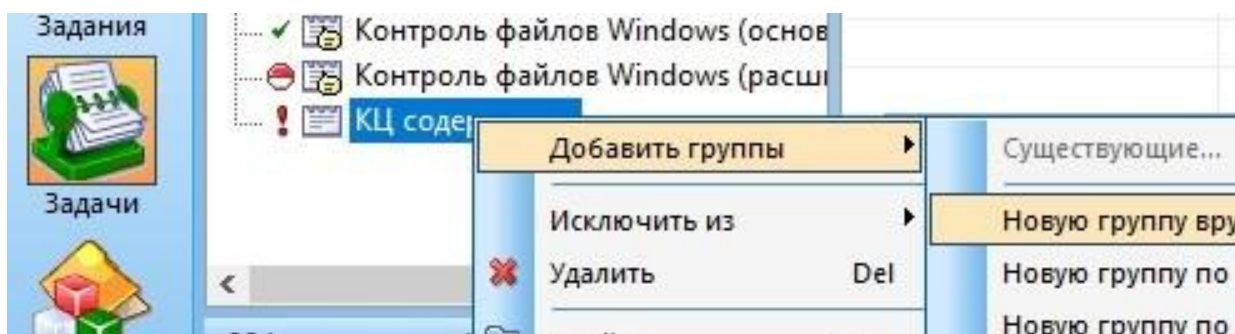


Рисунок 198 – Добавление группы

В появившемся диалоговом окне «Создание группы ресурсов» введите имя группы ресурсов и описание, значение параметра тип ресурсов должно быть установлено в «Файлы/каталоги» (рисунок 199). Нажмите кнопку «ОК».

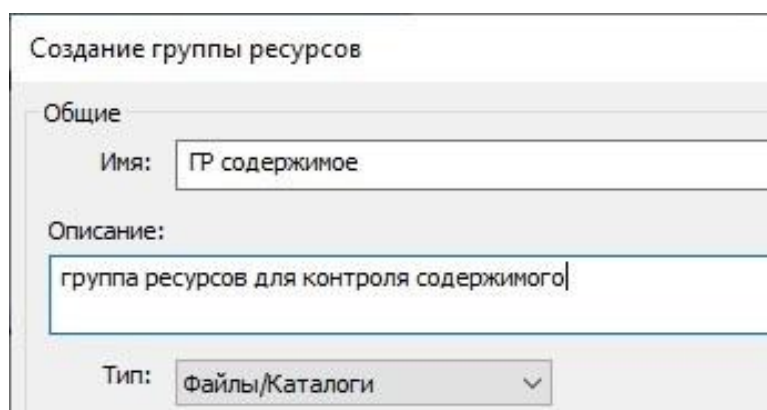


Рисунок 199 – Создание группы

В задачу добавится группа ресурсов. Пиктограмма рядом с именем задачи изменится с восклицательного знака на бело-красный круг. Нажмите на левой кнопкой мыши по знаку «+» рядом с именем задачи, затем выберите группу ресурсов, нажав один раз левой клавишей мыши по ее имени. При выборе группы ресурсов в правой части окна программы «Контроль программ и данных» отобразится список ресурсов, которые включены в эту группу. Для группы ресурсов этот список будет пустым, так как в нее не включен ни один ресурс (рисунок 200).

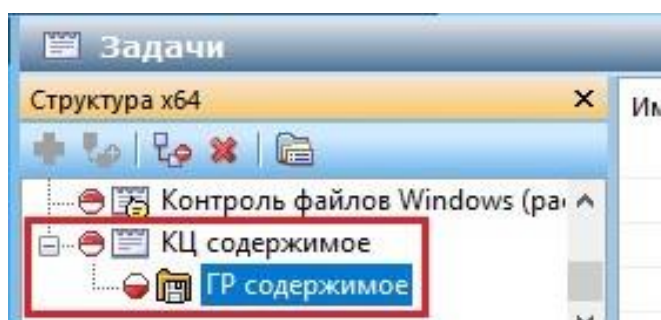


Рисунок 200 – Группа ресурсов

Нажмите правой кнопкой мыши по имени группы ресурсов и в контекстном меню выберите команду «Добавить ресурсы» - «Несколько новых...» (рисунок 201).

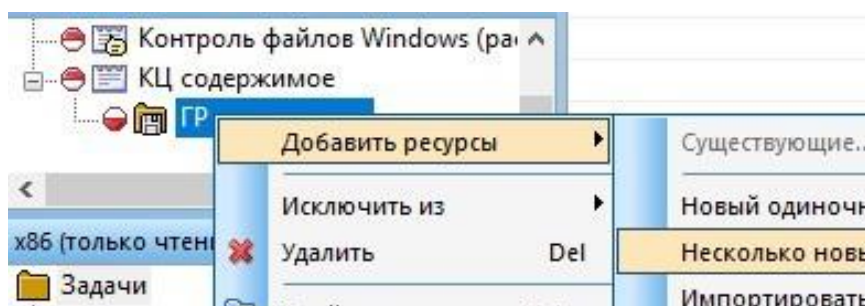


Рисунок 201 – Добавление ресурсов

В появившемся диалоговом окне «Создание ресурсов» нажмите кнопку «Добавить операцию...», в диалоговом окне «Выбор файлов» выберите из каталога C:\Resources\Dir1 файлы file1-1.txt, file1-2 и file1-3.txt. Нажмите «Открыть» (рисунок 202).

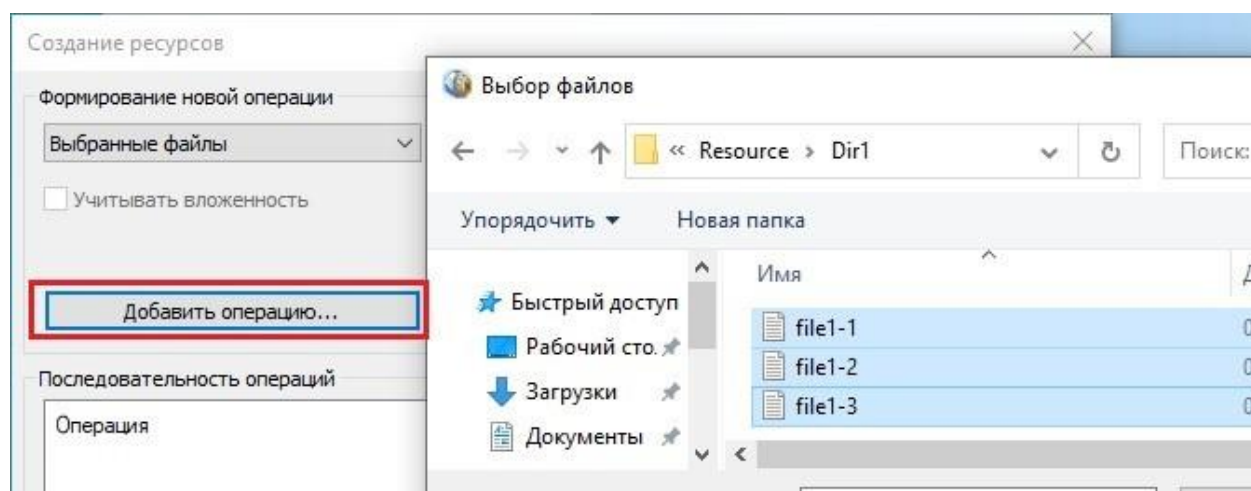


Рисунок 202 – Выбор файлов

Добавленные файлы отобразятся в диалоговом окне «Создание ресурсов» в списке «Последовательность операций». Нажмите кнопку «ОК». Файлы добавятся в группу ресурсов. Рядом с именем этой группы в окне структуры появится пиктограмма в виде галочки зеленого цвета. Она указывает на отсутствие ошибок (наличие ресурсов в группе). Рядом с именем задачи останется пиктограмма в виде красно-белого круга. Она показывает, что задача не назначена ни одному заданию контроля целостности.

Создайте новую задачу «КЦ существование» (контроль существования ресурсов). Нажмите правой клавишей мыши на имени созданной задачи, в контекстном меню выберите пункт «Добавить группы» - «Новую группу по каталогу» (рисунок 203).

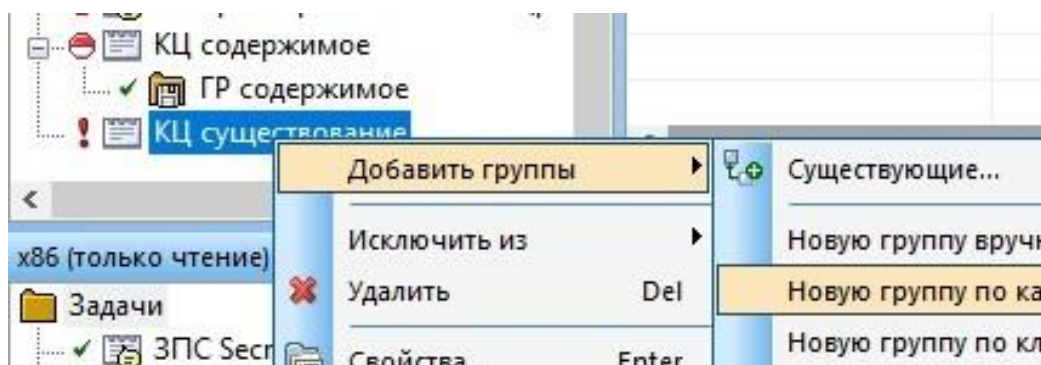


Рисунок 203 – Добавление группы

В окне обзора папок выберите каталог Resource\Dir2 (рисунок 204). Нажмите кнопку «ОК».

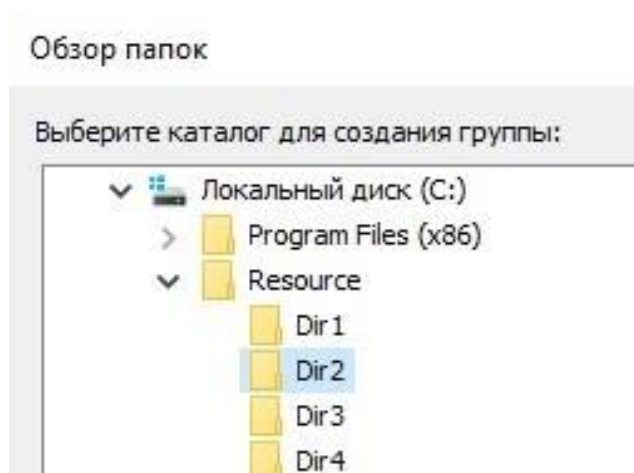


Рисунок 204 – Выбор каталога

Появится окно об успешном добавлении объектов (рисунок 205). Добавлено 4 объекта в модель данных (группа ресурсов, каталог и два файла). Нажмите «ОК».

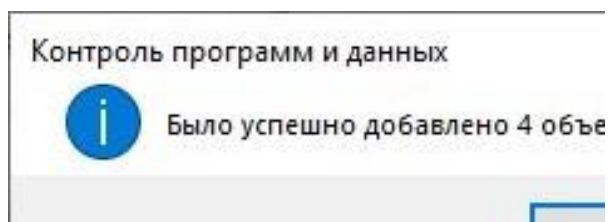


Рисунок 205 – Добавление объектов

Создайте задачу «КЦ атрибуты» (контроль атрибутов файлов). Добавьте в нее ручную группу ресурсов «ГР атрибуты» (группа ресурсов для контроля атрибутов) с типом «Файлы/Каталоги». В группу ресурсов добавьте два файла file3-1.txt и file3-2.txt из каталога Dir3 (рисунок 206).



Рисунок 206 – Создание задачи

Создайте задачу «КЦ права» (контроль прав). Добавьте в нее группу ресурсов по каталогу Dir4. Получится следующая структура задач (рисунок 207).

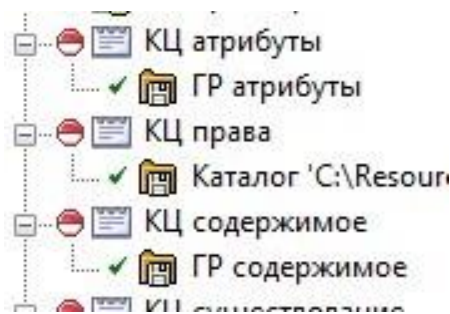


Рисунок 207 – Создание задачи «КЦ права»

Создайте задачу «КЦ реестр» (контроль ключей реестра) (рисунок 208).

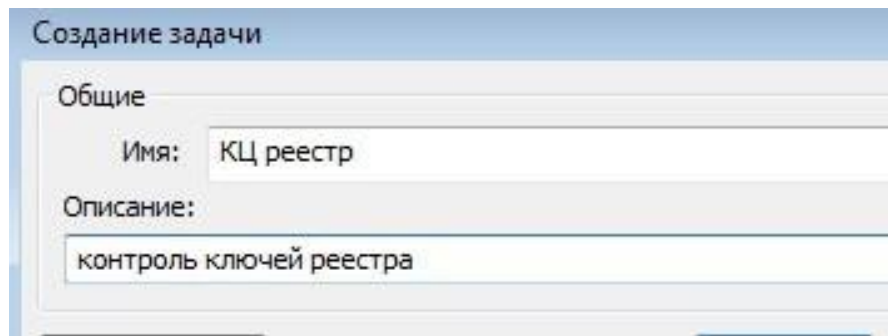


Рисунок 208 – Создание задачи «КЦ реестр»

Нажмите правой кнопкой мыши на названии задачи, в контекстном меню выберите «Добавить группы» - «Новую группу по ключу реестра» (рисунок 209).

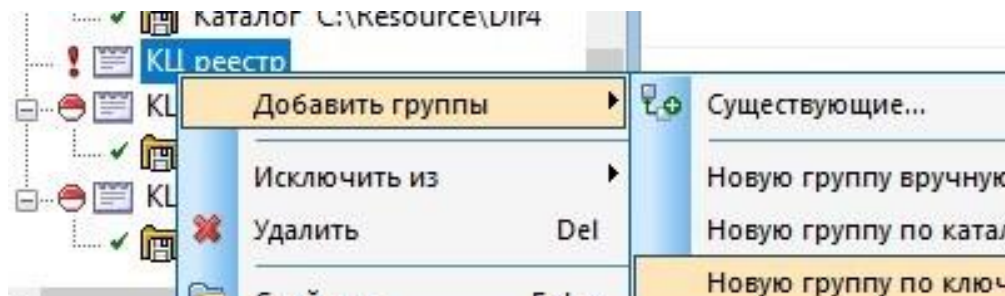


Рисунок 209 – Добавление группы

В окне «Просмотр реестра» раскройте узел HKLM\SOFTWARE\ и выберите узел TEST (рисунок 210). Нажмите «ОК».

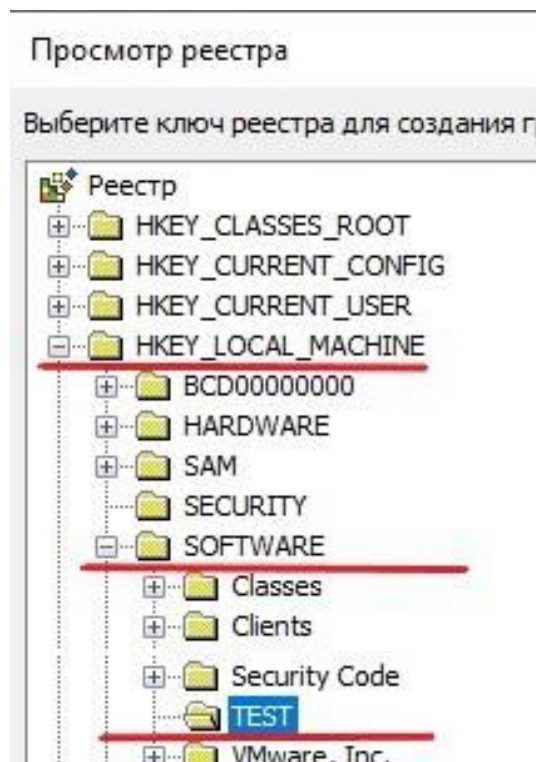


Рисунок 210 – Просмотр реестра

Появится окно об успешном добавлении объектов. Выберите в структуре группу ресурсов задачи, просмотрите добавленные объекты (рисунок 211).

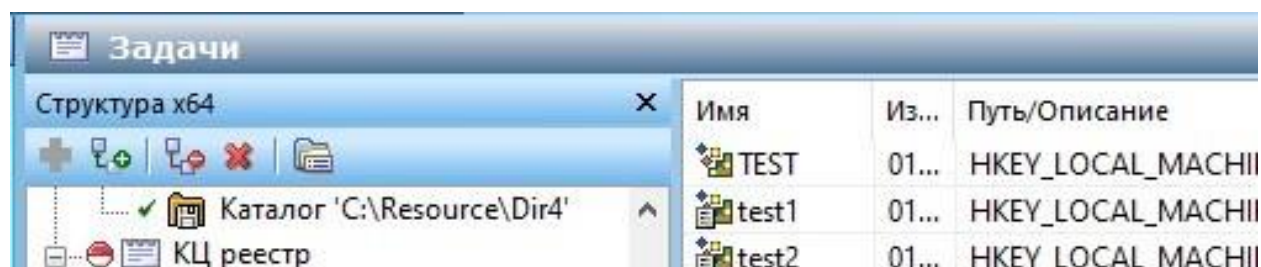


Рисунок 211 – Группа ресурсы задачи

Задачи контроля целостности и ресурсы сформированы. Теперь необходимо сформировать задания контроля целостности. Перейдите к категории «Задания». Нажмите кнопку «Добавить новый». В окне «Создание нового задания» установите переключатель в положение «Контроль целостности (КЦ)» (рисунок 212). Нажмите «ОК».

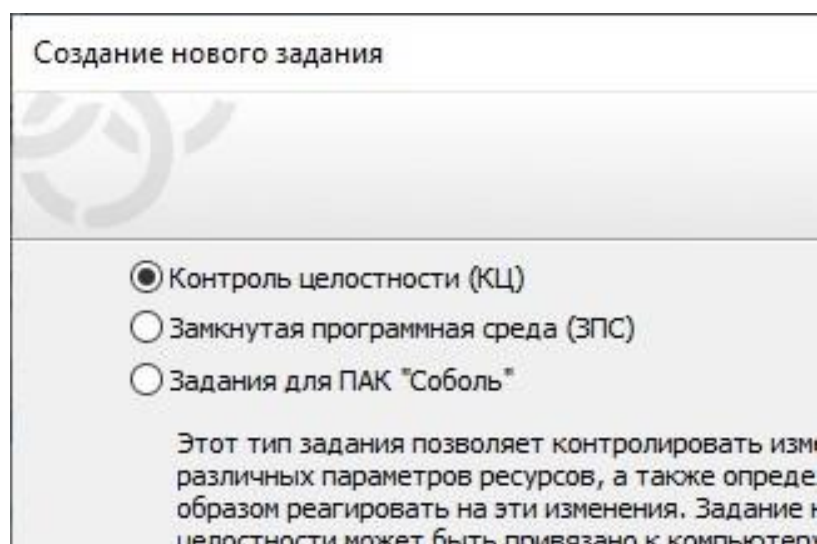


Рисунок 212 – Создание задания

В окне «Создание нового задания на КЦ» введите имя «Задание для контроля содержимого» (рисунок 213).



Рисунок 213 – Ввод имени задачи

В списке «Метод контроля ресурсов» выберите в выпадающем списке «Содержимое», значение параметра «Алгоритм» установите в «CRC32». В поле «Реакция на отказ» раскройте список «Действия» и установите значение «Заблокировать компьютер» (рисунок 214).

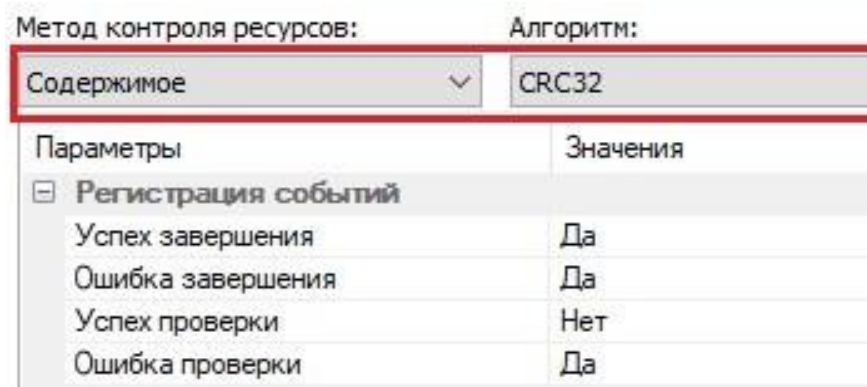


Рисунок 214 – Установка метода контроля ресурсов и алгоритма

Перейдите на вкладку «Расписание», в поле «Основные» установите флаг «При входе» (рисунок 215). Нажмите «ОК».

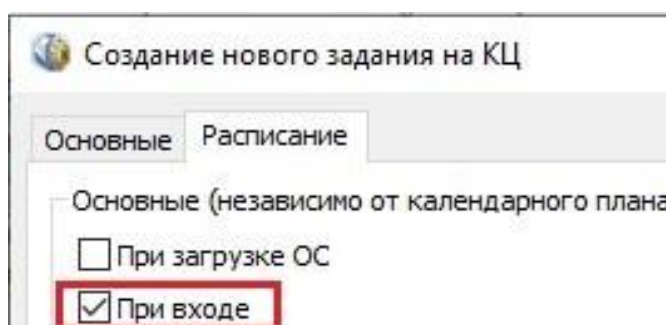


Рисунок 215 – Установка параметра «При входе»

Созданное задание появится в структуре с пиктограммой в виде восклицательного знака (рисунок 216), означающей, что задание не содержит задач и не назначено субъекту управления.

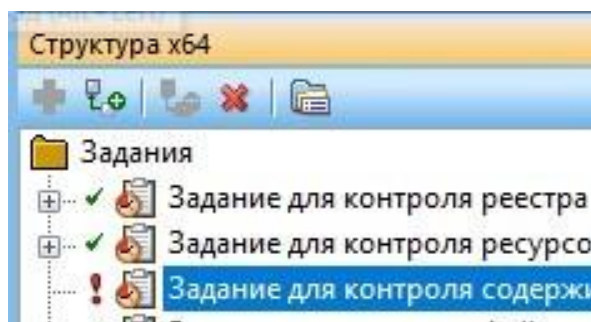


Рисунок 216 – Задание создано

Нажмите на задании правой кнопкой мыши и в контекстном меню выберите «Добавить задачи/группы» - «Существующие» (рисунок 217).

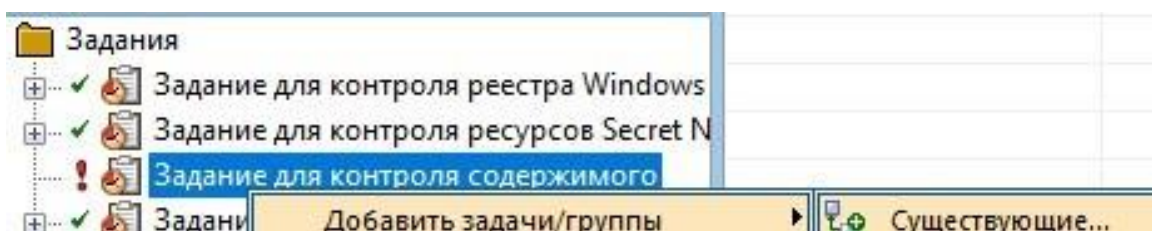


Рисунок 217 – Добавление задачи

В окне добавления подчиненных объектов выберите задачу «КЦ содержимое» (рисунок 218). Ноль в графе «Принадлежность» у задачи означает, что она не назначена еще ни одному заданию. Нажмите «ОК».

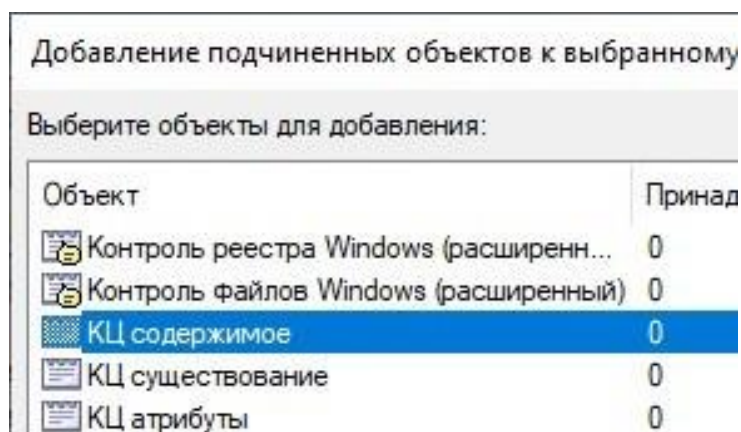


Рисунок 218 – Выбор задачи «КЦ содержимое»

Пиктограмма у задания сменился на красно-белый круг, что означает отсутствие связи задания с субъектом.

Добавьте задание «Задание для контроля существования». В свойствах задачи установите метод контроля «Существование». Для параметра «Действия» и установите значение «Заблокировать компьютер». На вкладке «Расписание» в поле «Календарный план» включите параметр, соответствующий месяцу и дню недели выполнения практического задания. Затем включите параметр «Временные параметры» и установите интервал контроля в 1-2 минуты (рисунок 219). Нажмите «ОК».

Календарный план

	Пн	Вт	Ср	Чт	Пт	Сб	Вс
Январь			■				
Февраль							
Март	■		✓				
Апрель							
Май							
Июнь							
Июль							
Август							
Сентябрь							
Октябрь							
Ноябрь							

☒ Временные пар

Часы контроля (0-

Каждый час

Рисунок 219 – Составление календарного плана

Добавьте созданному заданию существующую задачу «КЦ существование». Добавьте задание «Задание для контроля атрибутов». В параметре «Метод контроля ресурсов» установите значение «Атрибуты», в параметре «Действия» установите «Восстановить из эталона» (рисунок 220). На вкладке «Расписание» установите параметр «При входе».

Метод контроля ресурсов: Атрибуты

Алгоритм: Нет алгоритма

Параметры	Значения
☐ Регистрация событий	
Успех завершения	Да
Ошибка завершения	Да
Успех проверки	Нет
Ошибка проверки	Да

Рисунок 220 – Добавление задания «Задание для контроля атрибутов»

Добавьте созданному заданию существующую задачу «КЦ атрибуты».

Добавьте задание «Задание для контроля прав». В параметре «Метод контроля ресурсов» установите значение «Права доступа», в параметре «Действия» установите «Заблокировать компьютер», на вкладке «Расписание» установите флаг «После входа». Добавьте созданному заданию существующую задачу «КЦ права».

Добавьте задание «Задание для контроля реестра», установите метод контроля «Содержимое» и выберите алгоритм «Полное совпадение». Для

параметра «Действие» установите значение «Восстановить с блокировкой» (рисунок 221). На вкладке «Расписание» установите значение «При входе».

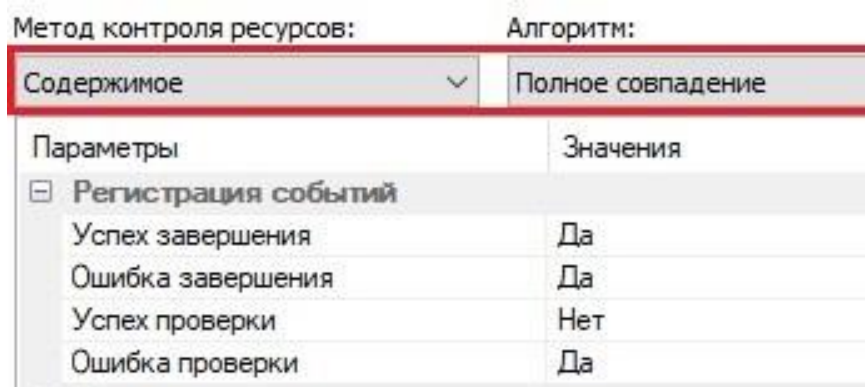


Рисунок 221 – Добавление задания «Задание для контроля реестра»

Добавьте созданному заданию существующую задачу «КЦ реестр».

Перейдите к категории «Субъекты управления». Выберите субъект SecretNetICheshDefault64. Нажмите правой кнопкой и в контекстном меню выберите «Добавить задания» - «Существующие» (рисунок 222).

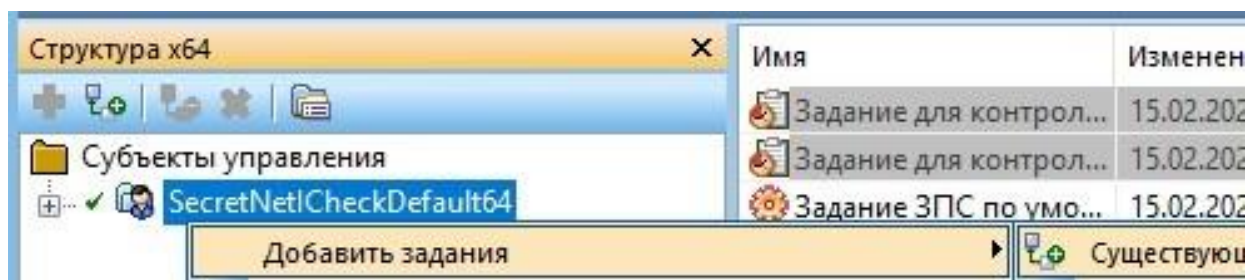


Рисунок 222 – Добавление существующих заданий

В окне добавления подчиненных объектов установите флаг «Выделить все» и нажмите кнопку «ОК» (рисунок 223).

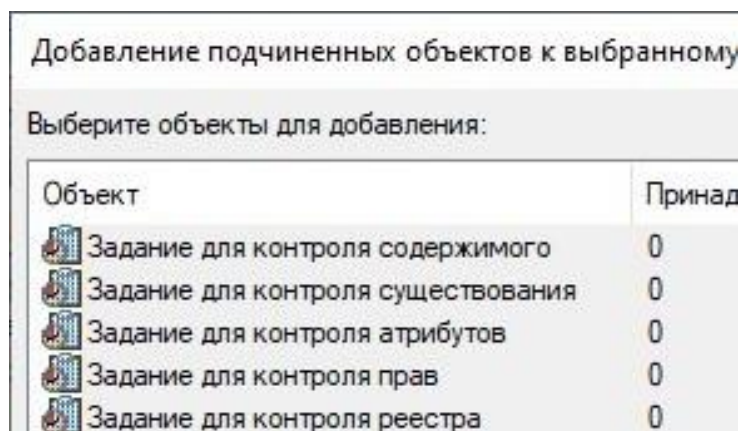


Рисунок 223 – Выбор всех объектов

В результате получится следующая структура модели данных (рисунок 224).

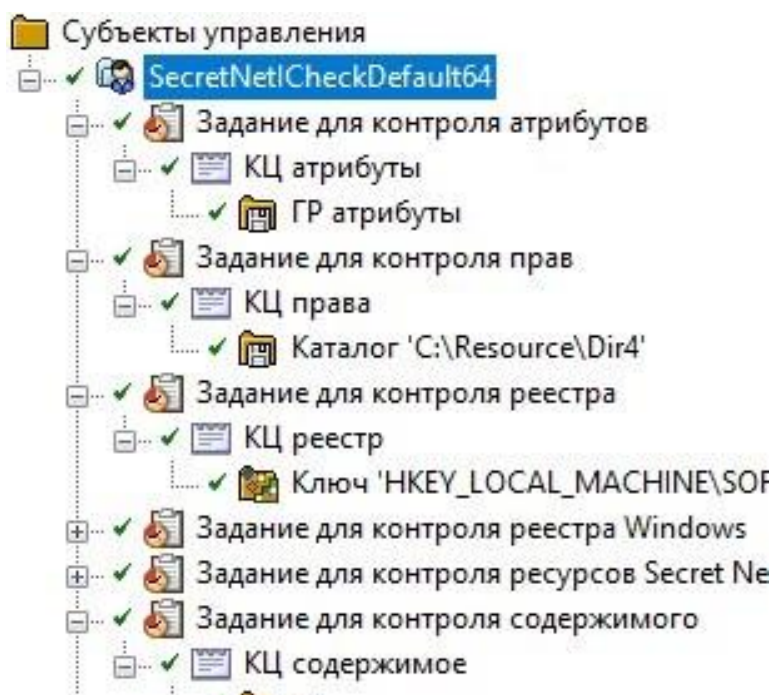


Рисунок 224 – Структура модели данных

Нажмите кнопку «Сохранить модель» (рисунок 225).

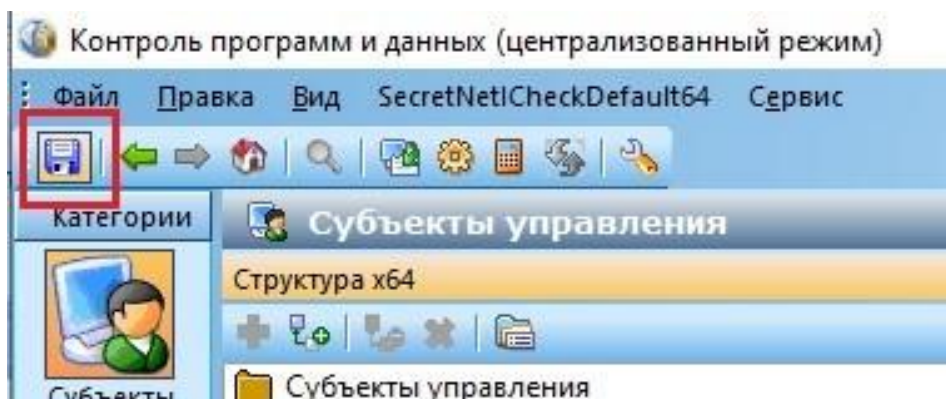


Рисунок 225 – Сохранение модели

После назначения заданий субъекту (в роли субъектов выступают компьютеры структуры управления) необходимо рассчитать эталонные значения контрольных сумм, которые будут использоваться для контроля целостности ресурсов. В окне программы в меню «Сервис» выберите пункт «Эталонные» и в выпадающем списке выберите пункт «Расчет» (рисунок 226).

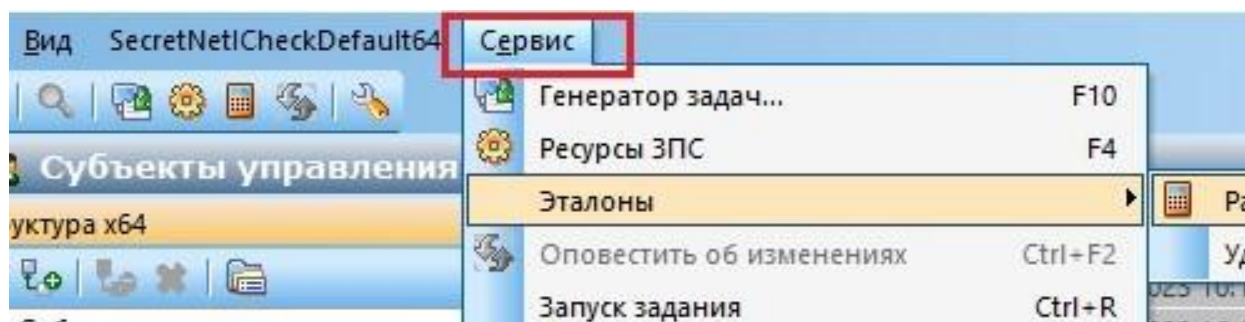


Рисунок 226 – Расчет эталонных значений контрольных сумм

В окне «Расчет эталонов» оставьте параметры без изменений и нажмите кнопку «ОК». После завершения расчета эталонов выдается сообщение о его результатах. Завершите сеанс Администратора.

7.11 Проверка заданий контроля целостности

Войдите под учетной записью user3.

Откройте содержимое файла C:\Resources\Dir1\file1-1.txt. Допишите несколько символов в начале файла. Сохраните изменения в файле. Переименуйте файл file1-2.txt (допишите символ в название). Переместите файл file1-3.txt в каталог Resources (вырезать – вставить). Завершите сеанс пользователя user3. Снова войдите под учетной записью user3. Компьютер будет заблокирован (рисунок 227).

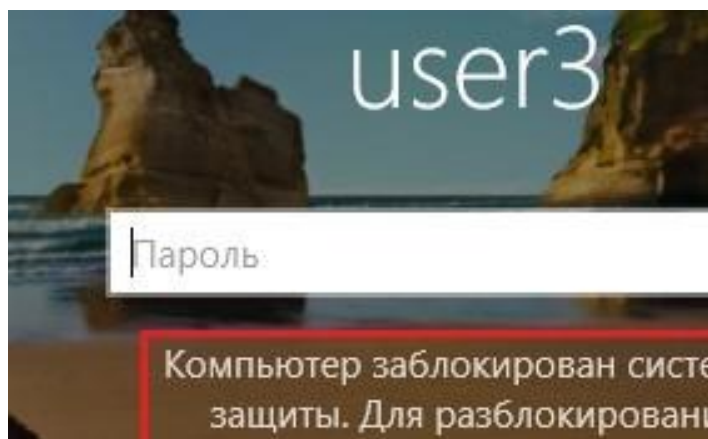


Рисунок 227 – Вход под учетной записью «user3»

Войдите под учетной записью Администратора. Нажмите «Да» в окне снятия блокировки (рисунок 228).

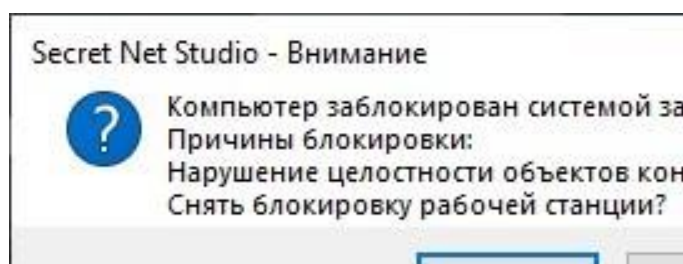


Рисунок 228 – Окно снятия блокировки

Запустите программу «Локальный центр управления». Перейдите к панели «Журналы». Двойным кликом на запросе «Все тревоги» загрузите журнал тревог (рисунок 229).

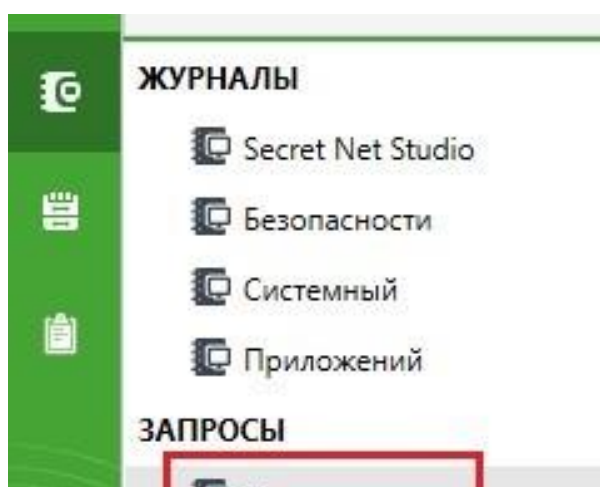


Рисунок 229 – Панель «Журналы»

В журнале тревог выберите события нарушения целостности. Нажмите клавиши Ctrl и D для отображения детальной информации о событии (рисунок 230).

