МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кафедра информационной безопасности

Зулькарнеев И.Р.

Программно-аппаратные средства защиты информации

Методические рекомендации по выполнению лабораторных работ

Тюмень 2020

Оглавление

Список сокращений

AD	Active Directory
API	Application Programming Interface
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IMAPI	Image Mastering Application Programming Interface
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LDS	Lightweight Directory Services
MS	Microsoft
MSDN	Microsoft Developer Network
NIPS	Network intrusion prevention system
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
SP	Service Pack
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDF	Universal Disk Format
USB	Universal Serial Bus
VPN	Virtual Private Network
XML	Extensible Markup Language
XPS	XML Paper Specification
АПКШ	Аппаратно-программный комплекс шифрования
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АСУ ТП	Автоматизированная система управления производственными и технологическими процессами
БД	База данных
БРП	База решающих правил

ВМ	Виртуальная машина
ГИС	Государственная информационная система
ЗПС	Замкнутая программная среда
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КрК	Криптографический контейнер
КЦ	Контроль целостности
ЛБД	Локальная база данных
МД	Модель данных
НСД	Несанкционированный доступ
ОС	Операционная система
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РДУ	Разграничение доступа к устройствам
СБ	Сервер безопасности
СЗИ	Средство защиты информации
СНК	Серийный номер клиента
СУБД	Система управления базами данных
УЗ	Учетная запись
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦБД	Центральная база данных

Введение

Условные обозначения

В рекомендациях для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого пособия.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/)

Глава 1
Принципы построения системы Secret Net Studio и способы ее развертывания

Назначение, примеры использования и преимущества системы защиты Secret Net Studio

Утечки информационных ресурсов, персональных данных ограниченного доступа или других конфиденциальных сведений могут иметь для коммерческих и государственных организаций самые негативные последствия. Прямые убытки из-за ставших доступными широкой аудитории новейших технологических решений, закрытых коммерческих сведений или иной секретной информации могут усугубляться для компании имиджевыми потерями, а в случае утечек персональных данных – штрафами со стороны регуляторов информационной безопасности и компенсациями по судебным искам.

В связи с этим для обеспечения в коммерческих и государственных структурах информационной безопасности ПО, обрабатываемых данных, персональных данных сотрудников и клиентов, а также конфиденциальной информации необходим комплексный подход, который должен предусматривать:

- защиту от вирусов и вредоносных программ;
- защиту от сетевых атак;
- защиту от подделки и перехвата сетевого трафика внутри локальной сети;
- защищенный обмен данными с удаленными рабочими станциями и т.д.;
- защиту информации от несанкционированного доступа;
- контроль утечек и каналов распространения защищаемой информации;
- защиту от действий инсайдеров;
- защиту от кражи информации при утере носителей и т.д.

Средство защиты информации Secret Net Studio предназначено для обеспечения безопасности ИС и предоставляет следующие возможности:

- защита от НСД к информационным ресурсам компьютеров;
- контроль подключаемых к компьютерам устройств;
- обнаружение вторжений в информационную систему (NIPS);
- антивирусная защита;
- межсетевое экранирование сетевого трафика;
- авторизация сетевых соединений;
- централизованное управление компонентами защиты и пользователями.

Одним из критериев выбора того или иного средства защиты внутренних корпоративных ресурсов является соответствие требованиям регуляторов информационной безопасности. Состав мер и требований по защите информации и персональных данных в информационных системах государственных или коммерческих структур определен следующими нормативными документами:

- Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных" (с изменениями);
- Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне";
- Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015) "О государственной тайне";
- Приказ ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Приказ ФСТЭК России №17 от 11.02.2013 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

- Приказ ФСТЭК России №31 от 14.03.2014 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды";
- Методический документ ФСТЭК России от 11.02.2014 "Меры защиты информации в государственных информационных системах";
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.8-2015 от 01.05.2015 "Обеспечение информационной безопасности при использовании технологий виртуализации".

СЗИ Secret Net Studio сертифицировано ФСТЭК России на соответствие требованиям защиты:

- АС до класса защищенности 1Б включительно (гостайна с грифом "совершенно секретно");
- ГИС до 1 класса защищенности включительно и ИСПДн до 1 уровня защищенности включительно;
- АСУ ТП до 1 класса защищенности включительно.

SNS может работать под управлением следующих ОС:

- MS Windows 10/8.1/8/7 SP1/Vista SP2;
- MS Windows Server 2012/2012 R2/2008 SP2/2008 R2 SP1.

Приведем некоторые варианты использования Secret Net Studio.

Защита филиальной сети. Secret Net Studio поддерживает построение иерархии серверов безопасности. При этом администратор дочернего СБ имеет полномочия управления защитой только "своих" рабочих станций. В филиалах организации обеспечивается репликация данных между серверами безопасности и возможность для главного администратора централизованного мониторинга и управления всей системой защиты.

Обеспечивается безопасность работы отдельных подразделений организации с соответствующей конфиденциальной информацией (бухгалтерия, финансовая служба, БД клиентов, интеллектуальная собственность, банковская тайна, медицинские и персональные данные). Компоненты защиты Secret Net Studio позволяют развернуть:

- защиту на уровне данных. Хранение конфиденциальных документов в зашифрованных контейнерах предотвращает утечки информации при утрате носителя или несанкционированном физическом доступе к нему, а теневое копирование любых выводимых на печать или съемный носитель сведений может использоваться для расследования возможных инцидентов, связанных с утечками;
- защиту на уровне приложений. Замкнутая программная среда позволяет запускать только рабочие приложения, обеспечивая защиту от недоверенных и вредоносных программ;
- защиту на уровне сети. Межсетевой экран запрещает непредусмотренные маршруты движения сетевого трафика. Авторизация сетевых соединений обеспечивает защиту от подмены серверов и настройку правил межсетевого экрана для конкретных пользователей, а также блокировку сети при несанкционированном доступе к компьютеру. Обнаружение и предотвращение вторжений от недоверенных компьютеров и внешних источников;
- защиту на уровне операционной системы, которая предусматривает:
  - усиленный вход в систему с использованием аппаратных идентификаторов для предотвращения несанкционированной аутентификации и доступа к конфиденциальной информации. При изъятии идентификатора для исключения доступа в момент отсутствия сотрудника на рабочем месте компьютер блокируется;
  - антивирус, который обеспечит надежную защиту от любого типа вредоносных программ, включая вирусы, которые не осуществляют запуск и выполняются в обход замкнутой программной среды;
  - дискреционный или мандатный контроль доступа для разграничения доступа разных сотрудников только к своим конфиденциальным данным и

исключения полного доступа ко всей конфиденциальной информации для снижения риска утечек;

- затирание удаляемой информации для исключения возможности доступа к конфиденциальной информации, оставшейся в памяти или на временно используемых носителях;
- контроль устройств – блокировка работы с любыми недоверенными внешними устройствами, разрешение использовать только проверенные и защищенные съемные диски, а также устранение возможных каналов осуществления утечки информации;
- контроль печати – выделение только разрешенных принтеров для печати конфиденциальной информации и устранение возможных каналов утечки информации.

Обеспечение безопасности удаленных рабочих мест для сотрудников, работающих вне офиса, например, в командировках, на выездных совещаниях, с территории контрагента либо с мобильного рабочего места. SNS позволяет построить канал связи с внутренней сетью, который защищен от перехвата и подделки. При этом компьютер надежно защищен от внешних вторжений и вредоносного ПО и обеспечена защита информации на случай кражи оборудования. Компоненты защиты обеспечивают:

- защиту на уровне данных. Хранение конфиденциальных документов в зашифрованном контейнере для предотвращения утечек информации при утрате или краже компьютера;
- защиту на уровне приложений – замкнутая программная среда позволит запускать только рабочие приложения;
- защиту на уровне сети. Межсетевой экран устанавливает контроль входящего трафика и защиту от передачи конфиденциальной информации в обход защищенного VPN-соединения. Обнаружение и предотвращение вторжений по сети от недоверенных компьютеров и внешних источников. VPN-клиент организует зашифрованное подключение к локальной сети через интернет. При этом обеспечивается защита любого типа подключений, включая открытые Wi-Fi-сети, подверженные атакам на перехват и подмену трафика, а также возможность VPN-подключения до авторизации для входа в домен;
- защиту на уровне операционной системы. Антивирус обеспечит надежную защиту от любого типа вредоносных программ, включая вирусы, которые не осуществляют запуск и выполняются в обход замкнутой программной среды. Кроме того, осуществляется затирание удаляемой информации для исключения возможности доступа к конфиденциальной информации, оставшейся в памяти или на временно используемых носителях.

Защита терминального сервера. Организация надежного разграничения доступа к терминальному серверу с разделением для пользователей правил сетевого доступа к конфиденциальной и неконфиденциальной информации на данном сервере. Система защиты Secret Net Studio позволяет полностью изолировать пользователей друг от друга и применить для каждого из них "свои" правила сетевой фильтрации, предоставив доступ только к необходимым для работы данным. В данном случае компоненты SNS могут обеспечить:

- защиту на уровне данных с организацией теневого копирования любой выводимой информации для расследования возможных инцидентов, связанных с утечками, и отслеживанием действий отдельных пользователей на одном компьютере;
- защиту на уровне приложений – ЗПС предотвратит запуск несанкционированного ПО на терминальном сервере кем-либо из пользователей;
- защиту на уровне сети. Межсетевой экран запретит непредусмотренные маршруты движения сетевого трафика. Авторизация сетевых соединений обеспечит настройку разных правил фильтрации экрана для пользователей сервера. Обнаружение и предотвращение вторжений от недоверенных компьютеров и внешних источников;
- защиту на уровне операционной системы, которая предусматривает:
  - усиленный вход в систему, в том числе с использованием аппаратных идентификаторов для упрощения доступа и защиты от несанкционированных подключений;

- антивирус, который обеспечит надежную защиту от любого типа вредоносных программ, включая вирусы, которые не осуществляют запуск и выполняются в обход замкнутой программной среды;
- дискреционный или мандатный контроль доступа для разграничения доступа пользователей сервера только к своим конфиденциальным данным и исключения полного доступа ко всей конфиденциальной информации для снижения риска утечек;
- контроль устройств, которые пользователи могут подключить к терминальному серверу (проброс удаленных устройств) и контроль буфера обмена с запретом на перенос буфера на пользовательскую рабочую станцию;
- изоляцию модулей – запрет взаимодействия между процессами разных пользователей, функционирующих на одном сервере.

В каждом из приведенных выше вариантов использования системы Secret Net Studio предусмотрен централизованный мониторинг защищенности информационной системы, защищаемых групп компьютеров по степени их важности и критичности обрабатываемой на них информации, что дает возможность уделять особое внимание тревогам на наиболее приоритетных рабочих местах (руководство, финансовая дирекция и т.д.), а также получать уведомления о наиболее важных событиях по электронной почте для максимально оперативного реагирования.

Таким образом, становятся очевидными основные преимущества применения системы Secret Net Studio:

- использование на всех защищаемых компьютерах организации единого агента безопасности, что предотвращает конфликты между различными защитными компонентами и приводит к снижению общей нагрузки на защищаемый компьютер за счет отсутствия дублирования функций защиты;
- снижение сложности защищаемой системы (нет "зоопарка" защитного ПО от разных вендоров) и простота обеспечения согласованной работы компонентов защиты. При этом обеспечивается возможность создания единой политики безопасности для всей организации или отдельных политик безопасности по отделам, уровням обрабатываемой информации или филиалам, с автоматическим применением политики для всех защищаемых компьютеров;
- повышение скорости реакции на угрозы безопасности за счет возможности оперативно изменять глобальную политику из одной точки, чтобы при обнаружении инцидентов своевременно противостоять возникающим угрозам;
- экономическая составляющая. Единая архитектура и единая консоль Secret Net Studio облегчают освоение новых защитных подсистем и способствуют снижению затрат на обучение персонала. Архитектура системы защиты допускает покомпонентное лицензирование и возможность покупки/ дозакупки только нужных защитных механизмов.

Имеется ряд ограничений на использование системы Secret Net Studio, связанных с политикой ее лицензирования. Приобретение лицензий на SNS предусмотрено по защитным комплексам системы (см. рис. 1):

- защита от НСД (контроль устройств, затирание данных, полномочное управление доступом, дискреционное разграничение доступа, ЗПС, контроль печати);
- контроль устройств (контроль устройств, контроль печати) – может приобретаться вместо лицензии на защиту от НСД;
- защита дисков и шифрование контейнеров;
- персональный межсетевой экран (ПМЭ, авторизация сетевых соединений и сегментов сети);
- антивирус;
- средство обнаружения вторжений (NIPS);
- шифрование трафика VPN.

Рис. 1. Схема лицензирования Secret Net Studio

Централизованное управление – не лицензируется (бесплатно). Разделения на автономную и сетевую версии не делается.

Компоненты базовой защиты от НСД (см. следующий раздел) входят во все лицензируемые наборы.

Срочные лицензии – стандартно на 1 год, технически допустим любой срок; бессрочные – до окончания жизненного цикла продукта.

Архитектура Secret Net Studio

Система Secret Net Studio состоит из следующих программных пакетов:

- клиент "Secret Net Studio" (далее – клиент) предназначен для реализации защиты компьютера, на котором он установлен, путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС Windows. Защитные механизмы – это совокупность настраиваемых программных средств, входящих в состав клиента и обеспечивающих безопасное использование ресурсов;
- "Secret Net Studio – Сервер безопасности" (далее – сервер безопасности или СБ) обеспечивает хранение данных централизованного управления, координацию работы других компонентов защиты в процессе централизованного управления системой, получение от клиентов и обработку информации о состоянии защищаемых компьютеров, управление пользователями и авторизацией сетевых соединений, а также централизованный сбор, хранение и архивирование журналов;
- "Secret Net Studio – Центр управления" (далее – программа управления или ПУ) обеспечивает управление параметрами объектов, отображение информации о состоянии защищаемых компьютеров и произошедших событиях тревоги, загрузку журналов событий, оперативное управление компьютерами и централизованное получение отчетов.

Рассмотрим структуру клиента системы Secret Net Studio – состав и функции его компонентов, поскольку именно он обеспечивает весь комплекс информационной защиты компьютера.

Клиент содержит следующие функциональные компоненты (см. рис. 2):

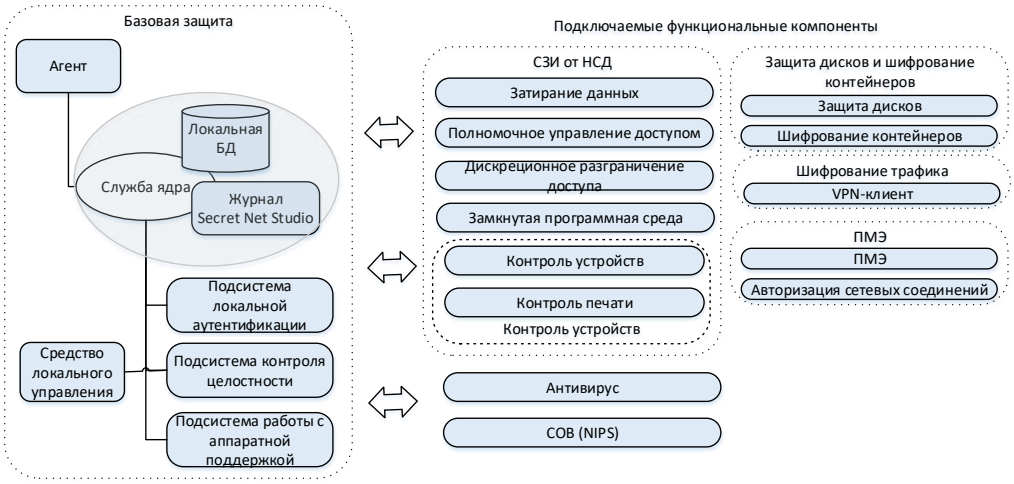


Рис. 2. Обобщенная структурная схема клиента

- базовая защита – объединяет основные программные службы, модули и защитные подсистемы;
- дополнительно подключаемые функциональные компоненты разделены согласно схеме лицензирования продукта (см. рис. 1):
  - средство защиты информации от несанкционированного доступа;
  - контроль устройств;
  - защита дисков и шифрование контейнеров;
  - антивирус;
  - средство обнаружения вторжений (NIPS);
  - шифрование трафика;
  - персональный межсетевой экран.

В группу базовой защиты (входит во все лицензируемые наборы – см. описание схемы лицензирования в предыдущем разделе) включены следующие программные службы, модули и защитные подсистемы (см. рис. 2):

- ядро – автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Эта служба осуществляет управление подсистемами и обеспечивает их взаимодействие. Функции ядра следующие:
  - обеспечивает обмен данными между подсистемами клиента и обработку поступающих команд;
  - обеспечивает доступ других компонентов к информации, хранящейся в локальной базе данных Secret Net Studio;
  - обрабатывает поступающую информацию о событиях, связанных с безопасностью системы, и регистрирует их в журнале Secret Net Studio.

  В службе ядра есть подсистема регистрации, которая регистрирует в журнале Secret Net Studio связанные с работой подсистем защиты события. При этом перечень подлежащих регистрации событий устанавливается администратором безопасности.

  Локальная БД Secret Net Studio размещается в реестре ОС Windows и специальных файлах. Она хранит информацию о настройках системы защиты, необходимых для работы защищаемого компьютера;
- агент – программный модуль в составе клиента, обеспечивающий взаимодействие с сервером безопасности. Агент принимает от СБ команды и отправляет ему данные о состоянии компьютера;
- средства локального управления обеспечивают управление объектами защиты (устройствами, файлами, каталогами), параметрами пользователей и защитных механизмов. В частности, администратор может формировать задания на контроль целостности ресурсов и работать с локальными журналами событий;
- подсистема локальной аутентификации используется в механизме защиты входа в систему и совместно с ОС Windows обеспечивает:

- проверку возможности входа пользователя в систему;
- оповещение остальных модулей о начале или завершении работы пользователя;
- блокировку работы пользователя;
- загрузку данных с персональных идентификаторов пользователя;
- усиленную аутентификацию пользователя при входе в систему.

При обработке входа пользователя в систему осуществляется формирование контекста пользователя: определение его привилегий, уровня допуска и т.д. Дополнительно с помощью модуля входа в систему реализуется функциональный контроль работоспособности системы Secret Net Studio;

- подсистема контроля целостности обеспечивает проверку неизменности ресурсов компьютера: каталогов, файлов, ключей и значений реестра. В составе механизма контроля целостности подсистема реализует защиту от подмены ресурсов, сравнивая их с определенными эталонными значениями. Данная подсистема выполняет контролирующие функции не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе (загрузка, вход пользователя, контроль по расписанию);
- подсистема работы с аппаратной поддержкой используется в механизме защиты входа в систему для работы с устройствами аппаратной поддержки. Она обеспечивает взаимодействие системы Secret Net Studio с определенным набором устройств и состоит из следующих модулей:
  - модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам аппаратной поддержки;
  - модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
  - драйверы устройств аппаратной поддержки (если они необходимы).

Перечислим подключаемые согласно схеме лицензирования функциональные компоненты клиента Secret Net Studio (см. выше рис. 2).

Компонент "СЗИ от НСД" включает в себя следующие подсистемы:

- контроль устройств (содержит взаимосвязанные механизм контроля подключения и изменения устройств и механизм разграничения доступа к устройствам);
- контроль печати (содержит механизм разграничения доступа к принтерам, а также механизмы настройки маркировки документов и настройки теневого копирования);
- замкнутая программная среда (предназначена для ограничения использования ПО на компьютере и разрешения доступа только к тем программам, которые необходимы пользователям для работы);
- полномочное управление доступом (обеспечивает разграничение доступа пользователей к конфиденциальным ресурсам и содержит механизм полномочного разграничения доступа);
- дискреционное управление доступом к ресурсам файловой системы (включает механизм дискреционного разграничения доступа, который позволяет предоставлять привилегии управления доступом к файловым ресурсам, назначать администраторов ресурсов, а также проводить настройки аудита операций с ресурсами);
- затирание данных (подсистема содержит механизмы затирания информации, которые обеспечивают безопасность повторного использования дискового пространства и оперативной памяти).

Компонент "Контроль устройств" содержит подсистемы контроля устройств и контроля печати, которые также входят и в "СЗИ от НСД". Поэтому данный компонент может приобретаться только вместо лицензии на защиту от НСД.

Компонент "Защита дисков и шифрование контейнеров" содержит подсистемы защиты информации на локальных дисках и шифрования данных в криптоконтейнерах.

Компонент "ПМЭ" содержит подсистемы, реализующие применение следующих механизмов защиты:

- персональный межсетевой экран;

- авторизация сетевых соединений.

Компонент "Антивирус" содержит механизмы защиты от вирусов и вредоносного ПО.

Компонент "СОВ" включает в себя механизмы обнаружения и предотвращения вторжений (NIPS).

Компонент "Шифрование трафика" содержит подсистему VPN-клиент, которая реализует безопасную передачу данных через общедоступные незащищенные сети. Для организации передачи данных используется технология "виртуальной частной сети" (Virtual Private Network – VPN), реализуемая аппаратно-программным комплексом шифрования (АПКШ) "Континент". При установке соединения с сервером доступа АПКШ "Континент" подсистема шифрования трафика выступает в роли VPN-клиента.

Механизмы защиты Secret Net Studio и принципы их работы

Механизмы защиты, которые обеспечивают работу описанных в предыдущем разделе компонентов Secret Net Studio, подробно описаны в документации системы (см. руководство администратора по принципам построения). Поэтому здесь приведем только основные их характеристики. Практическое применение данных механизмов мы рассмотрим при выполнении соответствующих лабораторных работ.

Защита входа в систему

Данный механизм обеспечивает предотвращение доступа посторонних лиц к компьютеру и содержит следующие средства:

- идентификация и аутентификация пользователей – эта процедура выполняется при каждом входе в систему. Штатный вход для ОС Windows предусматривает ввод имени и пароля пользователя или использование аппаратных средств, поддерживаемых операционной системой. Идентификация пользователей в SNS может выполняться: "по имени" – с вводом имени и пароля пользователя; "только по идентификатору" – с использованием персонального идентификатора, который поддерживается SNS; либо "смешанным" способом – с вводом своих учетных данных (имени и пароля) или с использованием персонального идентификатора, который поддерживается SNS. В системе защиты Secret Net Studio могут применяться аппаратные идентификаторы eToken, iKey, Rutoken, JaCarta, ESMART или iButton;
- механизм блокировки компьютера (в дополнение к стандартным возможностям ОС Windows) для предотвращения несанкционированного его использования может применяться в следующих случаях:
  - после определенного количества неудачных попыток входа пользователя в систему. Разблокирование компьютера в этой ситуации осуществляется администратором;
  - если пользователь выполнил стандартное действие для блокирования рабочей станции либо изъял свой идентификатор. Кроме того, временная блокировка может активироваться, если истек заданный интервал времени простоя компьютера. В этих случаях для снятия временной блокировки пользователю достаточно ввести свой пароль или предъявить идентификатор;
  - в результате работы подсистем защиты Secret Net Studio: при изменениях аппаратной конфигурации компьютера, при нарушении целостности контролируемых объектов или функциональной целостности системы Secret Net Studio. В таких ситуациях разблокировать компьютер может только администратор;
  - блокировка удаленно по команде администратора оперативного управления;
- аппаратные средства защиты от загрузки ОС со съемных носителей – см. строки 2 и 3 в табл. 1.

Табл. 1. Аппаратные средства, поддерживаемые в Secret Net Studio

Аппаратные средства	Основные решаемые задачи
Средства идентификации и аутентификации: - USB- ключи Rutoken S, Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash, eToken PRO*, ESMART Token, ESMART Token ГОСТ; - контактные смарт-карты Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), ESMART Token, ESMART Token ГОСТ с любыми совместимыми USB-считывателями	Идентификация и аутентификация во время входа пользователя после загрузки ОС. Идентификация и аутентификация во время входа пользователя с удаленного компьютера. Снятие временной блокировки компьютера. Хранение в идентификаторе пароля и криптографического ключа
Устройство Secret Net Card**	Те же (см. 1-ю строку таблицы). Запрет загрузки ОС со съемных носителей
Программно-аппаратный комплекс (ПАК) "Соболь" версии 3.0**	Те же (см. 2-ю строку таблицы). Идентификация и аутентификация пользователей до загрузки ОС. Контроль целостности программной среды компьютера до загрузки ОС

* В Secret Net Studio 8.2 помимо eToken PRO (Java) возвращена поддержка устаревших устройств eToken PRO (без приставки "Java") по причине их широкой распространенности.

** К разъему платы ПАК "Соболь" или Secret Net Card могут подключаться считывающие устройства идентификаторов iButton (поддерживаемые типы DS1992 – DS1996).

Функциональный контроль подсистем

Функциональный контроль проверяет загрузку и функционирование всех ключевых защитных подсистем к моменту входа пользователя в ОС (т.е. к моменту начала его работы).

Успешное завершение контроля отражается соответствующим событием в журнале Secret Net Studio. Если же были выявлены нарушения, то в журнале регистрируются события с детальными сведениями по данным нарушениям (это возможно при условии работоспособности ядра Secret Net Studio). При этом вход в систему разрешается только пользователям, входящим в группу локальных администраторов компьютера.

Одной из важных задач функционального контроля является обеспечение защиты ресурсов компьютера при запуске ОС в безопасном режиме (Safe mode). Этот режим запуска не является штатным для функционирования системы Secret Net Studio. Однако при необходимости администратор может его использовать для устранения неполадок.

Поскольку в безопасном режиме не действуют некоторые функции системы защиты, функциональный контроль в этих условиях завершается с ошибкой. В результате блокируется вход любых пользователей, кроме администраторов. Поэтому при надлежащем соблюдении правил политики безопасности, когда никто из обычных пользователей не обладает полномочиями администратора, доступ к ресурсам компьютера в обход механизмов защиты невозможен.

Регистрация событий

По умолчанию в журнале Secret Net Studio регистрируются все возможные события, кроме некоторых событий категории "Контроль приложений", а также некоторых событий категорий "Контроль целостности" и "Дискреционный доступ". Отдельные категории событий (например, события категории "Регистрация") регистрируются в обязательном порядке и их регистрацию отключить нельзя. Содержащиеся в журнале сведения содержат подробную информацию для анализа событий и позволяют контролировать работу механизмов защиты.

В процессе работы Secret Net Studio происходящие на компьютере события, связанные с безопасностью системы, регистрируются в журнале SNS, который хранится на системном диске в файле такого же формата, как и журнал безопасности ОС Windows. При этом у администратора есть возможность настройки перечня регистрируемых событий и параметров их хранения, что позволяет обеспечить подходящий уровень полноты описания событий аудита для расследования инцидентов, а также оптимальный объем сохраняемых сведений с учетом размера журнала и нагрузки на систему.

Контроль целостности

Механизм контроля целостности автоматически следит за неизменностью контролируемых объектов: файлов, каталогов, системного реестра и секторов дисков (последних – только при использовании ПАК "Соболь"). Каждый тип объектов имеет свой набор контролируемых параметров. Например, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов и на свое существование, т.е. на наличие по заданному пути. Также в системе предусмотрена возможность выбора времени контроля: при загрузке ОС, при входе пользователя в систему, по заданному расписанию и т.д.

При обнаружении несоответствий могут применяться различные варианты реакции на выявленные нарушения целостности, например, регистрация событий в журнале Secret Net Studio и блокировка компьютера.

Вся информация об объектах, методах и расписаниях контроля сосредоточена в **модели данных**, которая хранится в локальной БД системы SNS и представляет собой иерархический список объектов с описанием связей между ними. Используются следующие категории объектов (в порядке от низшего уровня иерархии к высшему):

- ресурсы;
- группы ресурсов;
- задачи;
- задания;
- субъекты активности (компьютеры, пользователи, группы компьютеров и пользователей).

Модель данных является общей для механизмов контроля целостности и замкнутой программной среды (см. ниже).

Управление локальными моделями данных на защищаемых компьютерах можно осуществлять централизованно. Для этого в глобальном каталоге создаются две модели данных – для компьютеров под управлением 32-разрядных версий ОС Windows и для компьютеров с 64-разрядными версиями ОС. Такое разделение позволяет учитывать специфику используемого ПО на защищаемых компьютерах с различными платформами.

Каждая из централизованных моделей данных является общей для всех защищаемых компьютеров под управлением версий ОС Windows соответствующей разрядности (32- или 64-разрядные версии).

Редактирование централизованных моделей данных осуществляется со следующими особенностями: для изменения доступна та модель данных, которая соответствует разрядности ОС Windows на рабочем месте администратора. При этом модель данных другой разрядности доступна только для чтения (но можно экспортировать данные из этой модели в другую).

Таким образом, если в системе имеются защищаемые компьютеры с версиями ОС различной разрядности, для централизованного управления моделями данных администратору следует организовать два рабочих места – на компьютерах с 32- и 64-разрядными версиями ОС Windows.

Замкнутая программная среда

Механизм замкнутой программной среды позволяет определить для любого пользователя компьютера индивидуальный перечень разрешенного для использования ПО. Система защиты контролирует и обеспечивает запрет использования следующих ресурсов:

- файлов запуска программ и библиотек, не входящих в перечень разрешенных для запуска и не удовлетворяющих определенным условиям;

- сценариев (скриптов, созданных по технологии Active Scripts), не входящих в перечень разрешенных для запуска и не зарегистрированных в БД.

Попытки запуска неразрешенных ресурсов регистрируются в журнале событиями "аудит отказов", которые определяются в SNS как события тревоги.

На этапе настройки механизма составляется список ресурсов, разрешенных для запуска и выполнения. Список может быть сформирован автоматически: на основании сведений об установленных на компьютере программах или по записям журналов, содержащих сведения о запусках программ, библиотек и сценариев. Также предусмотрена возможность ручного формирования списка.

Для файлов из списка ЗПС можно включить режим контроля целостности, поскольку эти механизмы (ЗПС и КЦ) используют единую модель данных. При запуске разрешенных программ можно дополнительно активировать механизм проверки заголовков исполняемых модулей, что повышает надежность разделения ресурсов на исполняемые и неисполняемые файлы, т.е. подлежащие и не подлежащие проверке.

Механизм замкнутой программной среды не блокирует запуск программ, библиотек и сценариев в следующих случаях:

- УЗ пользователя включена в группу "Учетные записи, на которые не действуют правила замкнутой программной среды" (по умолчанию содержит локальную группу "Администраторы"), которая входит в состав настроек политик ЗПС;
- включен мягкий режим работы подсистемы замкнутой программной среды. В этом режиме контролируются попытки запуска программ, библиотек и сценариев, но разрешается использование любого ПО (обычно используется на этапе настройки механизма).

Механизм изоляции процессов

Механизм изоляции процессов позволяет обеспечить изолированную среду для определенных процессов (запретить обмен данными с другими процессами) и может активироваться независимо от механизма ЗПС, хотя и использует БД КЦ-ЗПС, где защищаемому объекту исполняемого процесса ставится признак изолированности. Тем самым для этого процесса запрещается перенос данных в другие изолированные или неизолированные процессы. Под переносом данных здесь понимается перенос через буфер обмена или средствами Drag-and-Drop, а также операции программного взаимодействия с окном, например, получение текста объектов окна или заголовка окна.

Дискреционное управление доступом к ресурсам файловой системы

Механизм дискреционного управления доступом к ресурсам файловой системы обеспечивает:

- разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;
- контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;
- невозможность доступа к объектам в обход установленных прав доступа (если используются стандартные средства ОС или прикладные программы без собственных драйверов для работы с файловой системой, поскольку в SNS диспетчер доступа к файлам и директориям работает над стандартным диспетчером Windows);
- независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows: установленные в системе Secret Net Studio права доступа к файловым объектам не зависят от аналогичных прав доступа в ОС Windows и наоборот.

Аналогично реализации в ОС Windows матрица доступа в SNS представляет собой списки файловых объектов, для которых указаны учетные записи с правами доступа. Эти права разрешают или запрещают выполнение отдельных файловых операций. Для корректного учета в журнале аудита сведений по событиям разрешения или запрета доступа к файловым объектам необходимо выполнить соответствующие настройки на вкладке "Аудит" окна дополнительных параметров безопасности файлового объекта. Перечень предусмотренных прав доступа представлен в табл. 2.

Табл. 2. Перечень прав доступа

Право доступа	Действие для каталога	Действие для файла
Чтение (R)	Разрешает или запрещает просмотр имен файлов и подкаталогов	Разрешает или запрещает чтение данных
	Разрешает или запрещает просмотр атрибутов файлового объекта	
Запись (W)	Разрешает или запрещает создание подкаталогов и файлов	Разрешает или запрещает запись
	Разрешает или запрещает смену атрибутов файлового объекта	
Выполнение (X)	Разрешает или запрещает перемещение по структуре подкаталогов	Разрешает или запрещает выполнение
Удаление (D)	Разрешает или запрещает удаление файлового объекта	
Изменение прав доступа (P)	Разрешает или запрещает изменение прав доступа к файловому объекту. Пользователь, имеющий разрешение на изменение прав доступа к ресурсу, условно считается администратором ресурса	

Права доступа для файлового объекта могут быть заданы явно или наследоваться от вышестоящего элемента иерархии. Явно заданные права имеют более высокий приоритет по сравнению с наследуемыми. Права доступа считаются заданными явно, если для объекта отключен режим наследования прав.

По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в группу локальных администраторов. При этом для всех действуют разрешающие права доступа к любым ресурсам на чтение, запись, выполнение и удаление (RWXD). Эти права наследуются от корневых каталогов логических разделов. Во избежание непреднамеренной блокировки работы ОС нельзя изменять права доступа для корневого каталога системного диска (%SystemDrive%) и всего системного каталога (%SystemRoot%).

При копировании файлового объекта для его копии принудительно включается режим наследования прав доступа, даже если оригинальный объект обладает явно заданными правами.

Перемещение файлового объекта в пределах своего логического раздела осуществляется с сохранением явно заданных для него прав доступа. Если для объекта включен режим наследования, после перемещения этого объекта вступают в действие права того каталога, в который он перемещен. При перемещении объекта в другой логический раздел принудительно включается режим наследования прав.

Для файловых объектов можно детально настроить аудит выполняемых с ними операций. При работе механизма дискреционного управления доступом в журнале Secret Net Studio могут регистрироваться события успешного доступа к объектам, запрета доступа или изменения прав. По умолчанию регистрация событий успешного доступа не осуществляется, а события запрета доступа и изменения прав регистрируются для всех файловых объектов. Включение и отключение регистрации указанных событий осуществляется администратором безопасности при настройке параметров групповых или локальных политик.

Затирание удаляемой информации

Затирание информации на дисках необходимо для предотвращения восстановления и повторного использования удаляемой информации. Гарантированное уничтожение достигается путем автоматической записи последовательности случайных чисел на место удаленной информации. Для большей надежности может быть выполнено несколько циклов (проходов) затирания.

Данный механизм работает также и в оперативной памяти, исключая возможность повторного использования конфиденциальной информации или персональных данных пользователей после завершения работы программных

процессов и при любых операциях освобождения виртуальной памяти, например, при завершении потока.

Внимание! Очистка файла подкачки страниц выполняется стандартными средствами Windows при выключении компьютера и, соответственно, должна быть настроена в самой ОС. Только в этом случае при включении в SNS затирания информации на локальных дисках будет осуществляться и затирание файла подкачки.

Не осуществляется затирание файлов, помещаемых в Корзину, так как при этом они не удаляются с диска. Затирание таких файлов происходит после очистки содержимого Корзины.

Контроль подключения и изменения устройств компьютера

Механизм контроля подключения и изменения устройств обеспечивает:

- своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирование на эти изменения;
- поддержание в актуальном состоянии списка устройств компьютера, который используется механизмом разграничения доступа к устройствам, и запрет подключения к компьютеру определенных устройств либо незарегистрированных в списке устройств.

Начальная аппаратная конфигурация компьютера определяется на этапе установки системы – значения параметров контроля задаются по умолчанию. Дальнейшую настройку политики контроля устройств можно выполнить индивидуально для каждого из них или применять наследуемые параметры от родительских объектов – моделей, классов или групп, к которым эти устройства относятся.

Изменения аппаратной конфигурации отслеживаются системой защиты для устройств с включенным режимом контроля "Устройство постоянно подключено к компьютеру". При этом используются следующие методы контроля:

- статический контроль конфигурации. Каждый раз при загрузке компьютера подсистема получает информацию об актуальной аппаратной конфигурации и сравнивает ее с эталонной;
- динамический контроль конфигурации. Во время работы компьютера (а также при выходе из спящего режима) драйвер-фильтр устройств отслеживает факты подключения, отключения или изменения параметров устройств и, если произойдет изменение конфигурации, выдает оповещение об этом.

При обнаружении изменений аппаратной конфигурации система ожидает их утверждения администратором безопасности.

Разграничение доступа к устройствам

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, которые формируются механизмом контроля подключения и изменения устройств (см. выше). При этом системой Secret Net Studio предоставляются следующие возможности:

- установка стандартных разрешений и запретов на выполнение операций с устройствами;
- назначение устройствам категорий конфиденциальности или допустимых уровней конфиденциальности сессий пользователей – чтобы разграничить доступ с помощью механизма полномочного управления доступом.

Возможности по разграничению доступа зависят от типов устройств. Разграничение не осуществляется полностью или частично для устройств, имеющих особую специфику использования или необходимых для функционирования компьютера. Например, не ограничивается доступ к процессору и оперативной памяти, ограничены возможности разграничения доступа для портов ввода/вывода.

Для устройств с отключенным режимом контроля или запрещенных для подключения не действует разграничение доступа по установленным разрешениям и запретам на выполнение операций. Права доступа пользователей к таким устройствам не контролируются.

При установке клиентского ПО системы Secret Net Studio выставляются права доступа для всех обнаруженных устройств, поддерживающих такое разграничение доступа. По умолчанию предоставляется полный доступ трем стандартным

группам пользователей: "Система", "Администраторы" и "Все". То есть всем пользователям разрешен доступ ко всем устройствам, обнаруженным на компьютере. Далее администратор безопасности разграничивает доступ пользователей непосредственно к устройствам или к классам и группам устройств в соответствии с требованиями политики безопасности.

Полномочное управление доступом

Механизм полномочного управления доступом обеспечивает:

- разграничение доступа пользователей к конфиденциальной информации;
- контроль подключения и использования устройств с назначенными категориями конфиденциальности;
- контроль потоков конфиденциальной информации в системе;
- контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей;
- контроль печати конфиденциальных документов, что позволяет ограничить использование принтеров для печати документов, которым присвоены определенные категории конфиденциальности. По умолчанию на всех принтерах разрешается печать документов с любой категорией конфиденциальности.

По умолчанию в системе предусмотрены следующие категории конфиденциальности: "неконфиденциально" (для общедоступной информации), "конфиденциально" и "строго конфиденциально". При необходимости их можно переименовать, а также увеличить их количество до 16.

Категории конфиденциальности могут назначаться для следующих ресурсов:

- локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital;
- каталоги и файлы на дисках (FAT, NTFS).

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска, который выставляется средствами Secret Net Studio. По умолчанию пользователям назначен доступ к неконфиденциальной информации. Если уровень допуска пользователя ниже, чем категория конфиденциальности ресурса, – система блокирует доступ к этому ресурсу. После получения доступа к конфиденциальной информации уровень конфиденциальности программы (процесса) повышается до категории конфиденциальности ресурса. Это необходимо для того, чтобы исключить возможность сохранения конфиденциальных данных в файлах с меньшей категорией конфиденциальности.

Полномочное разграничение доступа на уровне устройств осуществляется следующим образом. Если устройство подключается во время сеанса работы пользователя с уровнем допуска ниже, чем категория устройства, система блокирует это подключение. При подключении такого устройства до начала сеанса работы пользователя – запрещается вход пользователя в систему. В режиме контроля потоков уровень конфиденциальности сессии пользователя должен соответствовать категориям всех подключенных устройств.

Функционирование устройства разрешено независимо от уровня допуска пользователя, если для этого устройства включен режим "Устройство доступно без учета категории конфиденциальности". Данный режим включен по умолчанию.

Доступ к содержимому конфиденциального файла предоставляется пользователю, если категория файла не превышает уровень допуска пользователя. При этом категория конфиденциальности устройства, на котором располагается файл, также анализируется и имеет более высокий приоритет по сравнению с категорией конфиденциальности файла. Если категория файла ниже категории конфиденциальности устройства – система считает категорию файла равной категории устройства. При обратной ситуации, когда категория файла превышает категорию конфиденциальности устройства, такое состояние расценивается как некорректное и доступ к файлу запрещается.

При использовании механизма в **режиме контроля потоков** конфиденциальной информации всем процессам обработки данных в системе присваивается единый уровень конфиденциальности, равный уровню сессии пользователя.

Нужный уровень конфиденциальности из числа доступных пользователю выбирается перед началом сессии работы на компьютере и не может быть изменен до окончания данной сессии.

В режиме контроля потоков сохранение информации разрешено только с категорией, равной уровню конфиденциальности сессии. Полностью запрещается доступ к данным, категория которых превышает уровень конфиденциальности сессии (даже если уровень допуска пользователя позволяет доступ к таким данным). Таким образом, режим контроля потоков обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации.

В режиме контроля потоков запрещается использование устройств с категорией конфиденциальности, отличающейся от выбранного уровня сессии. Если на момент входа пользователя к компьютеру подключены устройства с различными категориями конфиденциальности, вход запрещается по причине конфликта подключенных устройств. Использование устройств, которым назначена категория конфиденциальности выше, чем уровень допуска пользователя, ограничивается так же, как и при отключенном режиме контроля потоков.

В режиме контроля потоков запрещен вторичный вход в систему (независимо от настройки соответствующей политики безопасности SNS), т.е. обращение к совместно используемым файлам и папкам от имени другого пользователя и использование команды "Запуск от имени другого пользователя" (Run as different user).

Также режим контроля потоков позволяет установить ограничения на использование сетевых интерфейсов. Для каждого из них можно выбрать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователю. Если открыта сессия с другим уровнем конфиденциальности, функционирование этого интерфейса блокируется системой защиты. Это позволяет организовать работу пользователя в различных сетях в зависимости от выбранного уровня конфиденциальности сессии.

Механизм полномочного управления доступом осуществляет контроль вывода конфиденциальной информации на внешние носители – сменные диски, для которых включен режим доступа "без учета категории конфиденциальности". При копировании или перемещении конфиденциального ресурса на таком носителе может не сохраниться исходная категория конфиденциальности ресурса. Поэтому чтобы осуществлять вывод конфиденциальной информации на внешние носители в режиме контроля потоков, пользователь должен обладать соответствующей привилегией.

Контроль печати

Механизм контроля печати позволяет предотвратить несанкционированный вывод конфиденциальных документов на локальные и сетевые принтеры и обеспечивает:

- разграничение доступа пользователей к принтерам. Настройки соответствующих политик позволяют администратору безопасности сформировать списки доступных принтеров и установить для пользователя разрешение выполнять печать только на принтерах из этого списка;
- регистрацию событий вывода документов на печать в журнале Secret Net Studio, которая осуществляется в зависимости от состояния соответствующего параметра политики и зависит от состояния режимов маркировки (см. ниже) и теневого копирования (см. ниже) выводимых на печать документов;
- вывод на печать документов с определенной категорией конфиденциальности – при настройке политик администратор безопасности может ограничить печать на доступных принтерах документов всех категорий конфиденциальности или установить необходимые права пользователей и ограничения печати конфиденциальных документов;
- автоматическое добавление грифа в распечатываемые документы (маркировка документов);
- теневое копирование распечатываемых документов.

Для реализации функций маркировки и/или теневого копирования распечатываемых документов в систему добавляются драйверы "виртуальных принтеров". Виртуальные принтеры соответствуют реальным принтерам, установленным на компьютере. Список виртуальных принтеров автоматически формируется при

включении контроля печати. Печать в этом случае разрешается только на виртуальные принтеры.

При печати на виртуальный принтер выполняются дополнительные преобразования для получения образа распечатываемого документа в формате XML Paper Specification (XPS). Далее XPS-документ копируется в хранилище теневого копирования (если для принтера включена функция теневого копирования), модифицируется нужным образом и после этого передается для печати на соответствующее печатающее устройство.

Теневое копирование выводимых данных

Механизм теневого копирования обеспечивает создание в системе дубликатов (копий) данных, выводимых на отчуждаемые носители информации. Эти копии сохраняются в специальном хранилище, доступ к которому имеют только уполномоченные пользователи. Действие механизма распространяется на те устройства, для которых включен режим сохранения копий при записи информации.

При включенном режиме сохранения копий вывод данных на внешнее устройство возможен только при условии создания копии этих данных в хранилище теневого копирования. Если по каким-либо причинам создать дубликат невозможно, операция вывода данных блокируется.

Теневое копирование поддерживается для устройств следующих видов:

- подключаемые сменные диски (например, USB-флеш-накопители). При этом в хранилище теневого копирования создаются копии записанных файлов. Если файл открыт для редактирования непосредственно со сменного носителя, то при сохранении новой версии файла в хранилище будет создан его отдельный дубликат;
- дисководы гибких дисков;
- дисководы оптических дисков с функцией записи. При этом в хранилище создается образ диска, если для записи используется интерфейс Image Mastering API (IMAPI), или копии файлов, если запись осуществляется в формате файловой системы Universal Disk Format (UDF);
- принтеры. При этом используется механизм контроля печати и копии выводимой на печать информации сохраняются в формате XPS (XML Paper Specification) – открытый графический формат фиксированной разметки на базе языка XML, разработанный компанией Microsoft.

Внимание! Некоторые программные пакеты, имеющие функцию записи оптических дисков, используют собственные драйверы управления устройствами. Такие драйверы могут осуществлять доступ к устройству в обход механизма теневого копирования. Для обеспечения гарантированного контроля запись дисков необходимо осуществлять только с использованием штатных средств ОС Windows.

Защита информации на локальных дисках

Механизм защиты информации на локальных дисках компьютера (механизм защиты дисков) предназначен для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера. Загрузка считается санкционированной, если она выполнена средствами операционной системы с установленным клиентским ПО Secret Net Studio. Все другие способы загрузки ОС считаются несанкционированными (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере).

Механизм обеспечивает защиту информации при попытках доступа, осуществляемых с помощью штатных средств операционной системы.

Действие данного механизма основано на модификации загрузочных секторов (boot-секторов) логических разделов на жестких дисках компьютера. Содержимое загрузочных секторов модифицируется путем кодирования с использованием специального ключа, который автоматически генерируется при включении механизма. Модификация позволяет скрыть информацию о логических разделах при несанкционированной загрузке компьютера – разделы с модифицированными загрузочными секторами будут восприниматься системой как неформатированные или поврежденные.

При санкционированной загрузке компьютера осуществляется автоматическое раскодирование содержимого boot-секторов защищенных логических разделов при обращении к ним.

Выбор логических разделов, для которых устанавливается режим защиты (то есть модифицируются boot-секторы), осуществляет администратор.