СОБЫТИЯ		УГРОЗЫ		
	Дата ▼	Журнал	Событие	Категор.
	01.03.2023...	Secret Net St...	Обнаружено нар...	Контрол
	01.03.2023...	Secret Net St...	Нарушение целос...	Контрол
ДЕТАЛЬНО		ОБЩЕЕ	ПАРАМЕТРЫ	
Описание				
Нарушение целостности ресурса.				
Тип ресурса: Файл				
Имя ресурса: C:\Resource\Dir1\file1-1.txt				
Задание: Задание для контроля содержимого				
Метод контроля: Проверка содержимого				

Рисунок 230 – Отображение детальной информации о событии

В журнале тревог выберите события нарушения целостности. В описании событий просмотрите описание событий, вызвавших блокировку (рисунок 231).

Нарушение целостности ресурса.
Тип ресурса: Файл
Имя ресурса: C:\Resource\Dir1\file1-1.txt
Задание: Задание для контроля содержимого
Метод контроля: Проверка содержимого
Алгоритм расчета контрольных сумм: CRC32
Задача: КЦ содержимое
Группа ресурсов: ГР содержимое

Нарушение целостности ресурса.
Тип ресурса: Файл
Имя ресурса: C:\Resource\Dir1\file1-2.txt
Задание: Задание для контроля содержимого
Метод контроля: Проверка содержимого
Алгоритм расчета контрольных сумм: CRC32
Задача: КЦ содержимое
Группа ресурсов: ГР содержимое

Нарушение це
Тип ресурса: ф
Имя ресурса: i
Задание: Зада
Метод контро
Алгоритм расч
Задача: КЦ со,
Группа ресурс

Рисунок 231 – Описание событий

Таким образом, при выборе метода контроля «Содержимое» контролируется не только целостность ресурса (отсутствие изменений внутри файла), но и отсутствие изменений в названии и местоположении ресурса.

Восстановите измененное содержимое, название и расположение файлов. Завершите сеанс Администратора. Войдите под учетной записью user3. Вход будет разрешен.

Откройте содержимое файла C:\Resources\Dir2\file2-1.txt. Допишите несколько символов в начале файла. Сохраните изменения в файле. Переместите файл file2-2.txt в каталог Resources (вырезать – вставить). Дождитесь автоматической блокировки сеанса пользователя user3.

Войдите под учетной записью Администратора, восстановите местоположение файла file2-2.txt. Запустите программу «Локальный центр управления». Перейдите к панели «Журналы». Двойным кликом на запросе «Все тревоги» загрузите журнал тревог. В журнале тревог выберите последние события нарушения целостности. Нажмите клавиши Ctrl и D для отображения детальной информации о событиях.

Отобразятся только события, связанные с перемещением ресурса file2-2.txt, причем периодичность появления событий будет соответствовать настройкам задания проверки существования. Изменения в файле file2-1.txt не фиксируются как событие безопасности при контроле существования.

Завершите сеанс Администратора. Войдите под учетной записью user3. В каталоге C:\Resources\Dir3 нажмите правой кнопкой мыши на файле file3-1.txt.

В контекстном меню выберите пункт «Свойства» (рисунок 232).

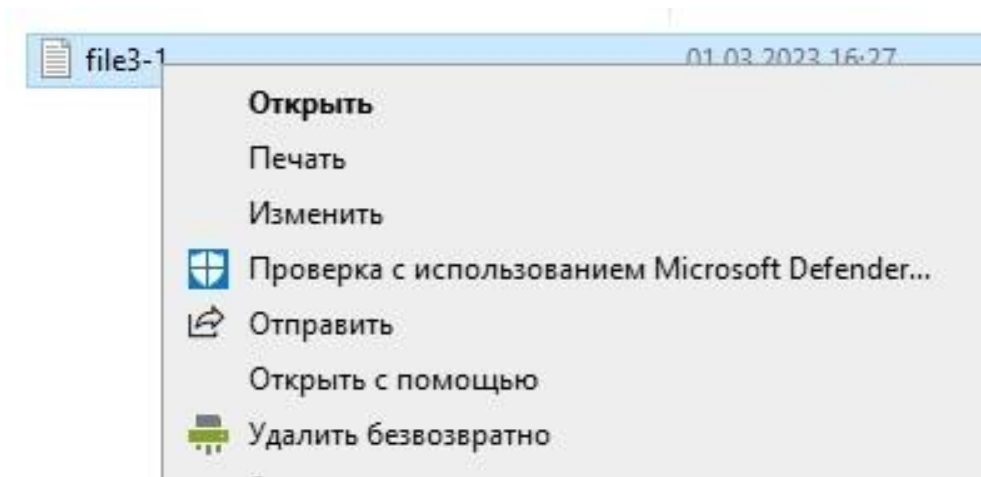


Рисунок 232 – Свойства файла

В окне свойств на вкладке снимите флаг «Только чтение» в поле «Атрибуты» (рисунок 233). Нажмите «ОК».

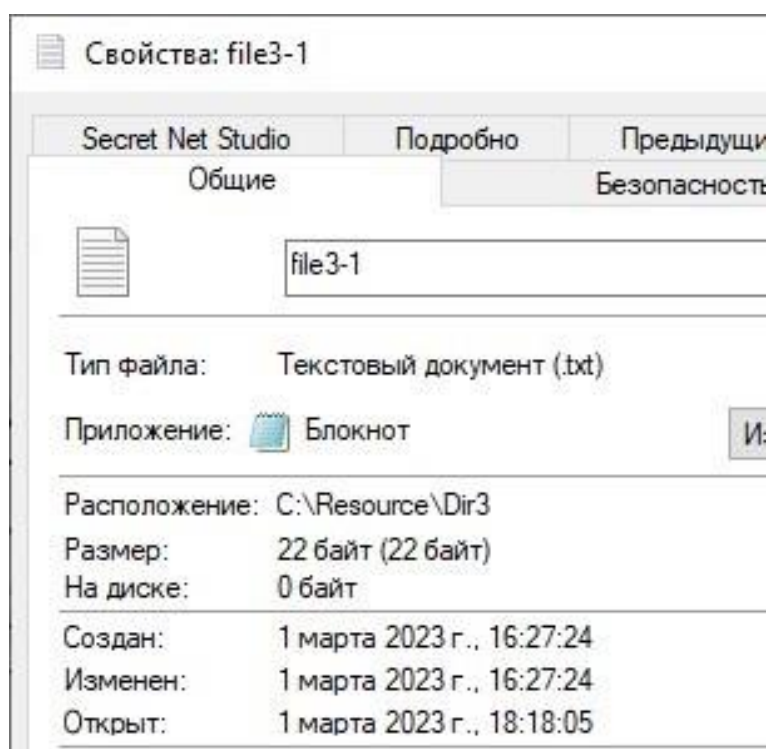


Рисунок 233 – Изменение атрибута файла

Откройте содержимое файла и внесите изменения (допишите несколько символов в начале файла). Сохраните внесенные изменения.

Нажмите клавиши Win и R, введите cmd и нажмите Enter. Запустится командная строка.

Введите команду `attrib -r -h C:\Resource\Dir3\file3-2.txt` и нажмите Enter. Вернитесь к окну программы «Проводник». В каталоге Dir3 отобразится ранее скрытый файл (рисунок 234).

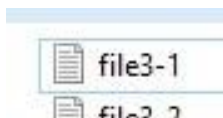


Рисунок 234 – Отображение файла

Завершите сеанс пользователя user3. Снова войдите под учетной записью пользователя user3. При входе пользователя будет произведен запуск задания контроля атрибутов (в соответствии с настройками). Откройте содержимое каталога C:\Resources\Dir3. В каталоге снова отображается только один файл file3-1.txt. Откройте свойства файла и просмотрите атрибуты. Будет восстановлено значение атрибута «Только для чтения». Откройте содержимое файла. Ранее внесенные изменения сохранились, поскольку при контроле атрибутов не контролируется содержимое файлов.

Завершите сеанс пользователя user3. Войдите под учетной записью Администратора. Загрузите журнал тревог в программе «Локальный центр управления». Найдите записи о последних событиях нарушения целостности при выполнении задания «Задание для контроля атрибутов». Просмотрите детальную информацию о событиях. Событие изменения файла file3-1.txt также будет зафиксировано (рисунок 235).

Нарушение целостности ресурса.
Тип ресурса: Файл
Имя ресурса: C:\Resource\Dir3\file3-1.txt
Задание: Задание для контроля атрибутов
Метод контроля: Проверка атрибутов
Алгоритм расчета контрольных сумм: Не
Задача: КЦ атрибуты
Группа ресурсов: ГР атрибуты
Описание: Изменились атрибуты файла.
Старое значение: архивный, только для ч
Новое значение: архивный.
Изменилось время последнего изменени
Старое значение: 01.03.2023 16:27:24.
Новое значение: 01.03.2023 18:22:49.

Рисунок 235 – Детальная информация о событиях

Откройте содержимое каталога C:\Resources\Dir4. Откройте окно свойств файла file4-1.txt, в окне свойств перейдите на вкладку «Безопасность» и нажмите кнопку «Изменить» (рисунок 236).

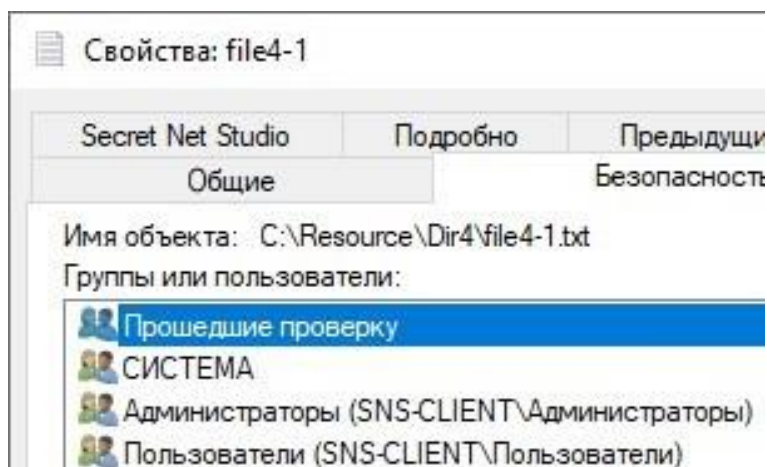


Рисунок 236 – Свойства файла «file4-1.txt»

В окне разрешений выберите группу «Пользователи» и в поле разрешений установите флаг «Запись» (рисунок 237). Нажмите «ОК» в окне разрешений и «ОК» в окне свойств.

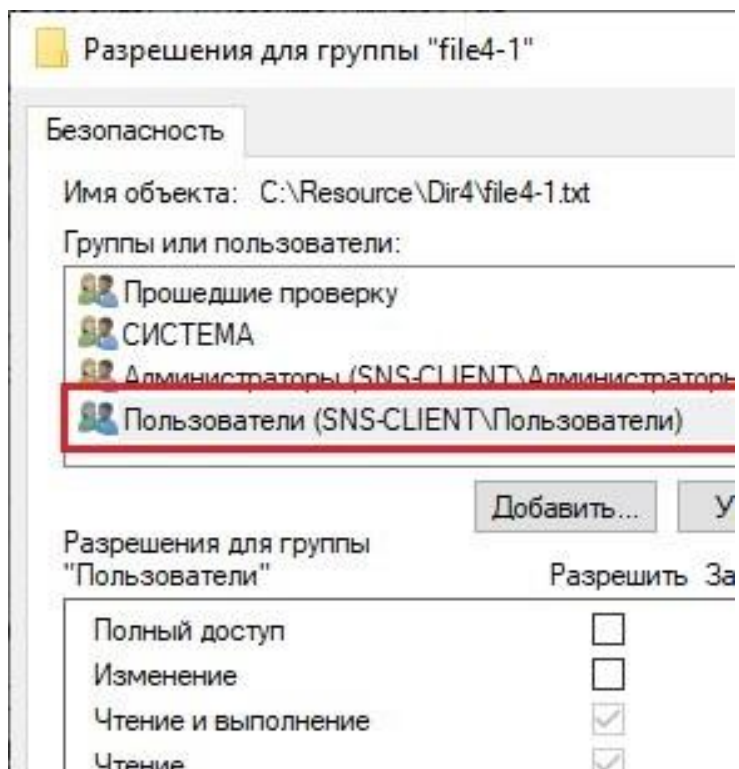


Рисунок 237 – Окно свойств

Завершите сеанс Администратора, войдите под учетной записью пользователя user3. После входа пользователя сработает блокировка. Войдите под учетной записью Администратора, снимите блокировку.

Восстановите значение прав файла file4-1.txt.

Запустите «Локальный центр управления», загрузите журнал тревог, просмотрите описание событий задания контроля прав. Нажмите Win и R, введите regedit и нажмите Enter. Раскройте узел HKLM\SOFTWARE\TEST (можно установить курсор в дерево реестра и набирать начало ключей для поиска), в правой части окна выберите параметр test1, нажмите правой кнопкой мыши и выберите пункт «Изменить» (рисунок 238).



Рисунок 238 – Редактор реестра

Введите новое значение параметра (рисунок 239) и нажмите «ОК».

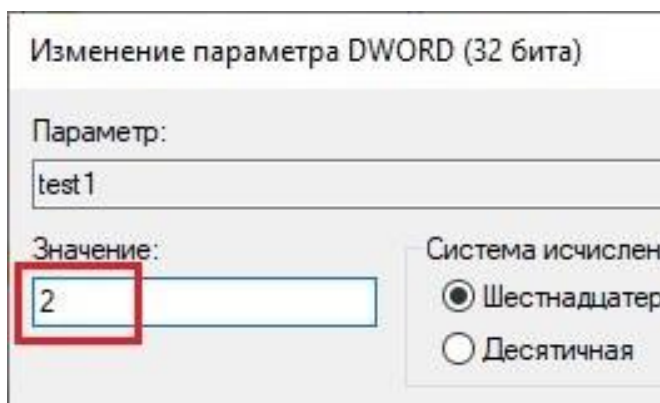


Рисунок 239 – Ввод нового значения параметра

Выберите второй параметр, нажмите правой кнопкой мыши и выберите пункт «Переименовать». Допишите в название параметра цифру и нажмите Enter (рисунок 240).



Рисунок 240 – Переименование второго параметра

Завершите сеанс Администратора. Снова войдите под учетной записью Администратора. Появится сообщение о блокировке. Нажмите «Да» для снятия блокировки (при входе произошла блокировка сеанса в соответствии с настройками задания, но, поскольку вход выполняется под Администратором, появляется окно для снятия блокировки). Запустите regedit. Раскройте узел HKLM\SOFTWARE\TEST (рисунок 241).

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не
test1	REG_DWORD	0x00000001 (1
test2	REG_DWORD	0x00000002 (2

Рисунок 241 – Узел «HKLM\SOFTWARE\TEST»

Значение параметра test1 было восстановлено, переименованный параметр test22 остался, и добавился новый параметр test2. В настройках задания был указан метод контроля «Полное совпадение» и действие «Восстановить с блокировкой». При методе контроля «Полное совпадение» создается копия контролируемых ресурсов целостности, поэтому значение параметра test1 было восстановлено. Поскольку параметр test2 был переименован, то при выполнении задания он не был обнаружен и восстановлен из копии (поэтому при использовании метода контроля «Полное совпадение» не рекомендуется устанавливать расписание «При входе» при контроле файлов большого размера, поскольку это может вызвать задержки входа). Удалите все параметры в ключе TEST (рисунок 242).

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение н
test1	REG_DWORD	0x00000001
test2	REG_DWORD	0x00000002
Изменить...		
Изменить двоичные данные...		

Рисунок 242 – Удаление параметров в ключе «TEST»

Завершите сеанс Администратора. Снова войдите под учетной записью Администратора. Снимите блокировку, запустите regedit. Раскройте узел HKLM\SOFTWARE\TEST. Значения параметров будут восстановлены.

Запустите «Локальный центр управления», загрузите журнал тревог, просмотрите описание событий задания контроля реестра.

Запустите программу «Контроль программ и данных (централизованный режим)». В структуре управления выберите субъект управления SecretNetICheshDefault. Нажмите правой кнопкой мыши на задании «Исключить из» - «Субъекта» (рисунок 243) и нажмите «Да» в окне подтверждения.

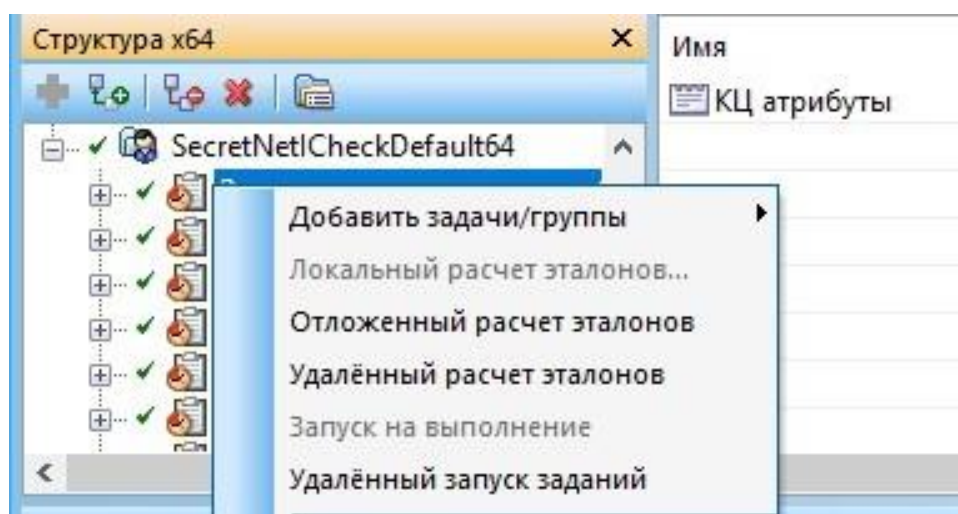


Рисунок 243 – Исключение субъекта

Исключите из структуры субъекта также задания контроля прав, реестра и существования (созданные при выполнении практической работы), кроме контроля содержимого. Сохраните изменения в модели. Закройте окно программы «Контроль программ и данных (централизованный режим)».

Завершите сеанс Администратора.

7.12 Настройка механизма замкнутой программной среды

Для настройки механизмов контроля целостности и замкнутой программной среды предназначена программа «Контроль программ и данных».

Для работы с программой предусмотрены следующие режимы:

- локальный режим работы — используется для редактирования локальной модели данных на компьютере;

– централизованный режим работы — используется для редактирования централизованной модели данных с описаниями объектов, контролируемых на защищаемых компьютерах. Централизованная модель данных применяется на клиентах в сетевом режиме функционирования совместно с локальными моделями, если они заданы. При этом приоритет имеют параметры централизованной модели.

При централизованном управлении, если в системе присутствуют компьютеры с версиями ОС различной разрядности, формируются две модели данных — для компьютеров с 32-разрядными ОС и для компьютеров с 64-разрядными ОС. Администратор с помощью программы может редактировать только одну централизованную модель данных, разрядность которой совпадает с разрядностью версии ОС Windows компьютера администратора. Поэтому при необходимости редактирования централизованной модели другой разрядности администратору следует использовать компьютер с версией ОС той же разрядности.

В соответствии с Унифицированными конфигурациями, настройка ЗПС требуется только на некоторых серверах, поэтому настройка параметров КЦ и ЗПС будет выполняться на виртуальной машине SNS-Client. В централизованном режиме при изменении модели данных выполняется синхронизация локальной базы и базы сервера, что может занять продолжительное время, поэтому в практической работе механизм ЗПС будет рассматриваться только локально.

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью Администратора. Запустите программу «Контроль программ и данных» (Пуск – Код безопасности – Контроль программ и данных).

После ввода PIN запустится окно программы. В поле «Субъекты управления» отображается только локальный компьютер (рисунок 244).

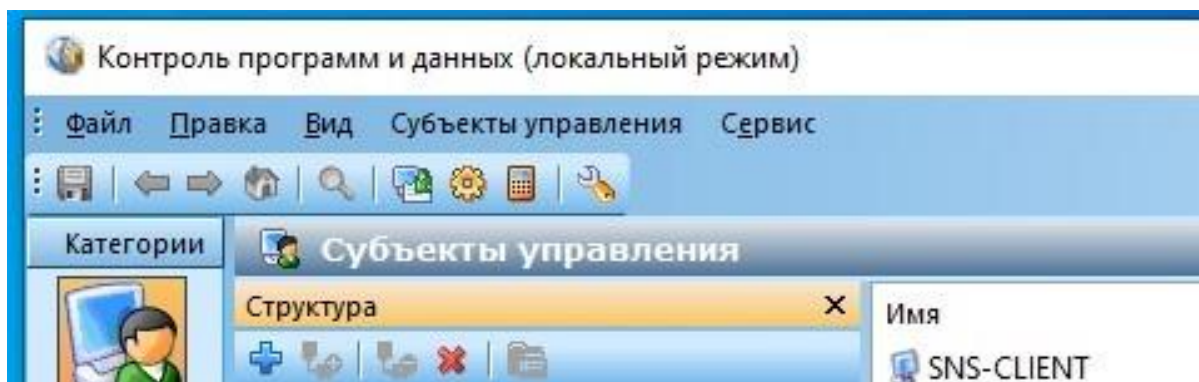


Рисунок 244 – Программа «Контроль программ и данных (локальный режим)»

Выберите в окне «Субъекты управления» субъект управления SNS_CLIENT. В правой части окна отобразятся задания, назначенные этому субъекту управления, созданные автоматически при установке СЗИ от НСД, а также задание для контроля содержимого, созданное ранее централизованно, причем настройки задания недоступны для изменения. С строке меню выберите пункт «Сервис» - «Настройки» (или нажмите клавишу F9) (рисунок 245).

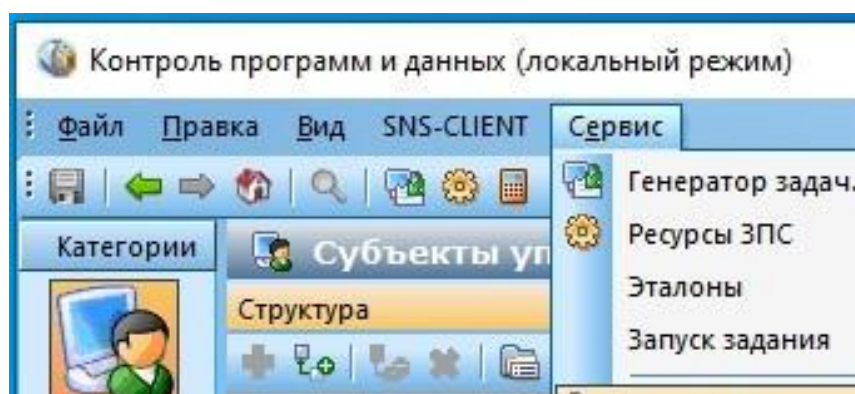


Рисунок 245 – Настройки

В окне «Настройки приложения» раскройте узел «Инструментарий» и выберите пункт «Подготовка для ЗПС», в правой части окна выберите «Расширения выполняемых», поставьте курсор в строку «Значения» и в конец строки допишите «.ovl» (рисунок 246). Нажмите кнопку «ОК».

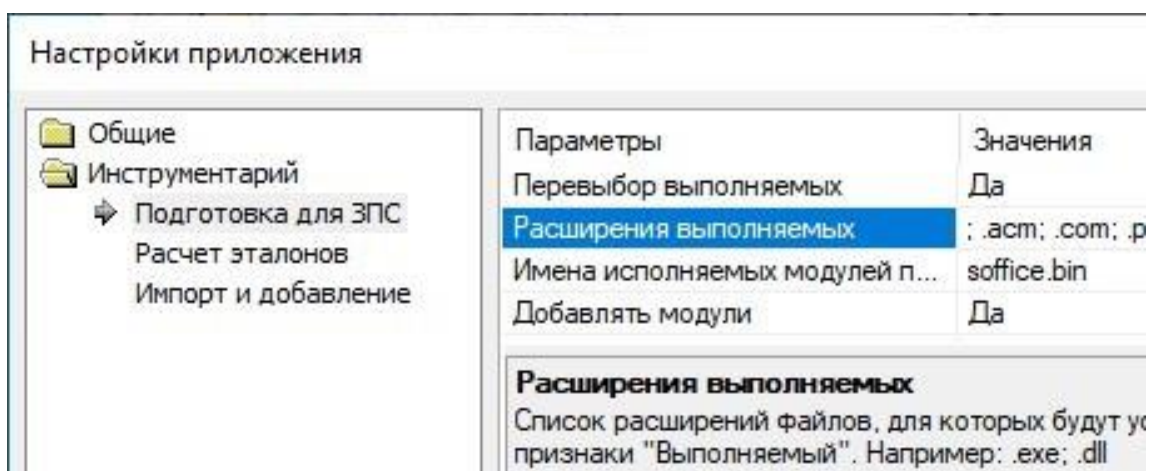


Рисунок 246 – Настройки приложения

7.13 Формирование замкнутой программной среды

В соответствии с документацией рекомендуется выполнить подготовку к построению ЗПС. Подготовка должна включать следующие действия:

- сбор сведений о защищаемых компьютерах (установленное ПО, пользователи и их функциональные обязанности);
- формирование перечня ресурсов, подлежащих контролю целостности;
- формирование перечня программ, с которыми разрешено работать разным группам пользователей.

Из числа компьютеров с установленным клиентом в сетевом режиме функционирования выделяются группы с полным совпадением, частичным совпадением и с уникальной конфигурацией ПО и данных. Осуществляется подготовка рабочего места администратора для проведения настройки. На рабочем месте необходимо установить все программное обеспечение, описание ресурсов которого предполагается выполнять автоматическими средствами добавления задач в модель данных.

Рекомендуемый порядок настройки модели данных в части ЗПС включает следующие действия:

- 1) формирование новой модели данных с настройкой контроля по умолчанию;
- 2) добавление в модель данных дополнительных объектов, таких как задачи для использования в ЗПС и задания ЗПС. Для формирования задач и

заданий ЗПС можно использовать метод накопления сведений о действиях пользователей во время работы. Данный метод предусматривает использование мягкого режима работы механизма и получение информации о запуске программ из журнала Secret Net Studio;

- 3) установление связей заданий ЗПС с субъектами;
- 4) определение списка ресурсов для контроля;
- 5) включение режима изоляции процессов;
- 6) создание эталонов контролируемых ресурсов;
- 7) предоставление привилегии для пользователей, при работе которых не должны действовать ограничения ЗПС;
- 8) включение жесткого режима работы механизма ЗПС.

В Унифицированных конфигурациях содержатся описания моделей замкнутой программной среды для различных разрядностей и версий операционных систем и программного обеспечения, применяемого в ТУ. В рамках практической работы будет рассмотрен общий порядок формирования модели данных.

В практической работе новая модель данных создаваться не будет, а будет использоваться модель данных, созданная при установке клиентской части СЗИ Secret Net Studio на защищаемый компьютер. Поэтому настройка ЗПС начинается с создания задач ЗПС. Для этого могут быть использованы как ручные методы, так и механизм генерации задач. Задачи создаются на основании сведений об установленных на компьютере программных продуктах. Для этого используются сведения MS Installer и ярлыки меню «Пуск» ОС Windows. Рекомендуется использовать механизм генерации при наполнении модели данных сложными задачами, включающими в себя большое количество ресурсов. С помощью генератора задач создадим задачу, позволяющую запускать программы, входящие в состав пакета MS Office. В левой части окна «Контроль программ и данных» выберите категорию «Задачи». В строке меню выберите раздел «Задачи», в списке выберите действие «Создать задачу» - «Через генератор задач» (рисунок 247).

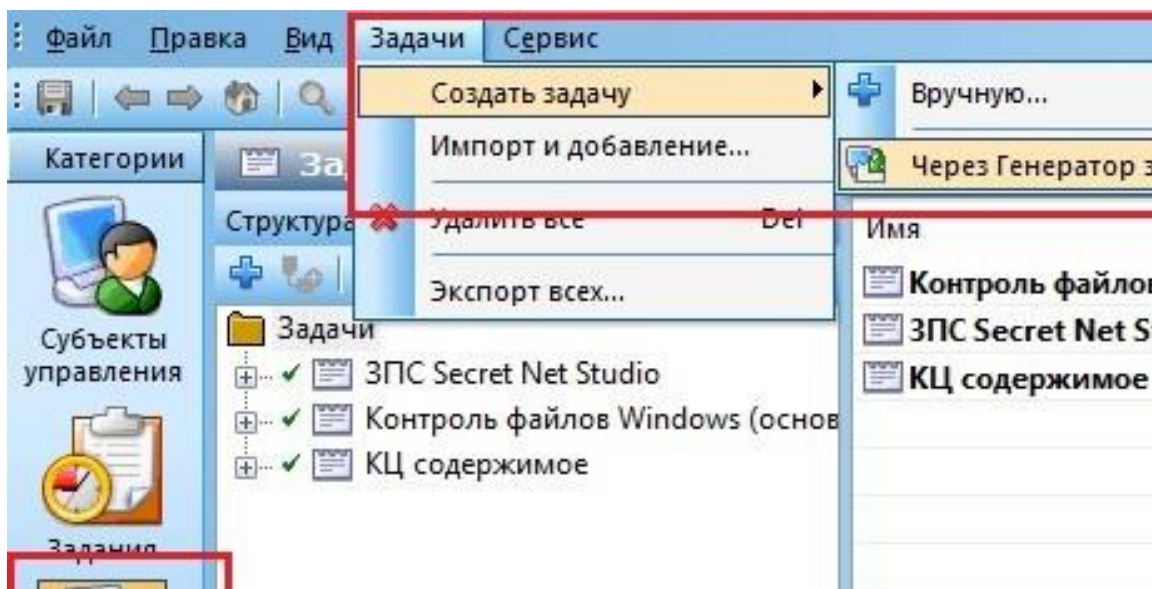


Рисунок 247 – Создание задачи через генератор задач

На экране появится диалоговое окно генератора задач по установленным программам. В списке «Поиск по:» должно быть установлено значение «ярлыкам из меню «Пуск» (ЗПС)». В списке ниже выберите строки «Excel» и «Word» (табличный и текстовый процессор из всего состава офисного пакета) (рисунок 248). В этом задании ЗПС будет разрешен только запуск этих двух компонентов. Дополнительные параметры оставьте без изменений и нажмите кнопку ОК.

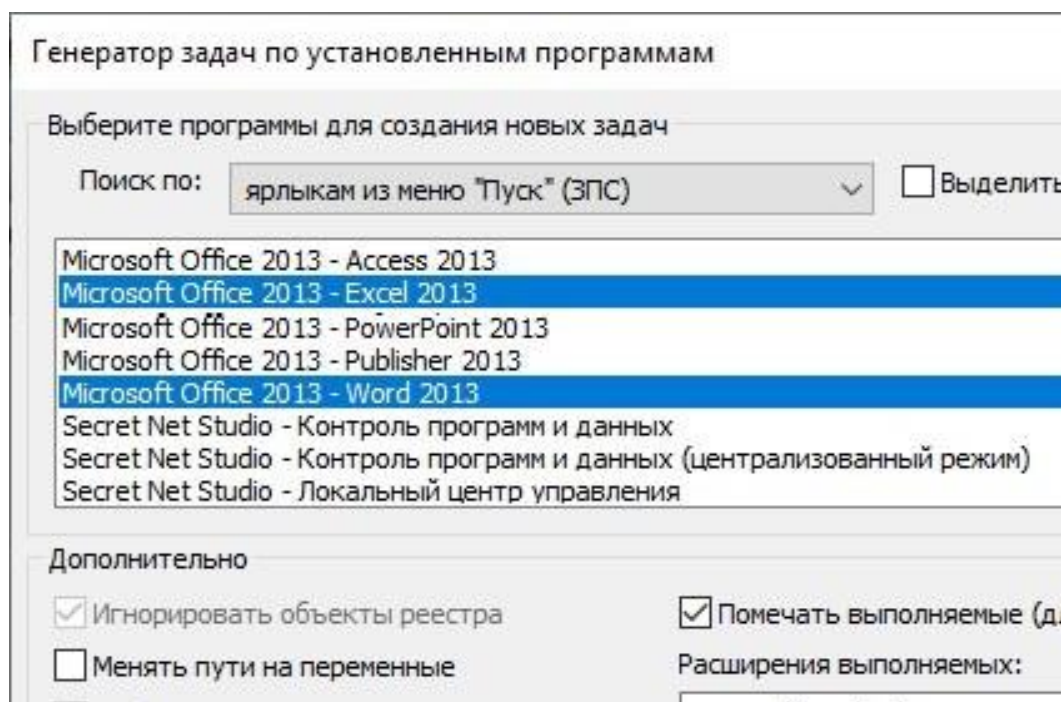


Рисунок 248 – Диалоговое окно генератора задач по установленным программам

Будет запущен процесс поиска установленных программ и добавления задач, который может занять некоторое время. После завершения процесса формирования задачи будет выдано сообщение с указанием затраченного времени (рисунок 249). Нажмите кнопку «ОК».

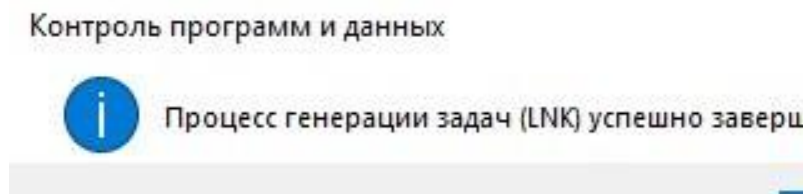


Рисунок 249 – Генерация задач успешно завершена

В списке задач появятся созданные задачи «...Excel 2013» и «...Word 2013». В правой части окна программы «Контроль программ и данных» в столбце «Описание» указано, что задачи сгенерированы по информации об установленных программах. В столбце «Принадлежность» указана цифра «0». Это означает, что задача не принадлежит ни одному заданию ЗПС, на это же указывает пиктограмма в виде красно-белого полукруга рядом с названием задачи в окне структуры. В столбце «Содержит» указана цифра «1», это означает, что в задачу включена группа ресурсов. Раскройте содержимое структуры задачи, нажав кнопку «+» в окне структуры рядом с названием задачи (рисунок 250).

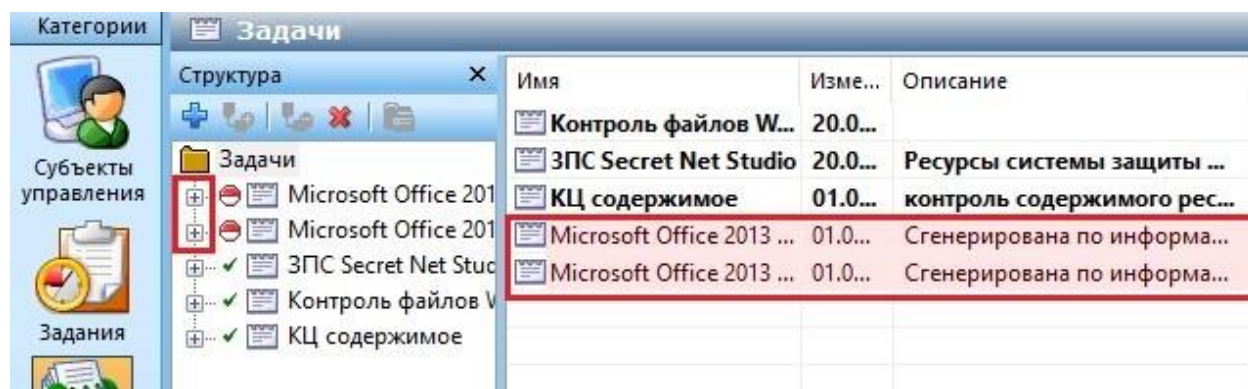


Рисунок 250 –Информация о задачах

Выберите в структуре задачи «Excel 2013» группу ресурсов, включенных в эту задачу. В правой части окна отобразится группа ресурсов, включенная в это задание (рисунок 251). Первым в списке группы ресурсов будет размещен исполняемый файл с расширением «.exe», соответствующий исполняемому

файлу программы, размещенный в каталоге установленного программного обеспечения. Далее в списке содержатся динамически подключаемые библиотеки, необходимые для работы приложения, определенные при формировании задачи. Просмотрите также группу ресурсов задачи «Word 2013». Структура группы ресурсов будет аналогичная.

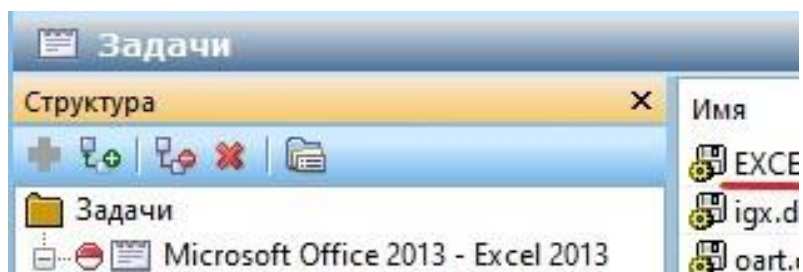


Рисунок 251 – Структура задачи «Excel 2013»

При формировании задания была автоматически сформирована модель данных, касающаяся определения ресурсов, входящих в задачу. Выберите категорию «Ресурсы» и просмотрите структуру ресурсов, включенных в задачу (рисунок 252).

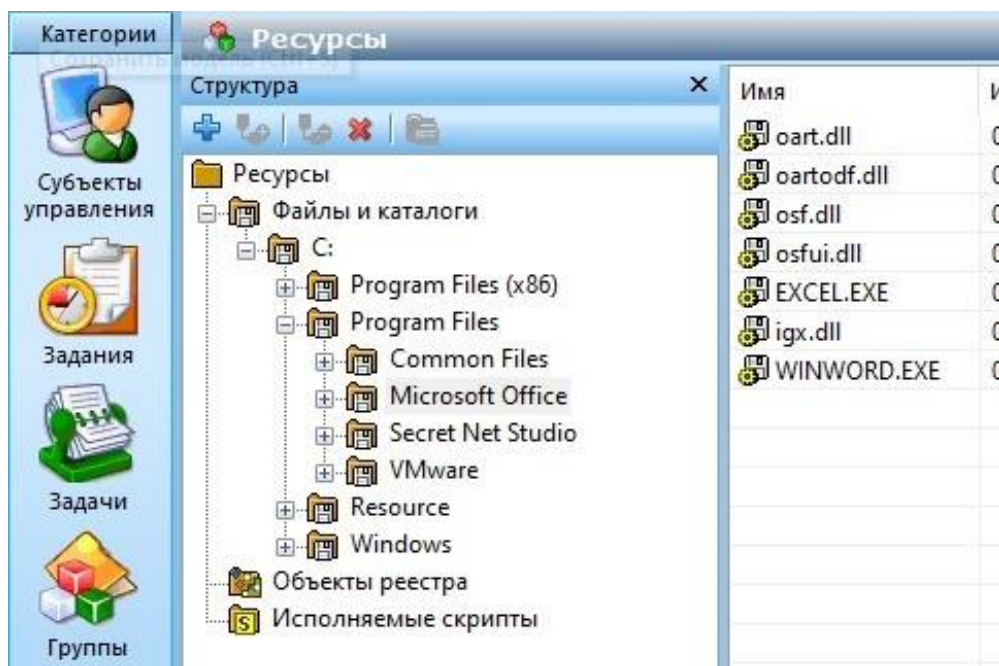


Рисунок 252 – Структура ресурсов

Далее выполните подготовку заданий.