Для реализации защитных функций механизма физический диск, с которого выполняется загрузка ОС, должен быть с основной загрузочной записью (Master Boot Record – MBR). При включении механизма на этом диске модифицируется MBR и часть остального пространства нулевой дорожки диска. Кроме того, часть служебных данных Secret Net Studio сохраняется в системном реестре.

Механизм обеспечивает защиту до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему NTFS, FAT32 или FAT16. Разделы могут быть на физических дисках с основной загрузочной записью (MBR) или с таблицей разделов на идентификаторах GUID (GUID Partition Table – GPT). Диски с другими типами разбиения на логические разделы не поддерживаются (например, динамические диски).

При использовании механизма защиты дисков на компьютере должна быть установлена только одна операционная система. Иначе после включения механизма в одной из них не гарантируется устойчивая работа остальных ОС.

Кроме того, в настройках BIOS компьютера должна быть отключена функция проверки загрузочных вирусов (если таковая поддерживается BIOS).

Шифрование данных в криптоконтейнерах

Система Secret Net Studio предоставляет возможность шифрования содержимого объектов файловой системы (файлов и папок). Для операций шифрования и расшифрования используются специальные хранилища – криптографические контейнеры или криптоконтейнеры (КрК) – физически это файлы, которые можно подключить к системе в качестве дополнительных дисков.

КрК является образом диска, но все действия с ним выполняются через драйвер механизма шифрования, который обеспечивает работу с пользовательскими данными в контейнере в режиме прозрачного шифрования. То есть пользователь после подключения криптоконтейнера в качестве диска выполняет операции с файлами на этом диске так же, как и на любом другом носителе. Дополнительных действий для шифрования или расшифрования файлов не требуется – все криптографические операции выполняются автоматически, "на лету", при обращении к этим файлам.

КрК можно подключать к системе с локальных дисков, сменных носителей или с сетевых ресурсов. Доступный объем для записи данных указывается в момент создания криптоконтейнера. Размер КрК фиксирован и не изменяется после создания. Предельное значение объема определяется исходя из свободного пространства на ресурсе и типа файловой системы. Минимальный размер контейнера – 1 МБ.

Для разграничения доступа пользователей к криптоконтейнерам в системе Secret Net Studio предусмотрены следующие права:

- чтение данных – предоставляет возможность только чтения файлов в КрК;
- полный доступ к данным – предоставляет возможность чтения и записи файлов в КрК;
- управление КрК – предоставляет возможность управления списком пользователей, имеющих доступ к КрК, а также чтения и записи файлов.

Создание криптоконтейнеров доступно пользователям с соответствующей привилегией (по умолчанию предоставлена учетным записям, включенным в локальную группу администраторов и локальную группу пользователей), которые имеют ключ шифрования. При этом создавший КрК пользователь получает право на управление им и в дальнейшем может делегировать (предоставить) это право доступа другому пользователю.

Для работы с шифрованными ресурсами пользователи должны иметь ключи шифрования. Процедуры генерации и выдачи ключей выполняются администратором безопасности. Для пользователей создаются ключевые пары, каждая из которых состоит из открытого и закрытого ключей. Открытые ключи хранятся в общем хранилище (для ключей локальных пользователей используется локальная БД Secret Net Studio, для доменных – хранилище глобального каталога). Закрытые ключи хранятся в ключевых носителях, присвоенных пользователям.

Носителями для хранения закрытых ключей (ключевой информации) могут являться идентификаторы или сменные носители, такие как дискеты, флеш-карты, USB-флеш-накопители и т.п.

Реализация ключевой схемы шифрования КрК базируется на алгоритмах ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ 28147–89. Во время криптографических операций генерируются и вычисляются определенные наборы ключей и дополнительных значений, используемых для доступа к КрК.

Персональный межсетевой экран

Система Secret Net Studio обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации. Могут использоваться правила фильтрации, которые уже описаны в SNS или созданы вручную администратором.

Подсистема межсетевого экранирования SNS реализует следующие основные функции:

- фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
- фильтрация пакетов служебных протоколов (ICMP, IGMP и т.д.), необходимых для диагностики и управления работой сетевых устройств;
- фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;
- фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);
- фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);
- фильтрация с учетом полей сетевых пакетов;
- фильтрация с учетом даты/времени суток.

Фильтрация сетевого трафика осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n). События, связанные с работой межсетевого экрана, регистрируются в журнале Secret Net Studio.

Подробнее о работе ПМЭ см. в главе 4.

Авторизация сетевых соединений

При действующем механизме авторизации сетевых соединений осуществляется добавление электронной подписи к сетевым пакетам, обеспечивается аутентичность и целостность передаваемых данных.

Аутентификация пользователей проводится собственным алгоритмом Secret Net Studio, основанным на протоколе Kerberos, который нечувствителен к попыткам перехвата паролей и атакам типа "Man in the Middle". С помощью данного механизма удостоверяются субъекты доступа и защищаемые объекты – это предотвращает несанкционированную подмену (имитацию) защищаемой информационной системы с целью осуществления некоторых видов атак.

Подсистема авторизации сетевых соединений обеспечивает:

- получение с сервера авторизации, входящего в состав компонента "Secret Net Studio – Сервер безопасности", правил авторизации соединений (список параметров соединений, которые необходимо подписывать);
- получение с сервера авторизации сессионных данных для подписания трафика;
- добавление в сетевой трафик подписи для пакетов, удовлетворяющих правилам авторизации. Возможно полное кодирование блока данных пакета;
- разбор подписи входящих пакетов и передачу информации о контексте удаленного пользователя в подсистему межсетевого экранирования для фильтрации по правилам.

Авторизация сетевых соединений осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n). В журнале Secret Net Studio регистрируются соответствующие события.

Подробнее о работе механизма авторизации сетевых соединений см. в главе 4.

Обнаружение и предотвращение вторжений

SNS реализует обнаружение и блокирование внешних вторжений, направленных на защищаемый компьютер. Осуществляется проверка сетевого трафика на предмет сетевых атак, зарегистрированных в базе решающих правил (БРП), и на прикладном уровне фильтруется входящий трафик. Атакующие компьютеры могут блокироваться на заданный промежуток времени.

Настройка параметров механизма осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления SNS.

Примечание. В состав SNS также входит компонент "Локальный центр управления", который позволяет управлять механизмом обнаружения и предотвращения вторжений непосредственно на защищаемом компьютере.

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

Функция	Описание
Детектор сетевых атак	Фильтрация входящего трафика, используемая для блокировки внешних атак. Функция работает на прикладном уровне модели OSI. Анализ входящих данных производится с помощью изучения поведения. Возможна блокировка атакующего хоста на определенный период времени
Сигнатурный анализ	Контроль входящего и исходящего трафика на наличие элементов, зарегистрированных в базе решающих правил для протокола HTTP

Антивирус

Secret Net Studio позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. При проверке компьютера (по заданному расписанию или по команде пользователя) осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др. Это позволяет обнаружить и заблокировать внешние и внутренние атаки, направленные на защищаемый компьютер.

Настройка параметров антивируса осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления Secret Net Studio.

Примечание. В состав Secret Net Studio входит также компонент "Локальный центр управления", который позволяет управлять антивирусом непосредственно на защищаемом компьютере.

Вся информация об активности механизма регистрируется в журнале SNS.

Для обеспечения антивирусной защиты предусмотрены следующие функции:

- постоянная защита – проверка файлов в режиме реального времени, обнаружение компьютерных вирусов сигнатурными и эвристическими методами при попытках получения доступа к исполняемым файлам, файлам документов, изображений, архивов, скриптов и других типов потенциально опасных файлов;
- контекстное сканирование – проверка, запускаемая пользователем из контекстного меню в проводнике Windows;
- сканирование по расписанию. Параметры проверки настраиваются администратором в программе управления. Пропущенное сканирование по расписанию (например, компьютер был выключен) принудительно запускается после восстановления работы компьютера;
- автоматическая проверка съемных носителей. Проверка выполняется автоматически при их подключении к компьютеру;
- список исключений обеспечивает создание списка файлов, которые игнорируются при проверке файлов в режиме реального времени и при сканировании по расписанию. Список исключений действует глобально для всех видов сканирования и не настраивается отдельно для разных режимов;

- выбор реакции на обнаруженные вирусы. Возможны следующие действия с зараженными объектами: удаление, изолирование (перемещение в карантин), блокировка доступа (только в режиме постоянной защиты), лечение. Выбор реакции на обнаруженные вредоносные программы осуществляется в настройках параметров антивируса;
- обновление антивирусных баз – автоматическое обновление базы с сервера обновлений, запускаемое в фоновом режиме, или ручное обновление базы из выбранной директории;
- контроль целостности сигнатур – проверка неизменности базы сигнатур при загрузке службы и при обновлении. При несанкционированном изменении базы создается запись в журнале Secret Net Studio.

Шифрование трафика с использованием VPN-клиента

В состав клиентского ПО системы Secret Net Studio включен VPN-клиент, предназначенный для организации доступа удаленных пользователей к ресурсам, защищаемым средствами АПКШ "Континент". VPN-клиент обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи. На стороне сервера доступа АПКШ "Континент" VPN-клиент системы Secret Net Studio рассматривается как отдельный абонентский пункт (АП).

При подключении абонентского пункта к серверу доступа выполняется процедура установки соединения в соответствии с протоколом TLS. В ходе этой процедуры осуществляется взаимная аутентификация абонентского пункта и сервера доступа. Завершается процедура установки соединения генерацией сеансового ключа, который используется для шифрования трафика между абонентским пунктом и сервером доступа.

При установке соединения между двумя абонентскими пунктами на первом этапе выполняется их аутентификация на сервере доступа. После успешной аутентификации обмен зашифрованными сообщениями между абонентскими пунктами выполняется напрямую без участия сервера доступа. Для шифрования сообщений используется сеансовый ключ.

Для аутентификации используются сертификаты X.509v3. Расчет хэш-функции выполняется по алгоритму ГОСТ Р 34.11-1994 или ГОСТ Р 34.11-2012.

Формирование и проверка электронной подписи осуществляются с применением алгоритма ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012.

Способы развертывания компонентов Secret Net Studio

Система Secret Net Studio может устанавливаться и функционировать в одном из следующих режимов:

- в **автономном** режиме, который предназначен для защиты отдельных рабочих станций и серверов и полностью настраивается администратором на том компьютере, где устанавливается SNS. Данный режим используется в тех случаях, когда централизованная установка SNS компонентов невозможна или нецелесообразна по тем или иным причинам. Управление защитными механизмами осуществляется только локально;
- в **сетевом** режиме (**с централизованным управлением**). Данный режим позволяет применить политики безопасности SNS в масштабах организации. Сетевой режим работы подразумевает централизованное управление механизмами защиты, а также централизованный аудит событий безопасности.

Далее мы рассмотрим некоторые особенности развертывания системы Secret Net Studio для выполнения перечисленных выше функций защиты.

Ранее в этой главе (см. раздел "Архитектура Secret Net Studio") мы уже разбирали общий состав устанавливаемых компонентов SNS. В случае автономной установки системы необходимо установить только ПО клиента Secret Net Studio и дальнейшую настройку компонентов защиты проводить локально с помощью программы "Локальный центр управления".

При реализации сетевого варианта развертывания Secret Net Studio структура системы Secret Net Studio строится по принципу подчинения защищаемых компьютеров сети серверу безопасности. Для этого компьютеры должны быть включены в состав **домена безопасности**, который формируется из объектов контейнера AD (организационного подразделения (OU) или всего домена).

Домен безопасности системы Secret Net Studio – это совокупность компьютеров, пользователей, серверов безопасности и их настроек, логически составляющих контейнер AD для выделенной группы администраторов безопасности SNS. В него входят все рабочие станции и серверы, относящиеся к конкретному контейнеру сети Active Directory – домену или организационному подразделению, включая объекты дочерних контейнеров. При этом несколько доменов безопасности (со своими серверами безопасности) могут образовывать лес доменов.

Другими словами, лес доменов безопасности – это структура объектов глобального каталога SNS, спроецированная на структуру домена Windows, а домен безопасности – это элемент структуры леса доменов безопасности.

Домены безопасности нужны в основном для разграничения полномочий администраторов безопасности по существующим подразделениям организации. Если нет задачи разграничения прав – следует использовать один домен безопасности.

Организационные подразделения являются логическими контейнерами, обычно используемыми для определения департаментов или других отделений. Использование OU позволяет быстро группировать пользователей и компьютеры для упрощения процесса администрирования.

Формирование первого домена безопасности в домене AD происходит при установке первого сервера безопасности.

В рамках леса доменов безопасности можно организовать функционирование нескольких серверов безопасности с подчинением по иерархическому принципу. При этом иерархия подчинения серверов не обязательно должна соответствовать структуре доменов в лесу. На рис. 3 представлен пример использования нескольких серверов безопасности СБ1 – СБ4 в структуре домена AD.

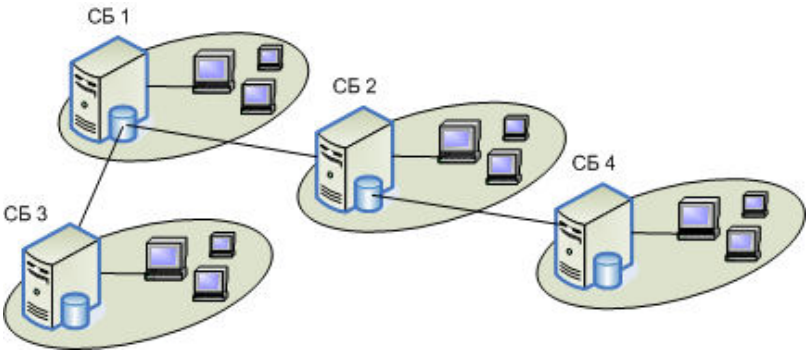


Рис. 3. Пример организации нескольких доменов безопасности

Следующий рисунок (см. рис. 4) иллюстрирует расширенный пример организации леса доменов безопасности в структуре леса доменов Windows.

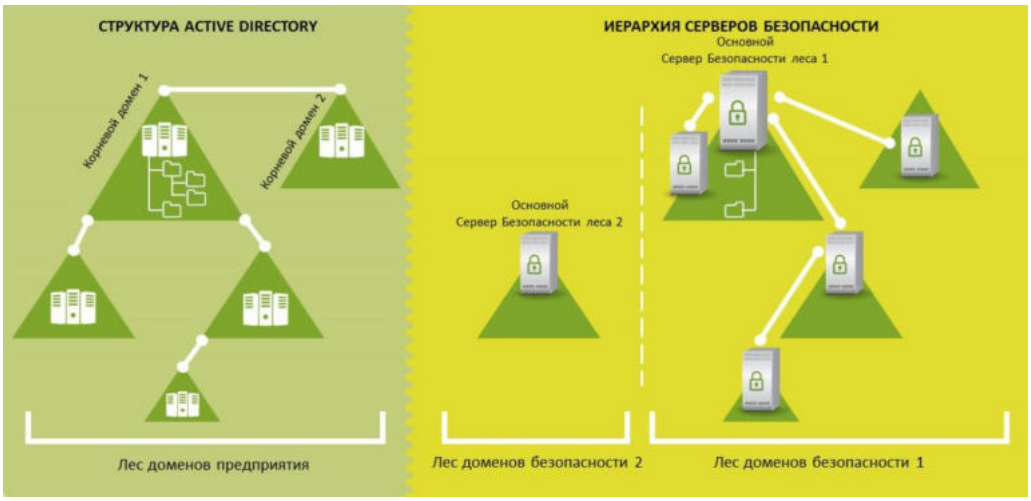


Рис. 4. Лес доменов безопасности в лесу доменов AD

Каждый сервер контролирует работу своей группы защищаемых компьютеров и имеет свою БД (здесь имеется в виду LDS). При этом некоторые операции доступны и в отношении объектов, относящихся к подчиненным серверам. Как

видно из рисунка (см. рис. 3), серверы безопасности СБ2 и СБ3 являются подчиненными по отношению к СБ1, а СБ4 – подчиненным по отношению к СБ2.

Сервер безопасности использует базу данных служб облегченного доступа к каталогам Active Directory (Active Directory Lightweight Directory Services, AD LDS). Контроль получения и применения параметров на защищаемых компьютерах осуществляется самим сервером безопасности.

Сетевую структуру системы Secret Net Studio можно формировать с учетом различных особенностей построения сети и распределения полномочий между администраторами. При этом:

- группа администраторов леса доменов безопасности – создается для управления глобальным каталогом и включает администраторов с правами конфигурирования леса;
- в каждом отдельном домене безопасности создается группа администраторов для управления в рамках этого домена безопасности.

Каналы взаимодействия компонентов системы Secret Net Studio показаны на рис. 5.

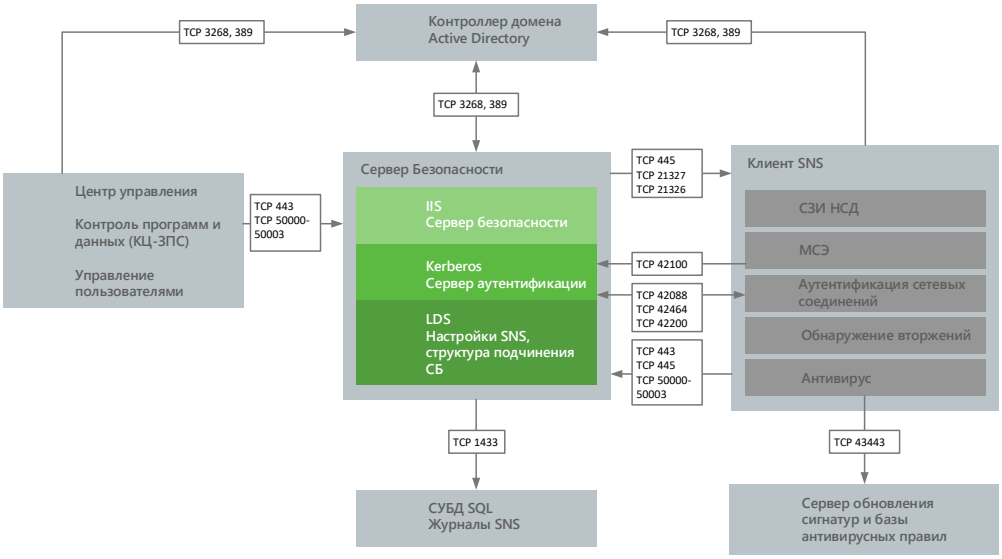


Рис. 5. Каналы взаимодействия компонентов системы Secret Net Studio

Обмен данными между клиентами и сервером осуществляется в режиме сессий. При передаче данных используется протокол https с использованием порта 443. На сервере безопасности должен быть установлен сертификат для обеспечения защиты соединений с сервером.

Администратор безопасности осуществляет настройку механизмов защиты и обработку сведений о тревогах в программе централизованного управления Secret Net Studio. Программа централизованного управления подключается к серверу безопасности по 443 порту (SSL) – тот в свою очередь обращается к хранилищу настроек AD LDS.

Администратор безопасности также может осуществлять настройку пользователей Secret Net Studio, централизованных заданий контроля целостности и замкнутой программной среды через дополнительные средства централизованного управления (Управление доменными пользователями, Контроль программ и данных (централизованный режим). При этих настройках соответствующие программы взаимодействуют с хранилищем настроек AD LDS напрямую.

Сервер безопасности состоит из нескольких компонентов, реализующих функции централизованного взаимодействия Secret Net Studio:

- сервер оперативного управления;
- сервер аутентификации;
- сервер хранения настроек AD LDS.

Сервер оперативного управления обеспечивает взаимодействие с подчиненными клиентами и предоставляет интерфейс для управления ими. Основные функции этого сервера следующие:

- получение информации от агентов о текущем состоянии рабочих станций;

- регистрация и обработка тревог;
- сбор, получение, архивация локальных журналов ОС и Secret Net Studio;
- отправка команд управления на защищаемые АРМ;
- применение параметров групповых политик, заданных в программе управления;
- обработка запросов к БД;
- централизованная установка клиентов Secret Net Studio, установка патчей;
- контроль лицензий компонентов Secret Net Studio.

Сервер аутентификации обеспечивает механизм аутентификации пользователей Secret Net Studio при сетевом взаимодействии и межсетевом экранировании. Его основными функциями является:

- обработка запросов клиентов на аутентификацию;
- выдача билетов безопасности пользователям и компьютерам с соответствующим установленным компонентом Secret Net Studio.

Сервер хранения настроек AD LDS реплицирует изменения из AD в AD LDS, а также служит основным местом хранения настроек и параметров Secret Net Studio. Основные функции сервера хранения настроек следующие:

- хранение настроек системы в целом;
- репликация настроек между серверами безопасности в иерархии леса доменов безопасности.

База данных сервера безопасности содержит централизованные журналы и оперативную информацию для мониторинга системы.

Локальные журналы с клиента Secret Net Studio передаются на сервер (по команде или по расписанию) и хранятся там в БД MS SQL.

База данных доменных служб AD LDS содержит параметры системы Secret Net Studio, относящиеся к компьютерам, пользователям и группам пользователей, списки серверов безопасности, списки электронных идентификаторов и других объектов для централизованного управления системой защиты.

Программы КЦ-ЗПС и управления пользователями обращаются напрямую в хранилище настроек.

При выполнении пользователями действий, нарушающих политики безопасности, события об этом регистрируются и передаются агентами Secret Net Studio с защищаемых ПК и фиксируются в программе управления как события тревоги.

Контроль применения и получения параметров защиты информации на защищаемых ПК в домене Secret Net Stuidio осуществляется сервером безопасности.

В таблице приведены сведения о протоколах и портах, используемых компонентами системы Secret Net Studio.

Протокол/порт	Назначение	Источник/получатель
TCP / 443	IIS, соединение ПУ с сервером безопасности, соединение клиента SNS с СБ, передача команд управления, передача журналов, получение политик	Программа управления / СБ Клиент SNS / СБ
TCP / 3268 (389)	Обращение к AD: считывание из АД значений параметров и запись в AD изменений	Программа управления / контроллер домена Клиент SNS / контроллер домена
TCP / 50000 – 50003	Обращение к AD LDS: считывание из AD LDS значений параметров и запись в AD LDS изменений	СБ / AD LDS Программа управления / AD LDS Клиент SNS / AD LDS
TCP / 21326	Служба подсистемы аппаратной поддержки	Клиент SNS / СБ
TCP / 21327	Служба подсистемы КЦ	Программа КЦ ЗПС / клиент SNS
TCP / 1433	SQL-сервер – хранение журналов	СБ / SQL-сервер

Для функционирования сервера безопасности требуется наличие системы управления базами данных (СУБД), реализуемой сервером СУБД MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах

(рекомендуется) или на одном. Установку сервера MS SQL необходимо выполнить в соответствии с требованиями производителя (см. на сайте компании Microsoft).

Внимание! Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении следующих условий на компьютере сервера MS SQL:

- включен режим поддержки сортировки кириллицы для экземпляра базы данных – для этого при установке экземпляра необходимо в параметрах сортировки для компонента Database Engine указать значение Cyrillic_ General_CI_AS;
- включен режим аутентификации, обеспечивающий проверку подлинности SQL Server и Windows, – для этого на сервере MS SQL необходимо включить смешанный режим аутентификации (mixed mode);
- если сервер MS SQL установлен на отдельном компьютере (не на компьютере сервера безопасности) – следует включить режим поддержки протокола TCP/IP. Режим по умолчанию отключен при использовании свободно распространяемого варианта SQL Server Express. Управление режимом осуществляется с помощью утилиты SQL Server Configuration Manager из состава ПО MS SQL Server. Значениям параметров "TCP Dynamic Ports" и "TCP Ports" для всех IP-адресов должны быть присвоены пустое значение и значение "1433" соответственно;
- если сервер MS SQL установлен на отдельном компьютере – в брандмауэре должно быть разрешено использование порта 1433 для соединения с СУБД. При этом на сервере MS SQL порт должен быть открыт на входящие соединения, а на сервере безопасности – на исходящие.

Варианты установки компонентов

Установка и развертывание компонентов защиты SNS подробно описаны в соответствующем руководстве администратора. Здесь мы приведем основные этапы этого процесса, а также остановимся на некоторых важных моментах, о которых следует помнить при подготовке к развертыванию Secret Net Studio в любой конфигурации.

Компоненты системы Secret Net Studio можно устанавливать при работе на компьютере локально или в терминальных сессиях. Также предусмотрены следующие методы автоматической установки клиента:

- централизованное развертывание средствами сервера безопасности;
- установка с использованием групповых политик.

Перед установкой компонентов SNS необходимо выполнить действия по подготовке к созданию структуры оперативного управления:

1. Подготовить организационные подразделения и включить в них нужные компьютеры для последующего формирования на их базе доменов безопасности.
2. Для каждого леса доменов безопасности создать группу пользователей, которая будет указана в качестве группы администраторов леса. Эти пользователи будут обладать правами на создание новых доменов безопасности в соответствующем лесу.
3. Создать группы пользователей, которые будут указаны в качестве групп администраторов доменов безопасности.

Примечание. В качестве группы администраторов домена безопасности не рекомендуется использовать стандартную доменную группу администраторов (Domain Admins). Иначе при подключении к серверу программы управления, установленной на этом же компьютере, может возникать ошибка из-за недостаточных привилегий пользователя, если включен механизм управления учетными записями (User Account Control — UAC). В этих условиях подключение будет разрешено только для первичной учетной записи администратора домена Windows. Чтобы начать сеанс работы с программой с нужными правами, можно использовать команду "Запуск от имени администратора" ("Run As Administrator") в контекстном меню ярлыка программы управления.

Для администраторов домена безопасности рекомендуется использовать специально созданную группу пользователей.

Общий порядок установки компонентов системы Secret Net Studio следующий:

1. На компьютере, который будет использоваться в качестве корневого сервера безопасности (не подчиненного другим серверам), выполнить следующие действия:
   - включить группу администраторов леса доменов безопасности и группу администраторов домена безопасности в локальную группу администраторов компьютера;
   - установить ПО сервера безопасности.

Внимание! После установки сервера безопасности нельзя переименовывать компьютер. Иначе сервер будет неработоспособен и недоступен для связи с другими компонентами системы Secret Net Studio.

2. Выполнить описанные в п. 1 действия на других компьютерах, которые будут использоваться в качестве подчиненных серверов безопасности.
3. На рабочих местах администраторов Secret Net Studio установить программу управления.

   Внимание! Объект нового СБ может появиться в структуре оперативного управления с некоторой задержкой. В программе управления, подключенной к другому серверу безопасности, загрузка обновленной структуры с новым сервером может произойти через несколько минут после установки ПО СБ (порядка 10–15 минут).

4. Установить ПО клиента системы SNS сначала на компьютерах серверов безопасности, а затем – на остальных компьютерах.

   Примечание. При наличии средства аппаратной поддержки Secret Net Card для его использования необходимо также установить специальный драйвер дополнительно к ПО клиента.

Рассмотрим частный случай развертывания компонентов Secret Net Studio с формированием одного домена безопасности на базе организационного подразделения AD. При этом все защищаемые компьютеры подчиняются одному серверу безопасности.

1. Средствами управления объектами Active Directory создать организационное подразделение и включить в него компьютеры, на которых будет установлено ПО системы SNS.
2. Создать доменные группы пользователей для администраторов леса доменов безопасности и администраторов домена безопасности, включив в них учетные записи, которые должны обладать соответствующими полномочиями.
3. На компьютере, который будет использоваться в качестве сервера безопасности, выполнить следующие действия:
   - включить группу администраторов леса доменов безопасности и группу администраторов домена безопасности в локальную группу администраторов компьютера;
   - установить ПО сервера безопасности.

   Внимание! Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, следует в этом же домене безопасности установить резервный сервер и при этом подчинить его основному серверу.

4. На компьютере администратора безопасности установить программу управления.
5. Запустить программу управления и установить соединение с сервером безопасности.
6. Настроить централизованную установку клиентского ПО Secret Net Studio на компьютерах организационного подразделения. Для этого добавить комплект установочных файлов клиента в список централизованно устанавливаемого ПО и сформировать задания развертывания.
7. Отслеживать выполнение заданий в программе управления. После установки клиентского ПО и перезагрузки компьютеров соответствующие им агенты будут появляться в структуре управления в качестве подчиненных объектов сервера безопасности.

Краткое описание стенда

Для выполнения лабораторных работ подготовлен специальный лабораторный стенд на платформе VMware vSphere из 6 виртуальных машин с установленными операционными системами.

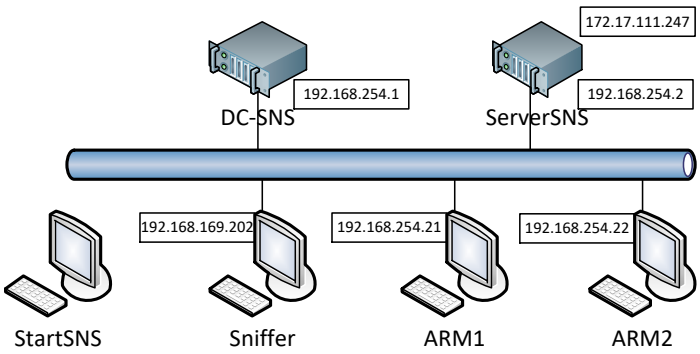


Рис. 6. Схема стенда Secret Net Studio

Стенд содержит виртуальную локальную сеть 192.168.254.X/24, объединяющую 4 виртуальные машины. ВМ Sniffer для перехвата сетевого трафика имеет сетевой интерфейс, подключенный к виртуальному коммутатору в режиме Promiscuous mode, с IP-адресом другой подсети.

Одна ВМ – StartSNS – является отдельной и не включена в виртуальную сеть.

Ниже приводится краткое описание всех ВМ стенда.

ВМ **DC-SNS.sn7.local** с гостевой ОС Microsoft Windows Server 2008 R2 SP1 выполняет функции контроллера домена **sn7.local**. Встроенная УЗ администратора контроллера домена: логин – **Администратор**, пароль – **P@ssw0rd**. Дополнительная доменная УЗ администратора домена безопасности: логин – **dadminsns1**, пароль – **P@ssw0rd**. Пользовательские доменные учетные записи "user1 – Иванов Иван Иванович" и "user2 – Иванова Мария Ивановна" с паролем **P@ssw0rd**.

ВМ **ServerSNS.sn7.local** с гостевой ОС Microsoft Windows Server 2008 R2 SP1 выполняет функции сервера безопасности Secret Net Studio, включена в состав домена sn7.local. Встроенная УЗ локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**.

ВМ **ARM1.sn7.local** с гостевой ОС Microsoft Windows 7 x64 SP1 выполняет функции защищаемого клиентского компьютера. Встроенная УЗ локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**.

ВМ **ARM2.sn7.local** с гостевой ОС Microsoft Windows 7 x64 SP1 выполняет функции рабочего места администратора безопасности, включена в состав домена sn7.local. Встроенная УЗ локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**. Дополнительная УЗ с правами локального администратора: логин – **user2**, пароль – **P@ssw0rd**.

ВМ **StartSNS** с гостевой ОС Microsoft Windows 7 x64 SP1 выполняет функции отдельного защищаемого компьютера. Встроенная УЗ локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**. Дополнительная УЗ с правами локального администратора: логин – **adminsns**, пароль – **P@ssw0rd**. Пользовательские УЗ: логин – **"user1 – Иванов Иван Иванович"** и **"user2 – Иванова Мария Ивановна"**, пароль – **P@ssw0rd**.

ВМ **Sniffer** с гостевой ОС Microsoft Windows 7 x64 SP1 выполняет функции рабочего места для перехвата сетевого трафика. Встроенная УЗ локального администратора: логин – **Администратор**, пароль – **P@ssw0rd**. Дополнительная УЗ с правами локального администратора: логин – **user**, пароль – **P@ssw0rd**.

Подробное описание стенда с инструкцией по его развертыванию см. в приложении.

Здесь и далее в лабораторных работах предполагается, что все ВМ стенда включены и работают.

По ходу выполнения лабораторных работ все необходимые изменения на стенде проводятся слушателями самостоятельно.

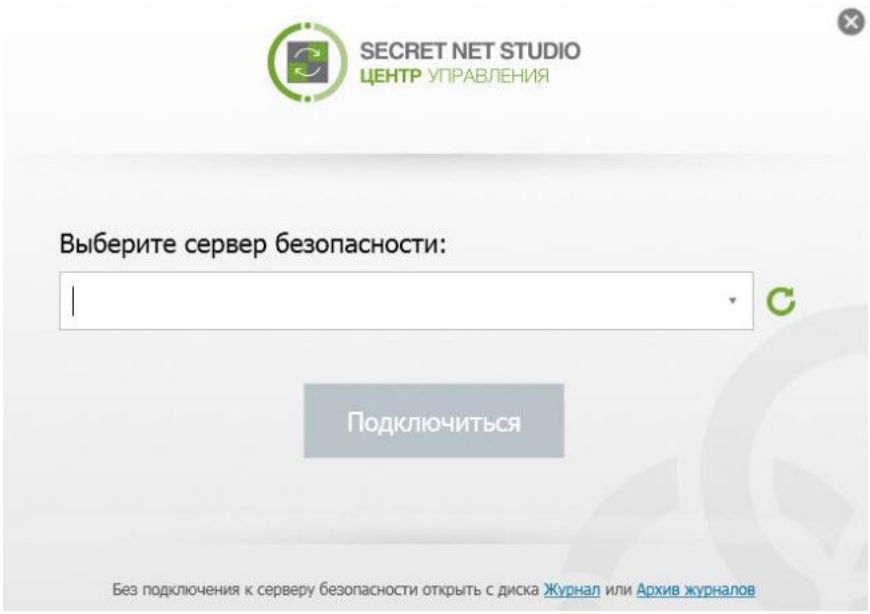
Лабораторная работа №1 "Сетевая установка компонентов Secret Net Studio на защищаемые компьютеры"

В рамках развертывания СЗИ Secret Net Studio в сетевом варианте на учебном стенде выполнены соответствующие подготовительные действия на компьютерах контроллера домена и сервера безопасности. После этого на ВМ ServerSNS установлено ПО сервера безопасности, а на ВМ ARM2 – программа "Центр управления" (программа управления, ПУ).

В данной лабораторной работе проводится завершающий этап развертывания СЗИ Secret Net Studio в сетевом варианте – установка на защищаемые компьютеры клиента Secret Net Studio.

1. С помощью программы управления следует подключиться к серверу безопасности и сформировать список устанавливаемого ПО и заданий развертывания. После этого на СБ и клиентских компьютерах установка ПО выполняется автоматически в фоновом режиме. При этом пользователи оповещаются о начале и завершении процесса установки, а после окончания установки выполняется перезагрузка компьютера.

Для подключения к СБ запустите на ВМ ARM2 программу управления: "Пуск / Программы / Код безопасности / Secret Net Studio / Центр управления". На экране появится стартовое окно программы.

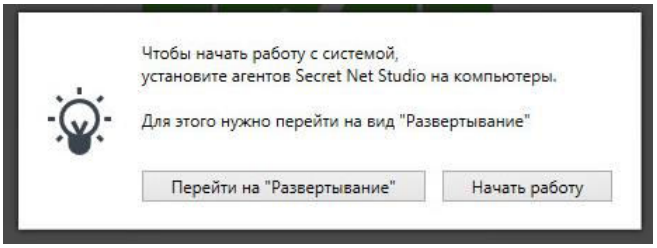


2. В поле "Сервер безопасности" введите имя сервера безопасности, с которым будет установлено соединение – **ServerSNS.SN7.local**, или нажмите справа от поля кнопку  для поиска зарегистрированных серверов безопасности.

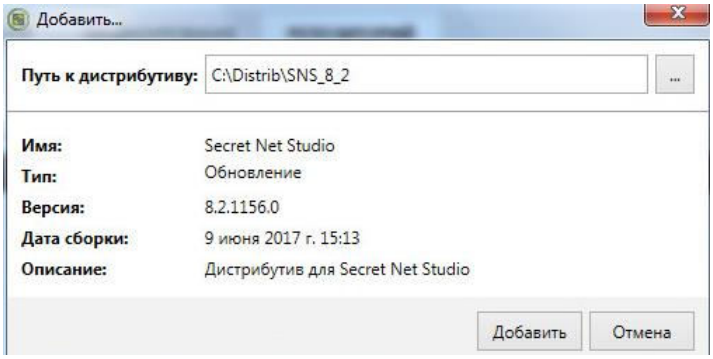
Примите к сведению. Программа предусматривает возможность запуска без подключения к серверу безопасности — для просмотра содержимого журналов, сохраненных в файлах. Для этого в нижней части стартового окна используются следующие команды:

- "Журнал" — для загрузки журнала из файла;
- "Архив журналов" — для загрузки архива журналов из файла.

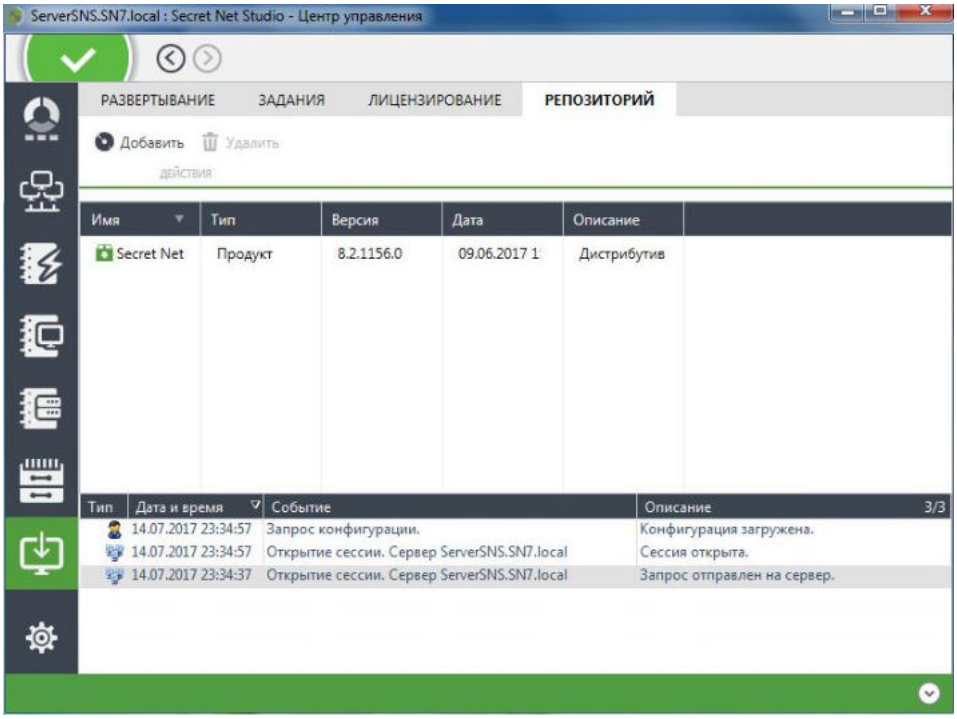
3. Нажмите кнопку "Подключиться" и дождитесь завершения процедуры подключения. В открывшемся окне программы управления появится окно подсказки с предложением перейти к развертыванию компонентов системы защиты.



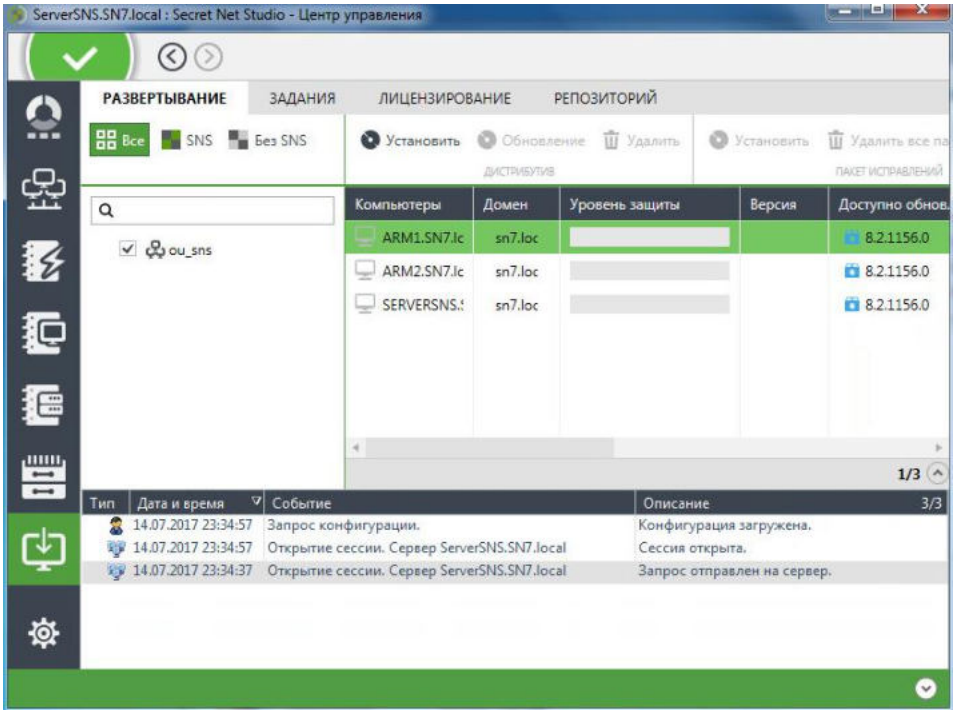
4. Нажмите кнопку "Перейти на "Развертывание". В панели "Развертывание" переключитесь на вкладку "Репозиторий", для добавления дистрибутива Secret Net Studio нажмите кнопку "Добавить" и укажите путь к папке установки: "C:\Distrib\SNS_8_2".



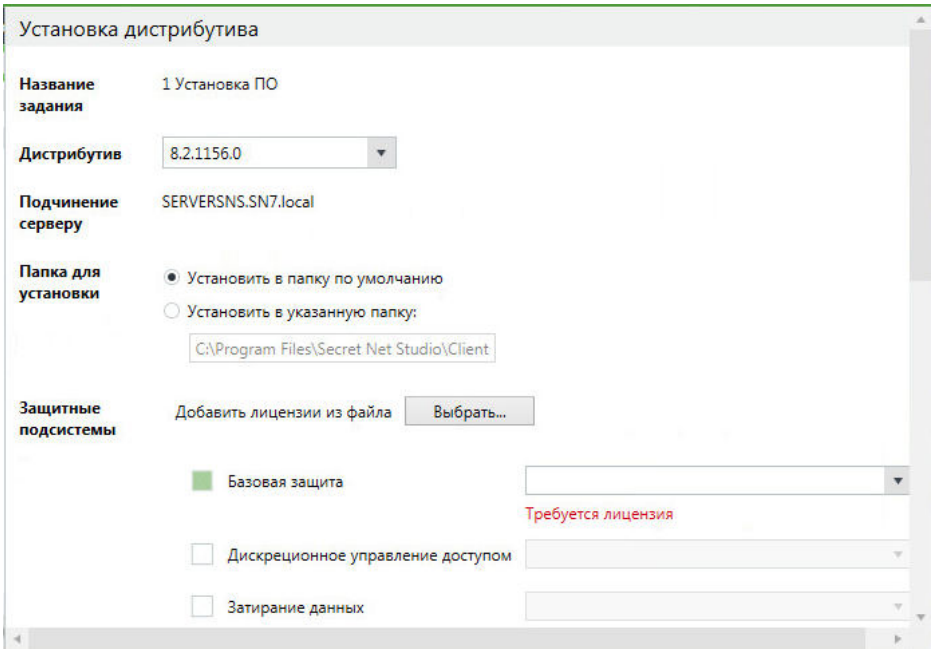
5. Нажмите кнопку "Добавить" и дождитесь завершения создания установочного комплекта на вкладке "Репозиторий" программы управления (процесс отправки файлов на сервер безопасности может занять продолжительное время). По окончании процесса в списке появится новый элемент, содержащий сведения о загруженном комплекте.



6. После формирования комплекта централизованно устанавливаемого ПО необходимо определить списки компьютеров, на которых в автоматическом режиме будет выполняться установка клиента SNS. В панели "Развертывание" перейдите на вкладку "Развертывание".



7. Используя клавишу [Ctrl], выберите компьютеры, для которых нужно сформировать задание: ServerSNS, ARM1 и ARM2. Вызовите контекстное меню одного из выделенных компьютеров и выберите опцию "Установить". В правой части окна появится панель настройки параметров задания.



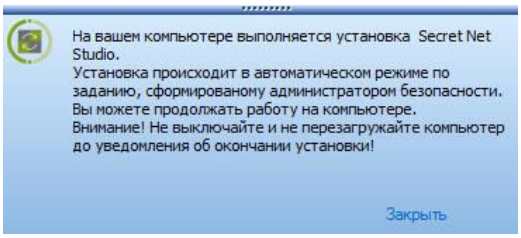
Примечание. Обратите внимание, что в список компьютеров для развертывания компонентов защиты не вошел контроллер домена. Это произошло потому, что ранее мы спроецировали домен безопасности не на весь домен "SN7.local", а только на входящее в его состав организационное подразделение "ou_sns". Для обеспечения в организации защиты уровня 1Б следует включать в домен безопасности всю структуру AD.

8. Настройте параметры задания:

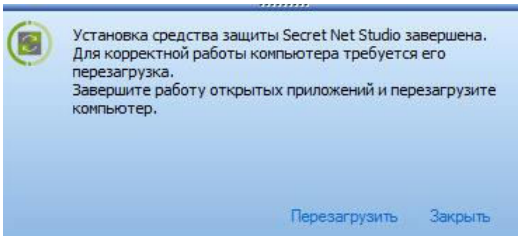
- "Дистрибутив" и "Папка для установки" – оставьте по умолчанию;
- "Защитные подсистемы" – нажмите кнопку "Выбрать" и выберите из папки "C:\Distrib\SNS_8_2\lic" файл с полным составом лицензий;
- прокрутите перечень лицензий вниз и для компонента "Антивирус" выберите "Антивирус (технология ESET)…";

- учетные данные локального администратора: "Имя" – **dadminsns1**, "Пароль" – **P@ssw0rd**.

9. В нижней части панели нажмите кнопку "Установить". Дождитесь окончания формирования заданий. Обратите внимание, что в окне ARM2 в области уведомлений на панели задач появилось уведомление о начале установки ПО.

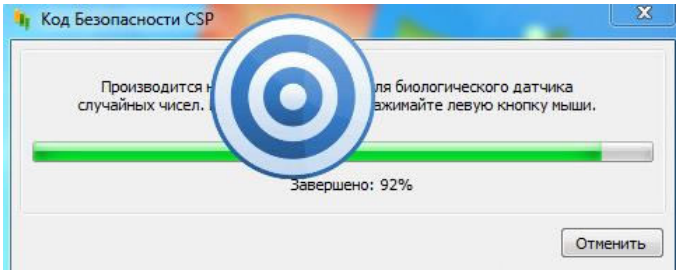


10. Ознакомьтесь с текстом уведомления, нажмите кнопку-ссылку "Закрыть" и перейдите на вкладку "Задания". Здесь вы можете видеть состояние процесса установки выбранного ПО на указанные компьютеры списка. До завершения процесса в области трея будет мигать значок Secret Net Studio  . После завершения установки в области уведомлений окна ARM2 появится сообщение об окончании установки.