Перейдите к категории «Задания», в структуре заданий выберите узел «Задания» и нажмите кнопку «Добавить новый» с изображением «+» (или нажмите клавишу Insert) (рисунок 253).

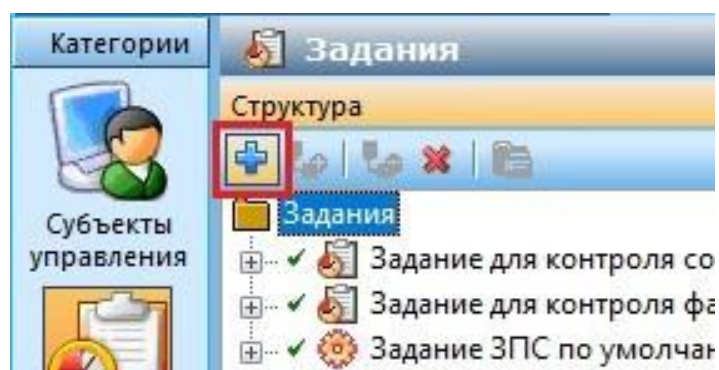


Рисунок 253 – Создание нового задания

В окне «Создание нового задания» установите переключатель в положение «Замкнутая программная среда» и нажмите кнопку «ОК» (рисунок 254).

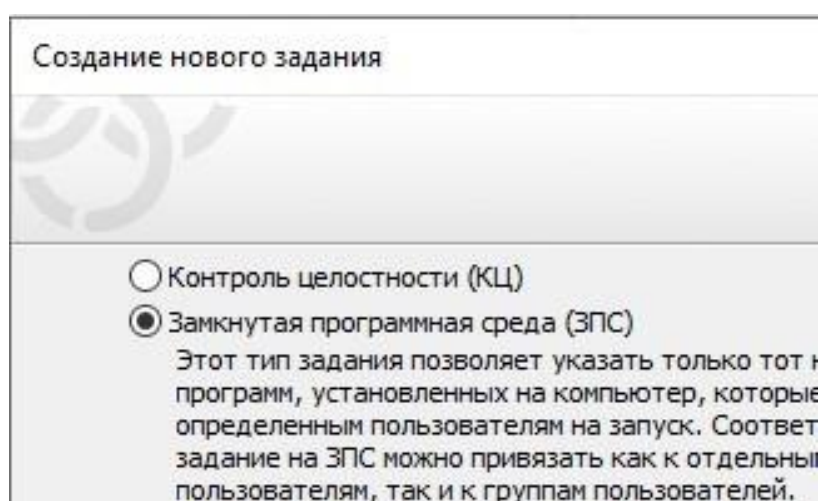


Рисунок 254 – Создание нового задания с типом «ЗПС»

В следующем окне введите название создаваемого задания и нажмите «ОК» (рисунок 255).

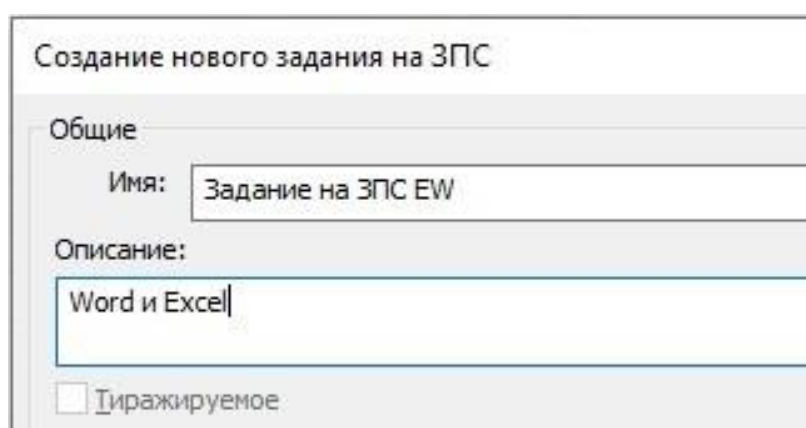


Рисунок 255 – Название и описание задания для Word и Excel

В списке заданий появится новое задание без подчиненных объектов (восклицательный знак) и не назначенное ни одному субъекту (рисунок 256).

Пиктограмма в виде шестеренки указывает на тип задания замкнутой программной среды.

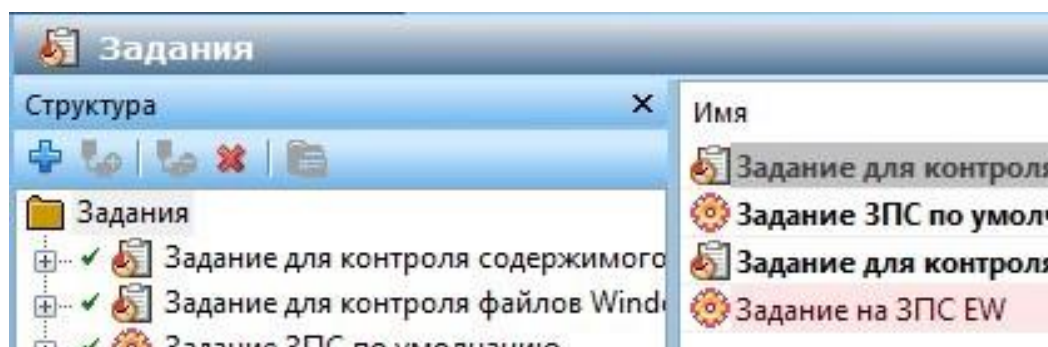


Рисунок 256 – Список заданий

Создайте еще одно задание замкнутой программной среды только для Word (рисунок 257).

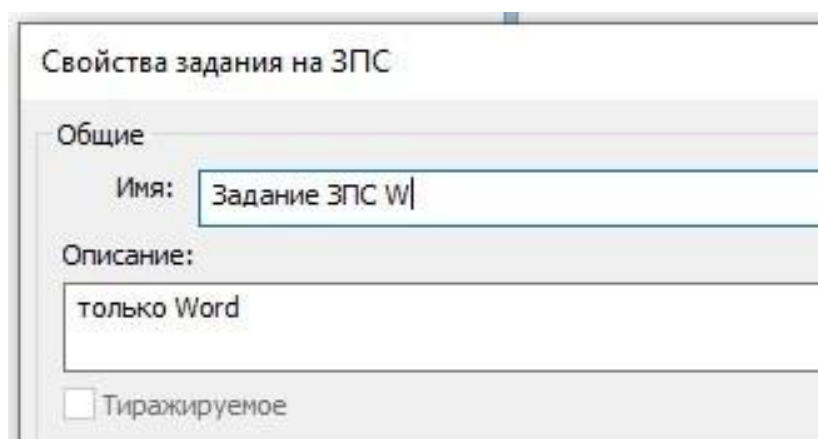


Рисунок 257 – Название и описание задания для Word

После добавления заданий необходимо добавить задачи в задания. Выберите задание ЗПС для Word, в контекстном меню выберите пункт «Добавить задачи/группы» - «Существующие» (рисунок 258).

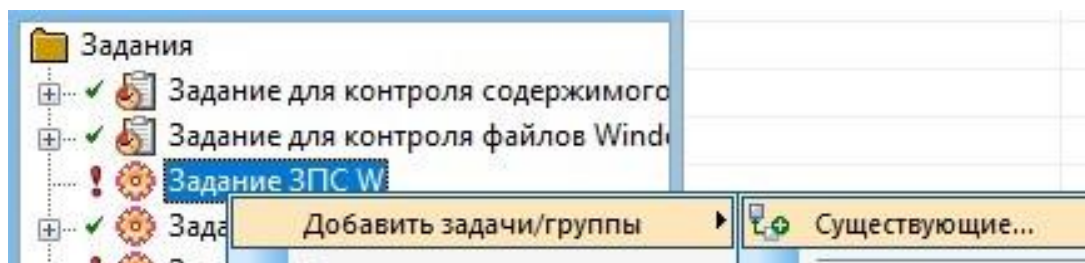


Рисунок 258 – Добавление задачи в задания

В окне выбора подчиненных объектов выберите задачу «...Word 2013» не принадлежащие ни одному заданию (рисунок 259). Нажмите кнопку «ОК».

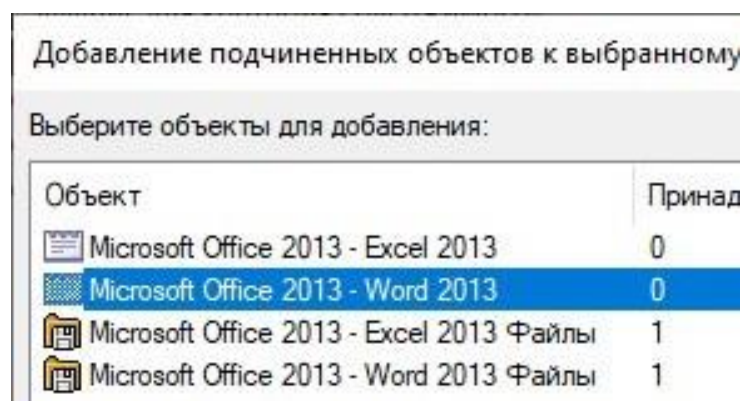


Рисунок 259 – Добавление подчиненных объектов

Пиктограмма задания в структуре заданий изменит вид, в списке задач появятся выбранные задачи, содержащие ресурсы, с указанием принадлежности заданию (рисунок 260).

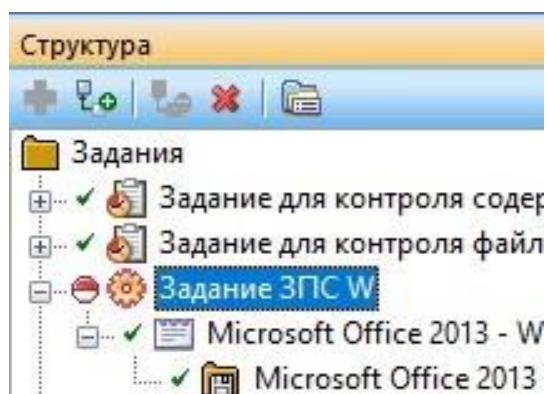


Рисунок 260 – Задание в структуре «Задания»

Выберите задание ЗПС для Word и Excel, добавьте в него обе задачи MS Office (рисунок 261).

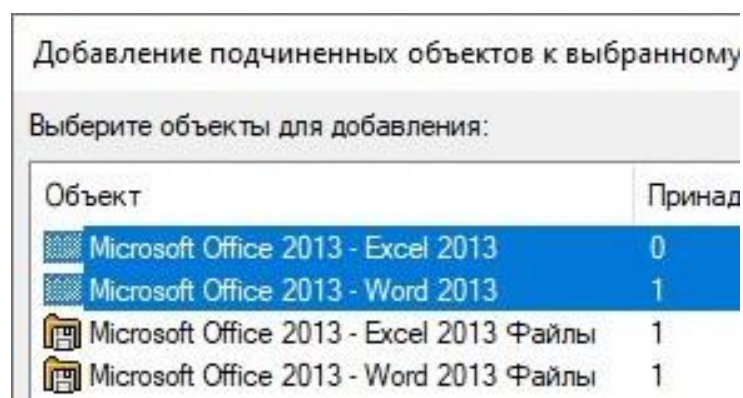


Рисунок 261 – Добавление задач

После формирования заданий, необходимо назначить их субъектам. При локальной настройке задания ЗПС назначаются пользователям и группам

пользователей защищаемого компьютера. При настройке в централизованном режиме задания можно назначить компьютерам или группам компьютеров.

Перейдите в категорию «Субъекты управления». Выберите субъект SNS-CLIENT, в контекстном меню выберите «Добавить задания» - «Существующие» (рисунок 262).

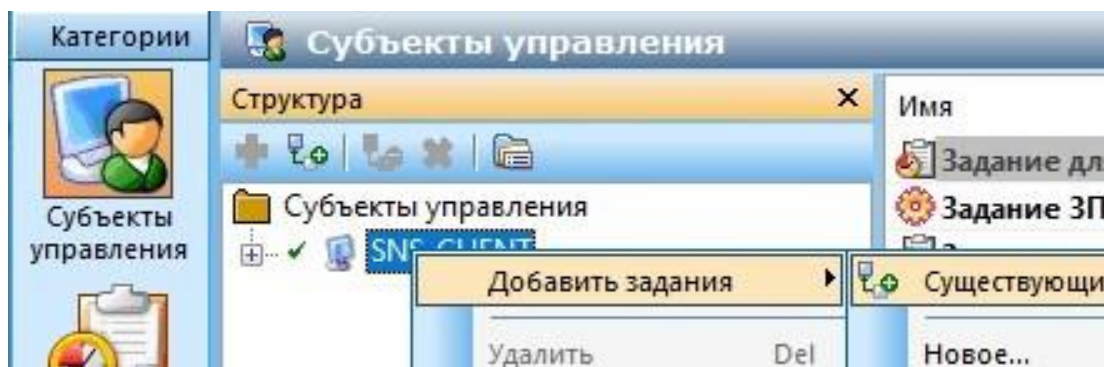


Рисунок 262 – Добавление существующего задания

В окне добавления объектов выберите задания «Задание ЗПС Word» (рисунок 263). Нажмите «ОК».

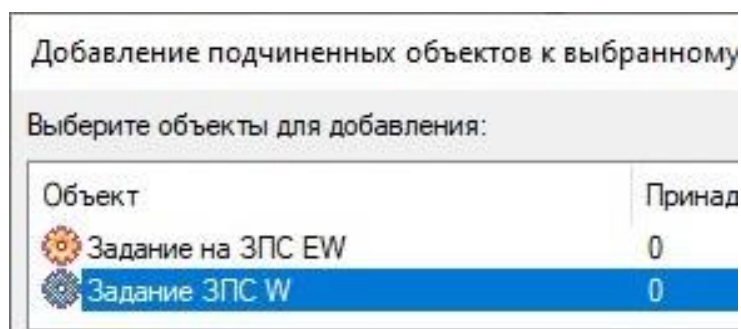


Рисунок 263 – Добавление задания «Задание ЗПС Word»

В структуре субъекта управления добавится задание. Раскройте структуру задания – все элементы структуры обозначены пиктограммой в виде зеленой галки, что означает наличие необходимых связей в модели данных (рисунок 264).

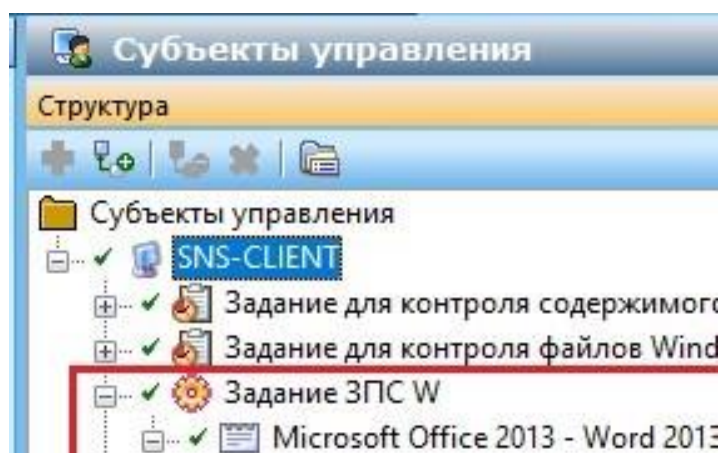


Рисунок 264 – Структура «Субъект управления»

После формирования модели данных необходимо включить использование режима замкнутой программной среды. Для работы ЗПС предусмотрены два режима работы: мягкий и жесткий. Мягкий режим нужен для настройки механизма, жесткий – это основной штатный режим работы. В мягком режиме пользователю разрешается запускать любые программы. Если при этом пользователь запускает программы, не входящие в перечень разрешенных, в журнале Secret Net Studio регистрируются соответствующие события тревоги. В жестком режиме разрешается запуск только тех программ, которые входят в список разрешенных. Запуск других программ блокируется, а в журнале Secret Net Studio регистрируются события тревоги.

Мягкий режим нужен для того, чтобы, не влияя на работу пользователей, накопить сведения в журнале о возможных ошибках, допущенных при настройке механизма ЗПС, и в последующем их устранить.

Включение механизма замкнутой программной среды осуществляется в свойствах субъекта управления. Выберите субъект SNS-CLIENT, в контекстном меню выберите пункт «Свойства» (рисунок 265).

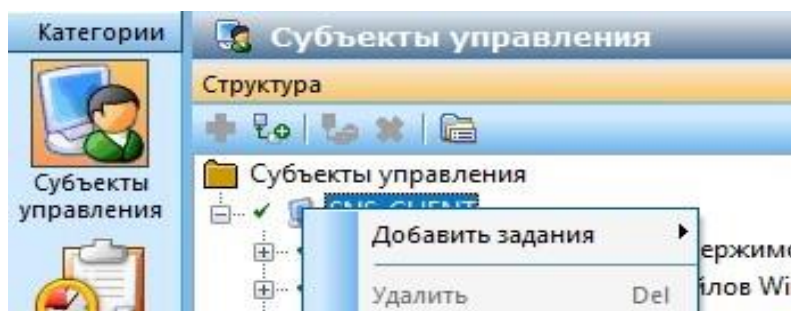


Рисунок 265 – Включение механизма замкнутой программной среды

В окне свойств субъекта установите флаги (рисунок 266):

- режим ЗПС включен;
- мягкий режим.

Нажмите кнопку «ОК».

В соответствии с Унифицированными конфигурациями должны быть также установлены флаги «Режимы заданы централизованно», «Проверять целостность модулей перед запуском» и «Проверять заголовки модулей перед запуском», однако эти флаги устанавливать не надо.

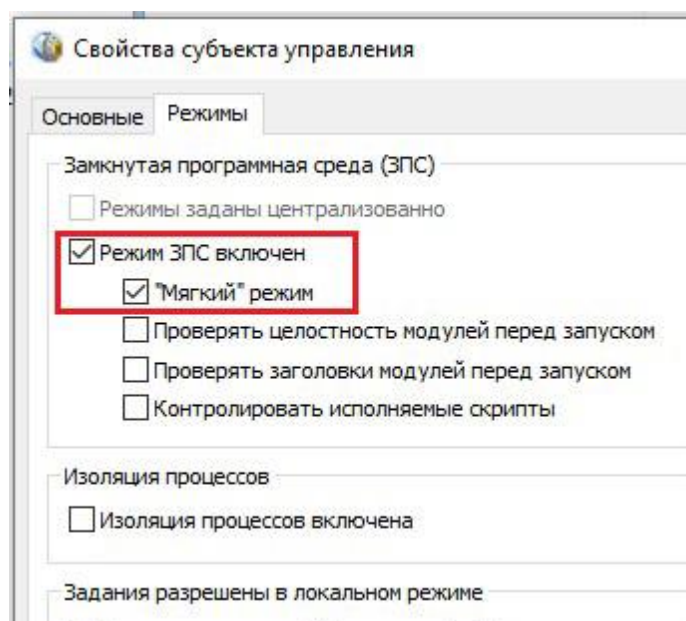


Рисунок 266 – Установка флагов в свойствах

Сохраните изменения в модели данных, нажав на кнопку «Сохранить» в панели инструментов программы «Контроль программ и данных» (рисунок 267).

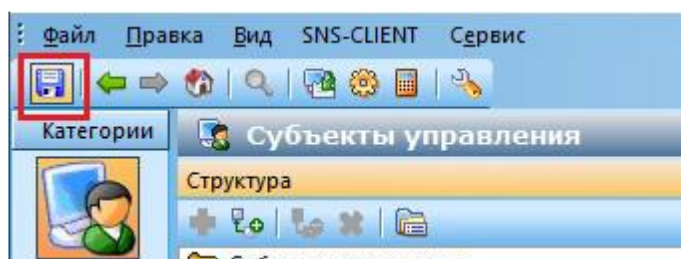


Рисунок 267 – Сохранение модели данных

Завершите сеанс Администратора.

Переключитесь к окну виртуальной машины SNS-Server. Войдите под учетной записью Администратора. Запустите программу «Центр управления».

На вкладке «Компьютеры» переключитесь к отображению структуры в виде таблицы. Выберите компьютер SNS-Client, нажмите правой кнопкой и в контекстном меню выберите «Журналы» - «Собрать журналы с компьютера» - «Secret Net Studio» (рисунок 268). Журнал компьютера SNS-Client будет очищен.

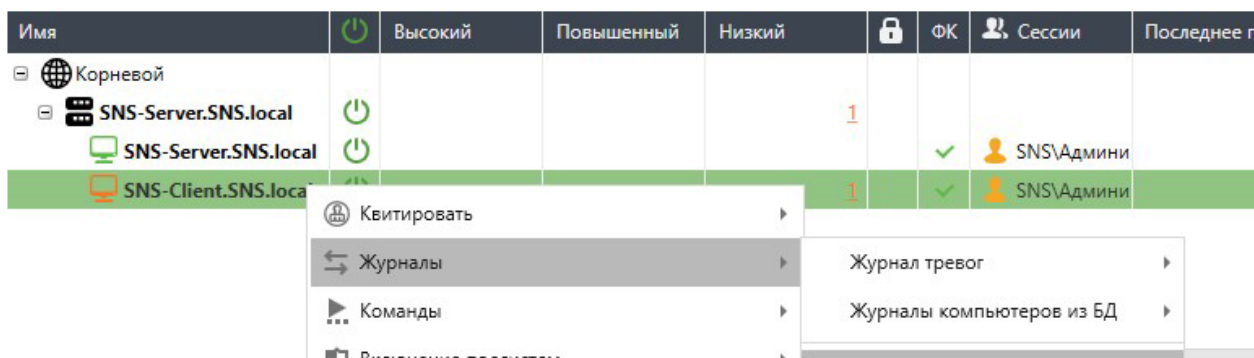


Рисунок 268 – Сборка журнала «Secret Net Studio» с компьютера

Переключитесь к окну виртуальной машины SNS-Client. Зарегистрируйтесь под учетной записью user3. Запустите программу MS Word (рисунок 269). Программа запустится. Закройте окно программы.

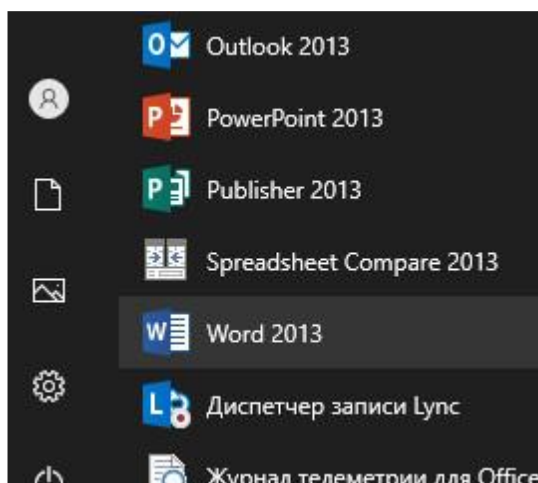


Рисунок 269 – Запуск MS Word

Запустите программу SumatraPDF (на диске C:/). Запуск программы также будет разрешен, поскольку включен мягкий режим работы замкнутой программной среды. Закройте программу и завершите сеанс пользователя user3.

Переключитесь к окну виртуальной машины SNS-Server. В программе «Центр управления» перейдите к панели «Статистика», на ней появится информация о тревогах. Нажмите на ссылку «В журнал» в виджете тревог низкого уровня (рисунок 270).



Рисунок 270 – Виджет тревог низкого уровня

Откроется журнал тревог, в котором будут события, связанные с запретом запуска программ и загрузки динамических библиотек (рисунок 271).

СОБЫТИЯ		УГРОЗЫ					
⚙	Дата ▼	Событие	Категор...	Источник	Комп...	Домен	👤
🔒	28.02.2023...	Запрет зап...	Замкнутая...	LocalProtec...	SNS-Client.S...	SNS	usi
🔒	28.02.2023...	Запрет зап...	Замкнутая...	LocalProtec...	SNS-Client.S...	SNS	usi

Рисунок 271 – Журнал тревог

Вернитесь к окну виртуальной машины SNS-Client, войдите под учетной записью Администратора.

Запустите программу «Контроль программ и данных». В категории «Задания» создайте новое задание для замкнутой программной среды. Введите название и описание задания (рисунок 272), нажмите кнопку «ОК».

Создание нового задания на ЗПС

Общие

Имя:

Описание:

☐ Тиражируемое

Рисунок 272 – Создание задания для замкнутой программной среды

Нажмите правой кнопкой мыши на созданном задании, в контекстном меню выберите «Добавить задачи/группы» - «Новую группу по журналу» (рисунок 273).

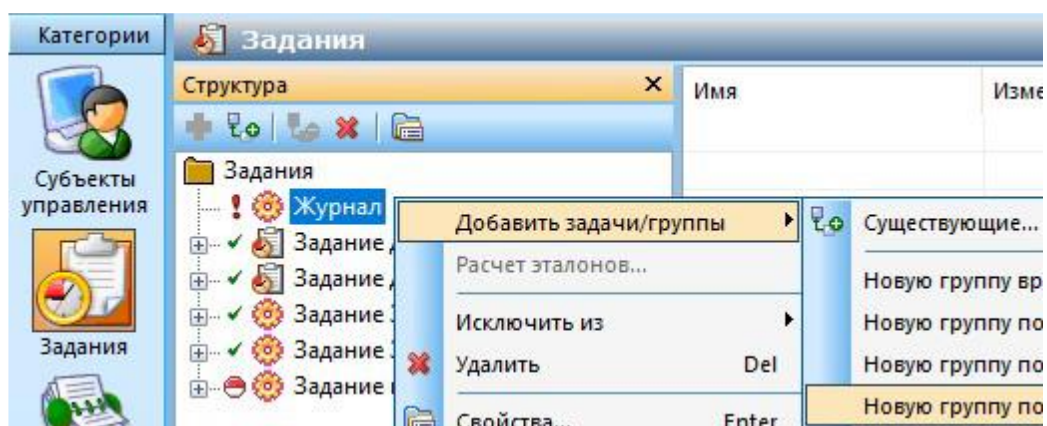


Рисунок 273 – Создание новой группы по журналу

В окне «Создание новой группы по журналу» должен быть установлен переключатель в положение «Загружаемые модули» (рисунок 274). Нажмите кнопку «ОК».

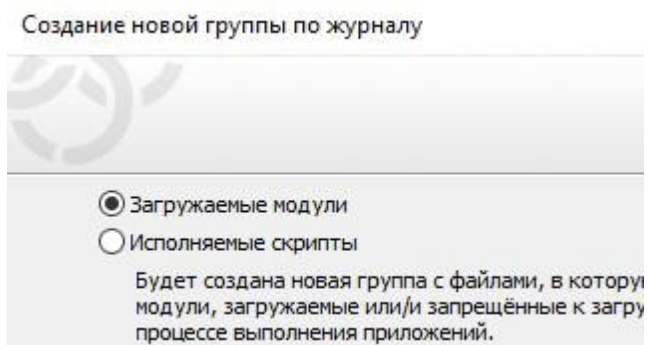


Рисунок 274 – Создание группы по журналу

В окне создания группы в списке «Способ:» выберите «Из журнала Secret Net Studio» (рисунок 275) и нажмите «ОК».

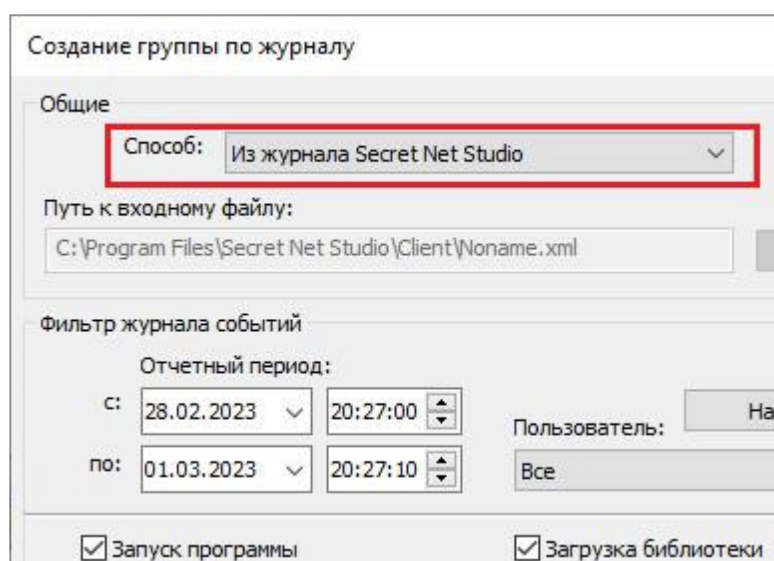


Рисунок 275 – Выбор способа «Из журнала Secret Net Studio»

После завершения процесса создания группы будет выведено сообщение с количеством добавленных объектов (рисунок 276). Нажмите «ОК». Просмотрите структуру созданного задания.

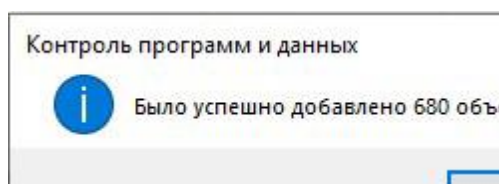


Рисунок 276 – Добавление новых объектов

Назначьте задание субъекту SNS-CLIENT. Сохраните изменения в модели.

Завершите сеанс Администратора и войдите под учетной записью user3. Запустите программу SumatraPDF. Закройте все программы и завершите сеанс пользователя.

Переключитесь к окну виртуальной машины SNS-Server, в «Центре управления» перейдите к панели «Статистика», обновите содержимое панели. Новых тревог не появится, поскольку программы и модули, запуск которых приводил к появлению тревог, теперь включены в модель ЗПС.

Мягкий режим работы ЗПС предназначен для настройки подсистемы. После завершения настройки необходимо его выключить.

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью Администратора. Запустите программу «Контроль программ и данных». Выберите категорию «Субъекты управления», откройте окно свойств субъекта SNS-CLIENT и перейдите на вкладку «Режимы». Снимите флаг «Мягкий режим» и нажмите кнопку «ОК» (рисунок 277). Сохраните изменения в модели.

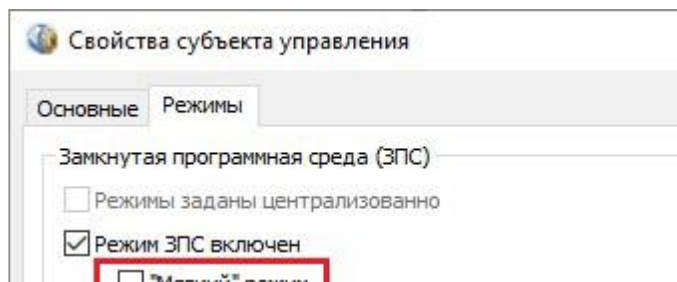


Рисунок 277 – Свойства субъекта управления

Завершите сеанс Администратора. Войдите под учетной записью user3.

Запустите программу Word. Запуск программы будет разрешен. Запустите программу SumatraPDF. Запуск также будет разрешен. Запустите программу Excel. Запуск будет запрещен (рисунок 278).

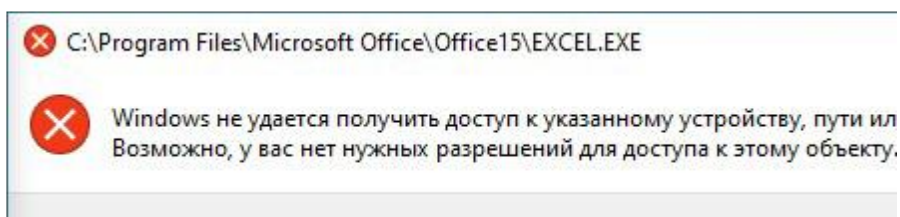


Рисунок 278 – Запуск запрещен

Завершите сеанс пользователя.

Переключитесь к окну виртуальной машины SNS-Server, в «Центре управления» перейдите к панели «Статистика», обновите содержимое панели. В виджете «Тревоги низкого уровня» нажмите на ссылку «В журнал».

В журнале тревог найдите последнее по времени событие типа «Запрет запуска». Нажмите Ctrl и D для просмотра детальной информации. В описании события будет отображено имя заблокированной программы, указан режим работы ЗПС (рисунок 279).

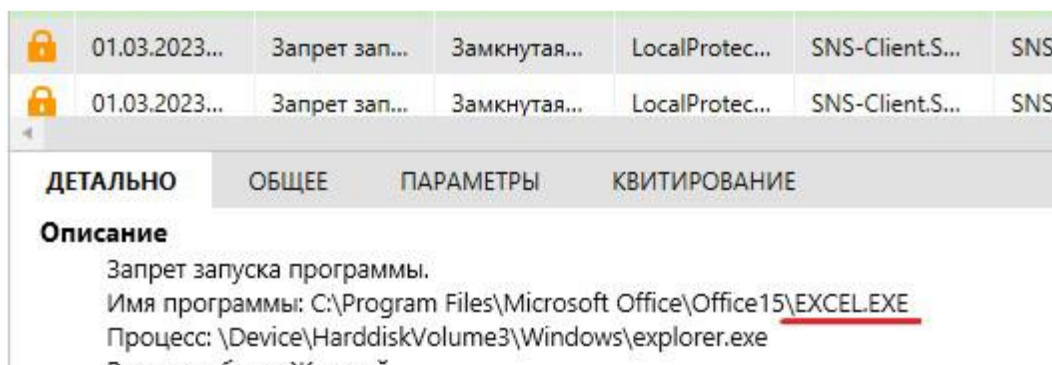


Рисунок 279 – Последнее по времени событие типа «Запрет запуска»

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью Администратора. Запустите программу «Контроль программ и данных». Выберите категорию «Субъекты управления», откройте окно свойств субъекта SNS-CLIENT и перейдите на вкладку «Режимы». Снимите флаг «Режим ЗПС включен» и нажмите «ОК» (рисунок 280). Режим отключен в рамках выполнения практической работы, т.к. основные действия, связанные с настройкой и проверкой ЗПС завершены.

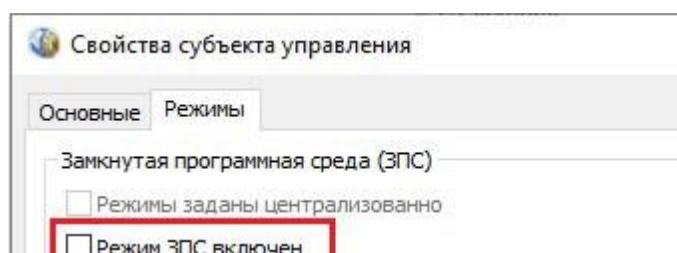


Рисунок 280 – Свойства субъекта управления

Элементы модели данных можно экспортировать и импортировать. Экспортировать и импортировать можно задания, задачи, группы ресурсов и ресурсы. Перейдите в категорию «Задания». В структуре присутствует задание «Задание ЗПС EW» с пиктограммой в виде красно-белого круга (рисунок 281). Это задание не назначено ни одному субъекту управления.

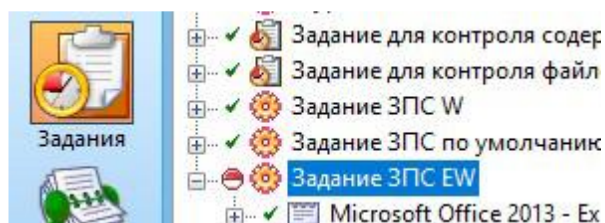


Рисунок 281 – Структура «Задания»

Рассмотрим на примере этого задания механизм экспорта/импорта заданий. Нажмите на задании правой кнопкой мыши, в контекстном меню выберите «Экспорт выбранных» (рисунок 282).

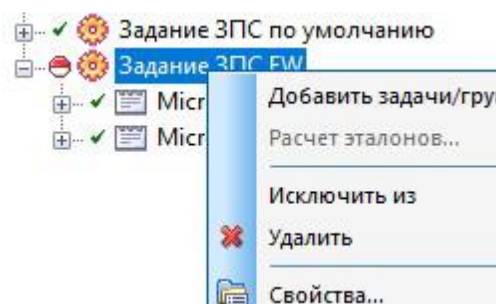


Рисунок 282 – Экспорт выбранных заданий

В окне «Экспорт выбранных объектов» нажмите кнопку «Выбрать» (рисунок 283). В окне выбора места сохранения файла введите название файла и нажмите кнопку «Сохранить». Затем нажмите кнопку «ОК» в окне экспорта. Появится сообщение об успешном экспорте выбранного объекта. Нажмите кнопку «ОК».

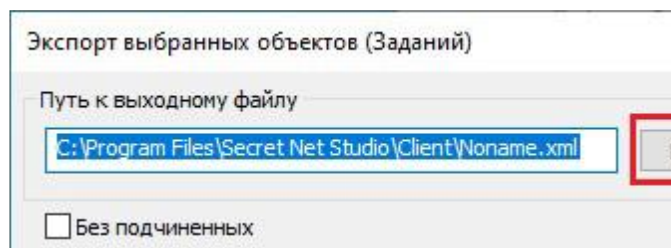


Рисунок 283 – Экспорт выбранных заданий

Выберите задание «Задание ЗПС EW», в контекстном меню задания выберите пункт «Удалить» (рисунок 284).

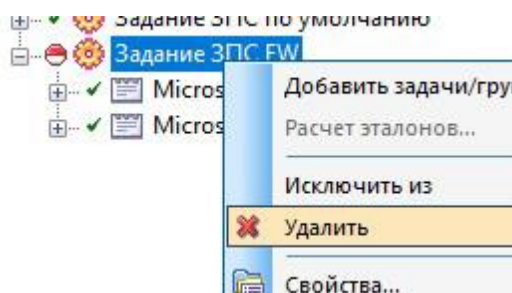


Рисунок 284 – Удаление задания

Установите флаг «Удалять подчиненные» и нажмите «Да» (рисунок 285). Задание вместе с подчиненными объектами будет удалено.