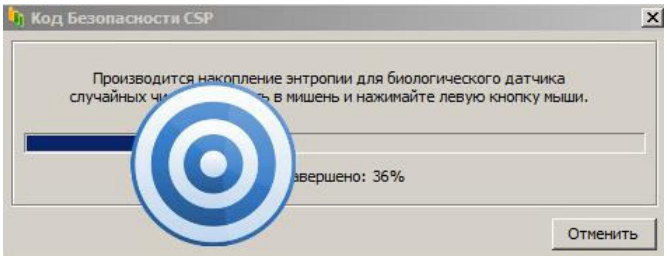
11. Ознакомьтесь с сообщением и перезагрузите ВМ ARM2. Обратите внимание, что загрузка ОС выполняется теперь под контролем защитных механизмов SNS.

12. Авторизуйтесь под учетной записью "dadminsns1". Если в составе Secret Net Studio устанавливался компонент "Шифрование трафика", на экране появится окно мастера накопление энтропии. Следуя его указаниям, выполните настройку биологического датчика случайных чисел.

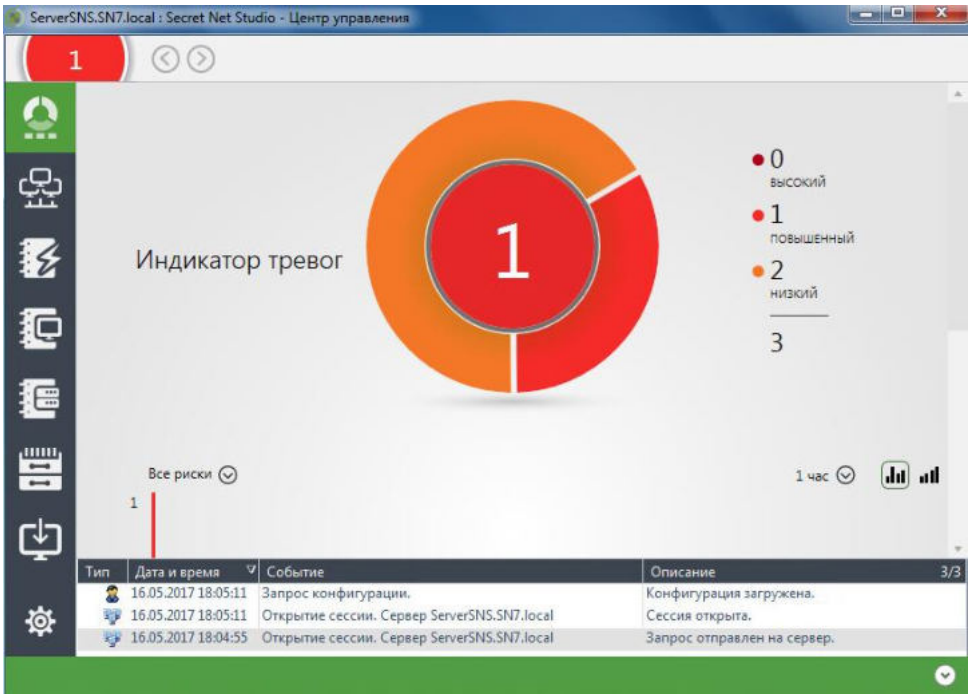


13. Обратите внимание, что в области уведомлений на панели задач в правом нижнем углу экрана появился значок системы Secret Net Studio  .

14. Последовательно, подключаясь к консолям ВМ ServerSNS и ARM1, проследите за ходом установки ПО и по завершении этого процесса перезагрузите ВМ. Авторизуйтесь под УЗ "dadminsns1". Если в составе Secret Net Studio устанавливался компонент "Шифрование трафика", по аналогии (см. пп. 11–13) проведите накопление энтропии для настройки биологического ДСЧ.



15. Проверьте работу установленных на ВМ ARM2, ServerSNS и ARM1 компонентов. Для этого в окне ВМ ARM2 запустите программу управления и подключитесь к серверу безопасности ServerSNS.



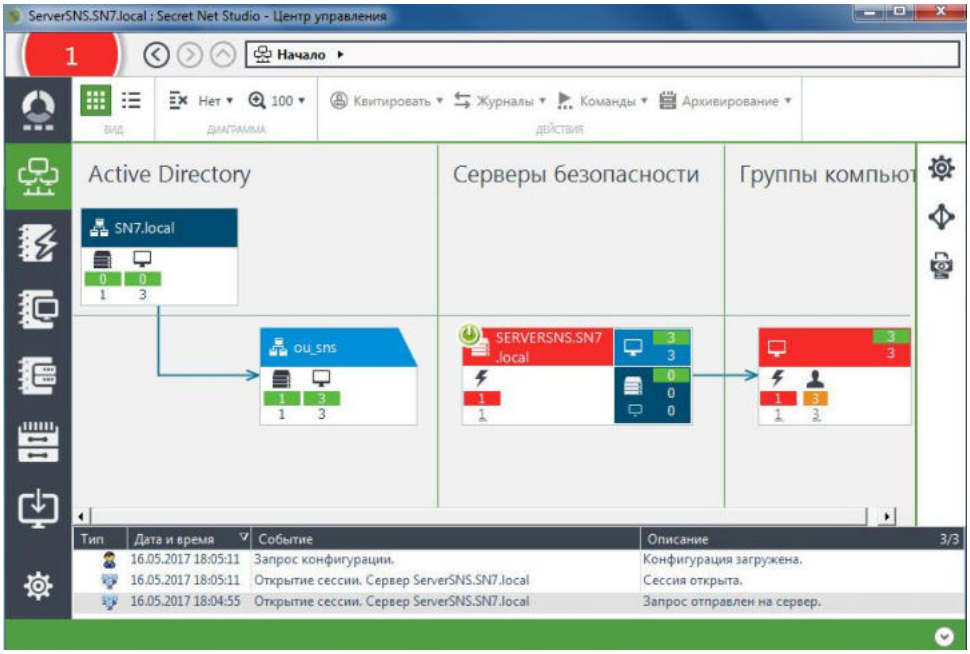
16. Обратите внимание, что в программе управления по умолчанию открылась панель "Начало" – кнопка  на панели навигации в левой части окна окрашена в зеленый цвет. Эта панель содержит сведения о соотношении системных событий тревоги и о состоянии групп объектов управления.

17. На панели навигации нажмите кнопку "Компьютеры"  . Произойдет переключение на панель "Компьютеры", которая содержит средства администрирования и управления компьютерами. По умолчанию данная панель открывается с видом "Диаграмма" – режимом, отображающим в графическом виде сведения о структуре оперативного управления. На диаграмме вы можете увидеть следующие виды объектов:

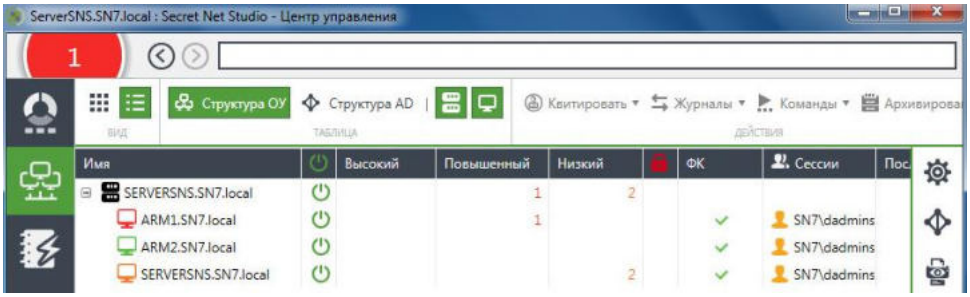
 – домен или организационное подразделение;

 – сервер безопасности;

 – компьютер или группа компьютеров.



18. Обратите внимание, что в верхней части окна программы управления теперь появились элементы панели управления "Компьютеры". Нажмите кнопку "Таблица" и переключитесь в режим для вывода иерархического списка объектов управления в табличном виде.



19. Обратите внимание, что по умолчанию защищаемые компьютеры показываются в таблице объектами структуры домена безопасности. В таблице, в частности, могут отображаться следующие значки:

обозначает, что объект подключен к серверу безопасности;

1 или 2 и пр. – цифры в колонках "Высокий", "Повышенный" и "Низкий" показывают количество соответствующих событий тревоги, произошедших на защищаемом компьютере и ожидающих квитирования (подтверждение приема) администратором безопасности (подробнее см. в главе 2);

значок в колонке с изображением замка обозначает, что соответствующий компьютер заблокирован;

в колонке "ФК" обозначает, что пройден функциональный контроль;

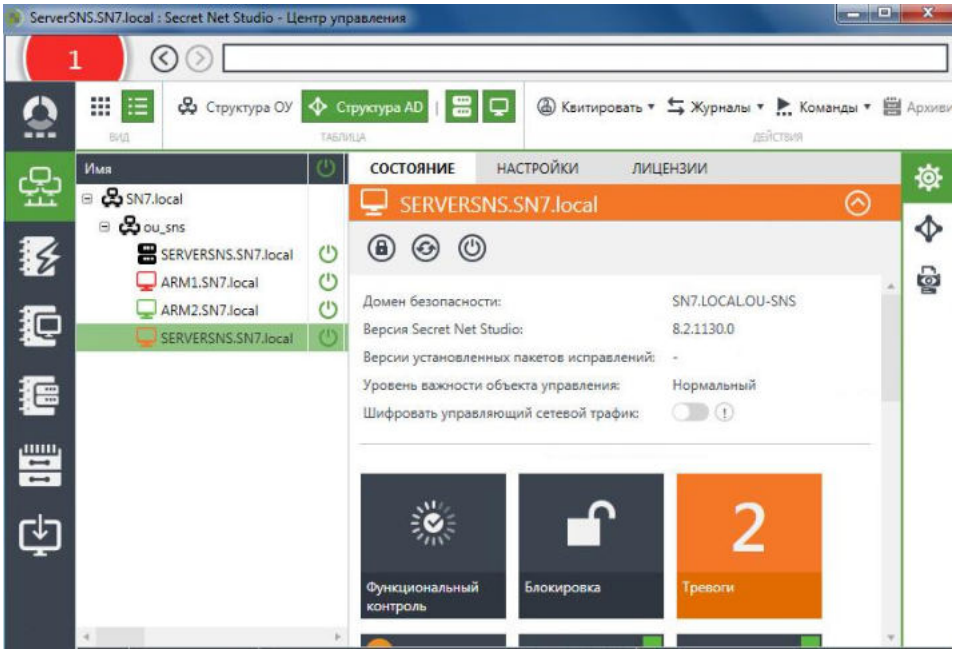
SN7\dadmins – значки в колонке "Сессии" показывают краткие сведения об открытых сессиях или активных пользователях. При этом цвет значка указывает на привилегированность – администратор или пользователь.

20. В верхней части окна на панели управления нажмите кнопку "Структура AD" Структура AD. Теперь объекты в таблице показываются в подчинении объекту домена AD.

21. Для того чтобы просмотреть свойства любого объекта управляемой структуры, выполните одну из операций:

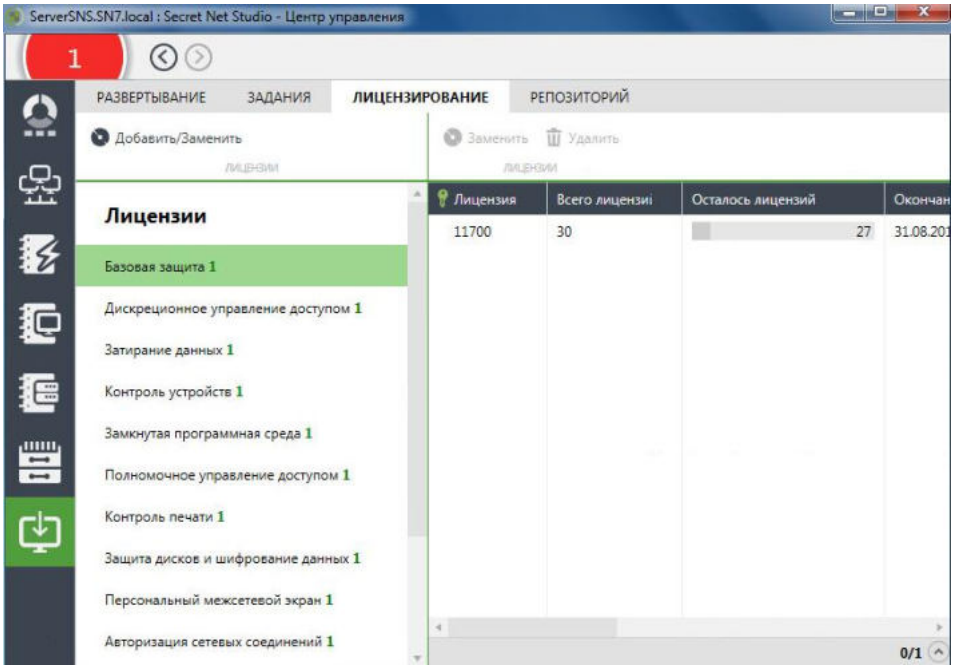
- вызовите контекстное меню объекта и выберите опцию "Свойства";

- выделите объект и в правой части окна нажмите кнопку "Свойства" .



Примечание. Обратите внимание, что через соответствующие кнопки окна свойств объекта (защищаемого компьютера) или через его контекстное меню компьютер можно заблокировать, перезагрузить или выключить.

22. На панели навигации нажмите кнопку "Развертывание" и перейдите на вкладку "Лицензирование", которая предназначена для просмотра и изменения сведений о зарегистрированных лицензиях на сервере безопасности.



В системе Secret Net Studio действуют лицензионные ограничения на использование ряда подсистем, реализующих применение механизмов защиты. Регистрация лицензий осуществляется с помощью специальных файлов.

Данная вкладка содержит сведения о лицензиях, зарегистрированных на сервере подключения (сервере безопасности, с которым установлено соединение программы):

- назначение лицензий (для каких подсистем применяются);

- общее количество и текущее количество незадействованных (оставшихся) лицензий;
- время окончания действия лицензированных возможностей;
- типы лицензий;
- сведения о компании – получателе лицензии.

Лицензии можно зарегистрировать при формировании заданий развертывания ПО. В процессе эксплуатации системы при необходимости можно зарегистрировать новые лицензии, а также заменить или удалить имеющиеся.

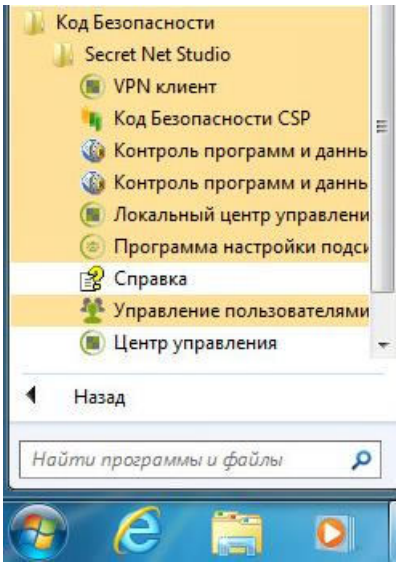
Закройте окно программы управления.

23. В окне консоли ВМ ARM2 из главного меню Windows раскройте группу программ: "Пуск / Программы / Код безопасности / Secret Net Studio" и просмотрите состав установленных компонентов. Обратите внимание на установленное ПО для централизованного управления:

- программа управления ("Центр управления");
- программа "Управление пользователями";
- программа "Контроль программ и данных".

В результате развертывания компонентов защиты Secret Net Studio было также установлено ПО для локального управления.

Мы будем использовать эти программные компоненты в других лабораторных работах.



Контрольные вопросы

1. Какие возможности по обеспечению информационной безопасности предоставляет Secret Net Studio?

2. На соответствие каким требованиям защиты сертифицировано СЗИ Secret Net Studio?

3. Под управлением каких ОС работает СЗИ Secret Net Studio?

4. Каковы основные преимущества применения системы Secret Net Studio?

5. Перечислите защитные компоненты Secret Net Studio. Какие из них лицензируются а) только срочными лицензиями, б) срочными лицензиями или бессрочно?

6. Какие программные модули и защитные механизмы входят в компонент базовой защиты?

7. Какие подсистемы защиты входят в состав компонентов а) базовой защиты, б) "СЗИ от НСД"?

8. Каковы особенности механизма идентификации и аутентификации пользователей в Secret Net Studio?

9. Какие аппаратные идентификаторы могут применяться в системе защиты Secret Net Studio?
10. Возможно ли в Secret Net Studio обеспечить идентификацию и аутентификацию пользователей до загрузки ОС?
11. Для чего в Secret Net Studio предназначен механизм функционального контроля подсистем?
12. Что обеспечивает механизм защиты "ЗПС"?
13. С какими устройствами хранения работает механизм "затирание данных"?
14. Какое количество категорий конфиденциальности может использоваться в Secret Net Studio? Каким ресурсам эти категории могут назначаться?
15. В каком формате копируются в хранилище файлы печатаемых документов при включенном механизме теневого копирования подсистемы контроля печати?
16. Каким категориям пользователей следует предоставлять доступ на чтение данных теневого хранилища?
17. На каких файловых системах может применяться механизм защиты информации на локальных дисках для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера?
18. Для каких вариантов использования можно разворачивать систему Secret Net Studio?
19. Что такое домен безопасности Secret Net Studio?
20. Какие функции могут выполнять отдельные организационные подразделения (Organizational Unit – OU) из структуры Active Directory при организации домена безопасности?
21. Какие протокол и порт используются при обмене данными между клиентами Secret Net Studio и сервером безопасности?
22. Какие компоненты включает в себя СБ? Каково их назначение?
23. Какие средства централизованного управления используются в Secret Net Studio?

Глава 2
Настройка и применение компонентов базовой защиты Secret Net Studio

В первой главе был представлен обзор состава компонентов системы Secret Net Studio и принципов работы ее механизмов защиты. Далее, при более детальном рассмотрении отдельных подсистем и защитных механизмов SNS, будем придерживаться схемы лицензирования и обобщенной структурной схемы клиента СЗИ Secret Net Studio (см. рис. 1 и 2 соответственно).

Данная глава посвящена настройке и управлению механизмами защиты, входящими в состав компонента базовой защиты SNS.

Напомним, что компоненты базовой защиты отдельно не лицензируются, а входят во все лицензируемые наборы и объединяют программные службы, модули и защитные подсистемы, обеспечивающие различные возможности разграничения доступа к ресурсам и контроль действий пользователей.

Организация управления системой защиты

Для организации управления защитой в системе Secret Net Studio предусмотрены следующие возможности:

- локальное управление – это управление механизмами защиты отдельного компьютера, которое осуществляется локальным администратором непосредственно на защищаемом компьютере. Используется в тех случаях, когда централизованное управление для данного компьютера недоступно или нецелесообразно. Программные средства для локального управления входят в состав клиента SNS, устанавливаются по умолчанию и могут применяться пользователями, входящими в группу локальных администраторов компьютера;
- централизованное управление – осуществляется администратором безопасности со своего рабочего места или с любого компьютера сети с установленными средствами централизованного управления.

Внимание! В соответствии с концепцией Secret Net Studio управление безопасностью в защищаемом домене рекомендуется осуществлять централизованно. Централизованное управление имеет приоритет перед локальным.

Для централизованной настройки и применения параметров безопасности на защищаемых компьютерах могут использоваться групповые политики. По умолчанию параметры заданы только в локальной политике.

В дополнение к настройкам локальной политики могут быть заданы параметры в политиках доменов, организационных подразделений и серверов безопасности. Эти параметры применяются на компьютерах, которые относятся к соответствующим доменам, организационным подразделениям или серверам безопасности, независимо от заданных значений в локальной политике каждого компьютера.

Параметры политик применяются в следующей последовательности:

- локальная политика;
- политика домена, т.е. политика, назначенная в режиме "Структура AD" на весь домен;
- политика организационного подразделения – применяется на всех компьютерах, входящих в это организационное подразделение. При наличии иерархии OU политика, заданная для нижестоящего организационного подразделения, имеет более высокий приоритет перед политикой вышестоящего OU;
- политика, заданная для сервера безопасности, – применяется на всех компьютерах, подчиненных этому серверу безопасности. При наличии иерархии серверов безопасности параметры политик на них применяются последовательно – начиная от сервера, которому компьютеры подчинены непосредственно, и далее до корневого сервера в иерархии. Таким образом,

параметры, заданные в политике для корневого сервера безопасности, имеют наивысший приоритет.

Параметры групповых политик на защищаемых компьютерах обновляются автоматически, т.е. этот механизм работает аналогично механизму применения политик ОС Windows. При необходимости администратор может использовать средства принудительного обновления политик, чтобы ускорить процесс применения централизованно заданных параметров на защищаемых компьютерах.

Настройка и применение локальной аутентификации

Централизованная настройка механизма защиты входа в систему выполняется посредством программы управления SNS с рабочего места администратора безопасности. Работа режимов данного механизма определяется следующими параметрами:

- "Запрет вторичного входа в систему" – если режим включен, блокируется возможность запуска команд и сетевых подключений с вводом учетных данных пользователя, не выполнившего интерактивный вход в систему;
- "Количество неудачных попыток аутентификации" – устанавливает ограничение на количество неудачных попыток входа в систему при включенном режиме усиленной аутентификации по паролю. При достижении ограничения компьютер блокируется и вход разрешается только администратору. Если установлено значение "0" – ограничение не действует;
- "Максимальный период неактивности до блокировки экрана" – устанавливает максимально возможный период неактивности, после которого компьютер автоматически блокируется средствами системы Secret Net Studio. Стандартными средствами ОС пользователи могут указать другой период включения блокировки (заставки) компьютера. Если в параметре ОС будет указано значение большее, чем в SNS, то параметр ОС не будет действовать, а будет применяться заданное в Secret Net Studio значение. Если установлено значение "0" – блокировка средствами SNS не осуществляется;
- "Разрешить интерактивный вход только доменным пользователям" – если данный параметр установлен, то интерактивно в систему могут войти только пользователи, зарегистрированные в домене. Интерактивный вход в систему локальных пользователей (включая локальных администраторов) запрещен;
- "Реакция на изъятие идентификатора":
  - "Не блокировать" – при изъятии идентификатора из считывающего устройства блокировка компьютера не выполняется;
  - "Блокировать станцию при изъятии USB-идентификатора" – выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора на базе USB-ключа или смарт-карты, использованного для идентификации пользователя в системе Secret Net Studio (например, eToken PRO (Java));
  - "Блокировать станцию при изъятии любого идентификатора" – выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора любого типа из числа поддерживаемых системой Secret Net Studio (iButton, eToken и др.). Функция блокировки при изъятии идентификатора действует в локальном сеансе работы пользователя, если идентификатор активирован средствами Secret Net Studio и пользователь предъявил этот идентификатор для входа в систему или разблокировал станцию по электронному идентификатору;
- "Режим аутентификации пользователя":
  - "Стандартная аутентификация" – при входе пользователя выполняется только стандартная аутентификация ОС Windows;
  - "Усиленная аутентификация по паролю" – при входе пользователя кроме стандартной аутентификации ОС Windows дополнительно выполняется аутентификация по паролю пользователя средствами системы Secret Net Studio. В этом режиме пользователи, пароль которых не был сохранен в базе данных системы Secret Net Studio, не смогут войти в систему (при этом администратор может разрешить пользователю разовый вход для сохранения пароля, включив параметр "Доверять парольной аутентификации Windows" в диалоге настройки свойств пользователя);

- "Режим идентификации пользователя":
  - "По имени" – для входа в систему пользователь должен ввести свои учетные данные, используя только стандартные средства ОС Windows;
  - "Только по идентификатору" – для входа в систему пользователь должен предъявить присвоенный ему в системе SNS идентификатор. Администратор может войти в систему без предъявления идентификатора только в административном режиме (см. ниже);
  - "Смешанный" – для входа в систему пользователь может предъявить присвоенный в системе SNS идентификатор или ввести свои учетные данные, используя стандартные средства ОС Windows.