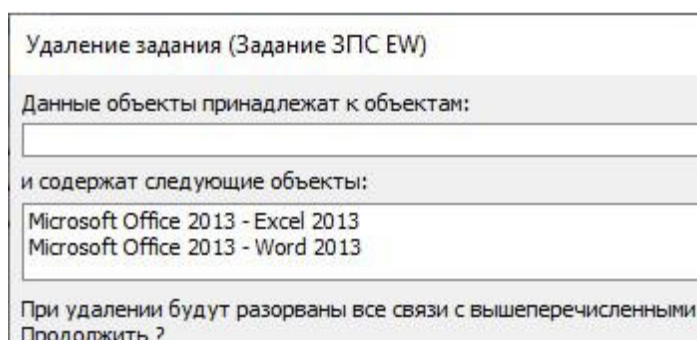


Рисунок 285 – Окно «Удаление задания (Задание ЗПС EW)»

В структуре нажмите правой кнопкой мыши на узле «Задания» и выберите пункт «Импорт и добавление» (рисунок 286).

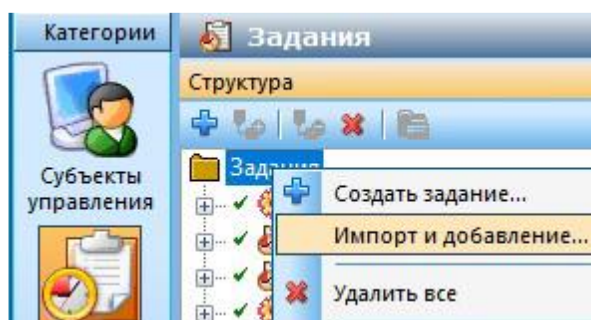


Рисунок 286 – Импорт задания

В окне импорта объектов нажмите кнопку «Выбрать», выберите экспортированный файл задачи, созданный ранее. Нажмите кнопку «Открыть» в окне выбора и кнопку «ОК» в окне импорта объектов. Появится окно с результатами импорта (рисунок 287). Нажмите «ОК».

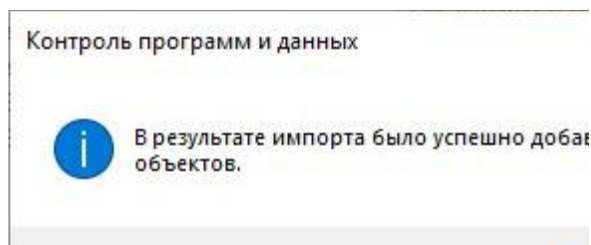


Рисунок 287 – Результат импорта

В структуре появится задание, включающее всю структуру (задачи и ресурсы) экспортированного ранее задания (рисунок 288).

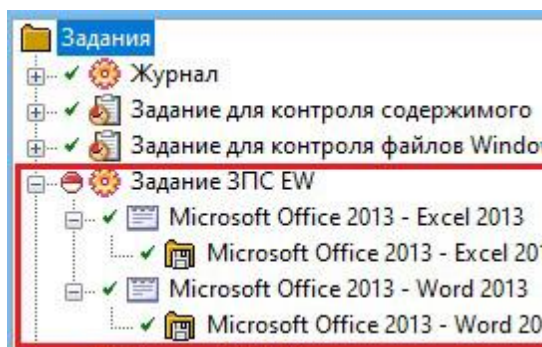


Рисунок 288 – Новое задание

Выберите субъект SNS-Client. Удалите вместе с подчиненными объектами из структуры все ранее созданные задания. Сохраните изменения в модели. Закройте окно программы.

7.14 Мониторинг в СЗИ Secret Net Studio

Мониторинг в СЗИ Secret Net Studio применяются для контроля состояния объектов управления – серверов безопасности и защищаемых компьютеров. Сведения об общем состоянии защищенности системы содержатся в панели «Статистика», которая открывается при запуске программы «Центр управления».

На компьютере SNS-Server запустите программу «Центр управления», подключитесь к серверу безопасности. Откройте панель «Статистика» (отображается по умолчанию при запуске «Центра управления»). В Центре

управления при выборе любой из панелей вверху окна отображается количество тревог, которые требуют внимания администратора (рисунок 289). В случае отсутствия тревог цвет индикатора становится зеленым.

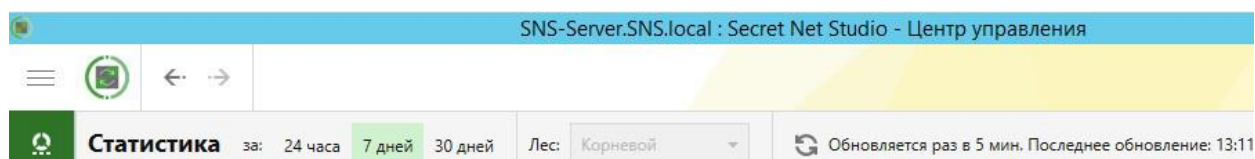


Рисунок 289 – Панель «Статистика»

Информационная панель «Статистика» состоит из виджетов. Виджетом является визуальный элемент интерфейса программы, наглядно характеризующий один системный параметр. По умолчанию на панели расположены виджеты тревог различного уровня, ошибок лицензий, функционального контроля, заблокированные компьютеры и т.п. (рисунок 290).

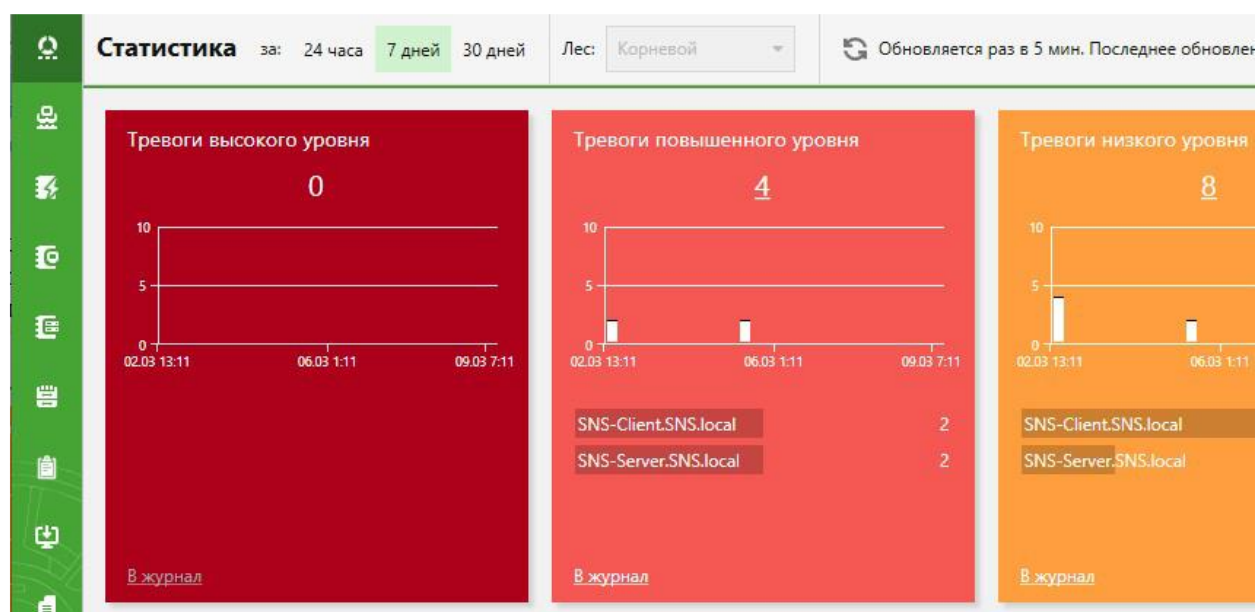


Рисунок 290 – Виджеты на панели «Статистика»

Панель статистики настраивается. Можно добавить виджеты, отображающие необходимую информацию, и удалить те, в которых нет необходимости. Нажмите на кнопку «Редактировать виджеты» с пиктограммой в виде карандаша в правом верхнем углу (рисунок 291).

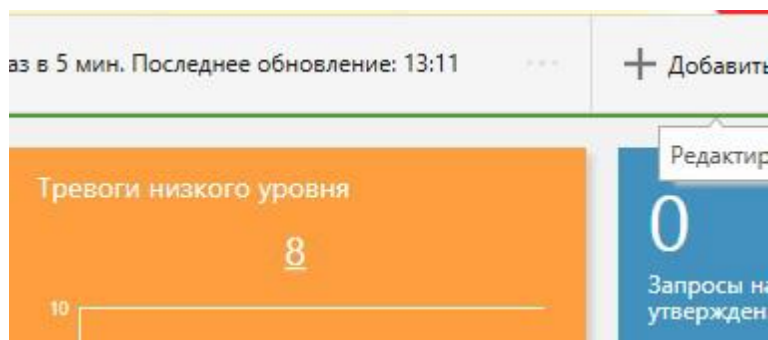


Рисунок 291 – Редактирование виджетов

Переключится внешний вид отображаемых виджетов – добавятся пиктограммы редактирования и удаления виджета. Удалим из панели статистики виджет со статистикой антивирусного средства, т.к. этот компонент системы защиты не используется. Для этого в виджете «Самые зараженные компьютеры» нажмите на кнопку «Удалить» (рисунок 292). Виджет будет удален из панели.

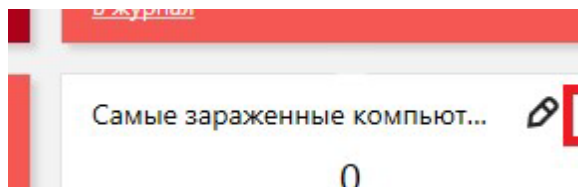


Рисунок 292 – Удаление виджета «Самые зараженные компьютеры»

Выберите виджет «Заблокированные компьютеры». Нажмите кнопку «Редактировать» (рисунок 293).

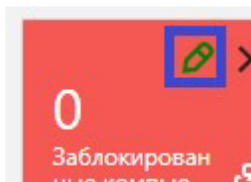


Рисунок 293 – Редактирование виджета «Заблокированные компьютеры»

Для этого виджета доступны только смена фона и названия. Введите название «Блокировки компьютеров», смените фон по желанию, нажмите кнопку «Сохранить» (рисунок 294).

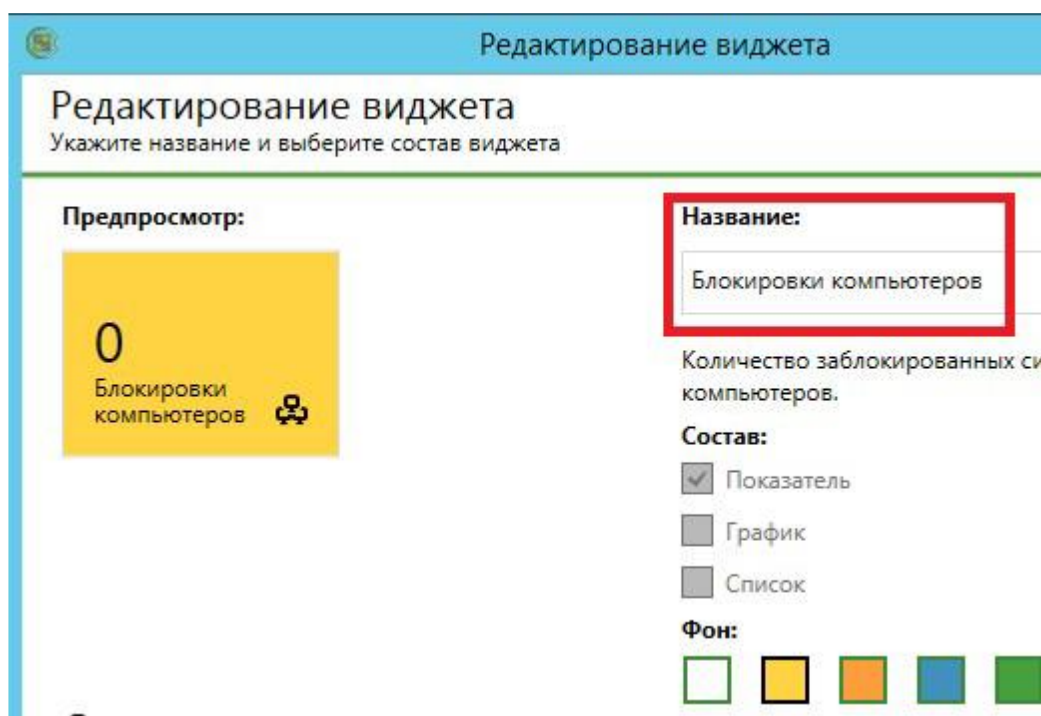


Рисунок 294 – Редактирование виджета «Заблокированные компьютеры»

Местоположение виджетов в панели изменяется перетаскиванием. Жажмите левой кнопкой мыши виджет «Запросы на утверждение АК» и переместите его в новое место. Отпустите кнопку мыши.

Для некоторых виджетов доступно три формы отображения информации: показатель, график и список. Можно выбрать один или несколько одновременных способов отображения.

Нажмите кнопку «Редактировать» в виджете «Тревоги высокого уровня». В окне редактирования виджета снимите флаги «Список» и «График» (рисунок 295). Обратите внимание на изменение размера виджета и блокировку последнего значения состава. Нажмите кнопку «Сохранить». В виджете будет отображаться только число тревог и пропадет ссылка «в журнал», которая является гиперссылкой на все зарегистрированные в соответствующем журнале события, связанные с данным системным параметром и всеми контролируруемыми объектами.

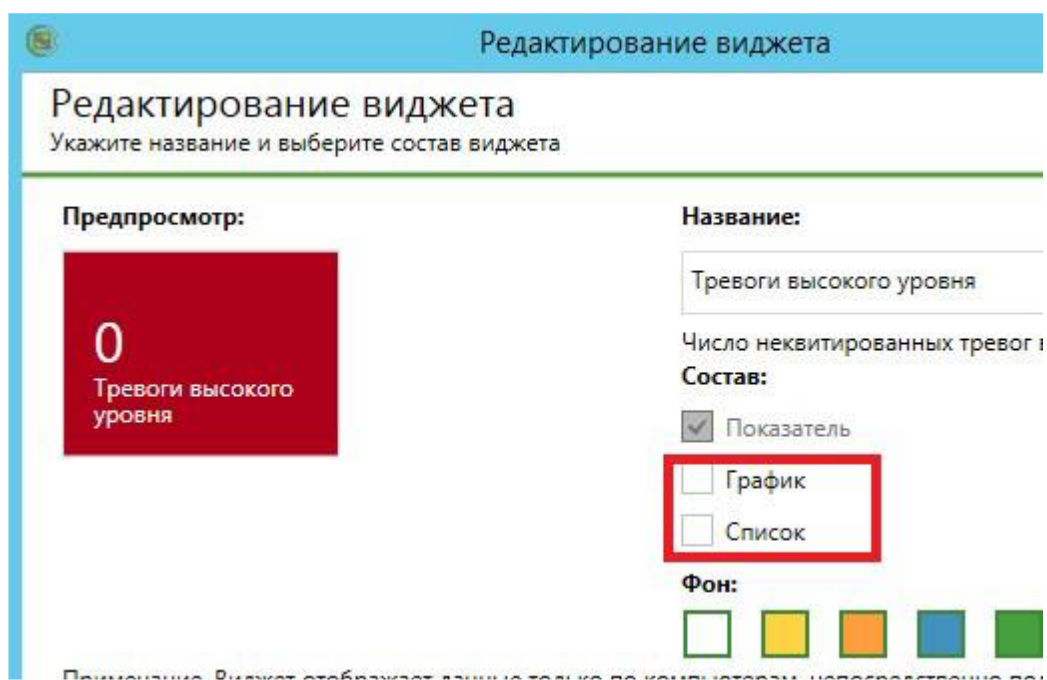


Рисунок 295 – Редактирование виджета

В соответствии с описанием процессов контроля эксплуатации в настройках виджетов необходимо отображать количество событий, поэтому значение «Показатель» надо оставлять для всех виджетов.

Для завершения редактирования отображаемых виджетов нажмите еще раз кнопку «Редактировать». Нажмите кнопку «Добавить виджет» (рисунок 296).

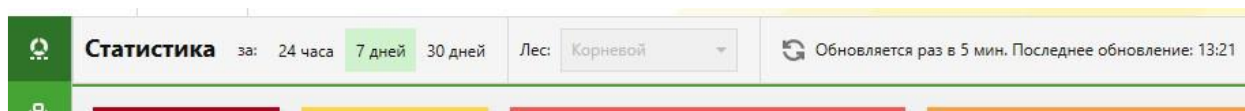


Рисунок 296 – Добавление виджета

В окне «Добавление виджета» в группе «Локальная защита» выберите «Контроль устройств». В правой части окна отобразится один возможный виджет для добавления. Нажмите кнопку «Редактировать» (рисунок 297).

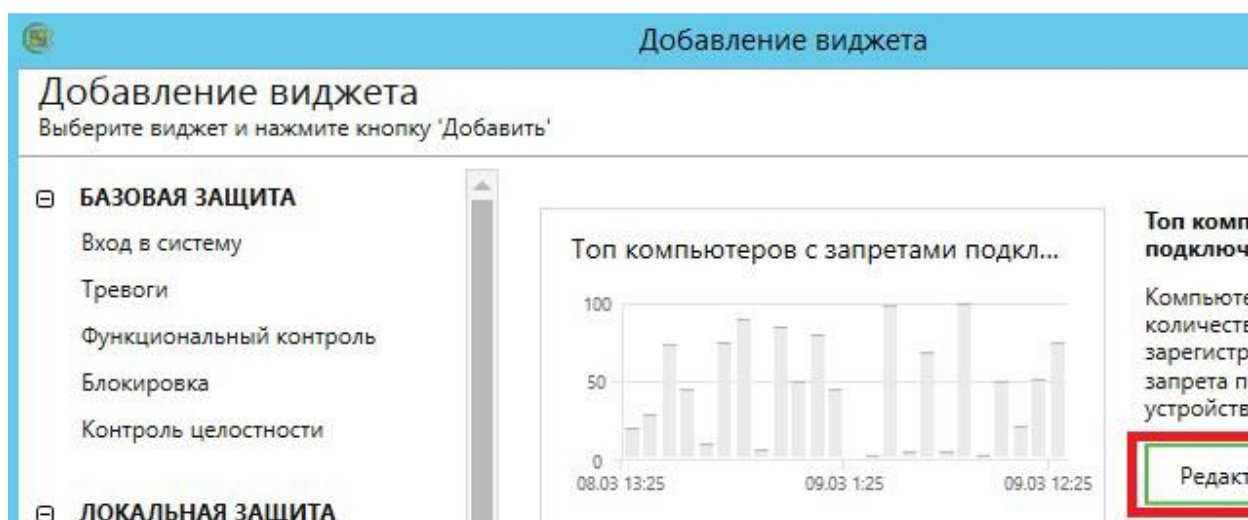


Рисунок 297 – Окно добавления виджета

В окне «Редактирование виджета» снимите флаг «График» и нажмите кнопку «Сохранить» (рисунок 298).

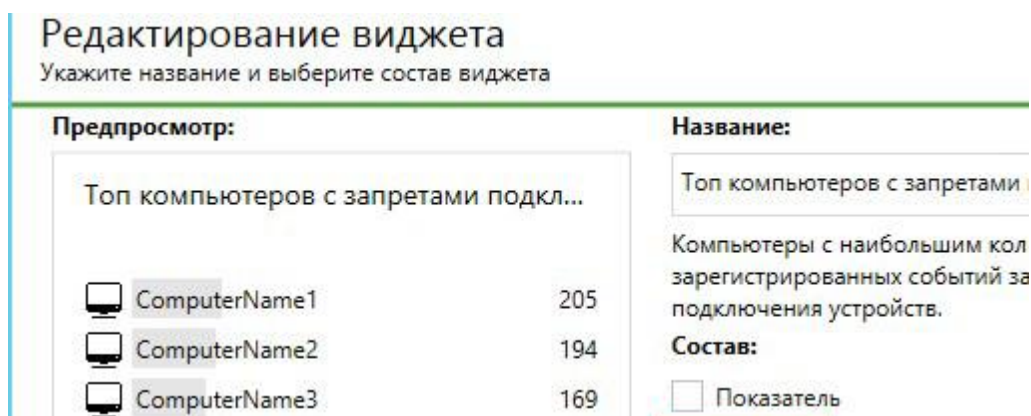


Рисунок 298 – Редактирование виджета

В окне «Добавление виджета» нажмите кнопку «Добавить». Новый виджет отобразится в панели статистики.

Добавьте виджеты «Использование СУБД» и «Переполнение журнала» из раздела «Дополнительные виджеты». Закройте окно добавления виджетов и отредактируйте панель статистики.

В панели статистики по умолчанию отображаются события за последние 24 часа. Для изменения периода надо выбрать переключатель рядом с надписью «Статистика». Установите период отображения «7 дней» или «30 дней». В виджетах отобразится информация об отсутствии данных (рисунок 299).

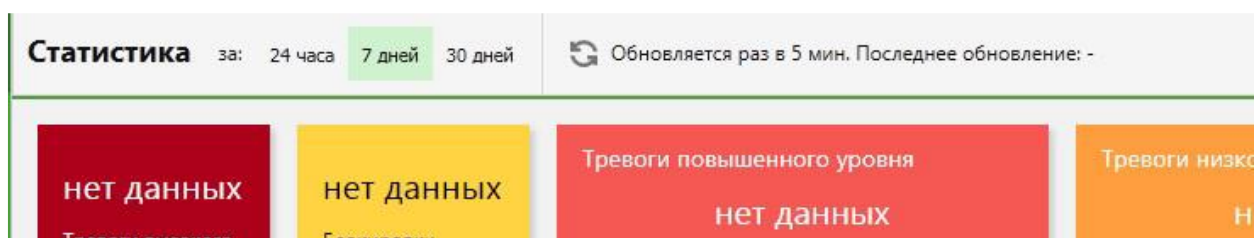


Рисунок 299 – Информация об отсутствии данных

Значения в виджетах отобразятся после периода обновления в 5 минут. Можно обновить панель принудительно, нажав кнопку «Обновить» рядом с выбором периода отображения статистики.

7.15 Анализ сообщений о тревогах, анализ событий в журналах, квитирование тревог

Переключитесь к виртуальной машине SNS-Client. Войдите под учетной записью user3. Подключите к виртуальной машине флеш-накопитель, который ранее не подключался к виртуальной машине (не добавлялся в конфигурацию при настройке подсистемы контроля устройств). Измените содержимое файла, включенного в ресурсы задания контроля целостности, для которого выполняется проверка содержимого файла.

Отключите флеш-накопитель от виртуальной машины. Завершите сеанс пользователя. Войдите под учетной записью пользователя user2. Компьютер будет заблокирован.

Переключитесь к виртуальной машине SNS-Server. Запустите консоль «Управление компьютером» (Win и R, compmgmt.msc), выберите узел «Диспетчер устройств». В правой части окна раскройте узел «DVD и CD-ROM дисководы», выберите устройство «VBOX CD-ROM ...», нажмите правой кнопкой мыши и в контекстном меню выберите пункт «Задействовать» (рисунок 300).

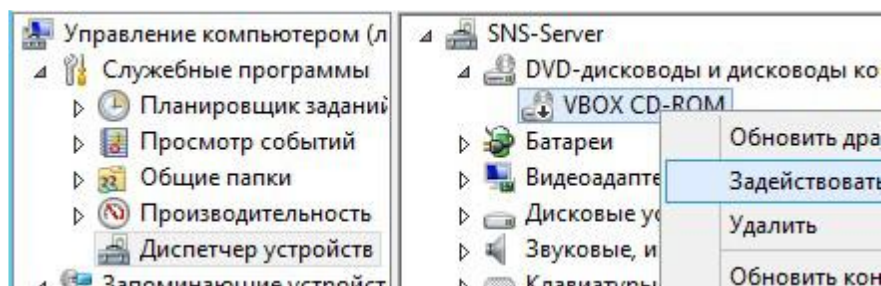


Рисунок 300 – Узел «DVD и CD-ROM дисководы»

Сработает блокировка компьютера. Войдите под учетной записью Администратора, разблокируйте компьютер.

В соответствии с регламентом по контролю эксплуатации, при анализе сообщений и оперативном контроле следует проверять количество событий в виджетах:

- тревоги высокого уровня;
- тревоги повышенного уровня;
- тревоги низкого уровня;
- запросы на утверждение аппаратной конфигурации;
- ошибки лицензий;
- ошибки функционального контроля;
- блокировки компьютеров;
- нарушения целостности.

В программе «Центр управления» на панели «Статистика» обновите сведения (рисунок 301).

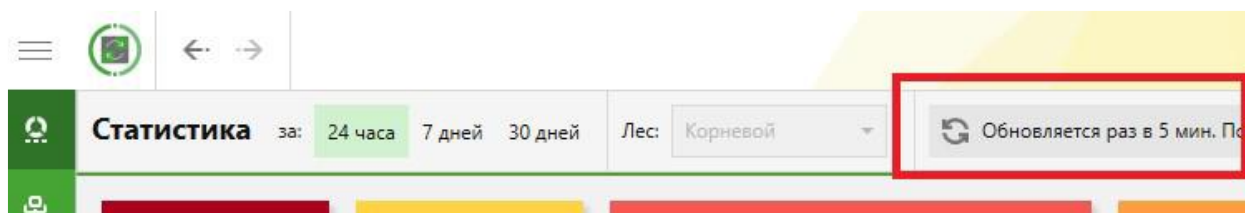
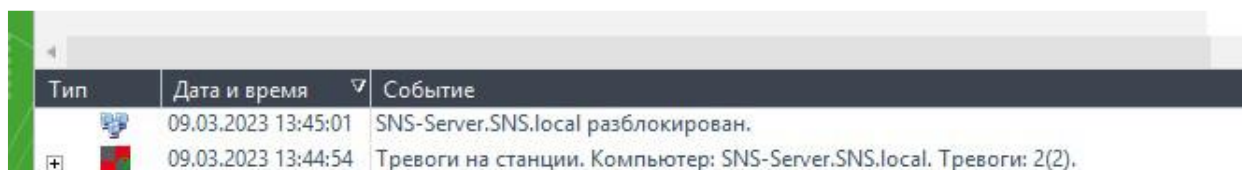


Рисунок 301 – Обновление сведений на панели «Статистика»

В виджетах появятся сведения о новых событиях. Также внизу окна программы «Центр управления» в панели событий появятся сообщения о тревогах на компьютерах SNS-Client и SNSServer (рисунок 302).



Тип	Дата и время	Событие
	09.03.2023 13:45:01	SNS-Server.SNS.local разблокирован.
	09.03.2023 13:44:54	Тревоги на станции. Компьютер: SNS-Server.SNS.local. Тревоги: 2(2).

Рисунок 302 – Панель событий

Если число событий в виджете не нулевое, то необходимо проанализировать событие, принять меры реагирования в соответствии с регламентом и квити́ровать события.

Квити́рование событий тревоги необходимо выполнять до архивирования журнала событий тревоги. Если в архив были помещены записи, не прошедшие процедуру квити́рования, значение счетчика событий тревоги уменьшается, и администратор безопасности может пропустить информацию о несанкционированном доступе. В этом случае для квити́рования событий следует восстановить журнал событий тревоги из архива в базу данных сервера безопасности, после чего появится возможность обработать информацию в обычном порядке.

Под квити́рованием событий тревоги понимается подтверждение о получении информации администратором безопасности с описанием принятых мер. Как правило, каждое событие тревоги требует выяснения причин его возникновения и выполнения экстренных действий для обеспечения безопасности информационной системы. После того как администратор безопасности принял к сведению и проанализировал обстоятельства возникновения события тревоги, необходимо подтвердить прием информации, выполнив процедуру квити́рования.

При квити́ровании администратор вводит текстовый комментарий с описанием причин и принятых мер, и этот комментарий сохраняется в системе вместе с признаком квити́рования события. Информация о самом событии тревоги не удаляется из журнала. В дальнейшем по журналу событий тревоги

можно определить, кто, когда и как отреагировал на произошедшие события. После квитирования всех событий, полученных от компьютера, этому объекту возвращается нормальный вид отображения.

Помимо квитирования событий тревоги с обязательным вводом комментария администратором безопасности, в программе предусмотрена возможность сброса счетчиков событий. Процедура сброса счетчиков предназначена только для случаев, связанных с настройкой системы защиты, и не должна применяться в штатном режиме функционирования.

Выберите виджет «Тревоги повышенного уровня» и нажмите левой кнопкой мыши на цифру, отображаемую в виджете (рисунок 303).

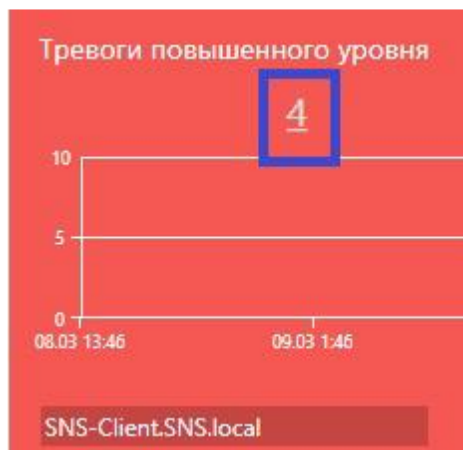


Рисунок 303 – Виджет «Тревоги повышенного уровня»

Автоматически откроется панель «Журналы тревог» и сформируется запрос «Повышенного уровня» (рисунок 304).

	СОБЫТИЯ		УГРОЗЫ				
	Дата	Событие	Категор...	Источник	Комп...	Домен	
За сутки	09.03.2023...	Компьютер...	Вход/выход	LocalProtec...	SNS-Server.S...	NT AUTHC	
За 7 суток	09.03.2023...	Обнаружен...	Контроль ц...	LocalProtec...	SNS-Client.S...	NT AUTHC	
Все высокого уровня	09.03.2023...	Компьютер...	Вход/выход	LocalProtec...	SNS-Client.S...	NT AUTHC	

Рисунок 304 – Журнал тревог

В списке событий отобразятся все события, которые были идентифицированы как тревоги. Выберите любое событие, нажмите правой кнопкой мыши и в контекстном меню выберите пункт «Раскраска событий» (рисунок 305).

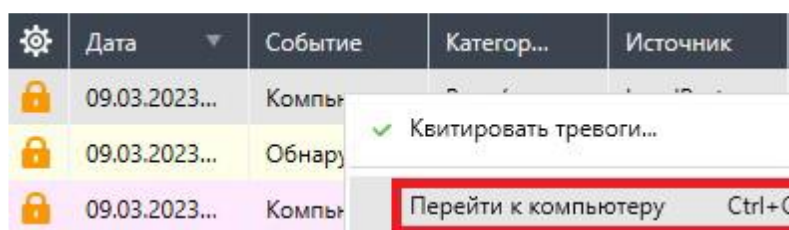


Рисунок 307 – Выбор «Перейти к компьютеру»

Откроется панель «Компьютеры», в которой будет выделен компьютер SNS-Server. Откройте окно свойств компьютера и перейдите на вкладку «Состояние». Пиктограмма компонента «Контроль устройств» будет синего цвета, что свидетельствует об изменении аппаратной конфигурации устройства. Нажмите на пиктограмму и просмотрите причину изменения конфигурации (рисунок 308).

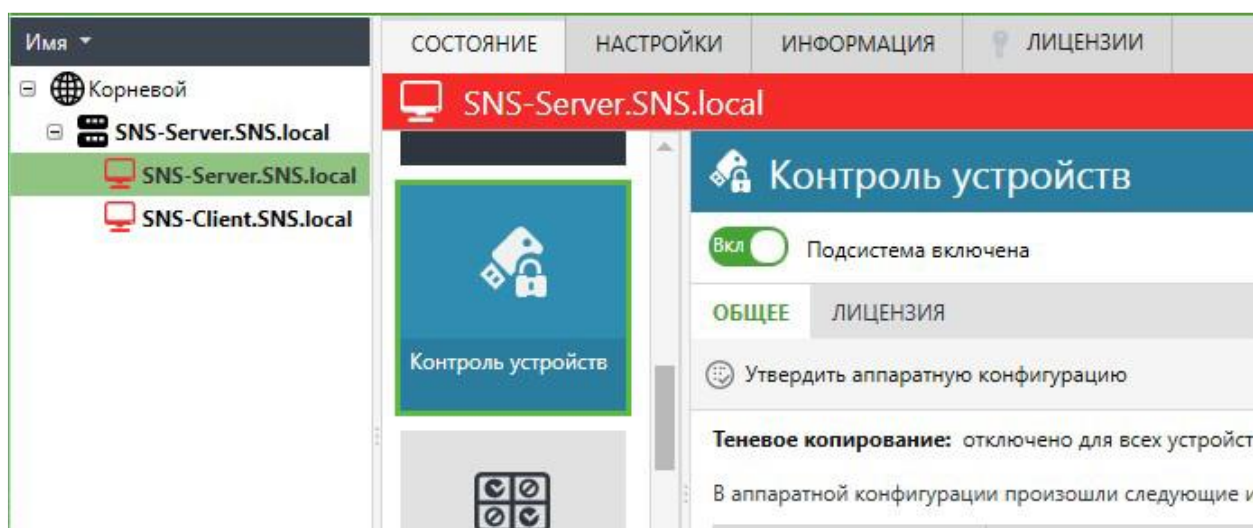


Рисунок 308 – Причина изменений конфигурации

Не утверждайте новую конфигурацию. Вернитесь к панели «Журнал тревог». В списке первое событие (связанное с блокировкой компьютера SNS-Server из-за изменения аппаратной конфигурации). Нажмите на событие правой кнопкой мыши и выберите пункт «Квитировать тревоги...» (рисунок 309).

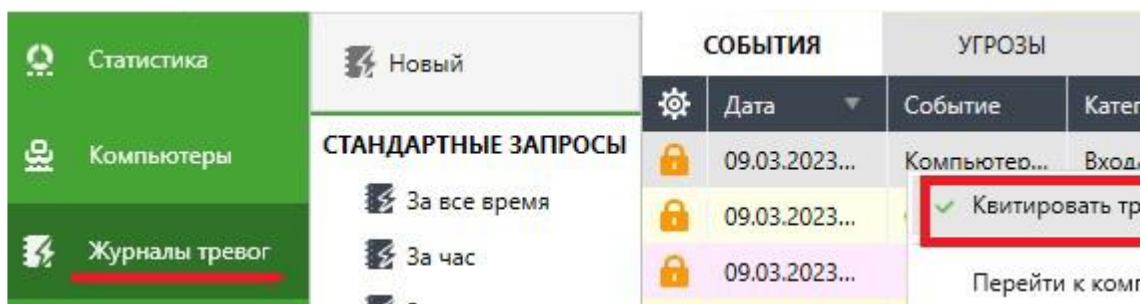


Рисунок 309 – Квитирование тревоги

В окне «Квитирование тревог» введите описание причины тревоги (если требуется в соответствии с регламентами обработки инцидентов) и нажмите кнопку «Квитировать» (рисунок 310).



Рисунок 310 – Описание причины тревоги

В строке журнала тревог появится символ «V», означающий, что для тревоги выполнено квитирование. Нажмите на заголовке столбца с пиктограммой в виде компьютера для сортировки событий по названию компьютера (рисунок 311).

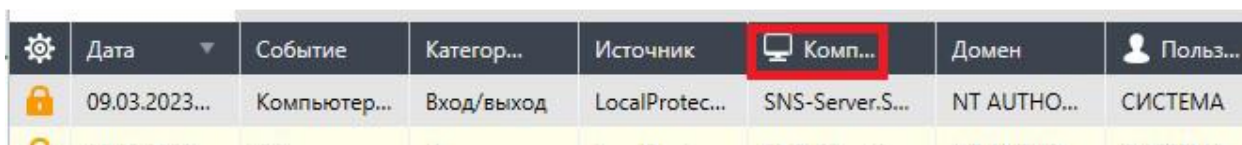


Рисунок 311 – Сортировка событий

Список будет отсортирован, события в начале списка будут относиться к компьютеру SNSServer, квитированное событие переместится. Выберите в списке первое событие, относящееся к компьютеру SNS-Server, зажмите клавишу Shift и нажмите на последнее событие такого типа. Будет выделено несколько событий (рисунок 312)

СОБЫТИЯ		УГРОЗЫ	
⚙	Дата	Событие	Категор...
🔒	09.03.2023...	Запрет под...	Разграниче...
🔒	09.03.2023...	Компьютер...	Вход/выход
🔒	09.03.2023...	Обнаружен...	Контроль ц...

Рисунок 312 – Отсортированные события

Нажмите правой кнопкой мыши на любом из выделенных событий и в контекстном меню выберите пункт «Квитировать тревоги». В окне квитирования отобразится, что выбрано несколько тревог, введите для них описание и нажмите кнопку «Квитировать» (рисунок 313).

Рисунок 313 – Квитирование угроз

Обратите внимание, что после квитирования в верхнем углу программы уменьшается значение количества тревог. Выберите другие группы событий, связанные с проверкой настроек подсистемы контроля устройств (изменение аппаратной конфигурации на SNS-Server). Квитируйте тревоги с указанием описания тревог. Тревоги, связанные с компьютером SNS-Client, не квитируйте. В панели событий (внизу экрана) отобразятся события квитирования тревог (рисунок 314).

Тип	Дата и время	Событие	Описание
👤	09.03.2023 14:09:39	Квитирование тревог. Количество квитуемых тревог: 3.	Квитиров...
👤	09.03.2023 14:03:36	Квитирование тревог. Количество квитуемых тревог: 1.	Квитиров...

Рисунок 314 – События квитирования тревог

В левой части окна нажмите в разделе «Запросы» кнопку «Обновить» (рисунок 315).

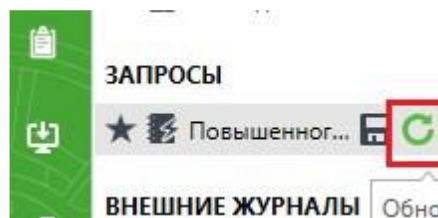


Рисунок 315 – Обновление запросов

Квитированные события исчезнут из журнала тревог. В списке останутся только события, связанные с компьютером SNS-Client. Вернитесь к панели «Статистика». Обновите содержимое панели. В виджете «Тревоги повышенного уровня» уменьшится количество тревог, в списке останется только компьютер SNSClient. Нажмите на количестве тревог в виджете «Тревоги низкого уровня» (рисунок 316).

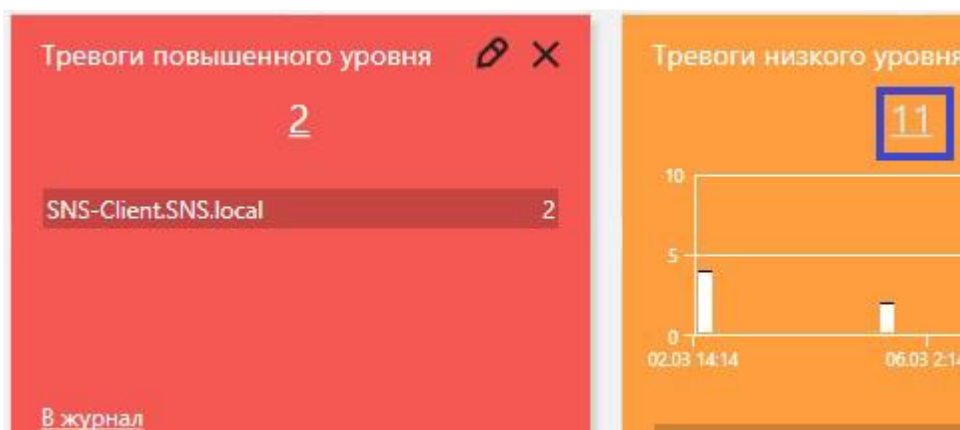


Рисунок 316 – Виджет тревог

Квитируйте все тревоги, источником которых является компьютер SNS-Server. Тревоги от SNS-Client не квитируйте. Обновите журнал тревог. Вернитесь к панели «Статистика». В виджете «Запросы на утверждение АК» нажмите на цифру (рисунок 317).



Рисунок 317 – Запросы на утверждение АК

Автоматически будет выполнен переход на вкладку «Состояние» компьютера SNS-Server. Нажмите кнопку «Утвердить аппаратную конфигурацию» (рисунок 318) и нажмите «Да» в окне подтверждения.

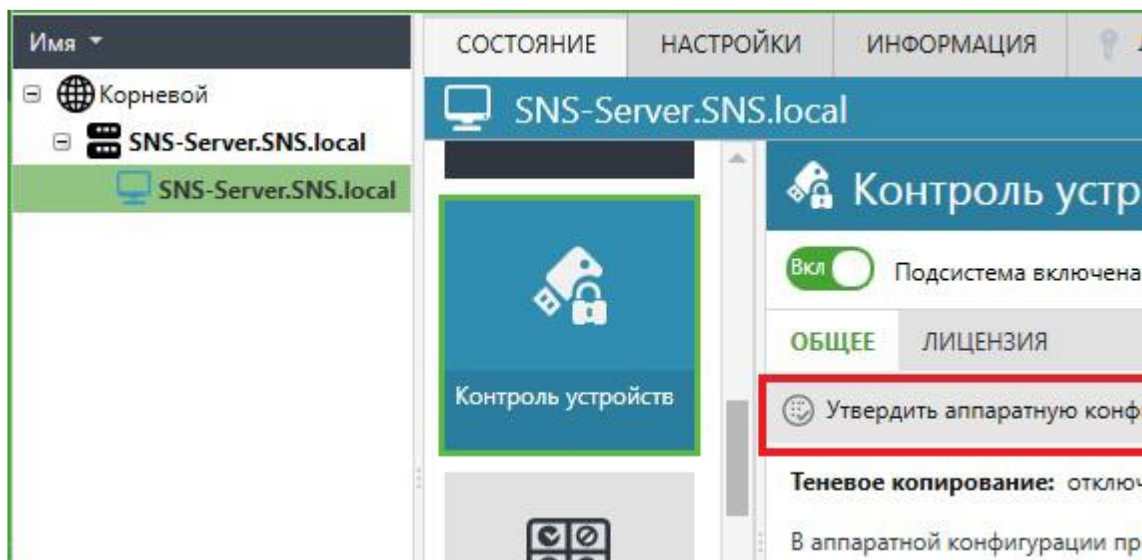


Рисунок 318 – Вкладка «Состояние»

Вернитесь к панели «Статистика». Обновите содержимое панели. Значение в виджете «Запросы на утверждение АК» обнулится. Выберите виджет «Топ компьютеров с запретом подключения...» и нажмите на названии устройства SNS-Client (рисунок 319).

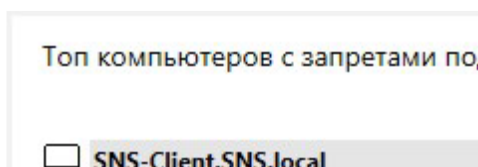


Рисунок 319 – Виджет «Топ компьютеров с запретом подключения...»

Произойдет автоматический переход на панель «Компьютеры» с отображением компонента «Контроль устройств» вкладки «Состояние» компьютера SNS-Client. Нажмите ссылку «Настройки» (рисунок 320). Будет выполнен переход на вкладку «Настройки», нажмите кнопку «Загрузить настройки».

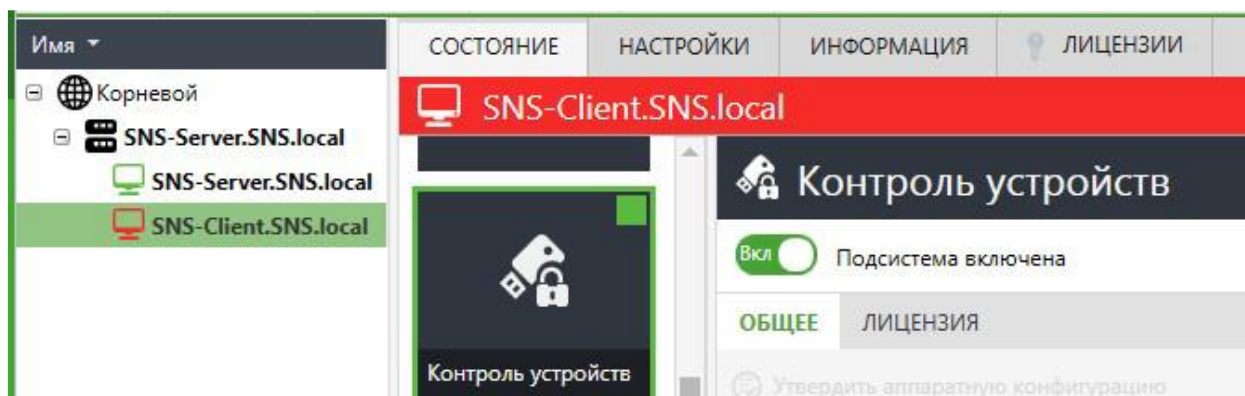


Рисунок 320 – Панель «Контроль устройств»

Настройки не загрузятся. Вернитесь к панели «Статистика», нажмите на число в виджете «Блокировки компьютеров» (рисунок 321).



Рисунок 321 – Виджет «Блокировки компьютеров»

Произойдет автоматический переход на компьютер SNS-Client в структуре управления. Перейдите на вкладку «Состояние» и выберите компонент «Блокировка», он будет красного цвета, на вкладке «Общее» будет отображена информация о причинах блокировки (рисунок 322).

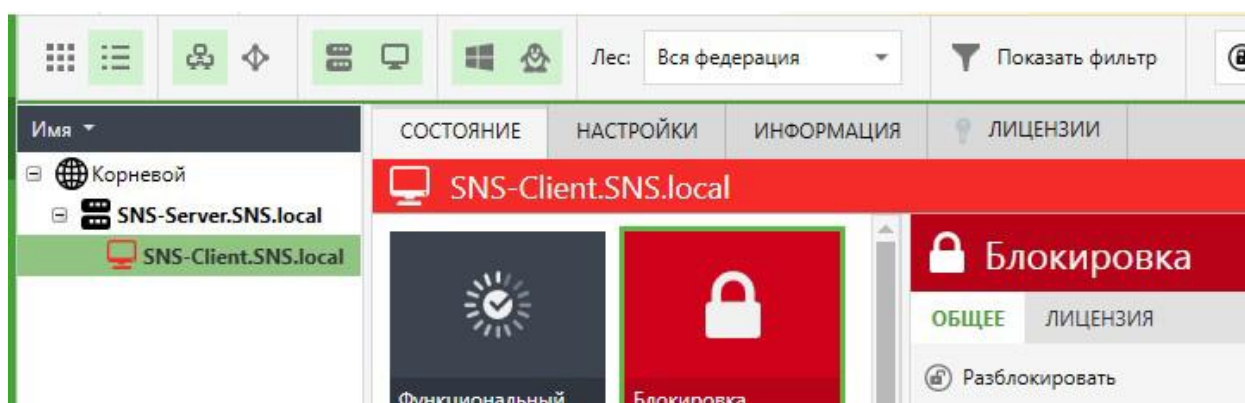


Рисунок 322 – Панель «Блокировка»

Вернитесь к панели «Статистика», нажмите на число в виджете «Компьютеры с нарушением целостности» (рисунок 323).

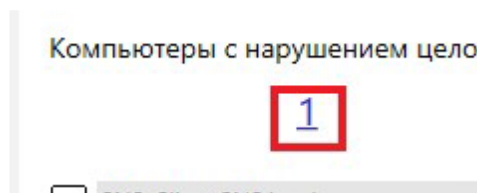


Рисунок 323 – Виджет «Компьютеры с нарушением целостности»

Произойдет переход к панели «Журналы тревог». Выберите в разделе «Запросы» журнал «Повышенного уровня», нажмите «Обновить» (рисунок 324).

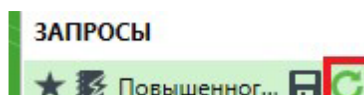


Рисунок 324 – Панель «Журналы тревог»

В списке тревог найдите событие «Компьютер заблокирован», просмотрите детальное описание события (рисунок 325). Определите причину блокировки (контроль целостности).

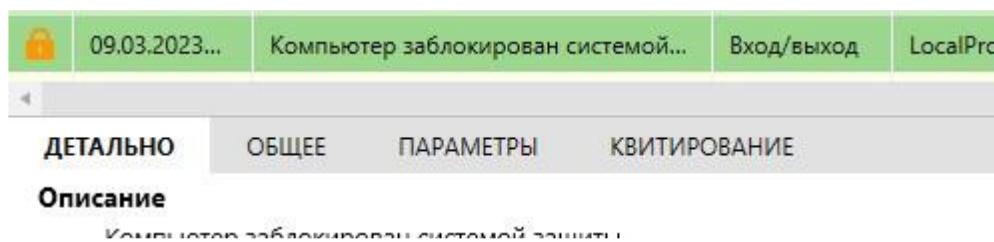


Рисунок 325 – Событие «Компьютер заблокирован»

Выберите событие, зафиксированное в момент блокировки компьютера. Просмотрите детальную информацию о событии (рисунок 326). В нем будет указано при выполнении какого задания контроля целостности произошла блокировка.

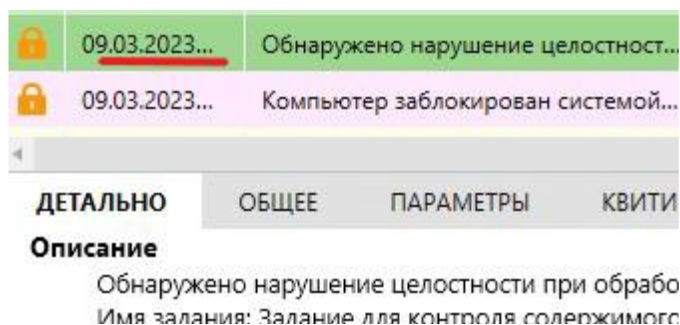


Рисунок 326 – Событие «Компьютер заблокирован»

Загрузите журнал «Тревоги низкого уровня» (через виджет в панели мониторинга), найдите событие тревоги, зафиксированное во время блокировки.

Просмотрите детальную информацию, в ней будет указано имя задания и имя ресурса, нарушение целостности которого привело к блокировке (рисунок 327).

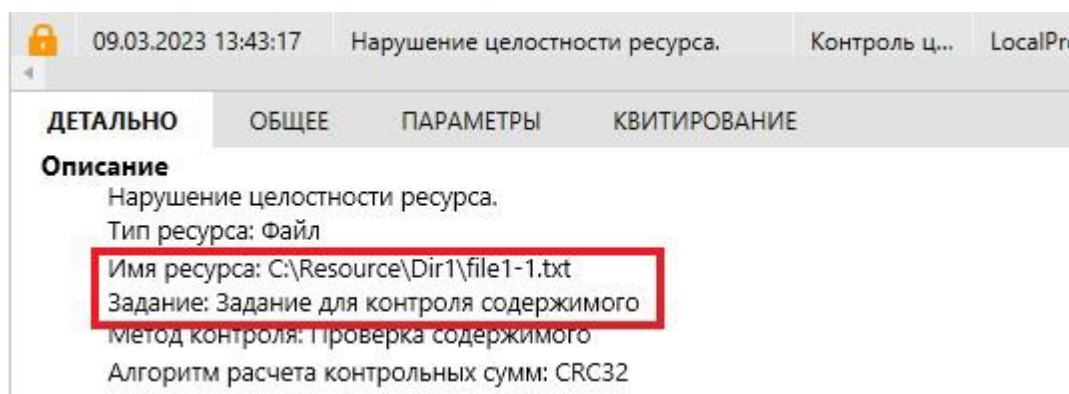


Рисунок 327 – Просмотр детальной информации

Квитируйте тревоги низкого и повышенного уровня, связанные с блокировкой компьютера и нарушением целостности (не квитируйте тревоги запрета подключения устройств).

После выяснения причин блокировки компьютера SNS-Client необходимо его разблокировать. Для этого можно воспользоваться командами оперативного управления. Команды оперативного управления могут применяться к агентам сервера подключения (сервер безопасности, с которым установлено соединение программы) и к агентам подчиненных серверов. При этом выбранный для управления компьютер должен быть включен. Если в данный момент исполнение какой-либо оперативной команды невозможно, эта команда или отсутствует в меню, или неактивна. Перечень команд оперативного управления включает следующие:

- заблокировать;
- разблокировать;
- перезагрузить;
- выключить;
- применить групповые политики.

Команда применения групповых политик рассматривалась при настройке параметров СЗИ от НСД. Перейдите к панели «Компьютеры». После выполнения предыдущих действий в списке компьютеров отображается только компьютер SNS-Client, поскольку ранее при переходе из панели статистики по ссылке в виджете блокировки автоматически установился фильтр «Включенные с признаком блокировки» (рисунок 328). Нажмите на кнопку «Свойства» для отображения списка устройств.

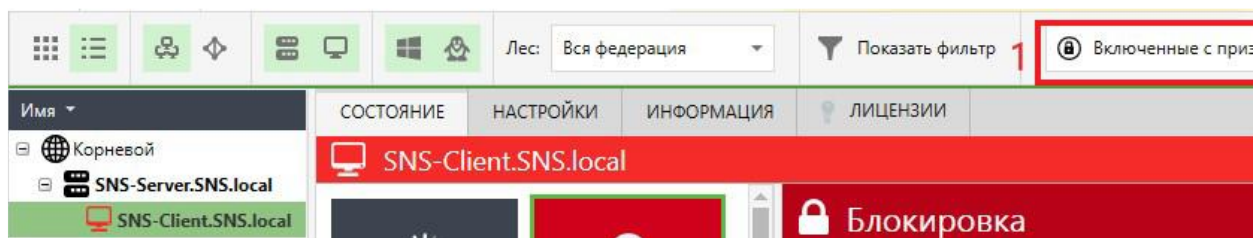


Рисунок 328 – Панель «Блокировка»

В списке отобразится компьютер SNS-Client, в графе «Блокировка» будет установлена пиктограмма с изображением красного замка (рисунок 329).

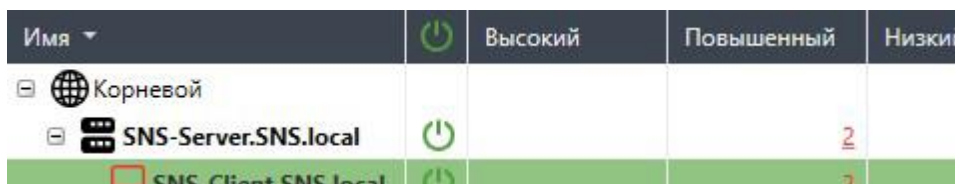


Рисунок 329 – Блокировка компьютера «SNS-Client»

Нажмите на строке с именем компьютера правой кнопкой мыши, в контекстном меню выберите «Команды» - «Разблокировать» (рисунок 330) и нажмите «Да» в окне подтверждения.

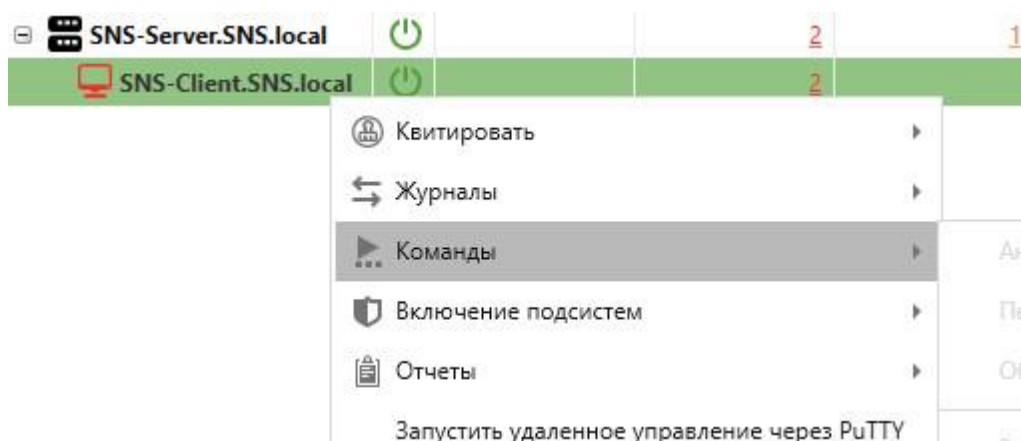


Рисунок 330 – Разблокировка компьютера «SNS-Client»

Через некоторое время компьютер пропадет из списка. В списке фильтрации выберите строку «Фильтр не задан» (рисунок 331), отобразится полный список компьютеров.

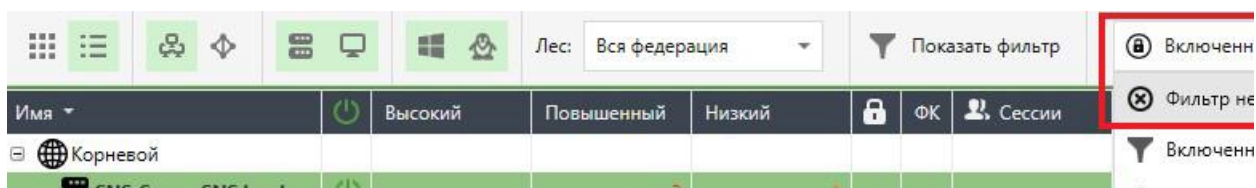


Рисунок 331 – Выбор «Фильтр не задан»

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью user2. После начала процедуры входа компьютер снова будет заблокирован, поскольку контроль целостности ресурсов выполняется при входе пользователя в систему. Войдите под учетной записью Администратора, снимите блокировку, устраните причину блокировки. Завершите сеанс Администратора. Войдите под учетной записью user2. Вход должен быть разрешен. Не завершайте сеанс user2, переключитесь к окну виртуальной машины SNS-Server.

На панели «Компьютеры» в списке выберите компьютер SNS-Client, в контекстном меню выберите команду «Заблокировать» (рисунок 332) и подтвердите блокировку.

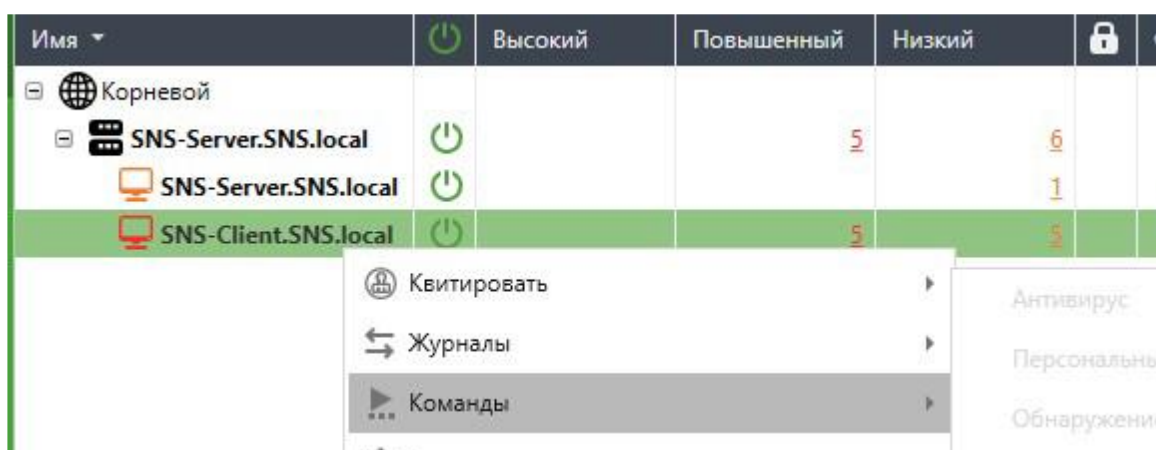


Рисунок 332 – Блокировка компьютера «SNS-Client»

Переключитесь к окну виртуальной машины SNS-Client. Компьютер будет заблокирован. Попробуйте войти под учетной записью user1, user2, user3. Доступ будет запрещен.

Переключитесь к окну виртуальной машины SNS-Server. Разблокируйте компьютер. Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью user2. Доступ будет разрешен.

Переключитесь к окну виртуальной машины SNS-Server. Откройте панель «Статистика». В ней появились новые тревоги различного уровня. Перейдите на панель «Компьютеры». Выберите в списке сервер безопасности. Нажмите правой кнопкой мыши и в контекстном меню выберите пункт «Квитировать» - «Все тревоги» (рисунок 333). Нажмите «Да» в окне подтверждения.

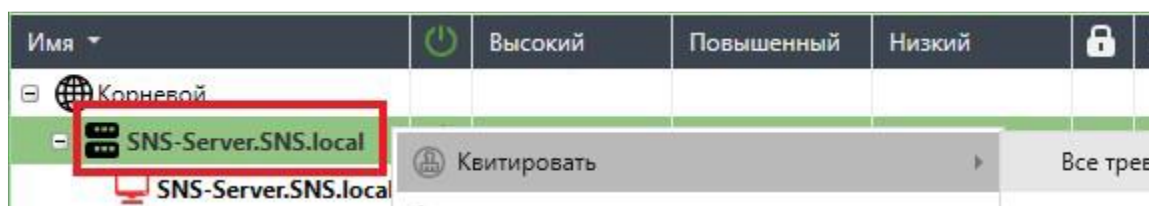


Рисунок 333 – Квитирование всех тревог

Счетчик тревог обнулится, пиктограммы компьютеров станут зеленого цвета. Вернитесь к панели «Статистика» и обновите содержимое. Все счетчики обнулятся.

7.16 Группы наблюдения

Группа наблюдения содержит информацию об общем состоянии уровня тревог в системе. Для оперативного мониторинга администратор может сформировать произвольные группы наблюдения, состоящие из компьютеров. Группа наблюдения является виджетом в панели «Статистика». Панель такого виджета содержит в себе перечень параметров наименование и показатель (общее число тревог всех уровней по всем компьютерам группы наблюдения).

Перейдите к панели «Компьютеры», включите отображение панели в виде диаграммы (рисунок 334).

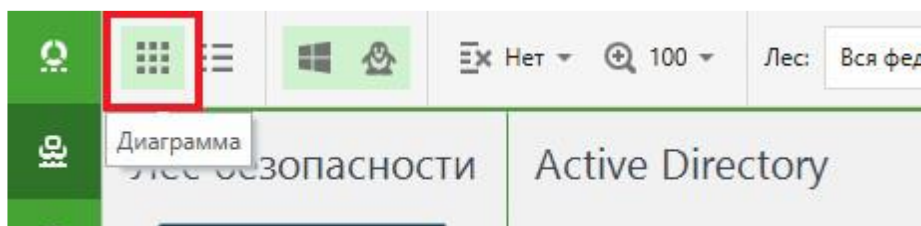


Рисунок 334 – Отображение панели в виде диаграммы

В правой части диаграммы в поле «Серверы безопасности» нажмите двойным кликом на пиктограмме сервера SNS-Server (рисунок 335).

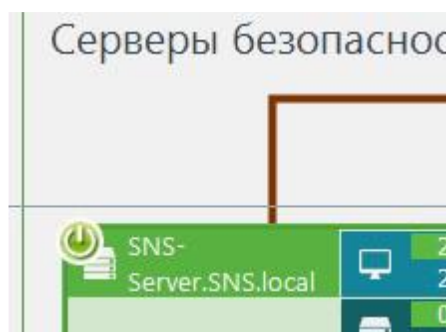


Рисунок 335 – Открытие сервера «SNS-Server»

В окне отобразится структура безопасности. Выделите компьютеры SNS-Client и SNS-Server (зажмите левую кнопку мыши и охватите областью выделения два компьютера) (рисунок 336).

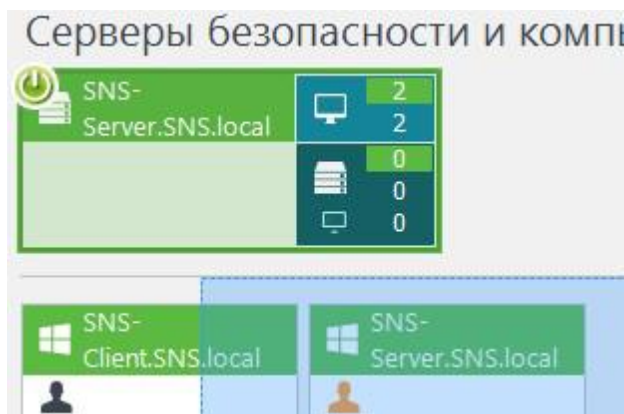


Рисунок 336 – Структура безопасности

Компьютеры будут выделены. Нажмите на любом компьютере правой кнопкой мыши, в контекстном меню выберите пункты «Наблюдение» - «Новое» (рисунок 337).

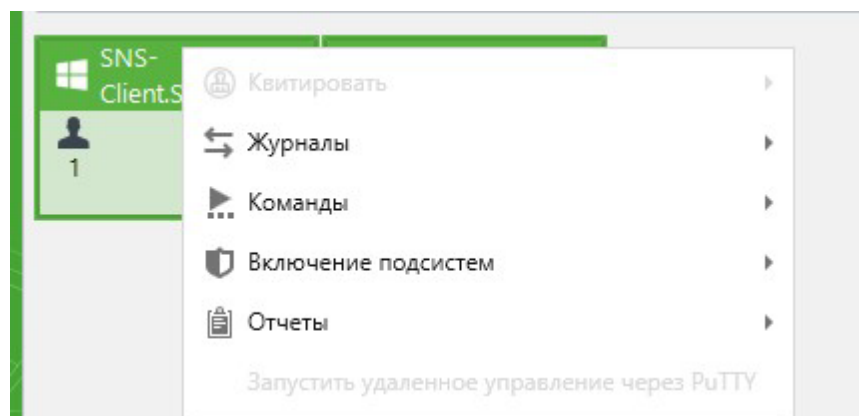


Рисунок 337 – Создание группы наблюдения

Введите название группы и нажмите кнопку «Создать» (рисунок 338).

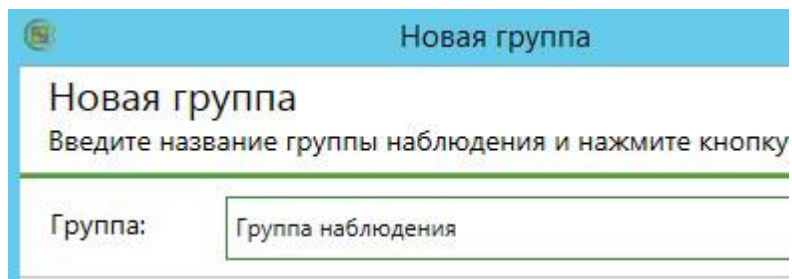


Рисунок 338 – Создание группы наблюдения

В строке навигации нажмите на пиктограмму с изображением сети компьютеров (рисунок 339). Внешний вид панели восстановится.

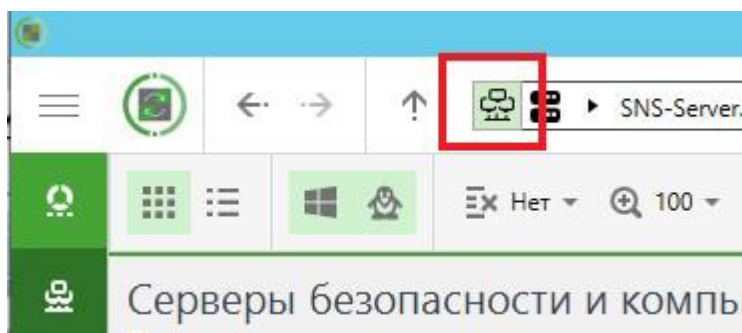


Рисунок 339 – Восстановление внешнего вида панели

Перейдите к панели «Статистика». В ней появится новый виджет (рисунок 340), отображающий тревоги выбранной группы.

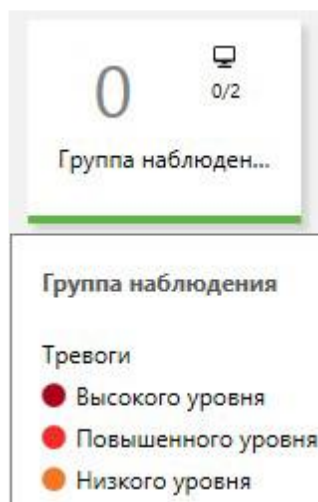


Рисунок 340 – Созданный виджет

7.17 Выявление изменений аппаратной конфигурации

В соответствии с Регламентом использования по назначению Оператор ИБ должен выполнять анализ изменений аппаратной конфигурации.

На компьютере SNS-Server запустите консоль «Управление компьютером» (Win и R, compmgmt.msc), выберите узел «Диспетчер устройств». В правой части окна раскройте узел «DVD и CD-ROM дисководы», выберите устройство «VBOX CD-ROM ...», нажмите правой кнопкой мыши и в контекстном меню выберите пункт «Отключить».

Сработает блокировка компьютера. Войдите под учетной записью Администратора, разблокируйте компьютер.

В программе «Центр управления» в нижней части окна программы появятся события, вызванные блокировкой. Раскройте описание событий кнопкой «+» (рисунок 341). В событиях присутствуют уведомления о блокировке, изменении аппаратной конфигурации и сигнал тревоги, обозначенный красно-зеленым квадратом. В описании тревоги присутствуют два события низкого и повышенного уровня, указанные в виде категории и идентификатора события, приведших к появлению сигнала тревоги. Нажмите на ссылку «Получить описание тревоги».

Тип	Дата и время	Событие	Описание									
	09.03.2023 15:57:55	SNS-Server.SNS.local разблокирован.	Уведомление									
	09.03.2023 15:57:50	Тревоги на станции. Компьютер: SNS-Server.SNS.local. Тревоги: 2(2).	Получить опи									
<table><tr><th>Источник</th><th>Категория (код)</th><th>Идентификатор (код)</th></tr><tr><td>LocalProtection</td><td>13</td><td>1293</td></tr><tr><td>LocalProtection</td><td>2</td><td>1016</td></tr></table>				Источник	Категория (код)	Идентификатор (код)	LocalProtection	13	1293	LocalProtection	2	1016
Источник	Категория (код)	Идентификатор (код)										
LocalProtection	13	1293										
LocalProtection	2	1016										
	09.03.2023 15:57:45	На агенте SNS-Server.SNS.local изменилась аппаратная конфигурация.	Уведомление									

Рисунок 341 – Получение описания тревоги

Описание тревоги дополнится подробностями (рисунок 342). Из описания видно, что тревога низкого уровня вызвана контролем конфигурации, а тревога повышенного уровня относится к категории входа-выхода, т.е. вызвана событием блокировки пользователя. Последняя графа таблицы, обозначенная зеленой галкой, отображает квитирование событий (события не квитированы).

	09.03.2023 15:57:50	Тревоги на станции. Компьютер: SNS-Server.SNS.local. Тревоги: 2(2).	Получить описание тревоги.						
Журнал	Агент	Дата	События	Код категории	Категория	Источник	Компьютер	Домен	Пользователь
Secret Net ...	Secret Net S...	09.03.2023 15:5...	1293	13	Контроль ко...	LocalProtecti...	SNS-Server.S...	NT AUTHORI...	СИСТЕМА

Рисунок 342 – Описание тревоги

Двойным кликом мыши раскройте описание первого события. Появится окно детальной информации о событии (рисунок 343).

Тип	Дата и время	Событие	Описание	2/125	Детально
	09.03.2023 15:57:55	SNS-Server.SNS.local разблокирован.	Уведомление от агента.		Описание Устройс Категор категор Устройство
	09.03.2023 15:57:50	Тревоги на станции. Компьютер: SNS-Server.SNS.local. Т...	Получить описание тревоги.		
	09.03.2023 15:57:45	На агенте SNS-Server.SNS.local изменилась аппаратная к...	Уведомление от агента.		

Журнал	Агент	Дата	Собы	Код катег	Категор	Источн	Комп	Домен	Польз	Порядковы	Уровень	
Secret ...	Secret ...	09.03.20...	1293	13	Контр...	LocalPr...	SNS-Ser...	NT AUT...	СИСТЕ...	12	Низкий	✓
Secret ...	Secret ...	09.03.20...	1016	2	Вход/в...	LocalPr...	SNS-Ser...	NT AUT...	СИСТЕ...	13	Повышенны	

Рисунок 343 – Описание первого события

Выберите в списке второе событие, информация о нем отобразится в окне «Детально». Закройте окно детальной информации выполнив двойной клик по событию. Перейдите на панель «Компьютеры», включите отображение структуры в виде таблицы. На панели инструментов в списке «Фильтр» выберите значение «Изменение аппаратной конфигурации» (рисунок 344).

Имя	Высокий	Повышенный	Низкий	ФК	Сессии
Корневой					
SNS-Server.SNS.local		1	1		

Лес:	Показать фильтр
Вся федерация	

⊗ Фильтр не зад
⊗ Фильтр не зад
⚠ Ошибки лице
⚠ Предупрежде

Рисунок 344 – Описание второго события

В структуре сервера безопасности останется только компьютер SNS-Server. Выберите компьютер в списке, откройте свойства, перейдите на вкладку «Состояние» и выберите подсистему «Контроль устройств» (рисунок 345). В соответствии с регламентами требуется проанализировать изменения конфигурации и, если изменения санкционированные, утвердить новую аппаратную конфигурацию. Утвердите новую аппаратную конфигурацию.

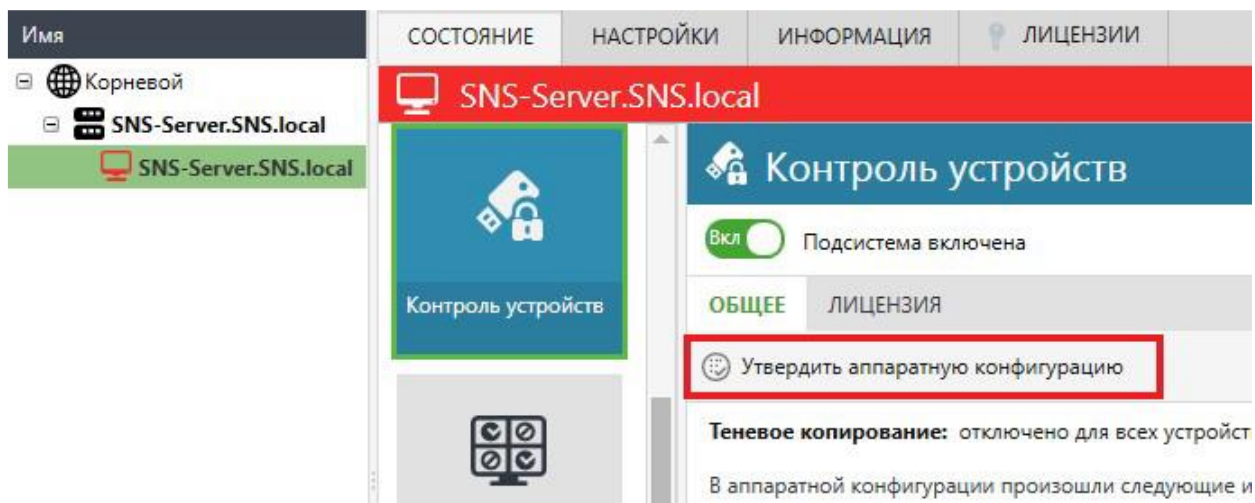


Рисунок 345 – Утверждение новой конфигурации

В панели инструментов сбросьте фильтр, установив значение «Фильтр не задан».

7.18 Контроль функционирования защитных подсистем

Согласно Регламенту по контролю эксплуатации Оператор ИБ выполняет проверку функционирования защитных подсистем СЗИ от НСД с использованием программ «Центр управления» и «Локальный центр управления» (для автономных СВТ) из состава СЗИ от НСД «Secret Net Studio».

Переключитесь к окну виртуальной машины SNS-Client, войдите под учетной записью Администратора, запустите программу «Локальный центр управления». В панели «Компьютер» на вкладке «Состояние» выберите компонент «Затирание данных» и отключите компонент, переведя переключатель в другое положение (рисунок 346). Выполните перезагрузку компьютера (shutdown /R /t 0).

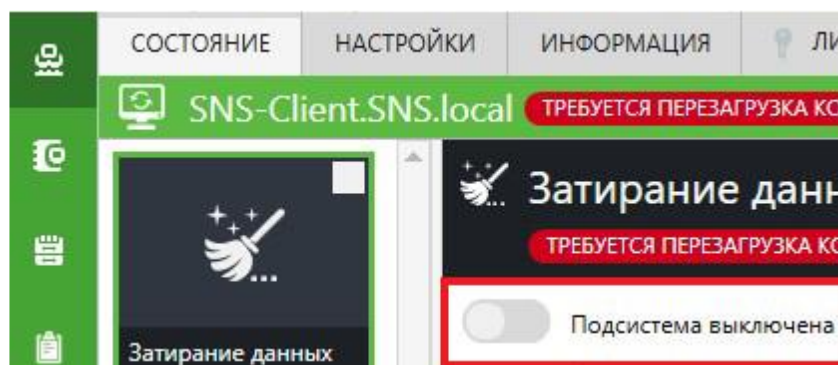


Рисунок 346 – Отключение компонента «Затирание данных»

В программе «Центр управления» перейдите к панели «Компьютеры», включите отображение структуры управления в виде таблицы. В панели инструментов нажмите кнопку «Свойства», если не отображается окно свойств (рисунок 347).