Локальная настройка механизма защиты входа в систему выполняется аналогично в программе "Локальный центр управления".

В Secret Net Studio предусмотрен режим интеграции с ПАК "Соболь". Побробные сведения об этом можно найти в руководстве администратора по настройке и эксплуатации Secret Net Studio.

Система защиты Secret Net Studio допускает смену пароля пользователя как администратором, так и самим пользователем. При включенном режиме усиленной аутентификации по паролю процедура административной смены пароля пользователя должна выполняться только в программе управления пользователями (с правами администратора домена безопасности). Если администратор сменит пароль пользователя с помощью других средств, то новый пароль не будет сохранен в БД системы Secret Net Studio, что приведет к невозможности входа пользователя по этому паролю.

При штатном функционировании системы Secret Net Studio вход любого пользователя компьютера, включая администратора, должен выполняться одинаково, в соответствии с механизмами защиты входа в систему. Во время загрузки компьютера перед входом пользователя система защиты проводит инициализацию защитных подсистем и их функциональный контроль. После успешного проведения всех проверок вход в систему разрешается.

Когда необходимо получить доступ к компьютеру в обход действующих механизмов или прервать выполнение инициализации подсистем, администратор может активировать специальный **административный режим входа**. Это может потребоваться в следующих ситуациях:

- при включенном режиме входа в систему "Только по идентификатору", если администратор не имеет персонального идентификатора;
- при повторяющихся ошибках функционального контроля, приводящих к длительному ожиданию инициализации защитных подсистем.

Для активации административного режима входа следует перезагрузить компьютер и при появлении сообщений об инициализации системных сервисов Secret Net Studio нажать и удерживать комбинацию клавиш [Ctrl+Shift+Esc] (или периодически ее нажимать) до появления экрана приветствия (приглашение на вход в систему).

Внимание! Административный режим входа следует использовать только в крайних случаях для восстановления нормального функционирования системы. Выполнив вход в административном режиме, устраните возникшую проблему и перезагрузите компьютер, чтобы восстановить обычный режим входа.

Настройка аппаратной поддержки

Управление персональными идентификаторами

Персональный идентификатор – это устройство для хранения информации для идентификации и аутентификации пользователя. В нем также могут храниться ключи для работы с зашифрованными данными в криптоконтейнерах.

Персональные идентификаторы, которые могут использоваться в Secret Net Studio, были представлены в табл. 1 (см. раздел "Механизмы защиты Secret Net Studio и принципы их работы" в главе 1). Для хранения ключей шифрования данных могут также использоваться сменные носители, такие как дискеты, флеш-карты, USB-флеш-накопители и т.п. К ним также применим термин "идентификатор".

Персональный идентификатор выдается пользователю администратором. Один и тот же персональный идентификатор не может быть присвоен нескольким пользователям одновременно. При этом одному пользователю можно присвоить несколько идентификаторов. Если используется ПАК "Соболь" в режиме интеграции с Secret Net Studio, максимально возможное количество присвоенных идентификаторов для одного пользователя – 32.

Администратор безопасности может выполнять следующие операции с персональными идентификаторами:

- инициализация идентификатора – форматирование, обеспечивающее возможность использования идентификатора в системе Secret Net Studio. При этом удаляются только данные SNS, но не полная инициализация идентификатора, предусмотренная производителем. Данная операция требуется, когда в персональном идентификаторе по каким-либо причинам была нарушена или отсутствует структура данных. Форматированию подлежат также и сменные носители, предназначенные для хранения ключей;
- присвоение (отмена присвоения) идентификатора – добавление в базу данных (удаление из БД) Secret Net Studio сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером;
- включение (отключение) режима хранения пароля в идентификаторе – добавление в базу данных (удаление из БД) Secret Net Studio сведений о включении для пользователя режима хранения пароля в идентификаторе. Совместно с признаком хранения пароля в идентификаторе может быть записан сам пароль пользователя либо, если пароль не был записан в процессе присвоения идентификатора, пользователь может записать его позже, при первом входе в систему по идентификатору. Если пароль пользователя сохранен в идентификаторе, то при входе в систему он не вводится с клавиатуры, а считывается из идентификатора. При отключении режима хранения выполняется также удаление пароля из памяти персонального идентификатора, но при этом идентификатор остается закрепленным за пользователем;
- включение и отключение режима разрешения входа в ПАК "Соболь" – при включенном режиме пользователю разрешено использовать для входа в ПАК "Соболь" идентификатор, присвоенный в системе Secret Net Studio.

Практическое применение персональных идентификаторов рассматривается в соответствующей лабораторной работе (см. ниже). Более подробные сведения об их применении см. в руководствах администратора по принципам построения и по настройке и эксплуатации системы.

Контроль целостности ресурсов

Как уже отмечалось в главе 1, механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера, а его действие основано на сравнении текущих и эталонных значений контролируемых параметров проверяемых ресурсов. При обнаружении несоответствия система оповещает администратора о нарушении целостности ресурса и выполняет заданное при настройке действие, например, блокирует компьютер, на котором это несоответствие обнаружено. Настройка механизма КЦ может осуществляться совместно с механизмом замкнутой программной среды (см. следующую главу). При этом используется единая **модель данных (МД)**, которая представляет собой иерархию объектов с описанием связей между ними. МД содержит 5 категорий объектов:

- **ресурс** – описание файла или каталога, переменной реестра или ключа реестра Windows. Однозначно определяет место нахождения контролируемого ресурса и его тип;
- **группа ресурсов** – объединяет несколько описаний ресурсов одного типа (файлы и каталоги или объекты системного реестра). Например, исполняемые файлы или ключи реестра, относящиеся к конкретному приложению. Однозначно определяется типом входящих в группу ресурсов;
- **задача** – набор групп ресурсов одного и того же или разных типов. Например, задача может одновременно включать группу системных файлов и группу объектов системного реестра Windows;

- **задание** – определяет параметры проведения КЦ-ЗПС. Например, методы контроля, алгоритмы расчета контрольных сумм, расписание проведения контроля, реакции системы на обнаруженные ошибки. Включает в себя набор задач и групп ресурсов, подлежащих контролю. Например, при использовании замкнутой программной среды может объединять описания исполняемых файлов, разрешенных для запуска определенной группе пользователей;
- **субъект управления** – им может быть компьютер и группа, включающая пользователей или компьютеры (а при локальном управлении – также и отдельные пользователи). Определяет компьютеры, на которых выполняется контроль целостности в соответствии с назначенными заданиями, и пользователей, которым разрешено запускать программы, заданные заданиями замкнутой программной среды.

Объекты одной категории являются подчиненными (вышестоящими) по отношению к объектам другой категории. Так, ресурсы являются подчиненными по отношению к группам ресурсов, которые, в свою очередь, подчинены задачам. Включение ресурсов в группы, групп – в задачи, а задач – в задания называется установлением связей между ними. В конечном итоге задания назначаются субъектам. МД, включающая в себя объекты всех категорий, между которыми установлены все нужные связи, – это подробная инструкция системе Secret Net Studio, определяющая, что и как должно контролироваться.

Модель данных состоит из двух частей: одна – относится к замкнутой программной среде, другая – к контролю целостности. Набор заданий для каждой из этих частей модели свой. При этом задачи, группы ресурсов и ресурсы могут входить как в одну, так и в другую часть модели.

Локальная база данных (ЛБД) КЦ-ЗПС организована на каждом компьютере в виде набора файлов, хранящихся в подкаталоге каталога установки Secret Net Studio, и содержит относящуюся к этому компьютеру модель данных.

В централизованном хранилище формируется центральная база данных (ЦБД) КЦ-ЗПС. Для организации централизованного управления создаются две отдельно хранящиеся модели данных – для компьютеров под управлением 32-разрядных версий ОС Windows и для компьютеров с 64-разрядными версиями операционных систем. Каждая из централизованных МД является общей для всех защищаемых компьютеров под управлением версий ОС Windows соответствующей разрядности.

Для настройки механизмов КЦ и ЗПС используется входящая в состав клиента SNS программа "Контроль программ и данных" (далее – программа управления КЦ-ЗПС), в которой можно использовать автоматические и ручные средства формирования элементов МД.

Ниже описан общий порядок настройки механизма КЦ.

1. Подготовка к построению модели данных. На этом этапе выполняется анализ размещения ПО и данных на защищаемых компьютерах и осуществляется подготовка к проведению настройки.

При проведении анализа разрабатываются требования к настройке КЦ и ЗПС, включающие в себя:

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

Из числа защищаемых компьютеров выделяются группы компьютеров 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.

2. Построение фрагмента модели данных по умолчанию. Этот этап выполняется только при формировании новой модели с нуля. В МД автоматически добавляются описания для важных ресурсов ОС Windows, а также описания ресурсов некоторых прикладных программ.

3. Добавление задач в модель данных. В МД добавляются описания задач (прикладное и системное ПО, наборы файлов данных и т.д.) для контроля целостности.

Целью данного этапа настройки является дополнение МД фрагментом, включающим список других необходимых задач (помимо ресурсов Windows и Secret Net Studio). Для этого могут быть использованы как ручные методы, так и специальный механизм генерации задач. Задачи создаются на основании сведений об установленном на компьютере ПО. 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.

Перед началом генерации администратор безопасности может просмотреть список установленного ПО и выбрать те приложения, для которых должны быть сгенерированы задачи. При этом в задачи будут автоматически включены ресурсы, связанные с исполняемыми модулями выбранного ПО. Можно также задать дополнительное условие фильтрации отбираемых ресурсов.

4. Добавление заданий и включение в них задач. Цель данного этапа – сформировать задания на основе задач, созданных на предыдущем этапе. Для заданий контроля целостности должна быть выполнена настройка, в которой указываются:

- методы и алгоритмы контроля защищаемых ресурсов;
- реакция системы в случае нарушения целостности ресурсов;
- перечень событий, регистрируемых в журнале;
- расписание, в соответствии с которым должна проводиться проверка.

5. Расчет эталонов. Для всех заданий рассчитываются эталоны ресурсов.

Данный этап необходим для контролируемых ресурсов, входящих в задания КЦ-ЗПС. Если МД создается с помощью мастера, то процедура расчета будет выполнена автоматически. Если же ее построение осуществляется с использованием генератора задач или вручную, расчет эталонов должен выполняться отдельно.

На этапе настройки механизмов КЦ и ЗПС целесообразно применять следующие способы расчета эталонов:

- расчет эталонов всех контролируемых ресурсов локальной МД (в этом случае в централизованном режиме работы программы "Контроль программ и данных" происходит расчет эталонов только тех ресурсов, которые относятся к тиражируемым заданиям);
- расчет эталонов контролируемых ресурсов, относящихся к определенному заданию.

В локальном режиме расчет эталонов может быть выполнен для всех ресурсов локальной МД, кроме тех, которые входят в тиражируемые задания (эталоны таких ресурсов рассчитываются централизованно).

В централизованном режиме эталоны тиражируемых заданий после расчета будут переданы на компьютеры для синхронизации. Эталоны ресурсов для новых нетиражируемых заданий рассчитываются на компьютерах автоматически после их передачи в ЛБД при синхронизации.

6. Включение механизма КЦ. Устанавливаются связи заданий контроля целостности с субъектами "Компьютер" или "Группа" (компьютеров). С этого момента механизм КЦ начинает действовать в штатном режиме.

Механизм КЦ включается, как только компьютеру будет назначено задание на КЦ с заданным расписанием (в централизованном режиме включение механизма на компьютере произойдет после синхронизации ЛБД данного компьютера с ЦБД).

7. Проверка заданий. Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности настроек заданий, которая заключается в немедленном выполнении задания независимо от расписания. Такая проверка позволяет своевременно исправить ошибки, связанные с некорректной настройкой заданий.

Проверка выполняется отдельно для каждого задания. При этом для задания должны быть рассчитаны эталоны, и оно должно быть связано с субъектом. Предусмотрены следующие режимы проверки:

- облегченный режим – события в журнале не регистрируются, и реакция на ошибки не отрабатывается. По завершении проверки выдается список обнаруженных ошибок;
- режим полной имитации – события регистрируются, и система отрабатывает реакцию на ошибки.

По завершении проверки выдается список обнаруженных ошибок.

В локальном режиме работы программы проверку можно выполнить для любых заданий КЦ, связанных с компьютером (включая задания, созданные централизованно). В централизованном режиме возможна локальная проверка тиражируемых заданий, а также удаленная проверка любых централизованных заданий на включенных компьютерах выбранных субъектов.

Практическую реализацию настройки механизма контроля целостности рассматриваются в соответствующей лабораторной работе (см. ниже).

Задачи, возникающие в процессе эксплуатации

Во время установки клиентского ПО системы Secret Net Studio проверяется наличие модели данных в БД КЦ-ЗПС. Если МД отсутствует, автоматически выполняется ее формирование и наполнение объектами по умолчанию.

При начальном формировании в модель добавляются следующие задания:

- "Задание для контроля ресурсов Secret Net Studio";
- "Задание для контроля реестра Windows";
- "Задание для контроля файлов Windows".

Задания включают готовые задачи с ресурсами, сформированными по предопределенному списку. Для этих заданий устанавливаются связи со следующими субъектами:

- с субъектом "Компьютер" – в локальной модели;
- с субъектом КЦ SecretNetICheckDefault (для 32-разрядных ОС) или SecretNetIcheckDefault64 (для 64-разрядных ОС), который содержит список защищаемых компьютеров домена безопасности с установленной версией ОС соответствующей разрядности – в централизованной модели.

Также в модель добавляются некоторые дополнительные задачи, не связанные с заданиями.

В процессе эксплуатации системы может возникнуть необходимость корректировки или пересмотра модели данных. Если предполагается кардинальная переработка модели, то лучше выполнить ее с нуля. Если переработке будет подвергнута небольшая часть модели, то в этом случае можно применить отдельные процедуры модификации модели.

Настройка аудита в системе

Настройка регистрации событий на компьютерах

По умолчанию в журнале Secret Net Studio регистрируются все возможные события, кроме некоторых событий категории "Контроль приложений", а также некоторых событий категорий "Контроль целостности" и "Дискреционный доступ". Отдельные категории событий (например, события категории "Регистрация") регистрируются в обязательном порядке, и их регистрацию отключить нельзя. Содержащиеся в журнале сведения содержат подробную информацию для анализа событий и позволяют контролировать работу механизмов защиты.

В программе управления можно изменить ограничение максимального объема журнала Secret Net Studio и политику перезаписи хранящейся информации. Допустимый диапазон значений параметра, определяющего размер журнала событий (в килобайтах), – от 64 до 4 194 240 Кб (с шагом 64).

Рекомендуемый максимальный размер для каждого из журналов – не менее 512 Кб.

Для обеспечения возможности аудита отслеживания процессов средствами системы защиты в журнале SNS можно настроить регистрацию событий запуска и завершения работы приложений (процессов):

- событий, относящихся к работе только тех приложений, запуск которых выполнен пользователем компьютера;

- событий запуска и завершения для всех процессов системы – не только пользовательских приложений, но и системных.

Примечание. Регистрация событий для всех процессов системы может существенно увеличить нагрузку на ядро Secret Net Studio и способствовать быстрому переполнению журнала записями о таких событиях. В большинстве случаев данный режим регистрации не является необходимым, поэтому по умолчанию включена регистрация событий, относящихся только к пользовательским приложениям.

Локальные журналы регистрации событий

На рабочих станциях с установленными средствами защиты SNS происходящие в системе события регистрируются в журналах:

- в журнале событий Secret Net Studio накапливается информация о событиях, регистрируемых на компьютере средствами системы защиты. Состав регистрируемых событий определяется параметрами действующей политики безопасности. Журнал использует такой же формат данных и состав полей записей, как и штатные журналы ОС Windows;
- в штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе.

Для локальной работы с журналами может использоваться программа "Локальный центр управления", которая позволяет загружать и просматривать записи журнала SNS и штатных журналов ОС Windows, хранящихся на компьютере локально.

Хранение и очистка локальных журналов

При регистрации событий записи о них помещаются в соответствующие локальные журналы (штатные журналы ОС Windows и журнал Secret Net Studio). Записи из локальных журналов могут загружаться в программу "Локальный центр управления" или в другую программу работы с журналами (кроме журнала Secret Net Studio).

Локальные журналы SNS хранятся в локальном хранилище до момента их передачи в централизованное хранилище на сервер безопасности. Отправку локальных журналов в БД СБ следует проводить своевременно, избегая их переполнения или чрезмерной нагрузки на СБ и каналы связи при их получении. Чтобы избежать проблем, связанных с несвоевременной передачей данных, администратору безопасности следует проверить и при необходимости откорректировать параметры сбора журналов.

После передачи локальных журналов SNS в БД СБ происходит очистка их содержимого.

По мере регистрации событий записи журналов в локальном хранилище могут замещаться новыми записями. Поведение системы в части перезаписи информации о событиях в журнале SNS настраивается отдельными параметрами.

В программе управления пользователь может экспортировать записи журналов в файлы. При экспорте журнала SNS экспортируются также файлы из хранилища теневого копирования, относящиеся к экспортируемым записям.

Возможна очистка журнала Secret Net Studio, при которой из локального хранилища удаляются все записи или выбранная их часть. Вместе с этим происходит очистка хранилища теневого копирования – удаляются файлы, которые были помещены туда при регистрации соответствующих событий.

Возможные действия пользователей над журналами определяются соответствующими привилегиями.

Предоставление привилегий доступа к журналам

Доступ к записям журналов предоставляется сотрудникам, ответственным за управление системой защиты. Права на загрузку записей и управление содержимым журналов определяются привилегиями пользователей для работы с локальными и с централизованными журналами.

Для локальной работы с журналами предоставляются следующие привилегии:

- "Просмотр журнала системы защиты" – пользователь может загружать для просмотра записи локального журнала Secret Net Studio;

- "Управление журналом системы защиты" – пользователь может загружать для просмотра записи локального журнала Secret Net Studio, а также осуществлять его очистку.

Примечание. Привилегия "Управление журналом системы защиты" включает в себя разрешение на просмотр журнала Secret Net Studio. Однако во всех случаях, когда пользователям нужна привилегия на управление журналом, рекомендуется предоставлять обе эти привилегии.

Оповещения о событиях тревоги

События тревоги считаются события, которые регистрируются в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибка". События тревоги различаются по степени значимости самих событий и уровню важности объекта, на котором они произошли.

Критические события могут иметь уровень тревоги "высокий" для объектов с высоким уровнем важности или "повышенный" – для объектов с обычным уровнем важности. Менее значимые события имеют уровень тревоги "повышенный" или "низкий" соответственно уровню важности объектов.

Уровень для событий тревоги, зарегистрированных на данном компьютере, определяется уровнем важности этого компьютера – его можно указать в программе управления Secret Net Studio, в разделе настроек "Учетная информация" (см. лабораторную работу №3 главы 2). Если для объекта указан высокий уровень важности, поступающие уведомления о событиях тревоги на этом объекте будут учитываться в системе с более высоким уровнем. То есть события с уровнями тревоги "повышенный" и "нормальный" будут интерпретированы системой с уровнями "высокий" и "повышенный" соответственно.

Сервер безопасности накапливает сведения о событиях тревоги в отдельном журнале. Журнал событий тревоги формируется из уведомлений, направляемых серверу от защищаемых компьютеров.

С помощью настройки отдельных параметров Secret Net Studio можно управлять фильтрацией событий тревоги для ограничения поступающих уведомлений от защищаемых компьютеров, за счет чего сократить сетевой трафик и обеспечить получение уведомлений только о важных событиях.

При возникновении на компьютере событий тревоги система защиты может локально оповещать об этом текущего пользователя компьютера. Режим локального оповещения можно включать и отключать для всех пользователей компьютера (компьютеров) или предоставить пользователям возможность управлять этим режимом самостоятельно.

Настройку режима оповещения можно проводить с помощью программы управления централизованно либо в локальном режиме.

При регистрации событий тревоги на защищаемых компьютерах, подчиненных серверу безопасности или его подчиненным серверам, система Secret Net Studio может автоматически оповещать об этом по электронной почте ответственных сотрудников. Например, можно настроить рассылку уведомлений следующим образом:

- при возникновении событий тревоги категории "Вход/выход" на защищаемых компьютерах, подчиненных данному серверу безопасности, уведомления направляются системному администратору;
- при возникновении событий тревоги категории "Полномочное управление доступом" на компьютерах, подчиненных данному серверу безопасности и входящих в отдельное подразделение, уведомления направляются начальнику этого подразделения;
- при возникновении любого события тревоги на любом защищаемом компьютере (из числа компьютеров, подчиненных данному серверу безопасности или его подчиненным серверам) уведомления направляются администратору безопасности и аудитору.

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, он должен выполнить процедуру квитирования, т.е. подтверждения получения информации с описанием принятых мер.

Режимы отображения сведений из журналов событий

Для анализа загруженной информации о событиях при работе с журналами в программе управления предусмотрены следующие режимы:

- режим "События" – основной и наиболее функциональный режим для просмотра и управления записями журналов, который позволяет выполнять все необходимые действия: квитирование, печать, экспорт и пр.;
- режим "Угрозы" отображает полученный в результате анализа загруженных записей список событий угроз и предназначен для представления администратору или аудитору наиболее важной для них информации из журналов.

События угроз представляют собой скоррелированные или разъясняющие сведения о зарегистрированных событиях тревог (например, событиях с признаками подбора пароля).

Правила поиска угроз могут создаваться администратором либо вручную "с нуля", либо непосредственно при работе с журналами на основании отдельных записей.

Подробнее о режимах "События" и "Угрозы" см. в лабораторной работе №3 ниже в этой главе.

Архивирование записей журналов из БД СБ

Для обеспечения сохранности информации, а также для вывода неактуальных сведений из БД и сокращения времени выполнения запросов к ней следует проводить регулярное архивирование (по расписанию либо по специальной команде из ПУ) из БД СБ записей журналов, поступивших от подчиненных защищаемых компьютеров. Сервер безопасности создает архивы журналов в файлах специального формата *.omax. В некоторых версиях СУБД действуют ограничения на объем БД и, если размер базы их превысит, то сохранение новой информации будет невозможно до очистки БД. Архивируются все записи журналов, имеющиеся в БД сервера безопасности на момент начала процесса архивирования (для журнала СБ – архивируются сведения о завершенных сессиях). Записи, помещенные в архив, удаляются из централизованного хранилища.

Внимание! Чтобы выполнять архивирование и очистку журналов, пользователю должна быть предоставлена привилегия "Архивирование/восстановление журналов".