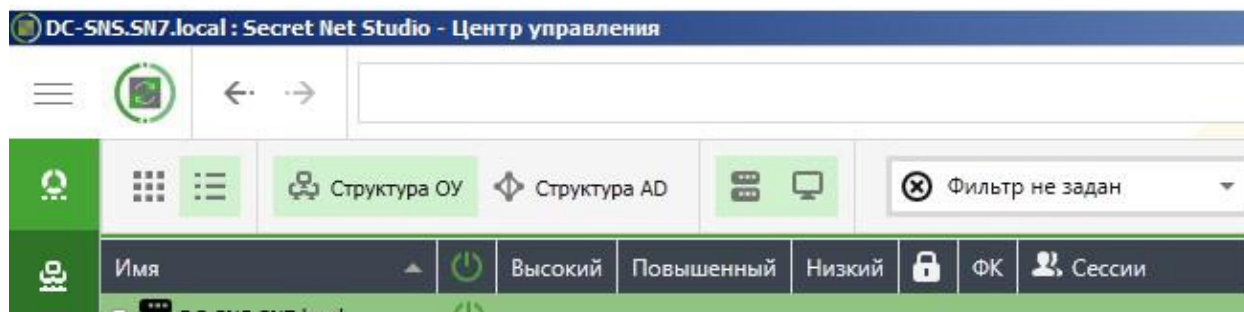


Рисунок 347 – Панель «Компьютеры»

Выберите в структуре компьютер SNS-Server, в окне свойств отобразится вкладка «Состояние». В средней части окна программы выводятся пиктограммы списка установленных на компьютере компонентов защиты, индикатор состояния компонента представлен в виде квадрата в правом верхнем углу. Зеленый цвет индикатора сигнализирует о нормальном функционировании компонента (рисунок 348), белый — о том, что компонент отключен. Отсутствие индикатора означает, что компонент либо не установлен, либо имеются ограничения по лицензии. Серый фон пиктограммы соответствует установленным компонентам, светло-серый – не установленным.

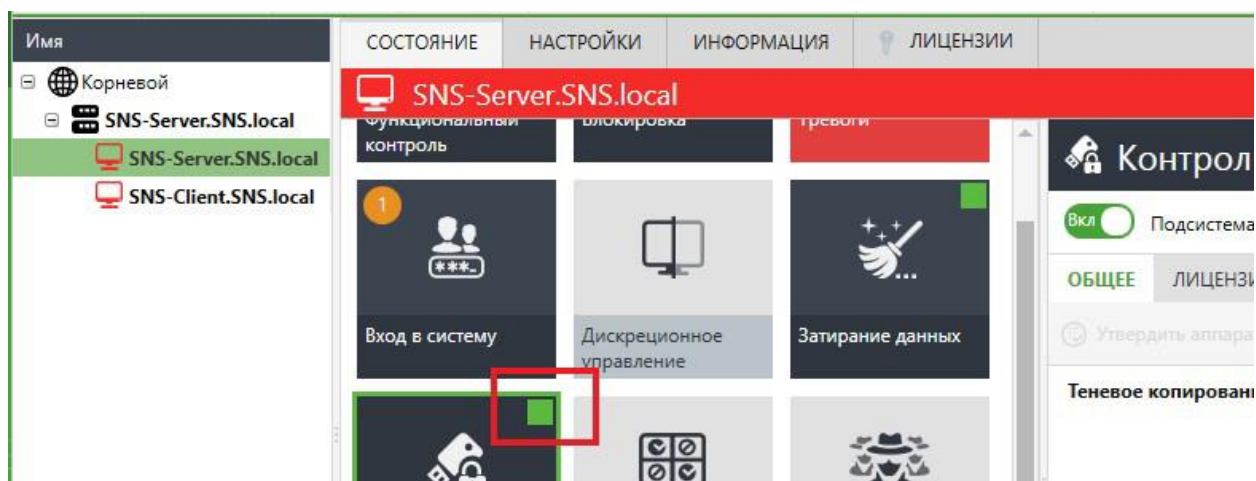


Рисунок 348 – Вкладка «Состояние»

Проверьте перечень и состояние компонентов на соответствие Унифицированным конфигурациям (некоторые компоненты используемой версии могут отсутствовать в списке):

- дискреционное управление доступом: отключено;
- затирание данных: включено;
- контроль устройств: включено;
- замкнутая программная среда: включено;
- полномочное управление: отключено;
- контроль печати: отключено;
- защита дисков и шифрование данных: отключено;
- персональный межсетевой экран: отключено;
- авторизация сетевых соединений: отключено;
- обнаружение вторжений: отключено;
- антивирус: отключено;
- паспорт ПО: включено;
- доверенная среда: отключено.

Некоторые обязательные компоненты не установлены. В соответствии с Регламентом по контролю эксплуатации далее следует регистрировать запрос/инцидент. В рамках практического задания это не выполняется.

В структуре управления выберите компьютер SNS-Client. Просмотрите на вкладке «Состояние» состояние и перечень компонентов защиты. У компонента «Затирание данных» пиктограмма белого цвета, что является признаком выключенного компонента (рисунок 349).



Рисунок 349 – Вкладка «Состояние»

Проверьте соответствие конфигурации требованиям Унифицированных конфигураций. На компьютере SNS-Client установлены и включены некоторые компоненты. Включите компонент «Затирание данных». После включения компонента появится сообщение о необходимости перезагрузки компьютера.

Выполните перезагрузку SNS-Client с использованием команды оперативного управления. Параметры остальных компонентов оставьте без изменения. Завершение перезагрузки отобразится в панели событий сообщением о включении компьютера (рисунок 350).

Тип	Дата и время	Событие
	09.03.2023 16:32:32	<u>SNS-Client.SNS.local включен.</u>
	09.03.2023 16:31:25	SNS-Client.SNS.local выключен.

Рисунок 350 – Панель событий

На автономных СВТ контроль функционирования осуществляется аналогичным образом на вкладке «Состояние» панели «Компьютер». Завершите сеанс Администратора.

7.19 Контроль назначения ролей эксплуатационного персонала

Войдите на компьютер SNS-Server под учетной записью user2. Запустите программу «Центр управления» (рисунок 351).

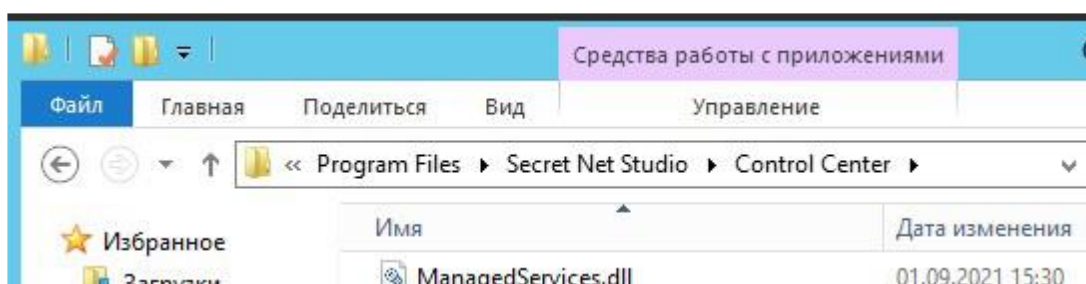


Рисунок 351 – Запуск программы «Центр управления»

В панели «Компьютеры» включите отображение в виде таблицы, выберите в структуре управления сервер безопасности SNS-Server, нажмите на кнопку «Свойства», в окне свойств перейдите на вкладку «Информация». В панели определите названия групп в полях «Администраторы домена безопасности» и «Администраторы леса доменов безопасности» (рисунок 352).

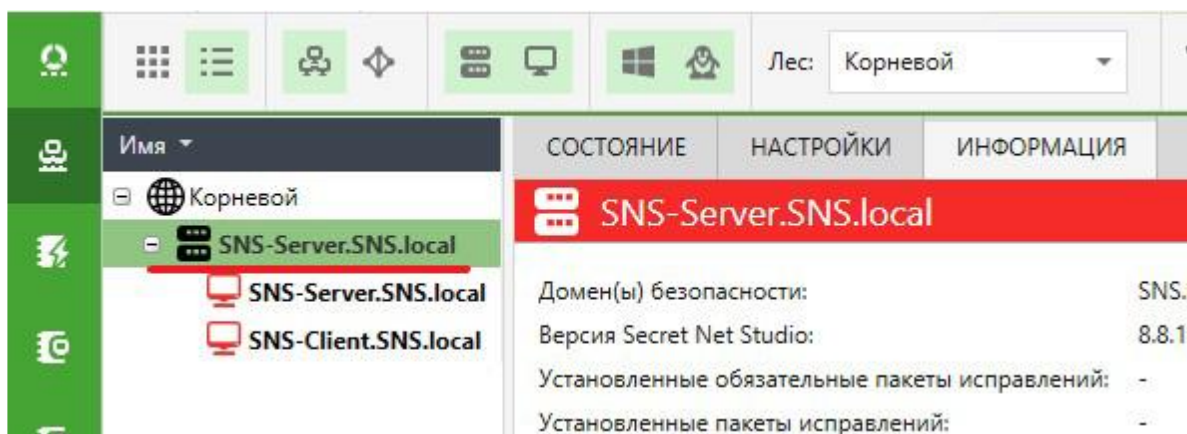


Рисунок 352 – Вкладка «Информация»

Запустите программу «Блокнот» (Win и R, введите notepad, нажмите Enter). В текстовый документ внесите названия групп, определенных на вкладке «Информация» (рисунок 353).

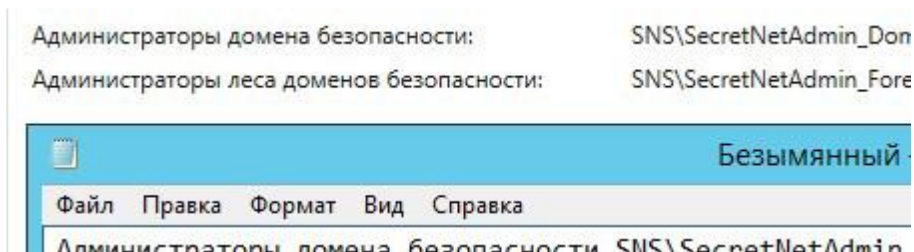


Рисунок 353 – Блокнот

Перейдите на вкладку «Настройки» и нажмите кнопку «Загрузить настройки». В структуре настроек выберите раздел «Параметры» и подраздел «Привилегии пользователей». Внесите в текстовый файл названия групп из списка групп (рисунок 354). Просмотрите действующие привилегии пользователей.

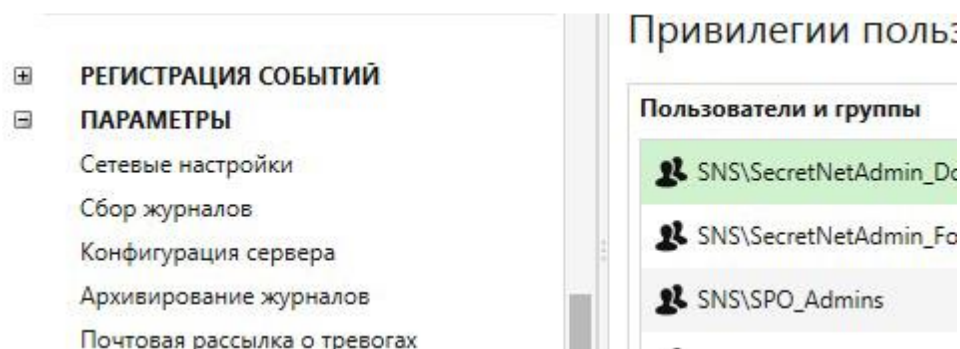


Рисунок 354 – Загрузка настроек

Запустите оснастку «Active Directory – Пользователи и компьютеры» (Win и R, введите dsa.msc, нажмите Enter), введите учетные данные user2. В дереве

иерархии нажмите правой клавишей мыши на домене SNS.local и в контекстном меню выберите пункт «Найти» (рисунок 355).

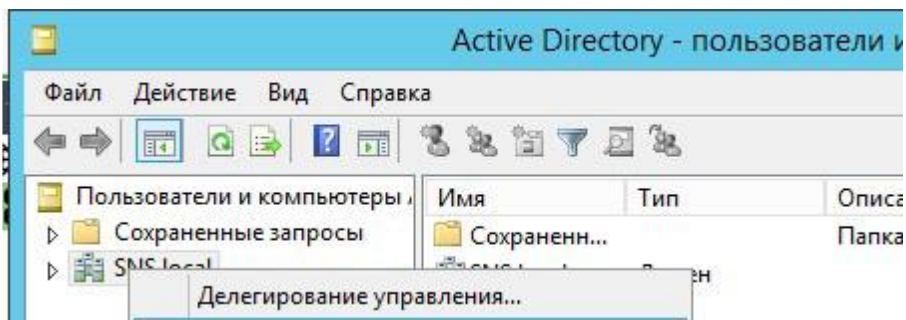


Рисунок 355 – Запуск «Active Directory – Пользователи и компьютеры»

Скопируйте название первой группы из текстового файла и нажмите «Найти» (рисунок 356).

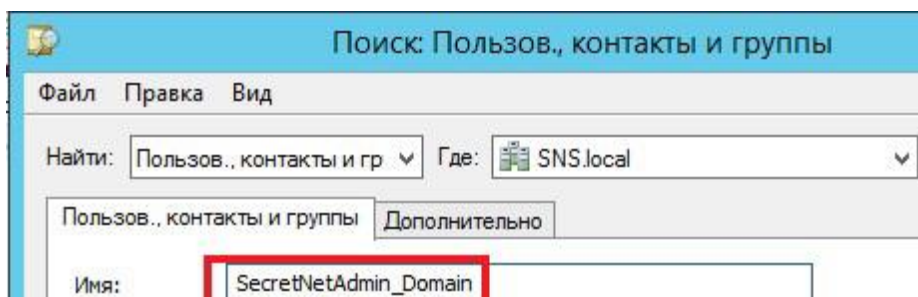


Рисунок 356 – Поиск группы

В окне «Результаты поиска» двойным нажатием левой кнопки мыши откройте свойства группы и перейти на вкладку «Члены группы» (рисунок 357).

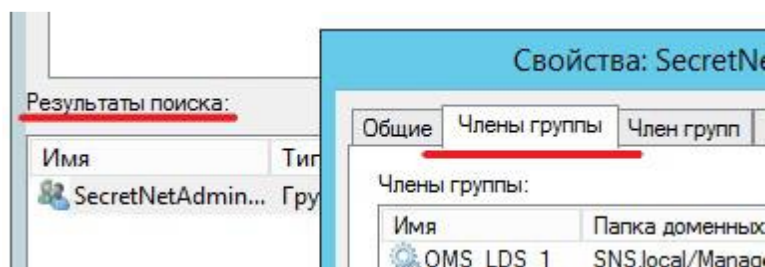


Рисунок 357 – Свойства группы

На вкладке «Члены группы» отражаются учетные записи работников, входящих в состав данной группы доступа, в соответствии с Регламентом... необходимо провести сверку состава участников группы с перечнем работников, назначенных на роли.

Закройте окно свойств группы. Проверьте состав групп, которым назначены привилегии. Определите, членом какой группы является текущий

пользователь user2. Закройте Блокнот и консоль «Active Directory – Пользователи и компьютеры».

7.20 Контроль установки СЗИ от НСД на СВТ

В программе «Центр управления» перейдите к панели «Развертывание», в верхней панели нажмите кнопку «... - Все» (рисунок 358).

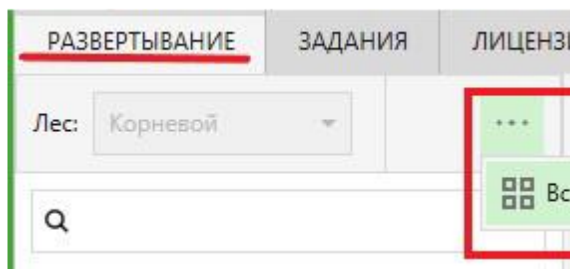


Рисунок 358 – Панель «Развертывание»

Установите курсор на главный в иерархии домен безопасности, нажмите правую кнопку мыши и выберите пункт «Сбросить с дочерними» (рисунок 359).

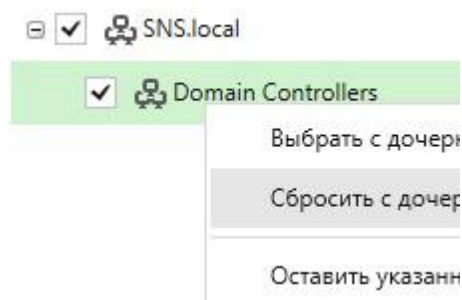


Рисунок 359 – Сброс с дочерними

В правой части окна отобразятся компьютеры, как с установленным клиентом SNS, так и без него. Нажмите кнопку «Экспорт» и сохраните файл на сетевой папке (\\VBOXSRV\Share).

Переключитесь к окну виртуальной машины SNS-Client, войдите под учетной записью user2. Откройте файл WorkstationsList.csv на сетевом диске.

Нажмите «Закрыть» в окне активации, закройте следующее всплывающее окно. Отобразится содержимое файла в табличном процессоре. Установите курсор в заполненную ячейку, нажмите сочетание клавиш Ctrl+A. На вкладке «Данные» в группе «Сортировка и фильтр» нажмите кнопку «Фильтр» (рисунок 360).

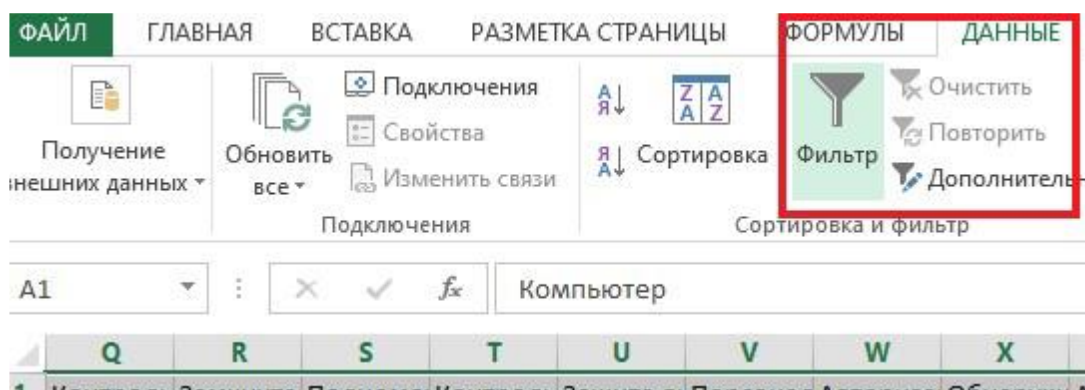


Рисунок 360 – Выбор пункта «Фильтр»

Раскройте фильтр в столбце «Версия», снимите флаг «-», нажмите «ОК» (рисунок 361). В таблице останутся только компьютеры с выбранной версией.

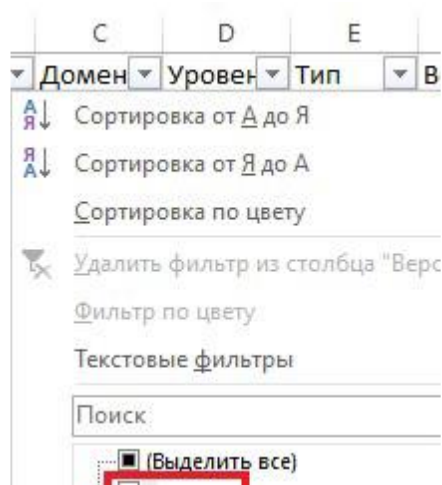


Рисунок 361 – Фильтр в столбце «Версия»

Раскройте фильтр «Версия», снимите флаг в поле с версией, установите флаг в поле «-», нажмите «ОК». Останутся строки с компьютерами, на которыми не установлено СЗИ от НСД. В соответствии с Регламентом следует определить компьютеры, на которых версия продукта отсутствует (-) или не актуальная. Закройте окно программы Excel. Завершите сеанс user2. Переключитесь к окну виртуальной машины SNS-Server.

7.21 Общие сведения о подсистеме регистрации событий

События, происходящие в системе, регистрируются в соответствующих журналах. Сведения о событиях сохраняются в виде записей, содержащих подробную информацию для анализа событий.

В журнале событий системы Secret Net Studio накапливается информация о событиях, регистрируемых на компьютере средствами системы защиты.

Сведения, содержащиеся в журнале Secret Net Studio, позволяют контролировать работу механизмов защиты (защита входа в систему, контроль аппаратной конфигурации, контроль целостности и др.). Состав регистрируемых событий определяется заданными параметрами действующей политики безопасности. В журнале Secret Net Studio используется такой же формат данных и состав полей записей, как и в штатных журналах ОС Windows.

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. К штатным журналам относятся:

- журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при работе приложений;
- системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;
- журнал безопасности – хранит информацию о доступе пользователей к компьютеру, применении групповых политик и изменении прав доступа, а также о событиях, связанных с использованием системных ресурсов.

Защитные подсистемы Secret Net Studio не осуществляют регистрацию событий в штатных журналах (за исключением журнала приложений, в котором могут регистрироваться некоторые специфические ошибки, связанные с функционированием ОС).

Программа управления при работе в локальном режиме позволяет осуществлять загрузку и просмотр записей штатных журналов, хранящихся на компьютере локально. При этом сохраняется возможность загрузки записей в другие средства работы с журналами ОС Windows.

При регистрации событий записи о них помещаются в соответствующие локальные журналы (штатные журналы ОС Windows и журнал Secret Net Studio) и хранятся на компьютере локально. Пока записи хранятся в локальном хранилище, их можно загрузить в программу управления в локальном режиме

или в другие программы, позволяющие осуществлять загрузку журналов (кроме журнала Secret Net Studio).

На клиентах в сетевом режиме функционирования локальные журналы хранятся в локальном хранилище до тех пор, пока они не будут переданы в централизованное хранилище на сервере безопасности. После передачи записей происходит очистка содержимого локальных журналов. В автономном режиме функционирования журналы могут храниться только в локальном хранилище. По мере регистрации событий записи журналов в локальном хранилище могут замещаться новыми записями. Перезапись информации в журналах осуществляется в соответствии с заданными параметрами регистрации событий.

В программе управления пользователь может выполнять экспорт записей журналов в файлы. Если пользователю предоставлена соответствующая привилегия, он может выполнять и очистку журналов.

7.22 Управление доступом к журналам регистрации событий

Настройка параметров журнала осуществляется на вкладке «Настройки» в разделе «Базовая защита» - «Журнал». Если параметры не настроены в политике сервера безопасности, то для каждого компьютера можно задавать свои локальные настройки как централизованно в программе «Центр управления», так и локально в программе «Локальный центр управления».

В рамках общей настройки параметров СЗИ от НСД выполнялась настройка параметров журнала. Для журнала был установлен максимальный размер и настроена политика перезаписи событий. Настроим привилегии пользователей на работу с журналом.

В программе Центр управления перейдите к панели «Компьютеры», включите отображение в виде таблицы, откройте свойства сервера безопасности, перейдите на вкладку «Настройки» и загрузите настройки политики сервера безопасности (рисунок 362).

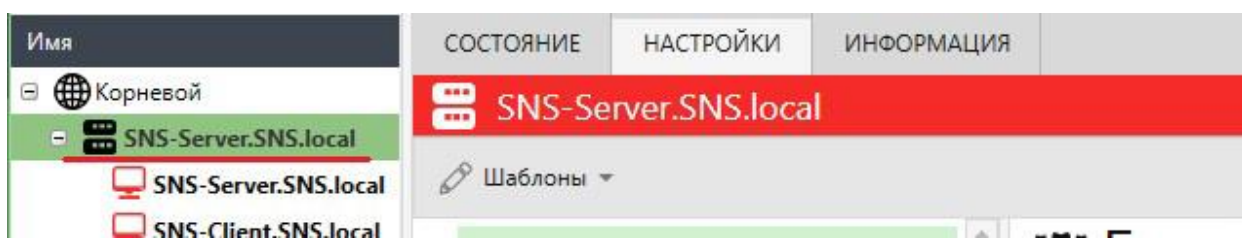


Рисунок 362 – Загрузка настроек политики сервера безопасности

В разделе политик «Базовая защита» выберите «Журнал». В настройках присутствуют два параметра «Учетные записи с привилегией просмотра журнала системы защиты» и «Учетных записи с привилегией управления журналом системы защиты» (рисунок 363).

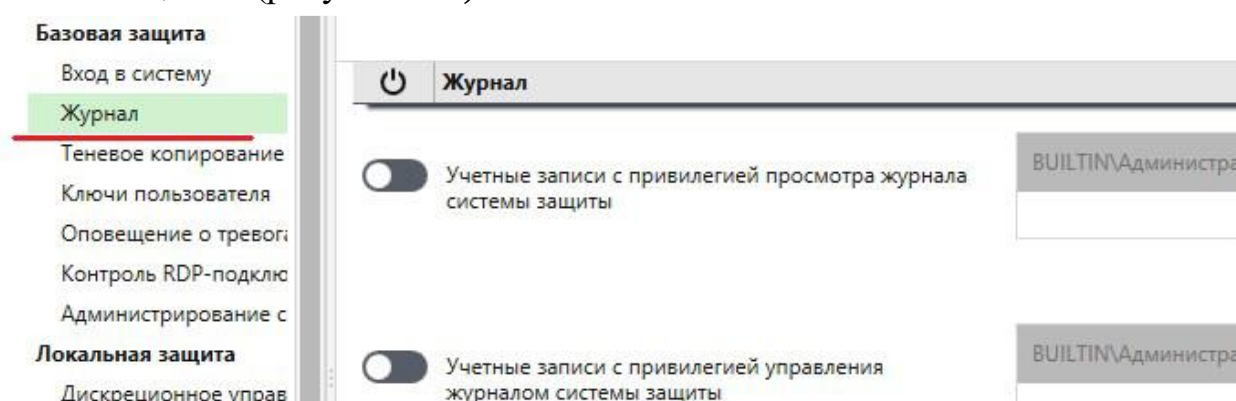


Рисунок 363 – Параметр «Журнал»

Первая привилегия позволяет только просматривать журнал СЗИ от НСД. Вторая привилегия – получать журнал, выполнять архивирование и очистку журнала. Сейчас привилегия есть только у локального администратора, т.к. использование параметра не включено в политику сервера безопасности.

Включите использование параметра «Учетные записи с привилегией просмотра журнала системы защиты» и нажмите кнопку «Добавить» (рисунок 364).

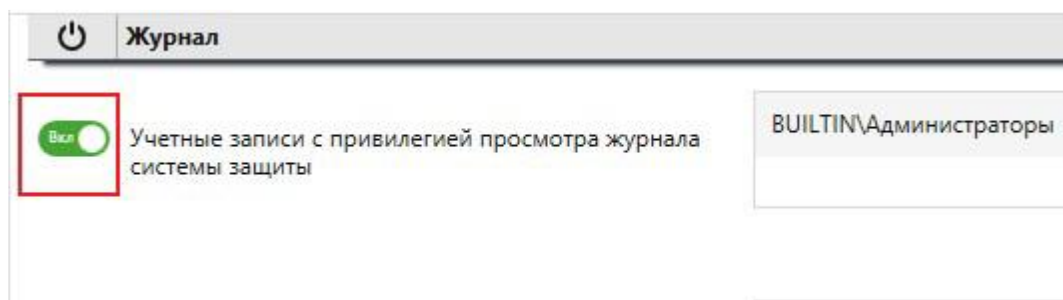


Рисунок 364 – Включение параметра «Учетные записи с привилегией просмотра журнала системы защиты»

В соответствии с Унифицированными конфигурациями привилегией должны обладать пользователи, входящие в группы SecretNetAdmin_Forest, SecretNetAdmin_Domain, SPOAdmins и Auditors. Добавим группы. В окне «Выбор:…» нажмите кнопку «Размещение» (рисунок 365), в окне «Размещение» раскройте узел «Весь каталог» и выберите SNS.local.

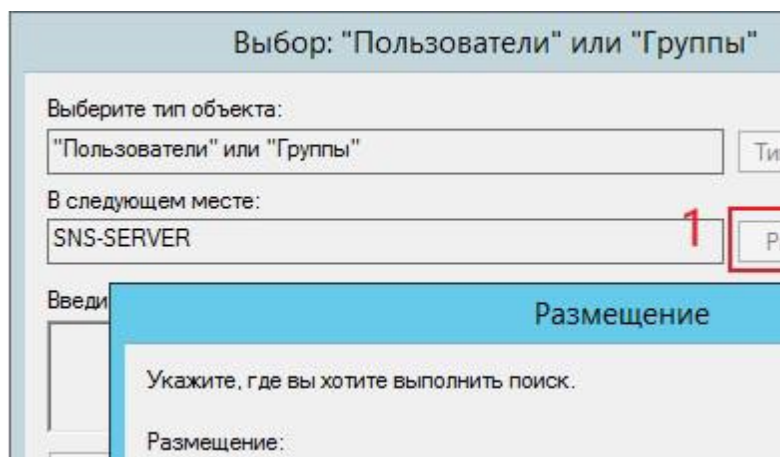


Рисунок 365 – Выбор группы «SNS.local»

Введите имена групп «SecretNetAdmin_Domain; SecretNetAdmin_Forest; SPOAdmins; Auditors», разделенных «;» (введите несколько первых букв названия и нажмите «Проверить имена», название группы допишется, поставьте «;» и вводите следующее) и нажмите кнопку «ОК» (рисунок 366).



Рисунок 366 – Добавление групп

Выберите группу локальных администраторов и нажмите кнопку «Удалить» (рисунок 367).

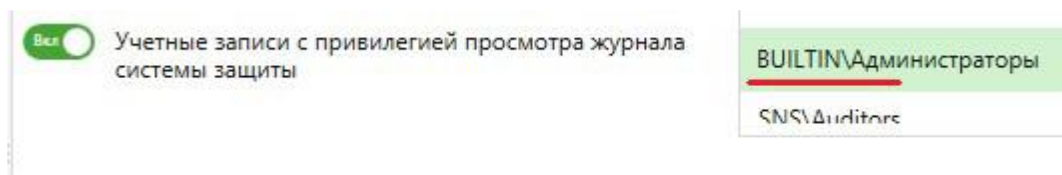


Рисунок 367 – Удаление группы локальных администраторов

Включите использование в политике сервера безопасности параметра «Учетные записи с привилегией управления журналом системы защиты». Добавьте группам SecretNetAdmin_Domain, SecretNetAdmin_Forest и Auditors привилегию управления журналом безопасности. Удалите группу локальных администраторов из списка групп с привилегией управления.

Нажмите кнопку «Применить» для сохранения настроек. В панели инструментов выберите «Команды» - «Применить групповые политики» (рисунок 368).

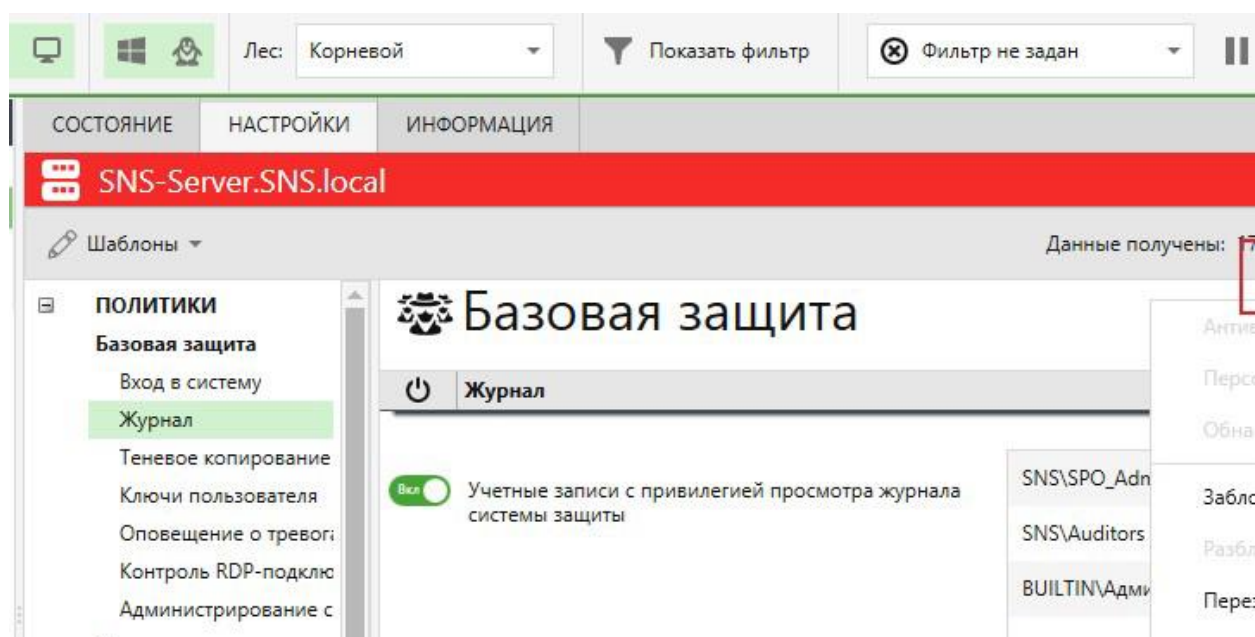


Рисунок 368 – Применение групповых политик

В списке компьютеров выберите компьютер SNS-Client. Загрузите настройки. Просмотрите привилегии пользователей и групп на действия с журналами и источник значения. В настройках должны быть добавлены группы и установлен источник SNS-Server.SNS.local (рисунок 369).

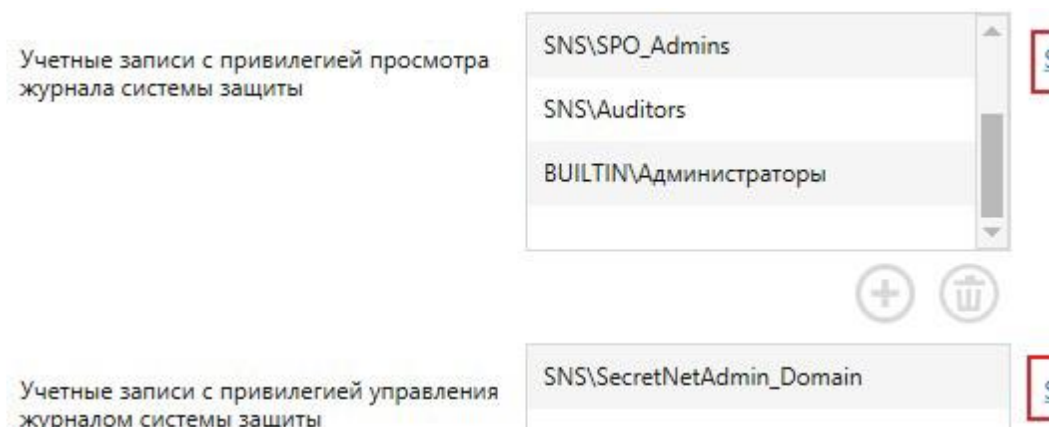


Рисунок 369 – Загрузка настроек

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью SNS\Администратор. Запустите программу «Локальный центр управления» (Пуск – Код безопасности – Локальный центр управления или через пиктограмму в трее). Перейдите к панели «Журналы» и загрузите журнал Secret Net Studio двойным кликом по названию журнала (рисунок 370).

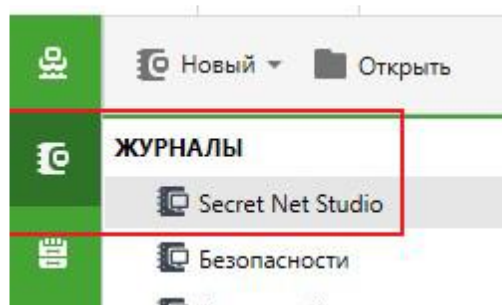


Рисунок 370 – Панель «Журналы»

Получение журнала будет доступно. В правой части окна нажмите кнопку «Экспорт журнала» (рисунок 371).

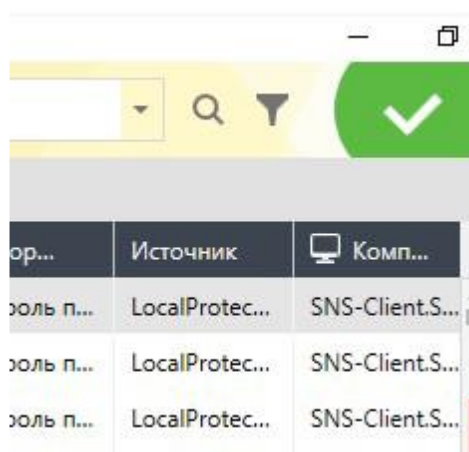


Рисунок 371 – Экспорт журнала

Установите переключатель в положение «Файл журнала Windows...» (рисунок 372). Станет доступен флаг «Удалять записи после экспорта». Не устанавливайте флаг очистки, нажмите кнопку «Экспортировать». Действие будет выполнено.

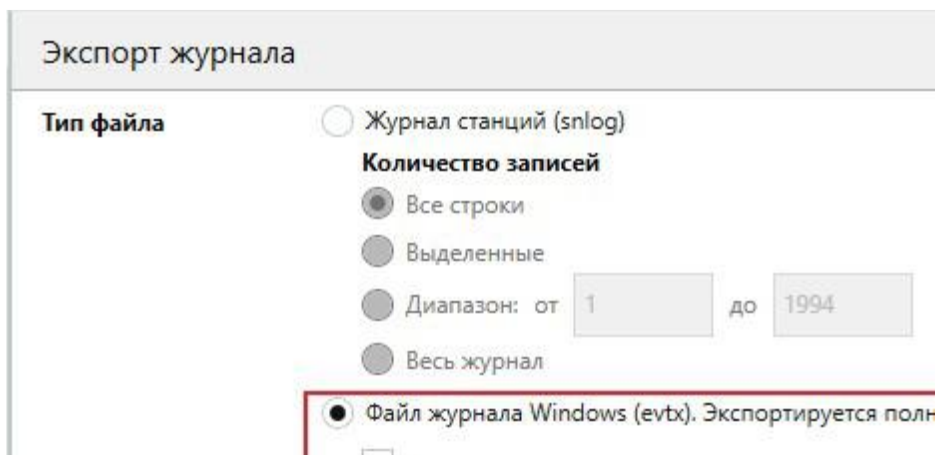


Рисунок 372 – Экспорт «Файл журнала Windows...»

Завершите сеанс Администратора. Войдите под учетной записью локального администратора SNS-Client\admin с паролем P@ssw0rd (рисунок 373).

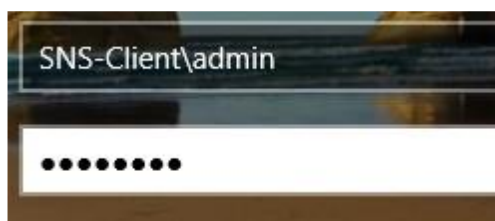


Рисунок 373 – Вход под учетной записью локального администратора SNS-Client\admin

Запустите программу «Локальный центр управления», перейдите к панели «Журналы». Журнал Secret Net Studio будет недоступен для просмотра (рисунок 374).

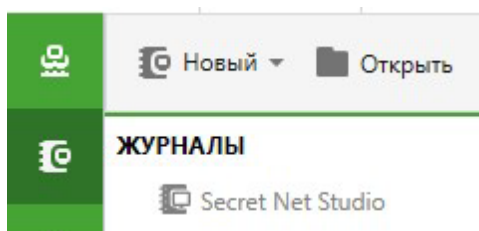


Рисунок 374 – Панель «Журналы» недоступен для просмотра

Завершите сеанс локального администратора. Войдите под учетной записью user1@SNS. Запустите программу Локальный центр управления. Загрузите журнал Secret Net Studio. Журнал будет доступен. Нажмите кнопку «Экспорт». Установите флаг «Файл журнала Windows...» (рисунок 375). Флаг «Удалять записи после экспорта» будет недоступен. Пользователь user1 является членом группы SPOAdmins, у которой отсутствует привилегия управления журналом, включающая действия по очистке журнала.

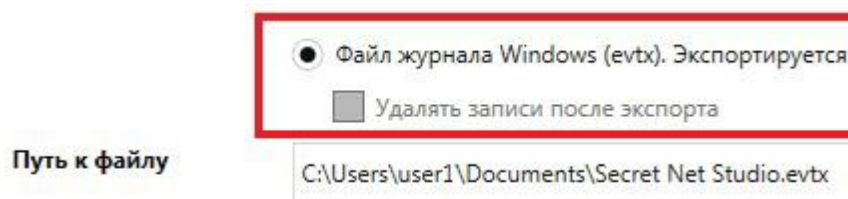


Рисунок 375 – Экспорт журнала под учетной записью «user1@SNS»

Завершите сеанс пользователя user1. Войдите под учетной записью user2. Запустите программу Локальный центр управления. Загрузите журнал Secret Net Studio. Журнал будет доступен. Нажмите кнопку «Экспорт». Установите флаг «Файл журнала Windows...», флаг «Удалять записи после экспорта» будет доступен (рисунок 376). Пользователь user2 является членом группы Auditors, у которых есть привилегия управления журналом.

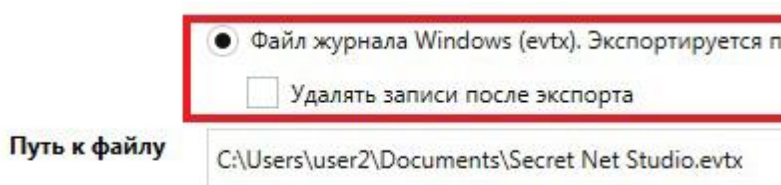


Рисунок 376 – Экспорт журнала под учетной записью «user2»

Завершите сеанс пользователя user2.

7.23 Настройка регистрации событий

Переключитесь к окну виртуальной машины SNS-Server. В программе «Центр управления» в панели «Компьютеры» выберите сервер безопасности, на вкладке «Настройки» выберите группу настроек «Регистрация событий» (рисунок 377).

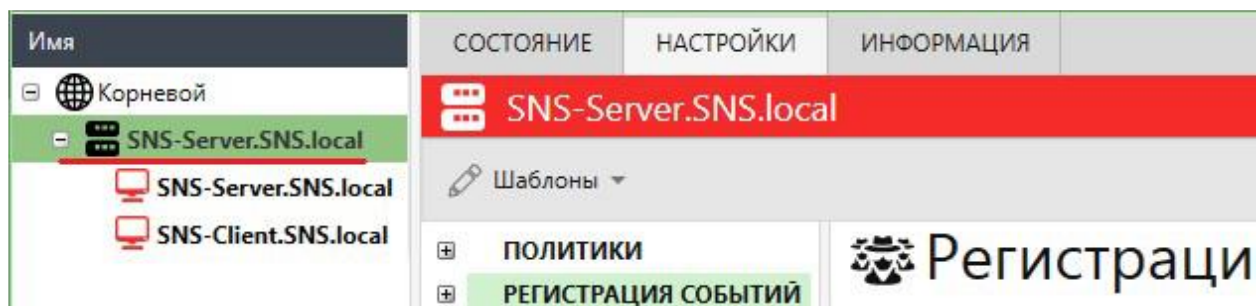


Рисунок 377 – Группа настроек «Регистрация событий»

В этом разделе настроек указываются события, которые заносятся в журнал СЗИ от НСД.

События сгруппированы по разделам. У каждого события один параметр — включен (флаг установлен) или отключен (флаг снят). Если регистрация события включена, то запись о событии заносится в журнал СЗИ от НСД. При настройке регистрации событий в политике сервера безопасности также присутствует параметр включения настройки в политику сервера безопасности или применение локального значения параметрами.

Настройте регистрацию событий в соответствии с Унифицированными конфигурациями.

Выберите раздел «Администрирование». Включите использование всех параметров в политике сервера безопасности (переведите переключатели в положение «Вкл»). Станет доступно изменение значений параметров. Все события должны быть включены (установлены флаги) (рисунок 378). Нажмите кнопку «Применить» для сохранения настроек.

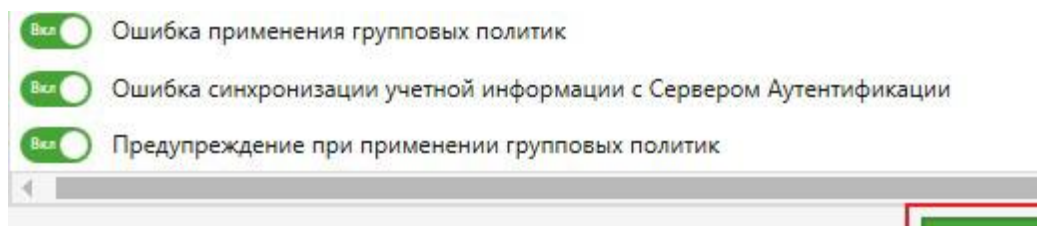


Рисунок 378 – Включение всех событий

Выберите раздел «Администрирование системы защиты». Включите использование всех параметров в политике сервера безопасности. Должна быть включена регистрация (установлены флаги) следующих событий:

- запрет несанкционированного вызова;

- попытка модификации или отключения защитного механизма;
- попытка модификации или удаления параметров системы защиты.

Регистрация события «Попытка доступа к защищенному процессу» должна быть отключена (рисунок 379).



Рисунок 379 – Раздел «Администрирование системы защиты»

Регистрация событий в разделе «Антивирус» не требуется, поскольку компонент защиты не используется, оставьте параметры без изменения.

Выберите раздел «Вход в систему». Включите регистрацию всех событий и использование параметров в политике сервера безопасности.

В разделе «Дискреционное управление доступом» настройка регистрации событий не требуется, оставьте значения параметров по умолчанию. Выберите раздел «Замкнутая программная среда». Все события должны быть включены и использоваться в политике сервера безопасности.

Выберите раздел «Затирание данных». Включите использование всех параметров в политике сервера безопасности. Регистрация всех событий должна быть включена, за исключением событий:

- для файла включены потоки целостности ReFS;
- добавление файлового объекта в очередь отложенной обработки;
- завершение удаления остаточных данных на локальном диске;
- начало удаления остаточных данных на локальном диске.

Отключите регистрацию этих событий, если они не выключены по умолчанию.

Выберите раздел «Защита диска и шифрование данных». Включите использование всех параметров в политике сервера безопасности. Все события должны быть отключены, за исключением событий «Отключена защита для диска» и «Установлена защита для диска». Выберите раздел «Ключи

пользователя». Все события должны быть включены и использоваться в политике безопасности сервера.

В разделе «Контроль печати» настройка регистрации событий не требуется, оставьте настройки по умолчанию.

Выберите раздел «Контроль приложений». Включите использование всех параметров в политике сервера безопасности. Регистрация всех событий должна быть отключена, за исключением событий «Запуск процесса», «Завершение процесса», «Запрет доступа к буферу обмена».

В разделах «Контроль устройств» и «Контроль целостности» должно быть включено использование всех параметров в политике сервера безопасности, регистрация всех событий должна быть включена.

В разделе «Обнаружение вторжений» настройка регистрации событий не требуется, оставьте параметры по умолчанию.

В разделах «Общие события» и «Паспорт ПО» все события должны быть включены и использоваться в политике сервера безопасности.

В разделе «Полномочное управление доступом» и «Теневое копирование» настройка регистрации событий не требуется, оставьте значения по умолчанию.

В разделе «ЦУ КЦ-ЗПС» все события должны быть включены и использоваться в политике сервера безопасности.

После настройки регистрации событий нажмите кнопку «Применить» для сохранения изменений.

Выберите команду «Применить групповые политики».

В списке компьютеров выберите компьютер SNS-Client и проверьте применение настроек регистрации событий. Затем проверьте настройки регистрации событий на компьютере SNSServer.

7.24 Работа с журналом регистрации событий

В базе данных сервера безопасности накапливаются следующие журналы:

- журнал событий тревоги, объединяющий все записи о событиях тревоги со всех управляемых компьютеров;

- журнал событий, объединяющий журнал Secret Net Studio и штатные журналы ОС Windows со всех управляемых компьютеров;
- журнал сервера безопасности.

Журнал событий тревоги предназначен для централизованного хранения информации о событиях тревоги, произошедших на защищаемых компьютерах. Событиями тревоги считаются события, которые регистрируются локально в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип «Аудит отказов» или «Ошибки». Журнал событий тревоги формируется из уведомлений о событиях тревоги, направляемых серверу безопасности. Работа с журналами тревоги рассматривается в теме по оперативному управлению.

Журнал станций предназначен для централизованного хранения содержимого локальных журналов, поступивших с защищаемых компьютеров. К локальным журналам относятся журнал Secret Net Studio и штатные журналы ОС Windows (журнал приложений, системный журнал и журнал безопасности). Передача локальных журналов на сервер осуществляется в соответствии с параметрами сервера (при заполнении 80% журнала). При регистрации событий записи о них помещаются в соответствующие локальные журналы и хранятся на защищаемом компьютере, для доступа к ним надо использовать программу «Локальный центр управления» на самом компьютере. Локальные журналы хранятся до тех пор, пока они не будут переданы в централизованное хранилище на сервере безопасности. После передачи записей происходит очистка содержимого локальных журналов.

Централизованное хранилище журналов размещается в базе данных сервера безопасности. Запуск процесса передачи локальных журналов с защищаемых компьютеров осуществляется автоматически в соответствии с настройками, либо вручную по команде из программы «Центр управления». Удаление записей журналов из централизованного хранилища происходит при архивировании журналов.

Архивируются все записи журналов, имеющиеся в БД сервера безопасности на момент начала процесса архивирования. Записи, помещенные в

архив, удаляются из централизованного хранилища. Запуск процесса архивирования осуществляется автоматически в соответствии с настройками, либо по команде.

В программе «Центр управления» перейдите к панели «Компьютеры», выберите компьютер SNS-Client, в контекстном меню компьютера выберите «Журналы» - «Собрать журналы с компьютера» - «Secret Net Studio» (рисунок 380).

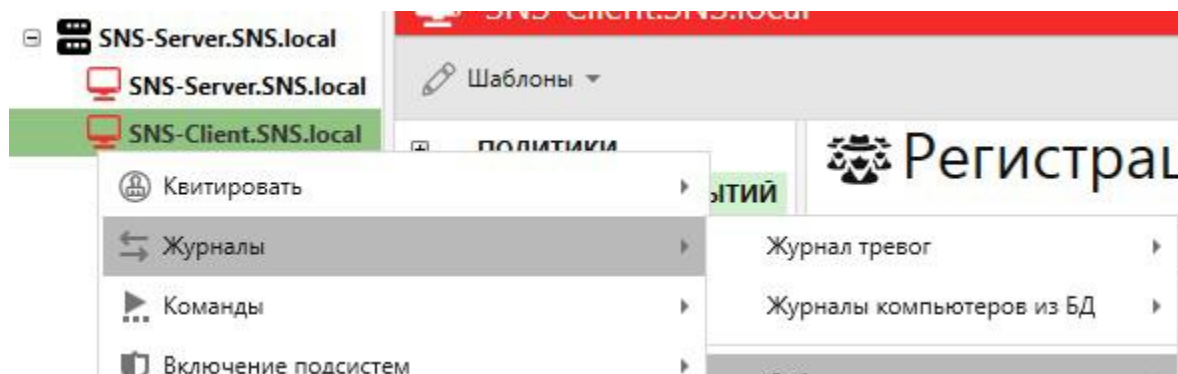


Рисунок 380 – Сбор журнала «Secret Net Studio»

В панели событий отобразится информация о запуске сбора журналов. После завершения сбора появится сообщение об успешном выполнении команды (рисунок 381).

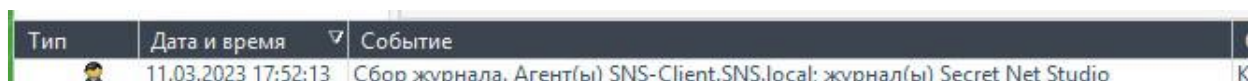


Рисунок 381 – Сообщение об успешном выполнении команды

Переключитесь к окну виртуальной машины SNS-Client. Войдите под учетной записью пользователя user2 (член группы Auditors). Запустите программу «Локальный центр управления», перейдите к панели «Журналы», загрузите журнал Secret Net Studio. В журнале будут содержаться события, связанные с контролем приложений, целостности и входа выхода, связанные с входом пользователя. Выберите самое раннее событие в журнале и откройте детальную информацию о событии (Ctrl и D или двойной клик по событию). В окне детальной информации будет указано, что произошла очистка журнала и указано место сохранения архивной копии на локальном компьютере (рисунок 382).

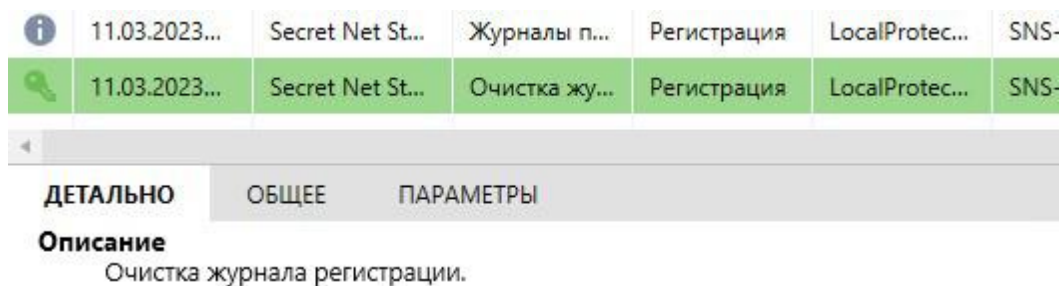


Рисунок 382 – Очистка журнала регистрации

Выберите следующее по времени событие с пиктограммой «i», в окне детальной информации будет указано, что журналы переданы на сервер безопасности (рисунок 383).

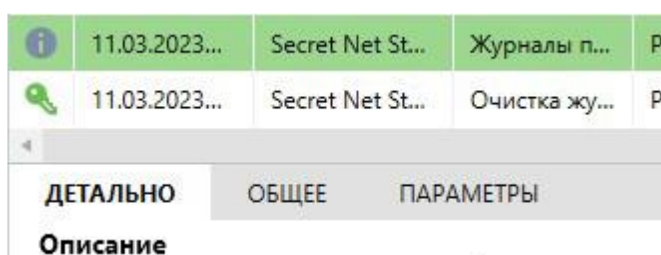


Рисунок 383 – Журналы переданы на сервер безопасности

Переключитесь к окну виртуальной машины SNS-Server. В программе «Центр управления» перейдите к панели «Журналы станций», нажмите кнопку «Новый» (рисунок 384).

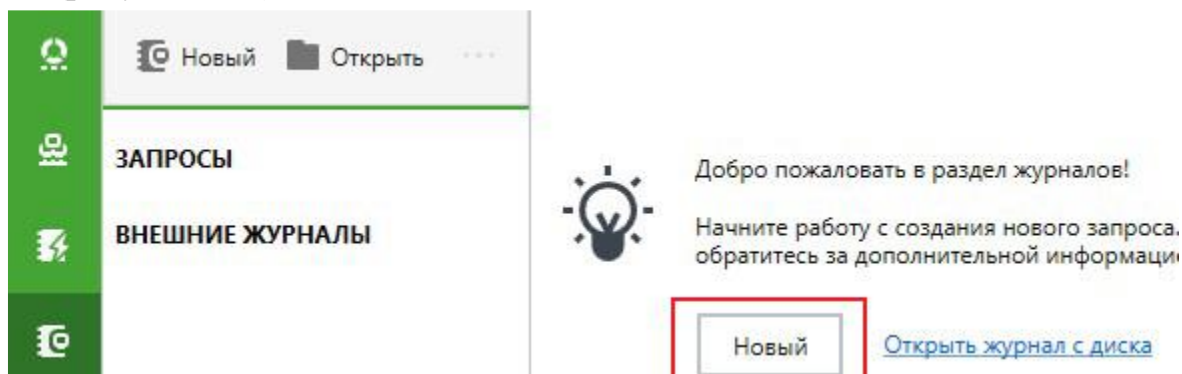


Рисунок 384 – Панель «Журналы станций»

Откроется окно «Конструктор запроса». В поле «Журналы» снимите флаги с журналов Windows (Приложений, Безопасности, Системный) и нажмите кнопку «Выполнить запрос к БД» (рисунок 385).

КОНСТРУКТОР ЗАПРОСА Новый запрос

Журналы

☒ Secret Net Studio ☐ Приложений

☐ Безопасности ☐ Системный

Период времени

☒ За все время

☐ За последний час

☐ За последние 24 часа

☐ За 7 дней

☐ За 30 дней

☐ Задать интервал: 10.03.2023 17:58:45 -

Количество последних событий

☒ Все события

☐ Указать количество: 100

БД сервера

SNS-Server.SNS.local

Рисунок 385 – Окно «Конструктор запроса»

Загрузится журнал из базы данных сервера безопасности. Общее количество загруженных записей отобразится внизу списка событий (рисунок 386).

	11.03.2023...	Secre
	11.03.2023...	...

1/246

Рисунок 386 – Журнал из базы данных сервера безопасности

В окне конструктора запроса появятся элементы управления правилами запроса. Нажмите кнопку «Добавить правило» и в выпадающем списке выберите «Пользователь» (рисунок 387).

КОНСТРУКТОР ЗАПРОСА Новый запрос

Журналы

☒ Secret Net Studio ☐ Приложений

☐ Безопасности ☐ Системный

Правила запроса

+ Добавить правило

Агент

Тип

Компьютер

Домен

Количество последних событий

☒ Все события

☐ Указать количество: 100

Рисунок 387 – Добавление правила

В окне конструктора запроса появится новое правило. Раскройте список «Условие» и установите флаг в строке user3 (рисунок 388). Нажмите кнопку «Применить запрос локально» для выборки из загруженного списка событий только тех, которые отвечают указанному правилу.

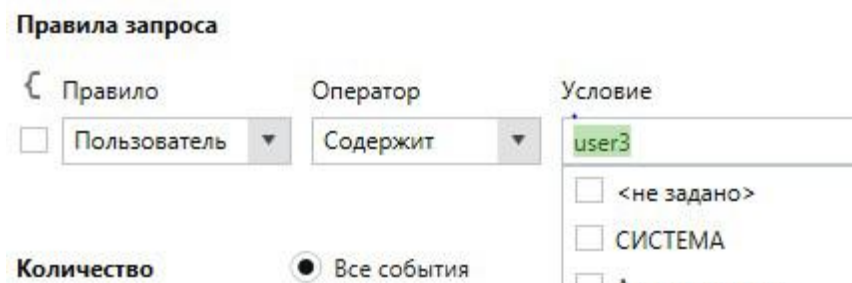


Рисунок 388 – Настройка правила запроса

Закройте окно конструктора запроса, нажав на кнопку «Запрос» в правой части окна программы (рисунок 389).

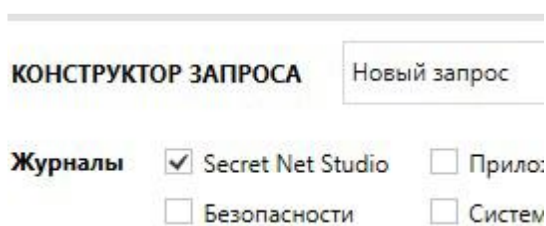


Рисунок 389 – Запрос событий

В нижней части окна отобразится количество событий, удовлетворяющих введенному правилу, из общего числа загруженных событий (рисунок 390).

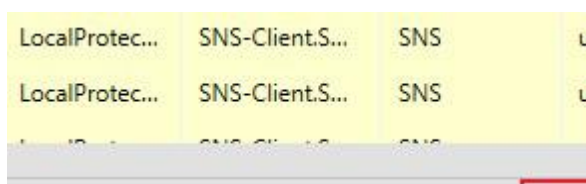


Рисунок 390 – Запрошенные события

В рабочей области отображаются события. В режиме «События» выводится список загруженных записей журналов в табличной форме. Это основной и наиболее функциональный режим для просмотра и управления записями (рисунок 391).

СОБЫТИЯ		УГРОЗЫ	
⚙	Дата	Журнал	Событие
🔑	02.03.2023...	Secret Net St...	Запуск про...
🔑	02.03.2023...	Secret Net St...	Запуск про...

Рисунок 391 – Режим для просмотра и управления записями

Нажмите правой кнопкой мыши на первом событии в таблице. Откроется контекстное меню (рисунок 392). С помощью контекстного меню записей выполняются необходимые действия: переход к компьютеру (автоматическое переключение к панели «Компьютеры» с выбором компьютера в структуре), копирование, печать, экспорт и др. Флаг «Раскраска событий» позволяет включать и отключать выделение событий различных категорий цветом.

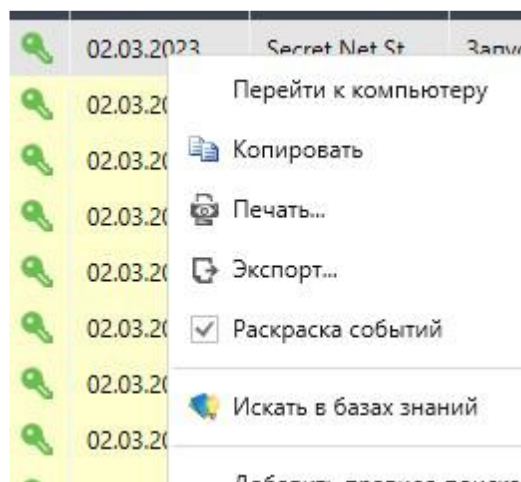


Рисунок 392 – Контекстное меню

Настройка раскраски событий осуществляется в меню настроек программы «Центр управления». Нажмите кнопку «Настройки» в левом нижнем углу программы и выберите ссылку «Настройки центра управления» (рисунок 393).

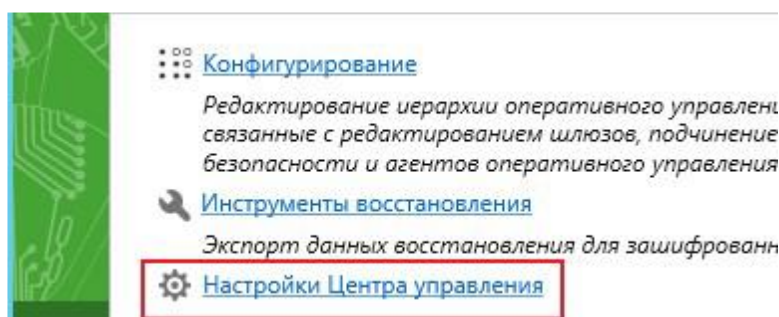


Рисунок 393 – Настройки центра управления

В окне настроек выберите раздел «Раскраска событий», выберите категорию «Контроль целостности» и нажмите кнопку «Редактировать» (рисунок 394).

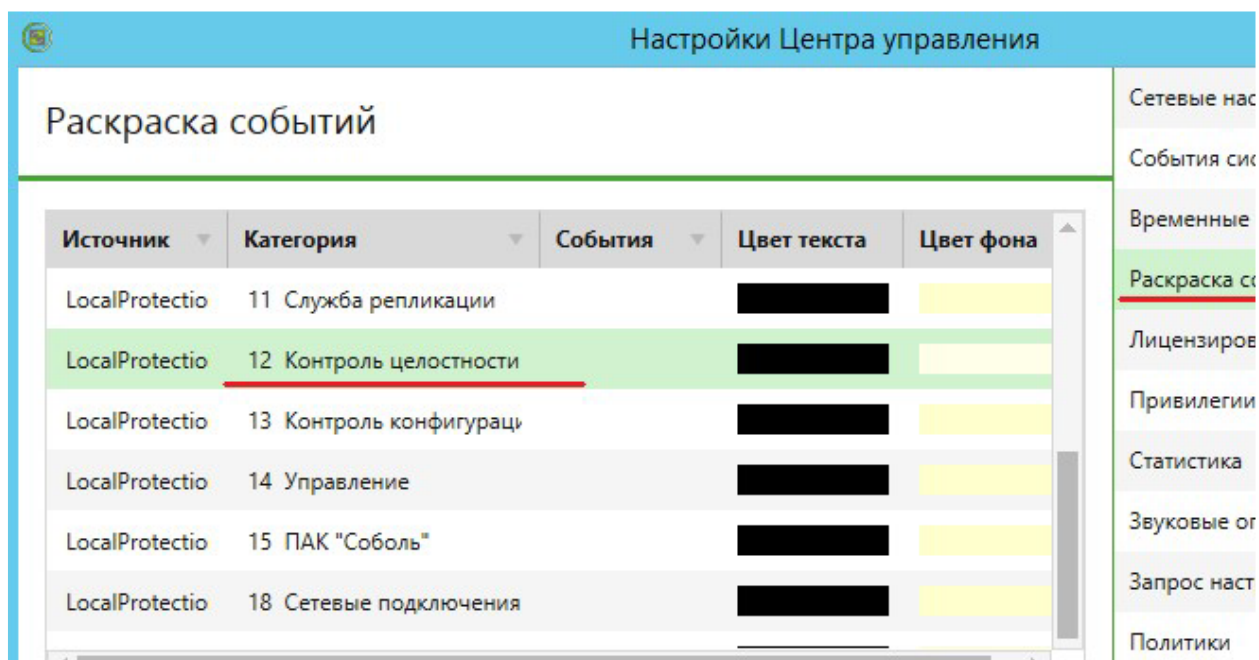


Рисунок 394 – Настройки центра управления

Откроется окно редактирования раскраски, в котором можно настроить определенный цвет событий, которые, например, необходимо отслеживать при анализе журналов. Раскройте список «События» и установите флаг события «Нарушение целостности ресурса» (рисунок 395). Сверните список, в поле «Раскраска событий» раскройте список «Цвет фона» и настройте любой цвет. Нажмите на кнопку «Применить».

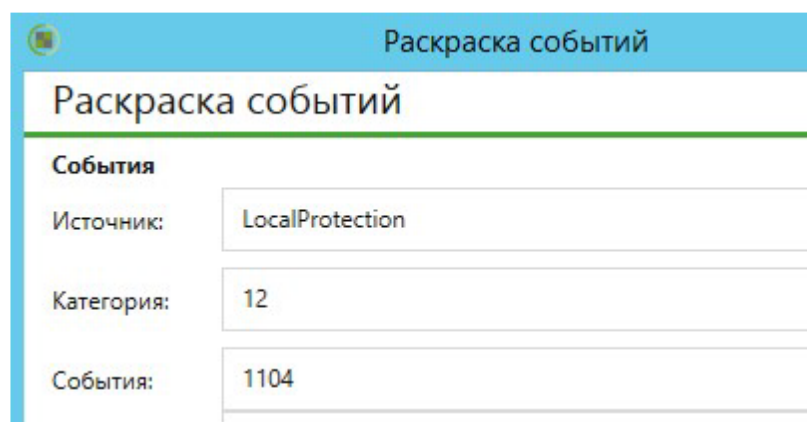


Рисунок 395 – Раскраска событий

Выберите раздел настроек «События системы». В ней выполняются настройки панели событий (отображение текущих событий в нижней части окна программы). Для выделения событий также доступна настройка раскраски (рисунок 396).

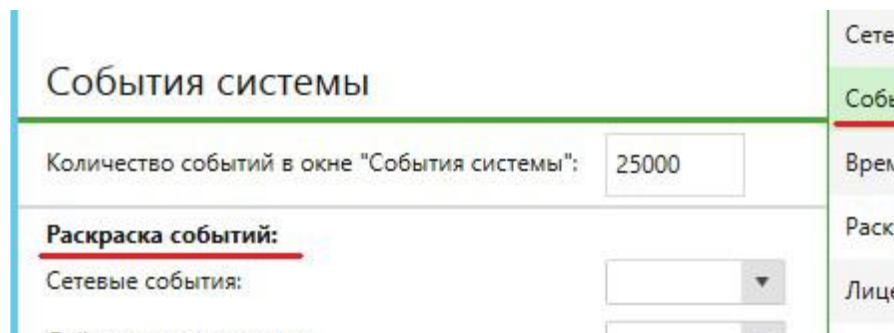


Рисунок 396 – События системы

Выберите раздел настроек «Привилегии». В окне отобразится список привилегий текущего пользователя. Нажмите кнопку «Сохранить», затем кнопку «Закрыть» возврата к главному окну программы.

Пролистайте список событий в журнале. Найдите события, для которых были заданы отдельные настройки цвета (если такие настройки выполнялись и событие присутствует в списке).

Кроме выделения цветом каждому событию соответствует определенная пиктограмма, например пиктограмма замка соответствует событию тревоги.

Перейдите на вкладку «Угрозы» (рисунок 397), в ней выводится список событий угроз, полученных в результате анализа загруженных записей. События угроз представляют собой сжатые или разъясняющие сведения о зарегистрированных событиях. Режим предназначен для представления администратору или аудитору наиболее важной для них информации из журналов.

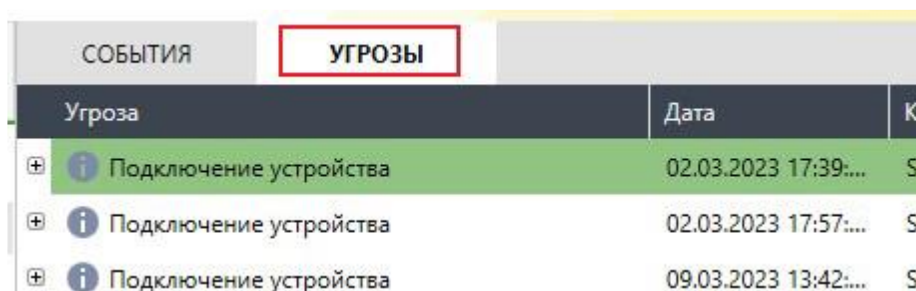


Рисунок 397 – Вкладка «Угрозы»

Под списком угроз также содержится счетчик с отображением текущей выбранной в списке угрозы и общего количества обнаруженных угроз. Также есть кнопка просмотра детальной информации о событии. Выберите в списке одну из угроз, связанной с контролем целостности ресурсов, раскройте подробности, нажав на кнопку + в начале строки (рисунок 398).



Рисунок 398 – Вкладка «Угрозы»

Раскроется описание события журнала, на основе анализа которого было сформировано сообщение об угрозе. Откройте окно детальной информации (Ctrl и D или в контекстном меню).

При выборе в списке угроз строки с названием угрозы, в окне детальной информации появится краткое описание угрозы, при выборе события, на основании которого детектирована угроза, в окне отобразится информация о событии (рисунок 399).

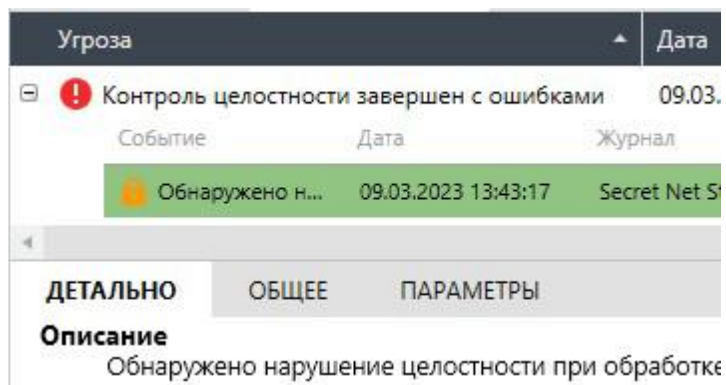


Рисунок 399 – Информация о событии

Закройте окно отображения детальной информации. Выборка угроз формируется по всем событиям журнала в базе данных сервера безопасности, а не только по результатам фильтрации на вкладке «События». К угрозам также можно применять фильтрацию. Нажмите на кнопку «Запрос» в правой части окна программы (рисунок 400).

СОБЫТИЯ		УГРОЗЫ	
Угроза		Дата	Компьютер
+	❗ Контроль целостности завершен с ошибками	09.03.2023 13:43:...	SNS-Client.S
+	❗ Контроль целостности завершен с ошибками	09.03.2023 14:25:...	SNS-Client.S

Рисунок 400 – Открытие поиска угроз

Откроется окно «Поиск угроз». В списке содержится набор предустановленных правил поиска угроз в списке событий. По умолчанию флаги всех правил установлены, соответственно в угрозах отображаются все события, соответствующие этим правилам. Снимите флаг «Правила поиска», снимутся флаги для всех правил (рисунок 401).

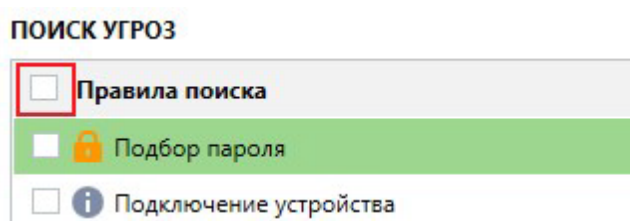


Рисунок 401 – Поиск угроз

Выберите правило «Контроль целостности завершен с ошибками» и нажмите кнопку «Редактировать правило угрозы» (рисунок 402).

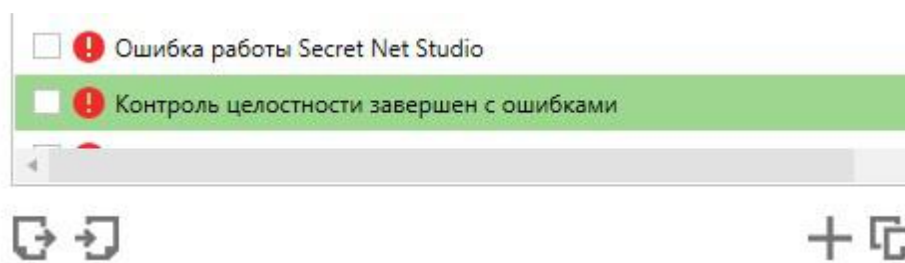


Рисунок 402 – Выбор правила поиска угроз

Откроется окно редактирования правила. В нем указаны условия, при совпадении которых событие идентифицируется как угроза. В данном случае это событие с типом отказа и кодом 1102 (Обнаружено нарушение целостности при обработке задания). Существует возможность изменения условий, добавления новых условий, удаления существующих (рисунок 403). Не вносите изменений в правило, нажмите кнопку «Далее». На следующей вкладке указываются дополнительные параметры. Нажмите кнопку «Отмена».

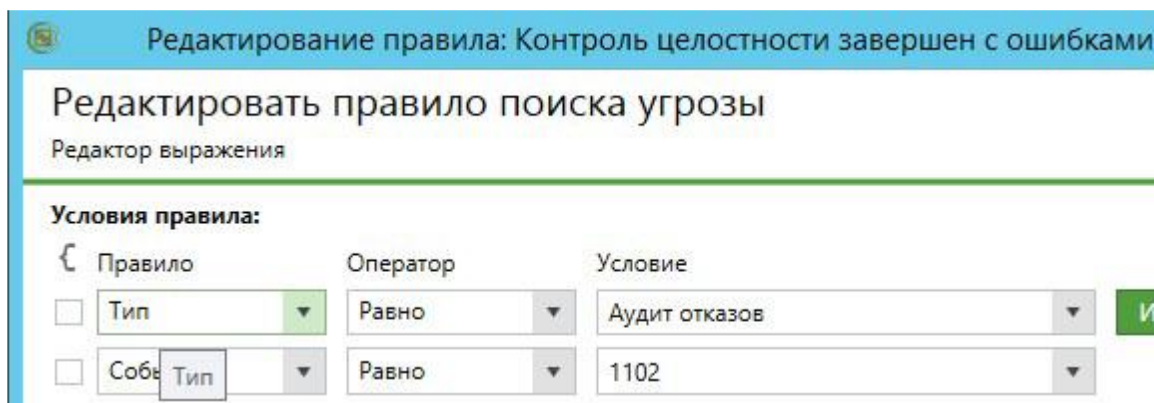


Рисунок 403 – Редактирование правил поиска угрозы

Помимо редактирования существующих правил можно создавать собственные правила поиска угроз. Внизу окна правил поиска нажмите кнопку «Добавить правило поиска угрозы» (рисунок 404).

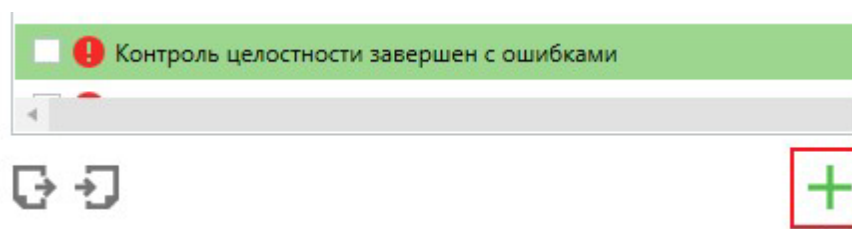


Рисунок 404 – Добавление правила поиска угроз

Откроется окно создания правила. Нажмите кнопку «Добавить правило» и выберите в списке стоку «Тип» (рисунок 405).

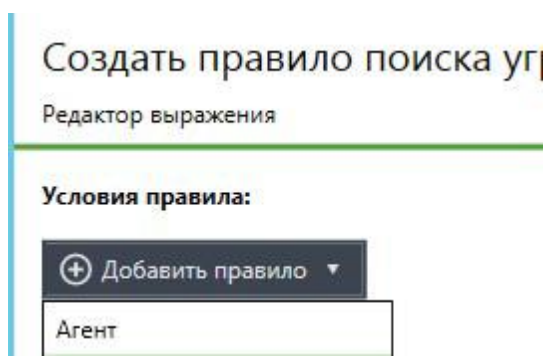


Рисунок 405 – Окно создания правила поиска угроз

В выпадающем списке «Условие» установите флаг «Аудит успехов» и нажмите кнопку «+» для добавления следующего условия (рисунок 406).

Правило	Оператор	Условие
Тип	Равно	Аудит успехов
		Аудит отказов
		Аудит успехов

Рисунок 406 – Добавление условия поиска угроз

В списке выберите «Событие». Появится новая строка условия. В поле «Условие» введите код 1025 и нажмите «Далее» (рисунок 407).

Правило	Оператор	Условие
Тип	Равно	Аудит успехов

Рисунок 407 – Ввод кода 1025 в поле «Условие»

На следующем шаге в поле «Журналы» оставьте только флаг «Secret Net Studio», в поле «Название правила» выберите пиктограмму, введите название и описание (рисунок 408). Нажмите кнопку «Готово».