Лабораторная работа №1 "Локальная настройка Secret Net Studio в соответствии с заданными параметрами"

В состав компонентов SNS, используемых для локального управления, входят следующие программные средства:

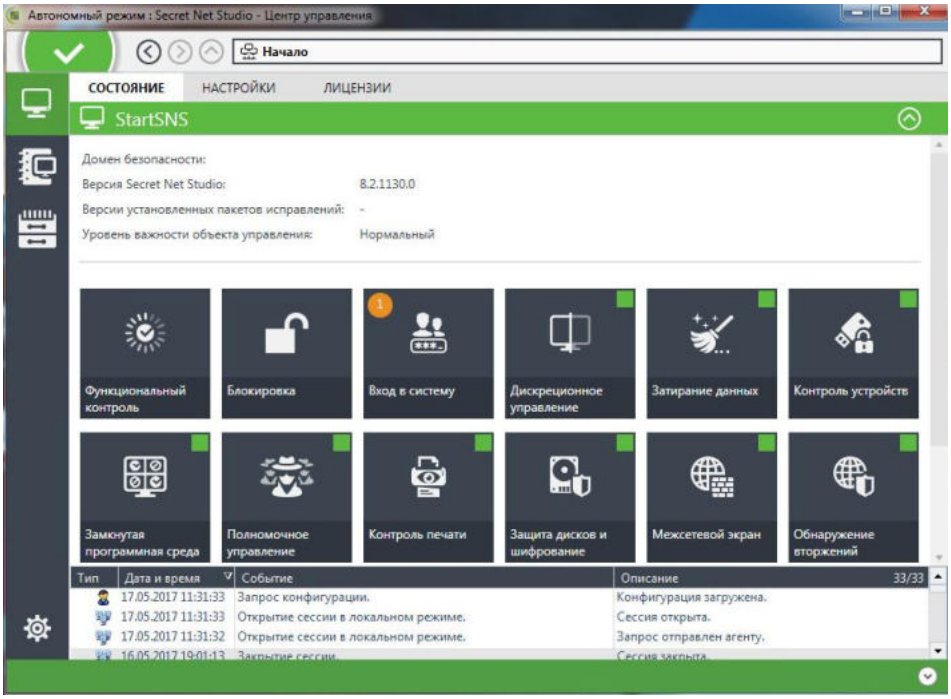
- значок Secret Net Studio в области уведомлений на панели задач Windows;
- дополнительная вкладка "Secret Net Studio" в диалоговом окне настройки свойств ресурса (файла, папки или устройства);
- программа настройки подсистемы полномочного управления доступом;
- диалоговое окно "Управление Secret Net Studio" в Панели управления Windows;
- программа "Локальный центр управления" (устанавливается в составе клиента Secret Net Studio);
- программа управления пользователями (для настройки параметров локальных пользователей);
- программа "Контроль программ и данных" в локальном режиме работы;
- дополнительные программные средства, описание работы с которыми приводится в руководстве администратора.

В данной лабораторной работе будут рассмотрены следующие операции:

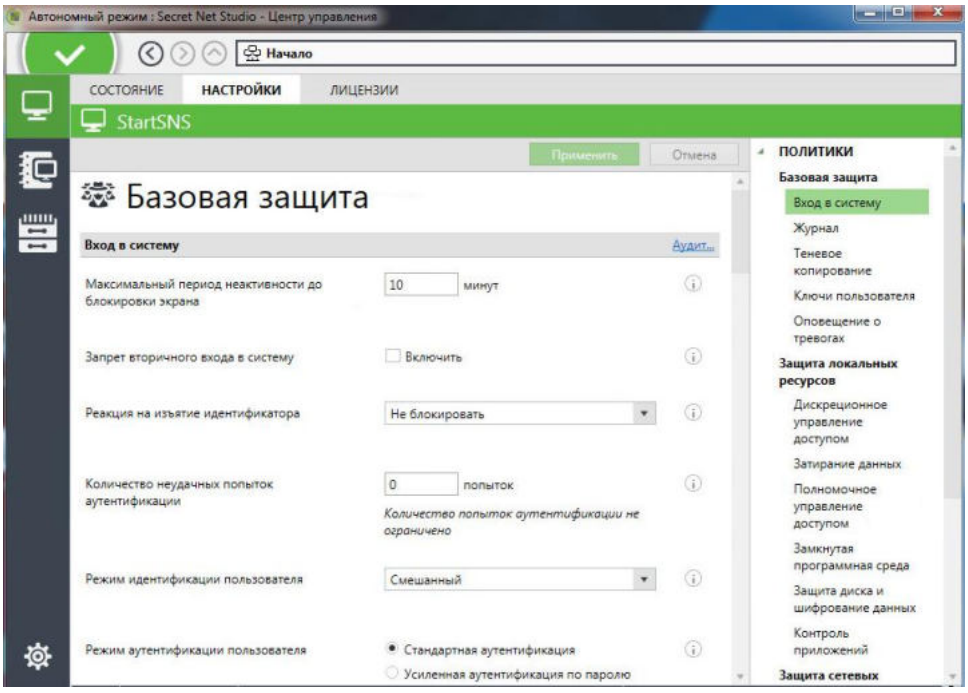
- изменение заданных по умолчанию параметров некоторых локальных политик безопасности для базовой защиты Secret Net Studio;
- изменение максимально допустимого размера журнала системы защиты Secret Net Studio и выбора регистрируемых в нем событий;
- просмотр локальных журналов в программе управления Secret Net Studio.

Программа "Локальный центр управления" позволяет просматривать хранящиеся на компьютере штатные журналы Windows и журнал SNS. Последний может просматриваться только средствами Secret Net Studio.

1. Откройте консоль BM StartSNS и авторизуйтесь в гостевой ОС под учетной записью администратора "adminsns".
2. Откройте программу управления в локальном режиме: "Пуск → Все программы → Код Безопасности → Secret Net Studio → Локальный центр управления". Откроется окно центра управления в автономном режиме.

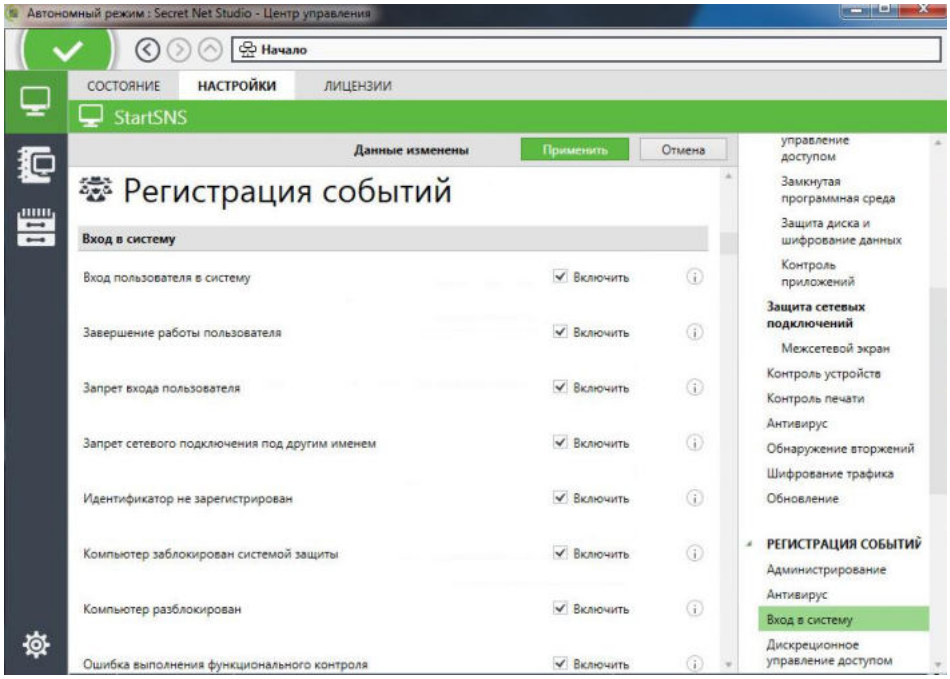


3. На панели управления "Компьютер" выберите вкладку "Настройки". В правой части окна вы увидите список настроек по разделам. В разделе "Политики / Базовая защита" выберите группу параметров "Вход в систему". В центральной части окна вы увидите текущие параметры выбранной группы.

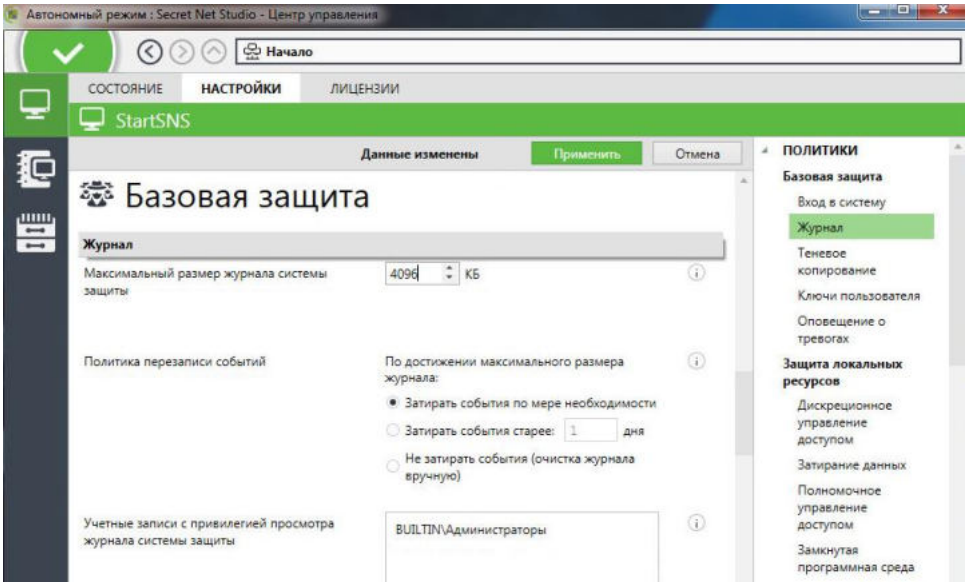


4. Обратите внимание на значок ⓘ справа от каждой настройки. Он позволяет просмотреть описание каждого параметра. Ознакомьтесь с этими описаниями.

5. Для политик группы "Вход в систему" установите следующие значения:
   - "Максимальный период неактивности до блокировки экрана" – **15** минут (настройка применяется после следующего входа в систему);
   - "Запрет вторичного входа в систему" – "Включить" (для применения данной настройки необходима перезагрузка компьютера);
   - "Реакция на изъятие идентификатора" – оставьте значение по умолчанию "Не блокировать";
   - "Количество неудачных попыток аутентификации" – **12** (настройка применяется после следующего входа в систему);
   - "Режим идентификации пользователя" – "По имени" (настройка применяется после следующего входа в систему);
   - Режим аутентификации пользователя" – "Стандартная аутентификация" (настройка применяется после следующего входа в систему).
6. Настройте регистрацию событий, относящихся к работе политик группы "Вход в систему". Для этого:
   - в правой части заголовка группы нажмите ссылку "Аудит". Обратите внимание, что в правой части окна теперь выбрана группа "Вход в систему" раздела "Регистрация событий", а в центральной части отображаются настройки этой группы;

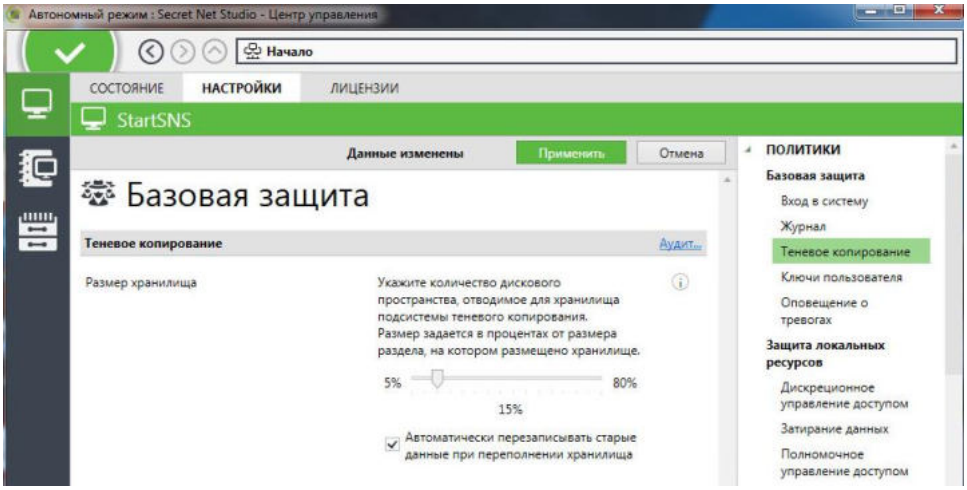


   - по умолчанию включена регистрация всех событий. С помощью значка ⓘ ознакомьтесь с описаниями событий. В рамках данной лабораторной работы не выключайте регистрацию событий.
7. В правой части окна в разделе "Политики", в категории базовой защиты выберите группу "Журнал". Установите следующие параметры:
   - "Максимальный размер журнала системы защиты" – **4096** Кб;
   - "Политика перезаписи событий" – "Затирать события по мере необходимости".

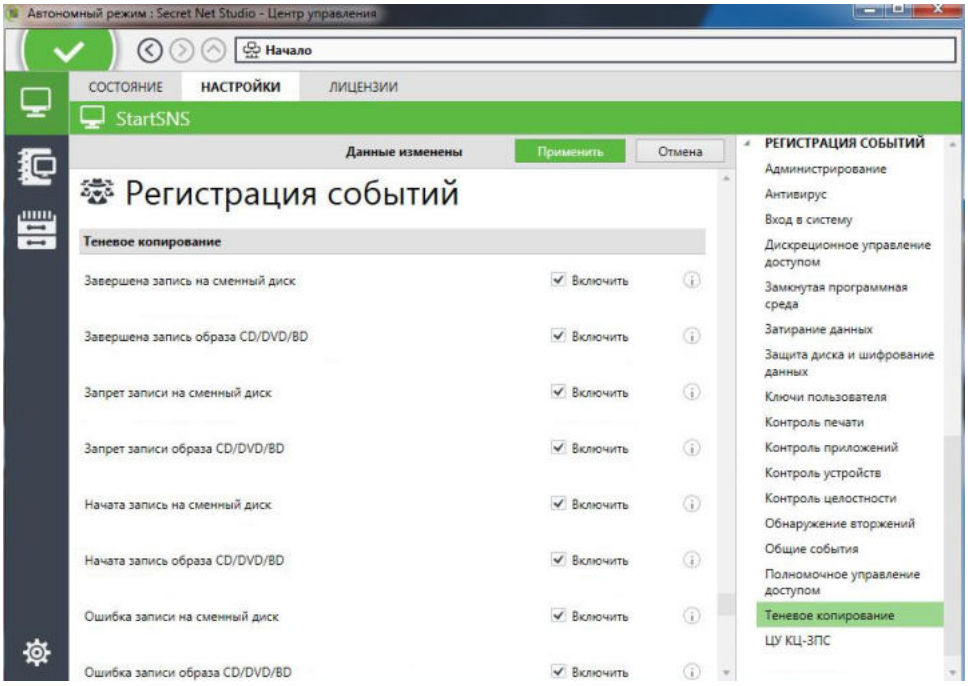


8. В разделе "Политики", в категории базовой защиты выберите группу "Теневое копирование". Установите следующие параметры:

- "Размер хранилища" – **15** %;
- "Автоматически перезаписывать старые данные…" – убедитесь, что в данном поле установлен флажок.



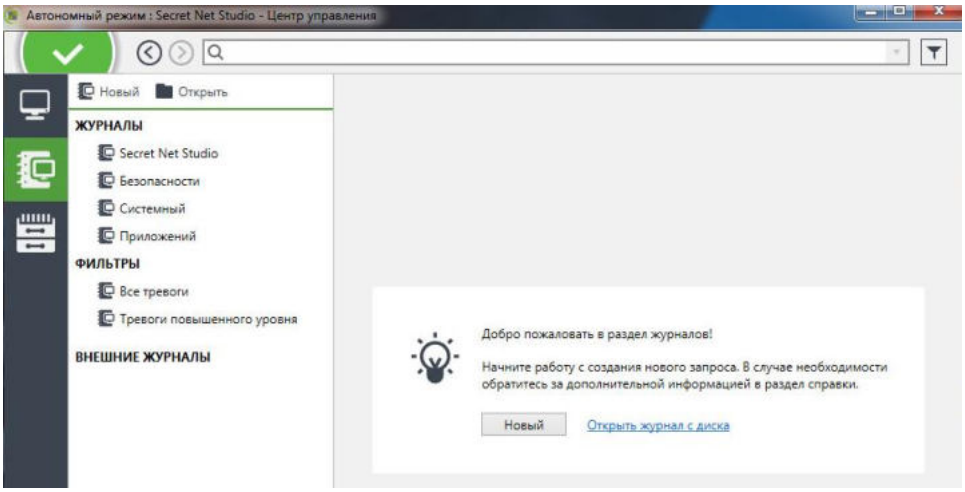
9. Используя описание п. 6 данной лабораторной работы (см. выше), просмотрите перечень типов регистрируемых событий группы "Теневое копирование".



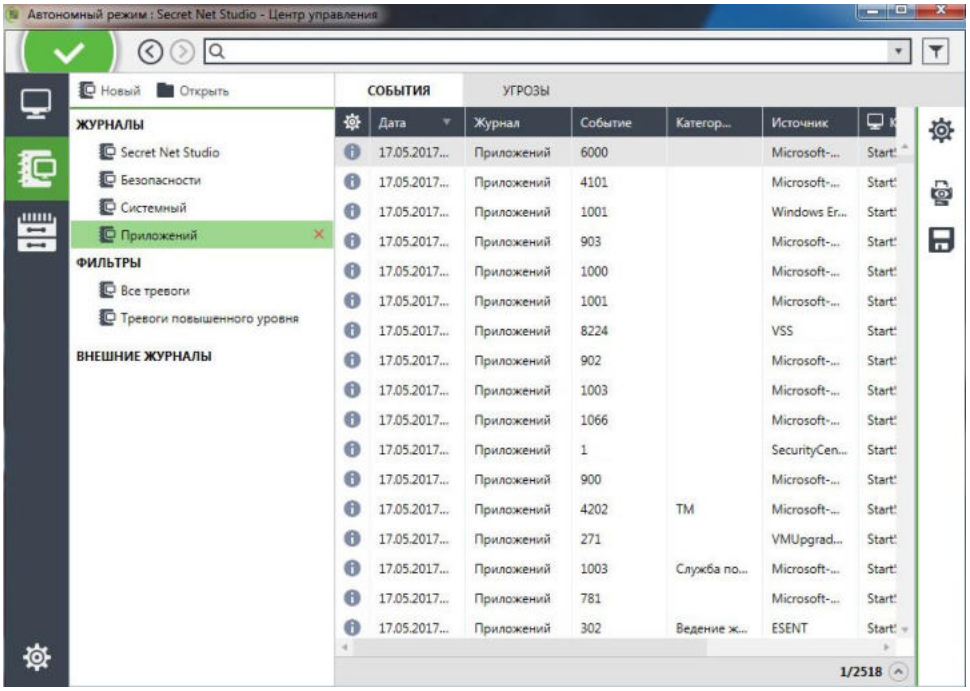
10. Чтобы активировать новые установленные значения параметров политик безопасности на вкладке "Настройки", нажмите кнопку "Применить" Применить. Дождитесь завершения операции сохранения изменений и обратите внимание на появившуюся запись об изменении политик в панели событий. Перезагрузите ВМ StartSNS и вновь запустите программу управления.

11. Просмотрите содержимое локальных журналов в программе управления Secret Net Studio. Для этого:

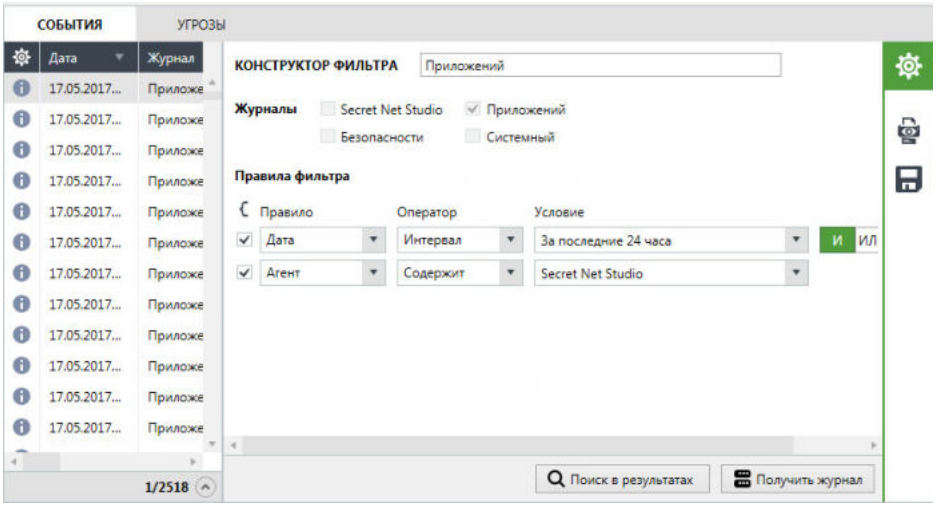
- в окне программы управления Secret Net Studio в панели навигации выберите "Журналы станций". Вы увидите перечень доступных для просмотра локальных журналов;



- для того чтобы просмотреть полное содержимое любого из журналов, достаточно выбрать его двойным щелчком мыши. Выберите журнал приложений. Обратите внимание, что открылась вкладка просмотра записей и в правой части окна появились кнопки, позволяющие распечатать или сохранить журнал в файл на диске;



- в случае необходимости получить более конкретную выборку записей журнала можно составить запрос на формирование выборки по определенным условиям. Нажмите в правой части окна кнопку "Запрос" и в раскрывшейся панели с помощью кнопки "Добавить правило" добавьте следующие правила: "Дата" – "Интервал" – "За последние 24 часа" и "Агент" – "Содержит" – "Secret Net Studio";



- нажмите кнопку "Поиск в результатах", закройте панель настройки запроса, нажав в правой части окна кнопку "Запрос" , и просмотрите полученный результат;
- подсистема запросов позволяет формировать выборки по более развернутым условиям, включая записи из любых локальных журналов. На панели инструментов нажмите кнопку "Новый" Новый, установите произвольные правила фильтра, нажмите кнопку "Получить журнал" и просмотрите результат;
- последовательно просмотрите журналы безопасности и Secret Net Studio.

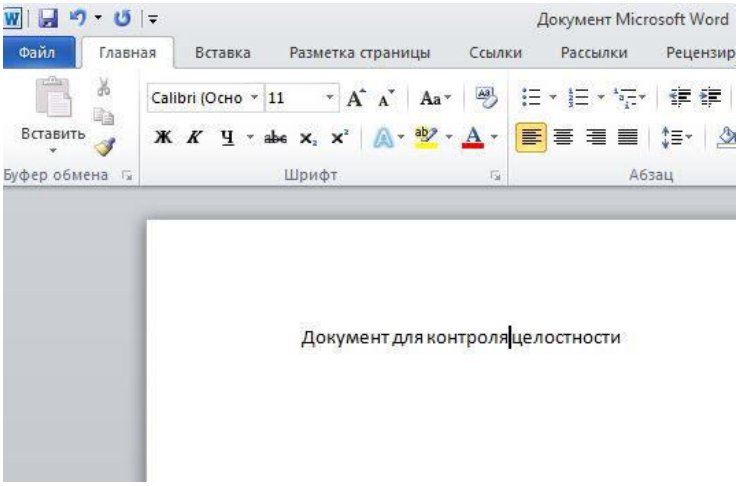
12. Изменены некоторые локальные политики, установлен максимальный размер журнала системы защиты Secret Net Studio, показана возможность выбора регистрируемых в нем событий и в программе управления SNS проведен просмотр локальных журналов.

Останьтесь в текущем окне ВМ StartSNS. Выполнение лабораторной работы завершено.