Создать правило поиска угрозы
Дополнительные параметры

Журналы: ☒ Secret Net Studio ☐ Безопасности ☐ Приложений ☐ Сис

Количество повторов события: 1 раз за 60 сек
☐ фиксировать одну тревогу за сессию пользователя

Название правила: очистка журнала

Описание: тест угроз

Рисунок 408 – Дополнительные параметры добавления правила поиска угроз

В списке правил добавится новое правило. Нажмите кнопку «Поиск» внизу окна. В списке угроз останутся только угрозы с названием, введенным при создании правила. Выберите одну угрозу и откройте окно детальной информации. В окне отобразится название угрозы и описание, указанное при создании правила (рисунок 409).

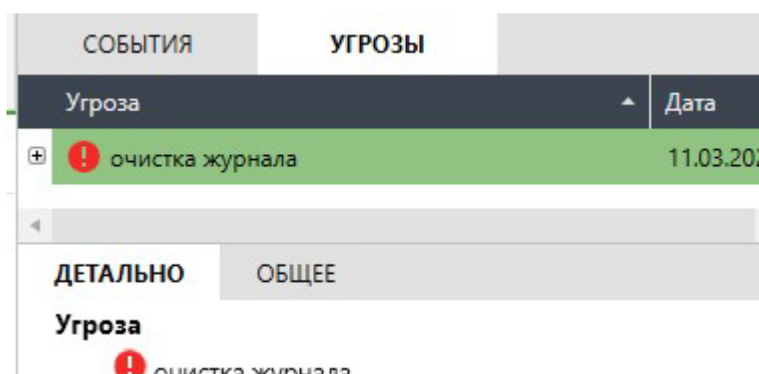


Рисунок 409 – Окно детальной информации

В окне выбора правил выберите созданное правило и нажмите кнопку «Удалить» (рисунок 410). Подтвердите удаление правила.

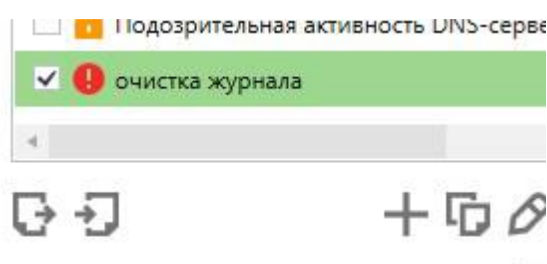


Рисунок 410 – Удаление правила

Установите флаг правила «Контроль целостности завершен с ошибками» и нажмите кнопку «Поиск». В окне угроз отобразятся только угрозы, связанные с событиями контроля целостности. Найдите событие, приведшее к блокировке компьютера SNS-Client. Определите дату и время появления события (рисунок 411).

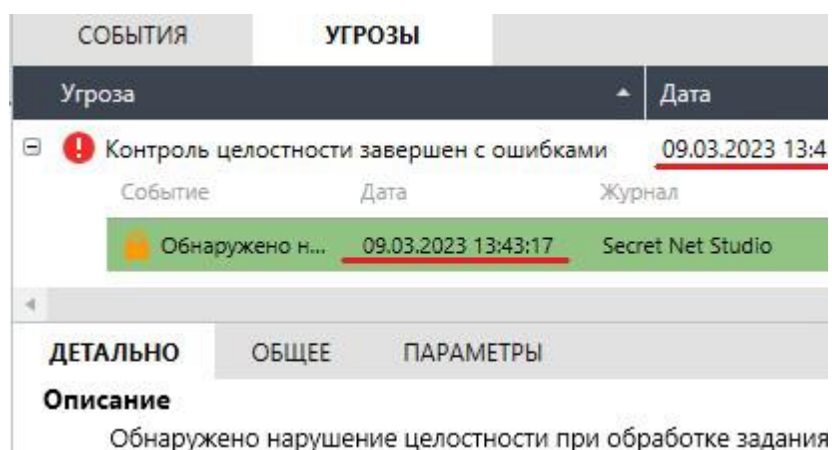


Рисунок 411 – Поиск события

Вернитесь к вкладке «События». Для поиска событий в списке можно воспользоваться фильтрацией. В правой части окна нажмите кнопку «Запрос». Откроется окно «Конструктор фильтра».

В конструкторе уже содержится правило, определяющее отображение событий только для пользователя user3. Удалите правило, нажав кнопку X в конце строки правила (рисунок 412).



Рисунок 412 – Удаление правила только для пользователя «user3»

Добавьте правила фильтрации для поиска событий, связанных с угрозой. Добавьте правило «Дата». В поле «Правило» в списке «Оператор» установите значение «Интервал», а в списке «Условие» выберите «Задать интервал» и установите интервал времени, предшествовавший появлению события нарушения целостности (рисунок 413)

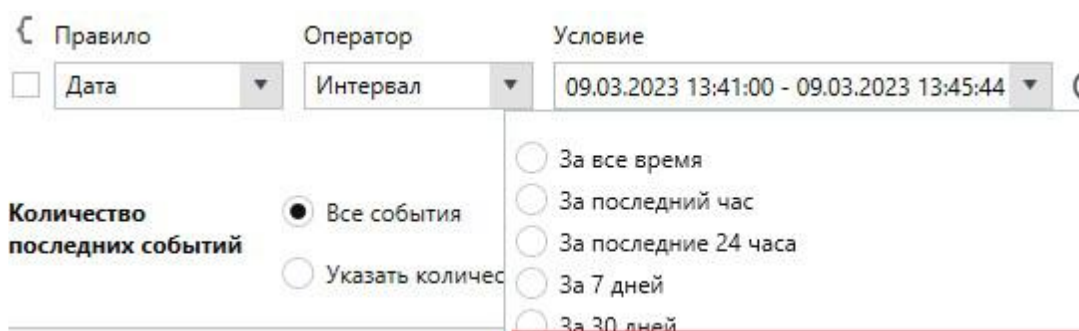


Рисунок 413 – Добавление правила фильтрации для поиска событий

Нажмите кнопку «+» для добавления дополнительного условия. В выпадающем списке выберите «Категория», в списке «Оператор» выберите «Содержит», а в списке «Условие» установите флаги «Вход/выход» и «Контроль целостности» (рисунок 414).

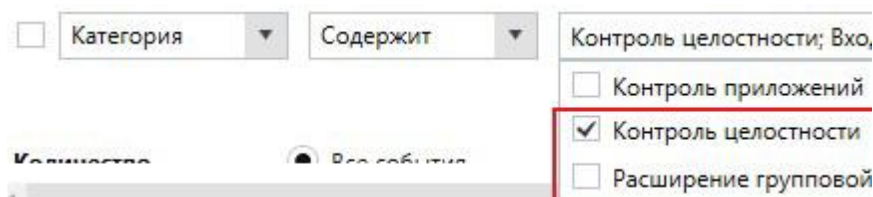


Рисунок 414 – Дополнительные параметры добавления правила

Нажмите кнопку «Применить запрос локально» для применения настроенного фильтра к записям загруженного журнала. Закройте окно фильтра, нажав на кнопку «Запрос» в правой части окна программы. Закройте окно детальной информации о событии (Ctrl +D). В списке событий отобразятся только те события, которые подходят по критериям, указанным в фильтре. Отсортируйте события по дате (от раннего к позднему), нажав на заголовок колонки «Дата» (рисунок 415)

СОБЫТИЯ		УГРОЗЫ	
Дата	Журнал	Событие	
29.09.2022 11:56:48	Secret Net St...	Изменено...	
29.09.2022 11:57:12	Secret Net St...	Завершени...	

Рисунок 415 – Сортировка событий по дате

В конце списка найдите события (с пиктограммой замка), относящиеся к категории «Контроль целостности» и откройте окно детальной информации о событии (рисунок 416). В окне детальной информации одного из событий указано название ресурса, нарушение целостности которого привело к появлению сообщения об угрозе, какое задание контроля целостности выполнялось и метод контроля целостности. При настройке задания контроля целостности было указано, что контроль проверки содержимого выполняется при входе пользователя в систему, следовательно, надо определить имя пользователя, который работал на СВТ перед блокировкой и изменил содержимое ресурса.

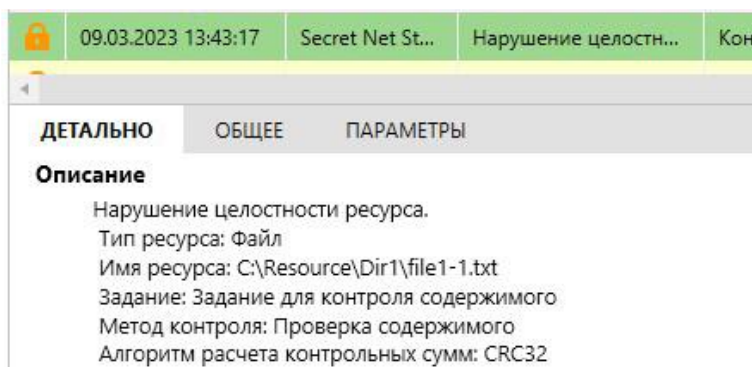


Рисунок 416 – Окно детальной информации о событии категории «Контроль целостности»

В списке событий найдите более раннее событие с категорией «Вход/выход» (рисунок 417). В детальной информации о событии содержится информация о завершении работы пользователя user3, следовательно, этот пользователь в процессе работы изменил содержимое контролируемого ресурса. Закройте окно детальной информации.

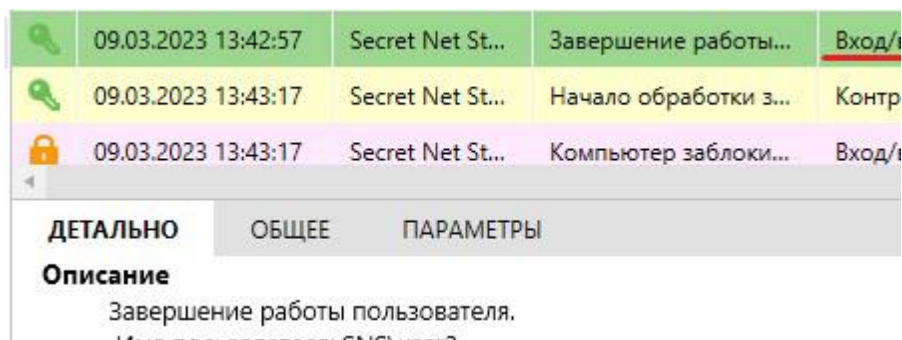


Рисунок 417 – Окно детальной информации о событии категории «Вход/выход»

Выберите событие завершения работы пользователя user3 в систему, нажмите клавишу Shift и выберите событие нарушения целостности (или последнее из событий, зафиксированных во время блокировки) (рисунок 418). Выделится несколько событий.

⚙	Дата	Журнал	Событие	Категория
Ключ	09.03.2023 13:41:10	Secret Net St...	Пользователь возоб...	Вход/выход
Ключ	09.03.2023 13:42:57	Secret Net St...	Завершение работы...	Вход/выход
Ключ	09.03.2023 13:43:17	Secret Net St...	Начало обработки з...	Контроль целостн
Замок	09.03.2023 13:43:17	Secret Net St...	Компьютер заблоки...	Вход/выход
Замок	09.03.2023 13:43:17	Secret Net St...	Нарушение целостн...	Контроль целостн
Замок	09.03.2023 13:43:17	Secret Net St...	Обнаружение повреж...	Контроль целостн

Рисунок 418 – Выбор событий нарушения целостности

В правой части окна нажмите кнопку «Печать журнала» (рисунок 419).

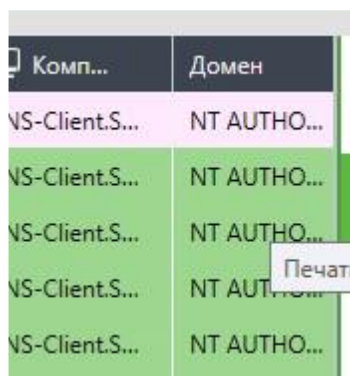


Рисунок 419 – Печать журнала

В окне «Печать журнала» установите переключатель «Количество записей» в положение «Выделенные» и установите флаг «Добавить в печать детальную информацию» (рисунок 420). Нажмите кнопку «Предпросмотр». Просмотрите содержимое, закройте окно предпросмотра. Нажмите еще раз кнопку «Печать журнала» в правой части окна.

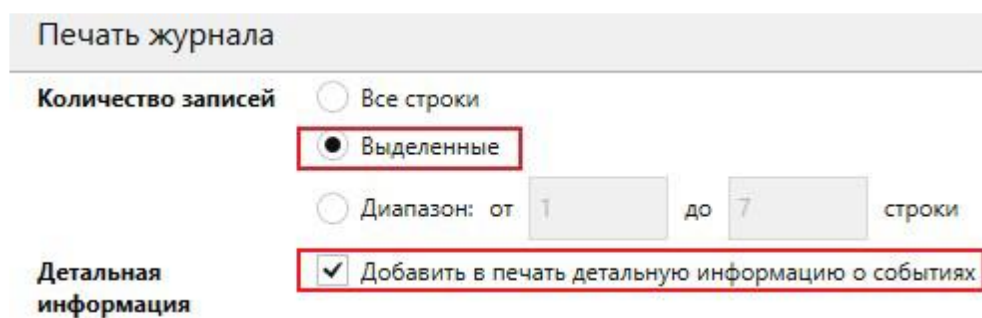


Рисунок 420 – Настройка печати журнала

Нажмите на кнопку «Экспорт журнала» (рисунок 421).

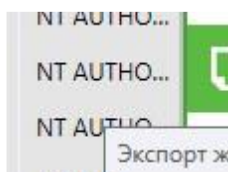


Рисунок 421 – Экспорт журнала

Укажите путь сохранения файла и название файла, остальные параметры оставьте без изменения и нажмите кнопку «Экспорт» (рисунок 422).

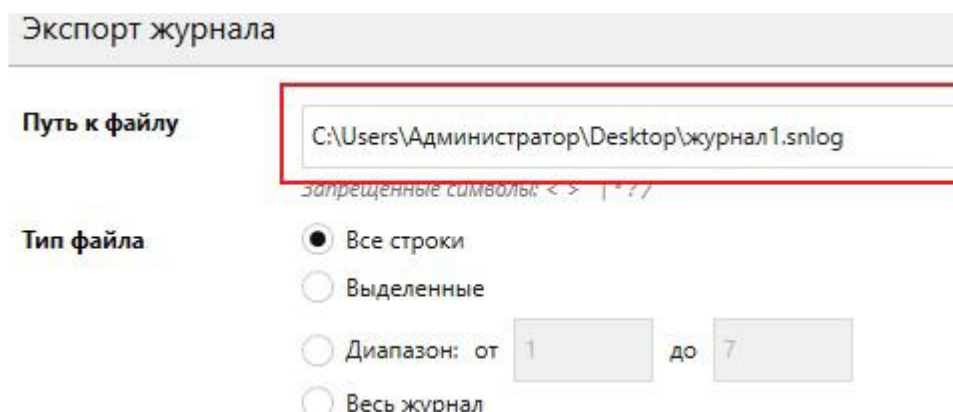


Рисунок 422 – Настройка экспорта журнала

После завершения экспорта закройте окно «Экспорт».

Нажмите кнопку «Открыть» над окном запросов (рисунок 423). Выберите файл журнала, созданный на предыдущем шаге.

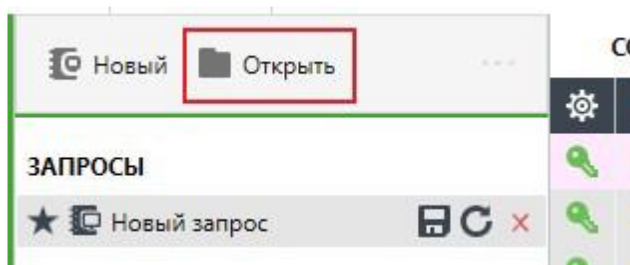


Рисунок 423 – Выбор файла журнала

Содержимое журнала загрузится для просмотра. Будут сохранены только события, оставшиеся в списке по результатам применения фильтра. Закройте загруженный журнал (рисунок 424).

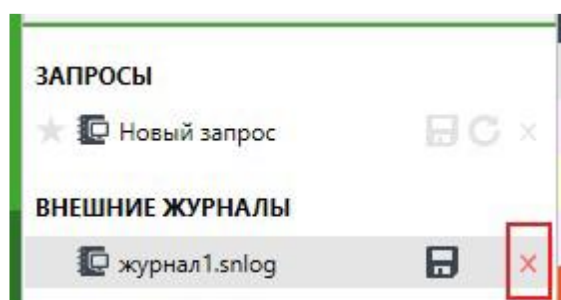


Рисунок 424 – Заккрытие журнала

Закройте также запрос событий, отображаемый ранее.

Перейдите к панели «Журналы сервера» и нажмите кнопку «Новый» (рисунок 425).

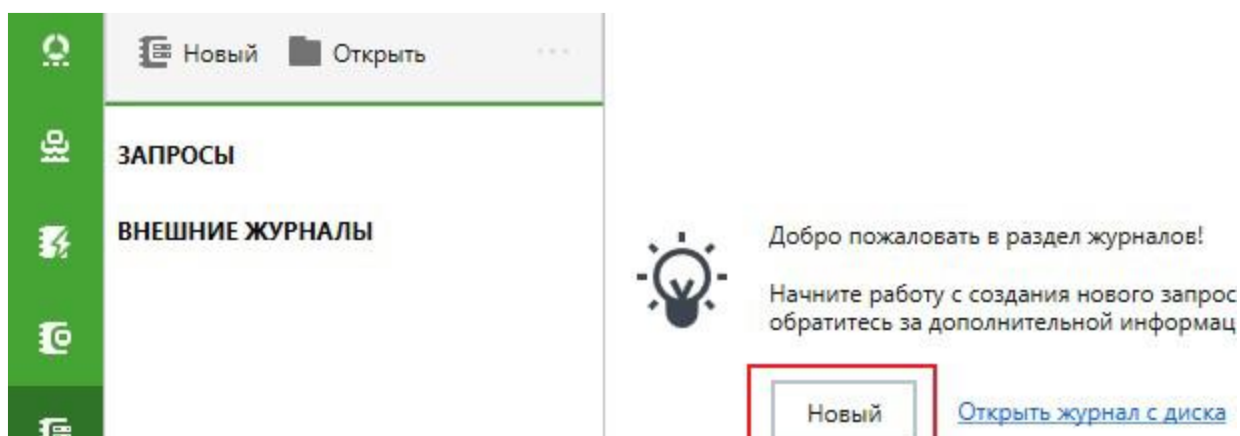


Рисунок 425 – Панель «Журналы сервера»

В открывшемся окне «Конструктор запроса» нажмите кнопку «Выполнить запрос к БД». Загрузится журнал сервера безопасности. В журнале сервера безопасности протоколируются сессии доступа к серверу, открываемые компонентами и программами Secret Net Studio, включая внутренние сессии самого сервера безопасности. Сведения о сессиях сохраняются в журнале в виде записей. Каждая запись включает в себя набор полей, в которых представлены следующие данные:

- общие данные о сессии: имя компьютера, инициаторы открытия (компонент и пользователь), время открытия и закрытия сессии;
- основные данные о выполнявшихся действиях в сессии: время выполнения каждого действия, результат, описание самого действия;
- дополнительные данные с детальными описаниями событий (системные идентификаторы объектов, кодовые обозначения результатов и другие параметры).

Окно журнала разделено на две половины. Слева выводится список сессий, справа – действия в сессии. Выберите первую сессию, в правой части отобразятся действия. Включите отображение детальной информации (рисунок 426). Просмотрите информацию, включаемую в журнал сервера безопасности.

Список сессий				Действия в сессии		
Компьютер	Класс кли...	Пользова...	Врем	Дата	Результат	Действие
SNS-Client.SNS.	Агент	SNS\SNS-CLIE	11.03	11.03.2023...	✓	Запрос гру
SNS-Server.SNS	Центр управле	SNS\Администр	09.03	11.03.2023...	✓	Запрос гру
SNS-Server.SNS	Центр управле	SNS\user2	09.03	11.03.2023...	✓	Запрос гру
SNS-Server.SNS	Центр управле	SNS\Администр	09.03	11.03.2023...		
SNS-Server.SNS	Центр управле	SNS\user2	09.03			
SNS-Client.SNS.	Агент	SNS\SNS-CLIE	09.03			
SNS-Client.SNS.	Агент	SNS\SNS-CLIE	09.03			

ДЕТАЛЬНО

ОБЩЕЕ

Операция: Запрос групповых пол
безопасности

Дополнительно:

Рисунок 426 – Отображение детальной информации

В правой части окна нажмите кнопку «Запрос». В поле «Правило» задайте «Имя пользователя», в параметре «Условие» выберите пользователя «SNS\Администратор» (рисунок 427). Нажмите кнопку «Применить запрос локально».

КОНСТРУКТОР ЗАПРОСА

Новый запрос

Правила запроса

Правило	Оператор	Условие
Имя пользова...	Содержит	SNS\Администратор

Рисунок 427 – Конструктор запроса

В списке сессий отобразятся сессии, связанные с Администратором. Просмотрите содержимое сессий других пользователей.

Вернитесь к окну запроса и удалите правило фильтрации. Затем обновите отображаемые события (рисунок 428).

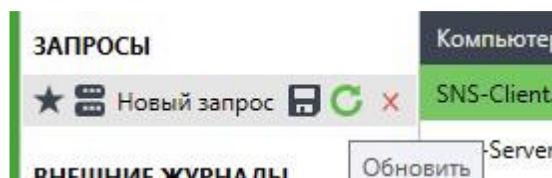


Рисунок 428 – Обновление отображаемых событий

Перейдите к панели «Компьютеры». Выберите сервер безопасности, нажмите правой кнопкой мыши, выберите в контекстном меню пункт «Архивирование» - «Создать архив журналов» (рисунок 429).

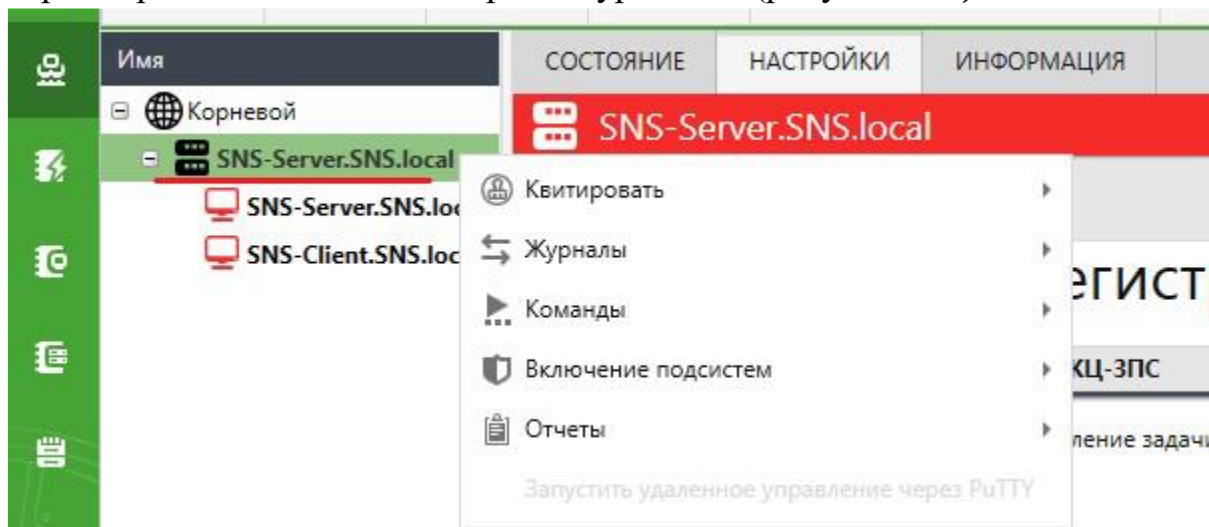


Рисунок 429 – Создание архива журналов

Установите параметры архивирования и нажмите кнопку «Архивировать» (рисунок 430). Будет создан архив журналов.

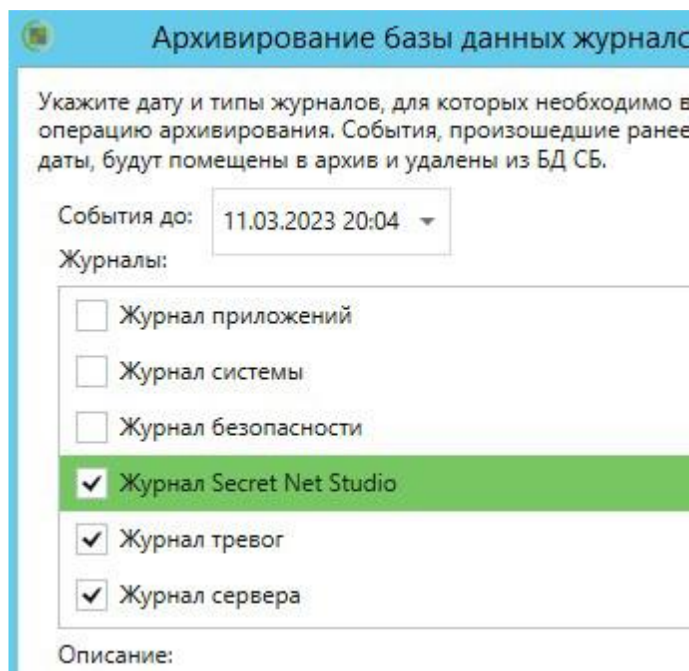


Рисунок 430 – Установка параметров при создании архива журналов

Перейдите к панели «Журналы станций». Нажмите на кнопку «Новый», укажите в параметрах запроса «За все время» и нажмите кнопку «Выполнить запрос к БД». Список событий будет пуст, поскольку после архивирования происходит очистка БД. Перейдите к панели «Статистика». Обновите содержимое панели. Просмотрите состояние виджета свободного места в базе данных, количество тревог различного уровня и т.д. Счетчики тревог обнулятся, т.к. очистилась БД сервера безопасности (рисунок 431).

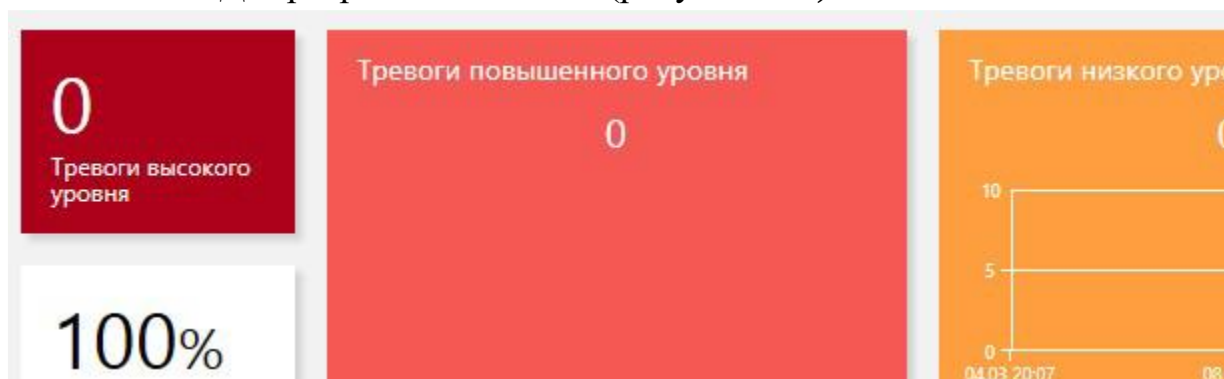


Рисунок 431 – Обновленная панель «Статистика»

Путь сохранения архивов указан в параметрах сервера безопасности. В панели «Компьютеры» откройте свойства сервера безопасности, загрузите настройки, перейдите к группе настроек «Параметры» и выберите пункт «Конфигурация сервера» (рисунок 432).

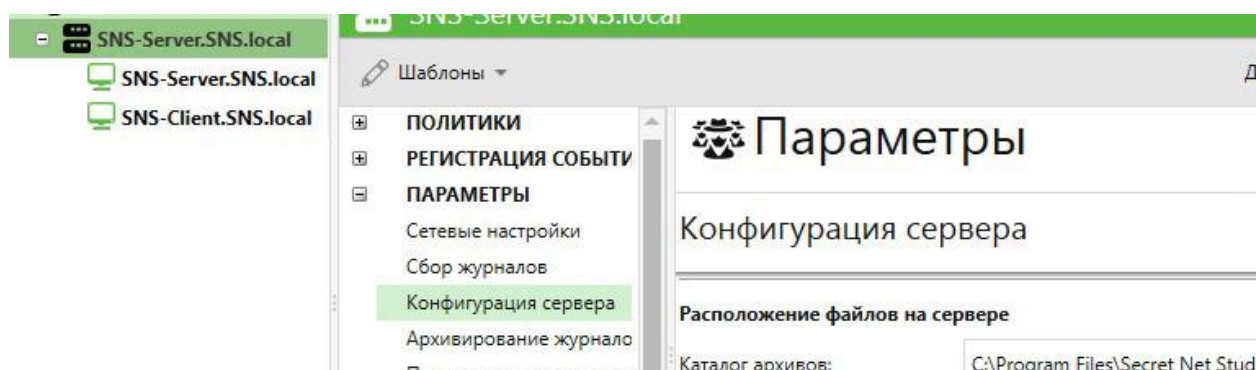


Рисунок 432 – Параметр «Конфигурация сервера»

Скопируйте путь к каталогу сохранения архивов.

Перейдите к панели «Архивы» и нажмите кнопку «Открыть» (рисунок 433).

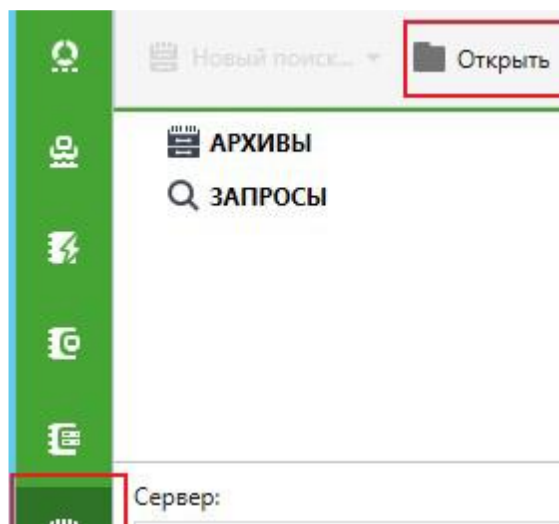


Рисунок 433 – Панель «Архивы»

В окне открытия окна вставьте скопированный путь в адресную строку и нажмите клавишу «Enter» (рисунок 434). Выберите в списке архив и нажмите кнопку «Открыть».

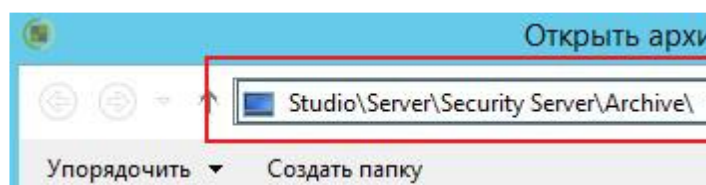


Рисунок 434 – Открытие архива

Загрузится архив журналов. Структура архива отображается в левой панели. Архив содержит журнал сервера, а также журналы рабочих станций. Выберите в списке «Журнал сервера» и нажмите кнопку «Загрузить журнал» (рисунок 435).

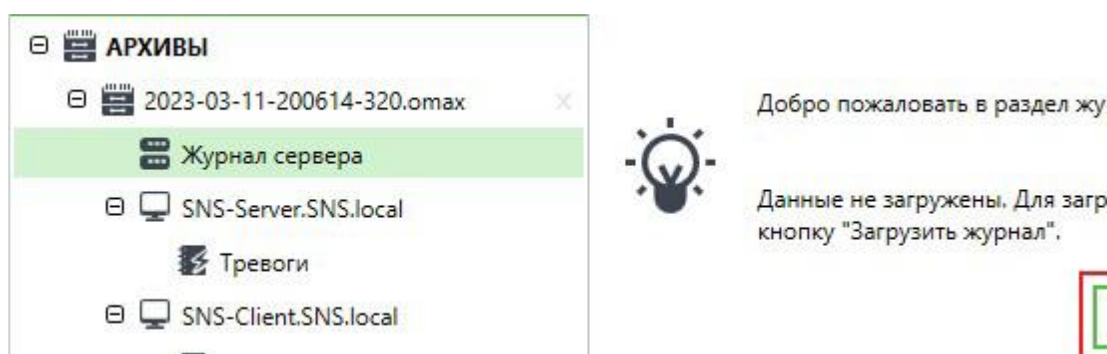


Рисунок 435 – Загрузка журнала

В правой части окна нажмите кнопку «Запрос». Задайте новое правило, указав правило «Действие» и условие «Квитирование тревог» (рисунок 436). Нажмите кнопку «Применить запрос локально».

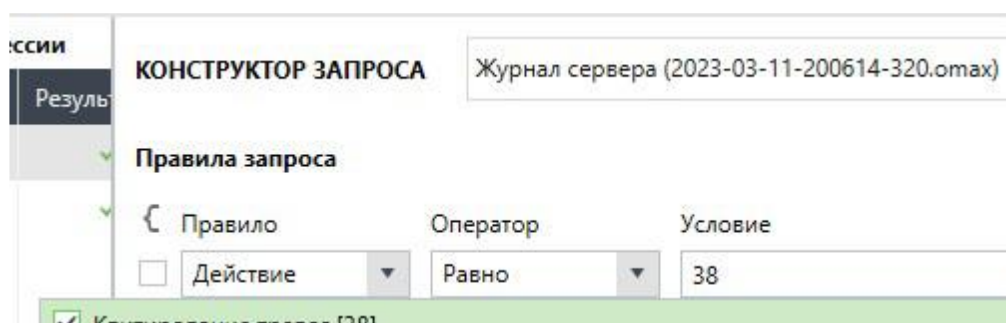


Рисунок 436 – Применение запроса локально

Выберите в списке слева сессию. Нажимая на клавиатуре клавишу управления курсором «↓» найдите в описании сессии события квитирования тревог в журнале сервера безопасности, выполненные ранее (рисунок 437).

Список сессий				Действия в сессии	
Компьютер	Класс кли...	Пользова...	Время отк...	Дата	Результат
SNS-Client.SNS.	Агент	SNS\SNS-CLIE	09.03.2023 13:0	09.03.2023...	✓
SNS-Server.SNS	Центр управле	SNS\Администр	05.03.2023 11:2	09.03.2023...	✓
SNS-Server.SNS	Центр управле	SNS\Администр	05.03.2023 11:2	09.03.2023...	✓
SNS-Client.SNS.	Агент	SNS\SNS-CLIE	05.03.2023 9:50	09.03.2023...	✓
SNS-Server.SNS	Центр управле	SNS\Администр	02.03.2023 17:1	09.03.2023...	✓

Рисунок 437 – Поиск события квитирования тревог в журнале сервера безопасности

Закройте архив сервера безопасности (рисунок 438).

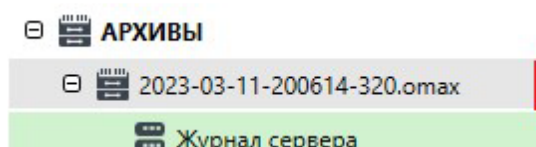


Рисунок 438 – Закрытие архива сервера безопасности

8 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации.

Методы и средства физической культуры, снижающие их воздействие

Защита информации в современном мире является важным аспектом для многих организаций и государств. Эксперты по обеспечению информационной безопасности играют ключевую роль в обеспечении безопасности данных и информационных систем. Однако, выполнение этой ответственной работы может подвергать специалистов различным вредным психофизиологическим факторам, которые негативно влияют на их психоэмоциональное состояние.

Одним из таких факторов является постоянное напряжение и стресс, связанные с необходимостью обеспечения безопасности информации и борьбой с киберугрозами. Эксперты по защите информации часто сталкиваются с высоким уровнем ответственности и огромным давлением, так как от них зависит сохранность и целостность конфиденциальных данных. Долгие часы работы в напряженной обстановке могут приводить к эмоциональному и физическому истощению, а также к возникновению тревожности и депрессии.

Однако, существуют различные методы и средства физической культуры, которые могут помочь специалистам по защите информации снизить воздействие вредных психофизиологических факторов и поддерживать свое психоэмоциональное состояние на должном уровне.

Например, регулярные физические упражнения являются одним из наиболее эффективных способов снятия напряжения и стресса. Физическая активность способствует выработке эндорфинов - гормонов счастья, которые улучшают настроение и снижают уровень тревожности. Рекомендуется заниматься физическими упражнениями, такими как бег, плавание или занятия в спортивном зале, регулярно и в умеренных количествах.

Также необходимо обращать внимание на правильный режим работы и отдыха. Эксперты по защите информации часто подвергаются переработкам и длительным рабочим сменам, что может негативно сказываться на их здоровье и эмоциональном состоянии. Важно обеспечивать себе достаточное количество

времени для отдыха и сна, а также планировать свое время таким образом, чтобы в нем было место для хобби, увлечений и встреч с друзьями.

Наконец, стоит уделить внимание поддержанию социальных связей. Общение с коллегами, друзьями и семьей играет важную роль в психологическом благополучии. Обсуждение проблем и разделение своих эмоций с близкими людьми может помочь справиться со стрессом и негативными эмоциями.

В заключение, эксперты по защите информации сталкиваются с вредными психофизиологическими факторами, которые могут негативно влиять на их психоэмоциональное состояние. Однако, с помощью методов и средств физической культуры, таких как регулярные физические упражнения, правильный режим работы и отдыха, а также поддержание социальных связей, эксперты могут снизить воздействие этих факторов и поддерживать свое психоэмоциональное состояние на высоком уровне.

Список используемых источников

1 Федеральный закон от 21.07.2014 № 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" [Электронный ресурс] – URL: <http://publication.pravo.gov.ru/Document/View/0001201407220042?index=1>.

2 ISO/IEC 27001:2013 "Информационная технология. Техника безопасности. Системы менеджмента информационной безопасности. Требования" [Электронный ресурс] – URL: <https://www.iso.org/ru/standard/27001>.

3 Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации" [Электронный ресурс] – URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264>.

4 Закон Российской Федерации № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" [Электронный ресурс] – URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102140498>.

Заключение

В результате выполнения выпускной квалификационной работы был разработан практикум по контролю применения средств защиты информации от несанкционированного доступа.

В процессе выполнения выпускной квалификационной работы был проведен обзор требований нормативно-правовых документов по контролю СЗИ, обзор способов контроля с использованием СЗИ, была разработана структура практикума, лабораторный стенд для проведения практикума, рекомендации по проведению практикума, варианты заданий для проведения практикума, было составлено методическое пособие, а также были составлены рекомендации по снижению влияния вредных психофизиологических факторов, влияющих на психоэмоциональное состояние специалиста по защите информации и методы и средства физической культуры, снижающие их воздействие

Таким образом, все пункты технического задания на выпускную квалификационную работу были выполнены в полном объеме.