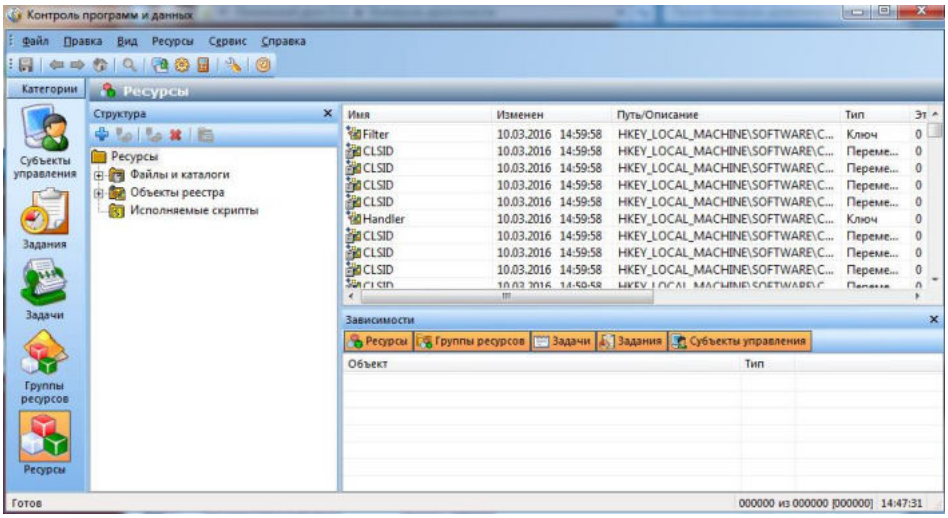
Лабораторная работа №2 "Настройка механизма контроля целостности"

Принципы работы механизма контроля целостности и порядок его настройки были описаны в главе 2. В данной лабораторной работе проводится начальная настройка этого механизма и проверяется его работа на примере контроля целостности текстового файла формата Microsoft Word.

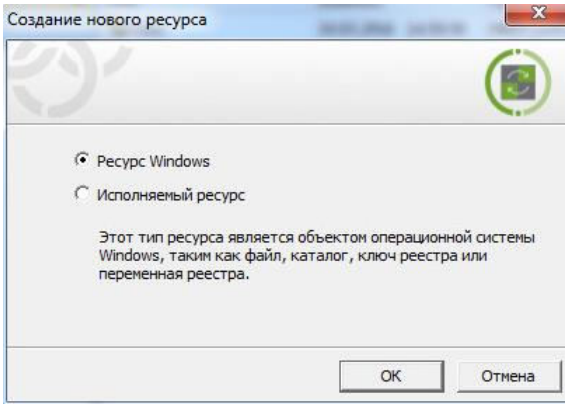
1. В окне ВМ StartSNS на диске "C:" создайте папку "Контроль целостности". В этой папке создайте файл "Документ Microsoft Word.docx" с произвольным содержанием, который будет контролируемым ресурсом в МД КЦ.



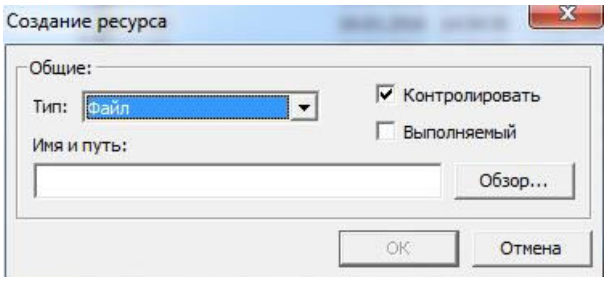
2. Запустите программу "Контроль программ и данных" в локальном режиме: "Пуск → Все программы → Код Безопасности → Secret Net Studio → Контроль программ и данных" и в открывшемся окне выберите категорию "Ресурсы".



3. Подготовьте описание контролируемого ресурса (созданного ранее файла) в модели данных КЦ. Для этого:
   - в поле "Структура" вызовите контекстное меню папки "Ресурсы" и выберите опцию "Создать ресурс(ы) / Одиночный";

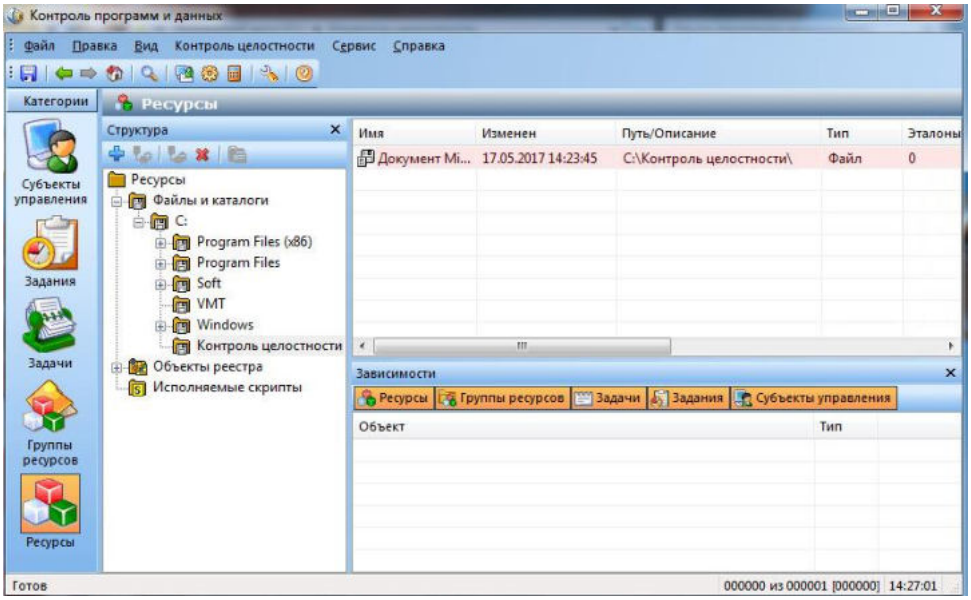


- в окне создания нового ресурса выберите тип "Ресурс Windows" и нажмите кнопку "ОК" – откроется следующее диалоговое окно создания ресурса;



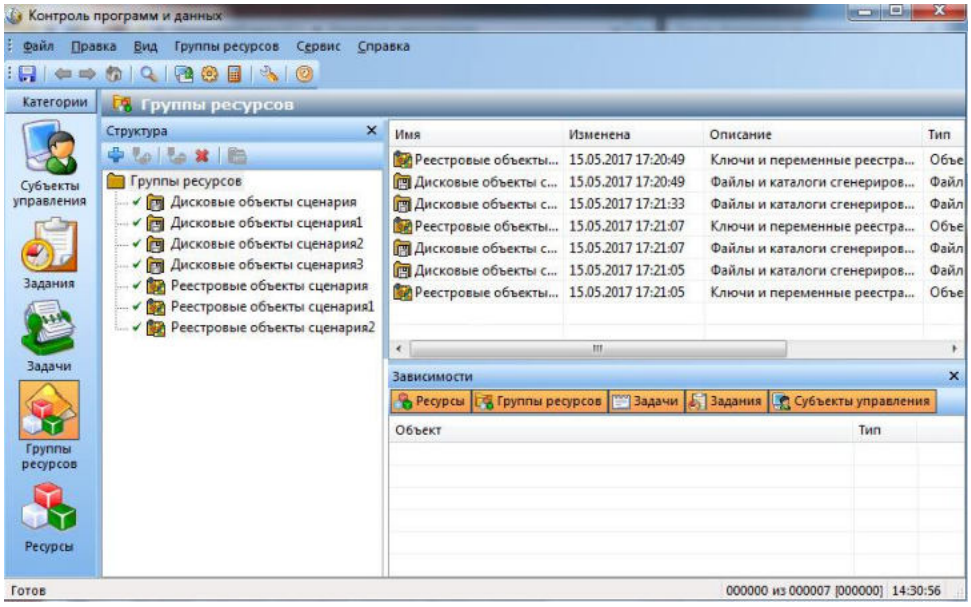
- в поле "Тип" оставьте установленный по умолчанию тип ресурса "Файл", через кнопку "Обзор" укажите путь к созданному в п. 1 файлу "Документ Microsoft Word.docx" и нажмите кнопку "ОК". Описание ресурса готово, и вы вернулись в окно "Контроль программ и данных".

4. В окне "Контроль программ и данных" в поле "Структура" разверните ветку "Ресурсы / Файлы и каталоги / C:" и в папке "Контроль целостности" найдите запись с описанием выбранного вами файла для контроля.

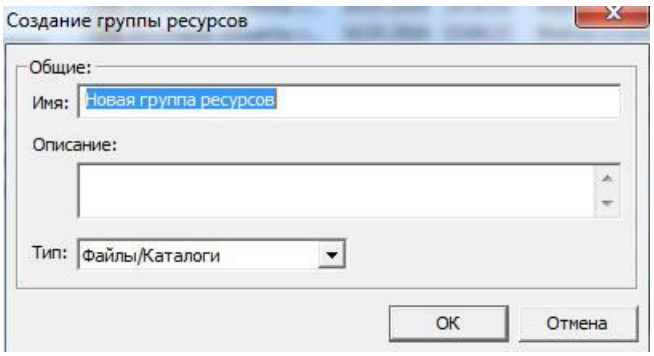


5. Согласно описанию МД КЦ, сформируйте группу ресурсов и добавьте в нее подготовленный ресурс. Для этого:

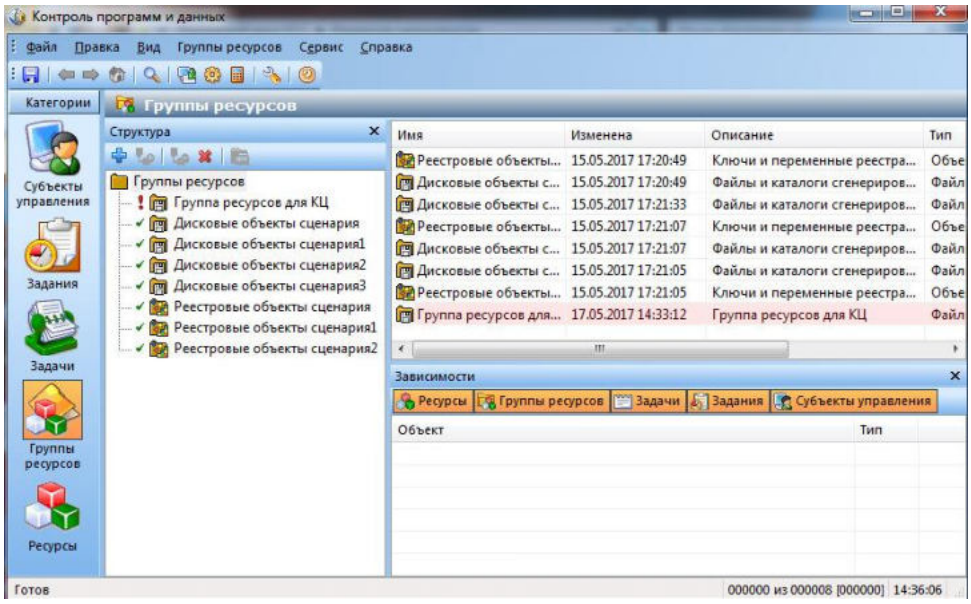
- в окне "Контроль программ и данных" выберите категорию "Группы ресурсов";



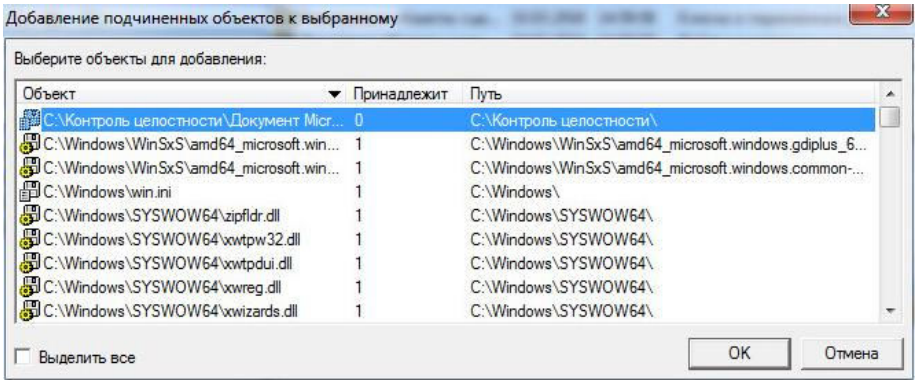
- в поле "Структура" вызовите контекстное меню папки "Группы ресурсов" и выберите опцию "Создать группу / Вручную" – откроется диалоговое окно;



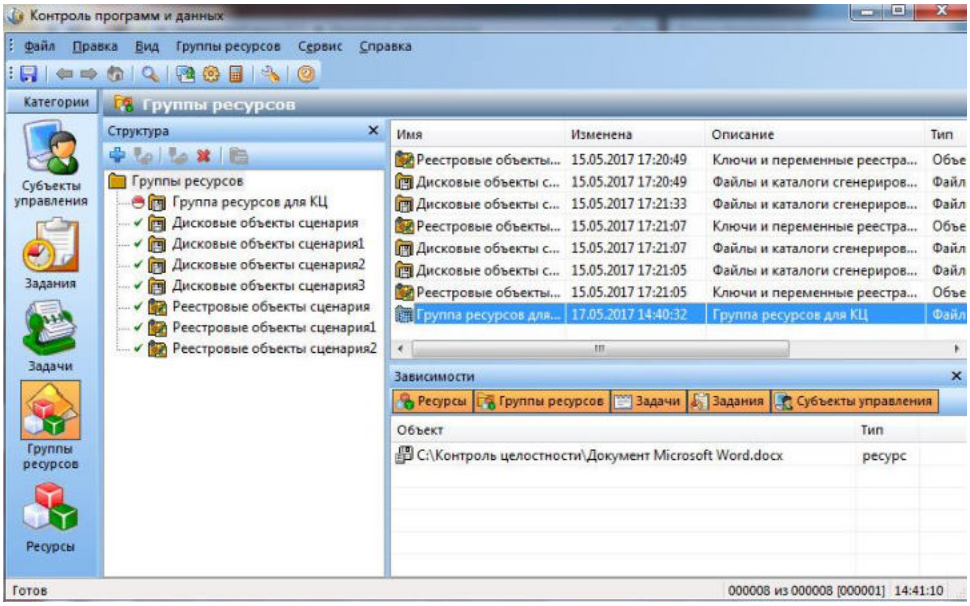
- в окне "Создание группы ресурсов" заполните поля: "Имя" – введите "Группа ресурсов для КЦ", "Описание" – произвольно. Нажмите кнопку "ОК". В окне "Контроль программ и данных" появится запись с названием созданной группы. Обратите внимание, что эта группа пока пустая;



- в группу "Группа ресурсов для КЦ" добавьте созданный ранее ресурс. Для этого на записи группы щелкните правой кнопкой и выберите опцию "Добавить ресурсы → Существующие";

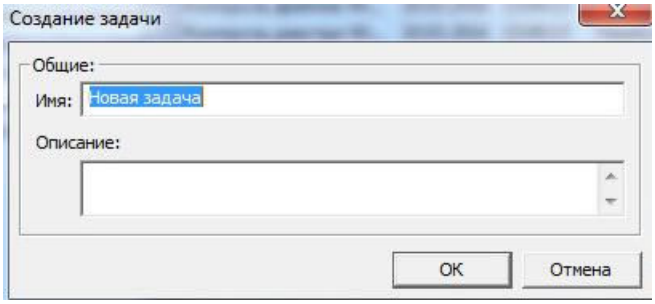


- в открывшемся диалоговом окне выделите запись подготовленного вами ранее файла ресурса "C:\Контроль целостности\Документ Microsoft Word.docx" и нажмите кнопку "ОК" – в созданную группу добавлен файл ресурса.

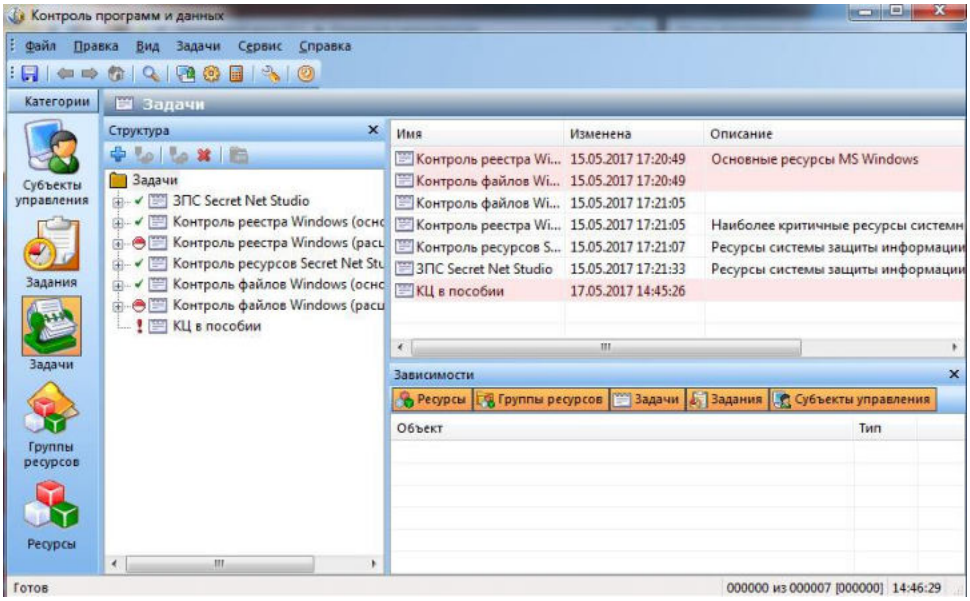


6. В окне "Контроль программ и данных" создайте новую задачу и добавьте в нее подготовленную для контроля группу ресурсов. Для этого:

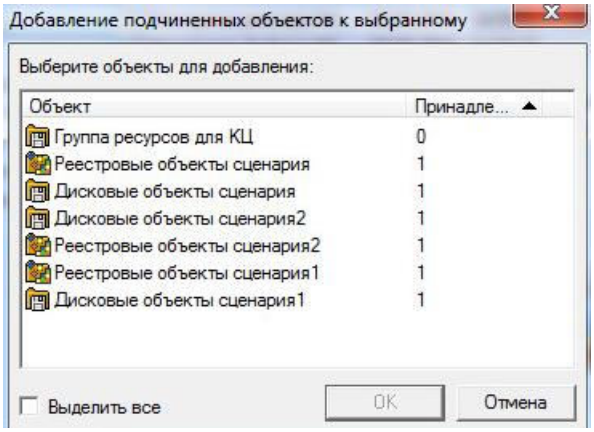
- выберите категорию "Задачи", вызовите контекстное меню папки "Задачи" и выберите опцию "Создать задачу / Вручную". Откроется диалоговое окно;



- введите в поле "Имя" – имя задачи "КЦ в пособии", в поле "Описание" – произвольный текст;
- нажмите кнопку "ОК". В структуре "Задачи" окна "Контроль программ и данных" появилась новая запись;



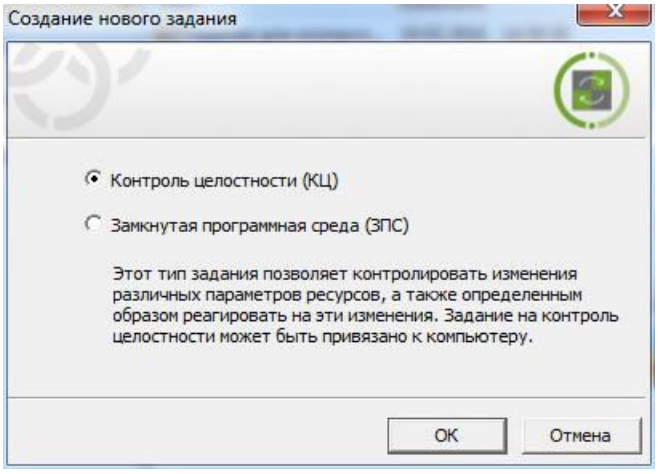
- в созданную задачу добавьте группу ресурсов для КЦ. Для этого вызовите контекстное меню задачи "КЦ в пособии" и выберите опцию "Добавить группы / Существующие". Откроется диалоговое окно;



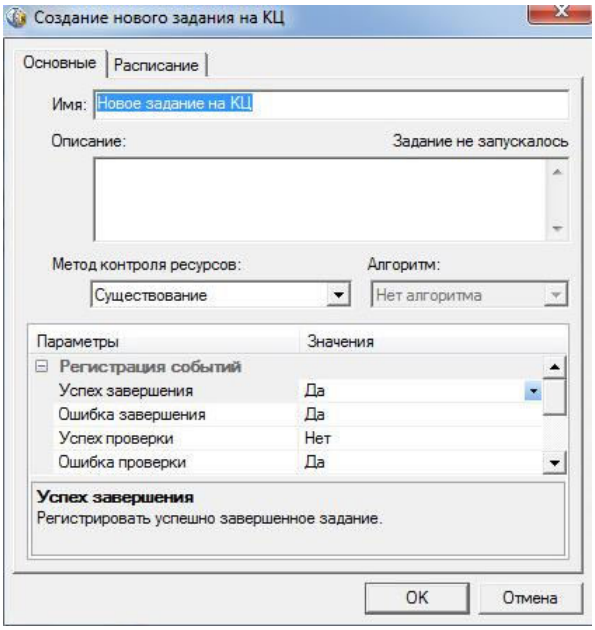
- в окне "Добавление подчиненных объектов к выбранному" выберите запись "Группа ресурсов для КЦ" и нажмите кнопку "ОК" – задача создана и в нее добавлена группа.

7. В окне "Контроль программ и данных" создайте новое задание. Для этого:

- откройте категорию "Задания" и в контекстном меню папки "Задания" выберите опцию "Создать задание". Откроется диалоговое окно;

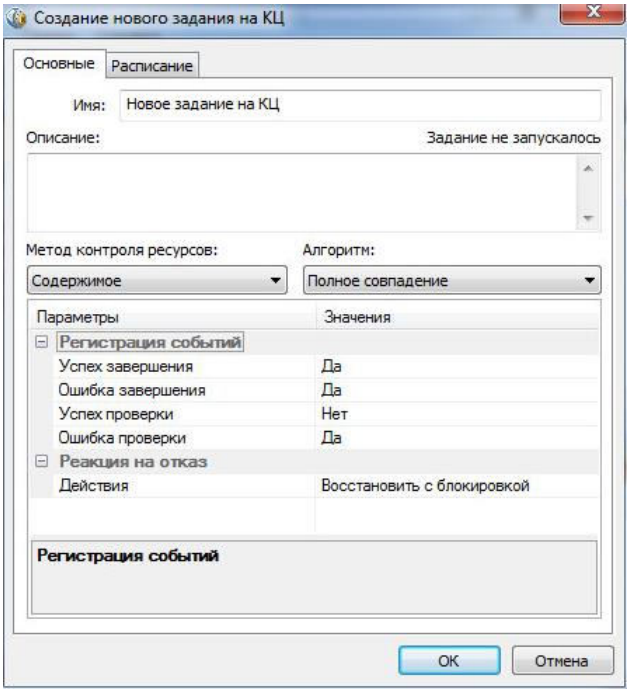


- обратите внимание, что опция "Контроль целостности (КЦ)" выбрана по умолчанию и нажмите кнопку "ОК". Откроется диалоговое окно "Создание нового задания на КЦ";



- в окне "Создание нового задания на КЦ" установите параметры: "Метод контроля ресурсов" – "Содержимое", "Алгоритм" – "Полное совпадение", в группе "Реакция на отказ" для параметра "Действие" выберите "Восстановить с блокировкой" (значение контролируемого параметра ресурса восстанавливается из эталона. Компьютер блокируется, и снять блокировку сможет только администратор безопасности);

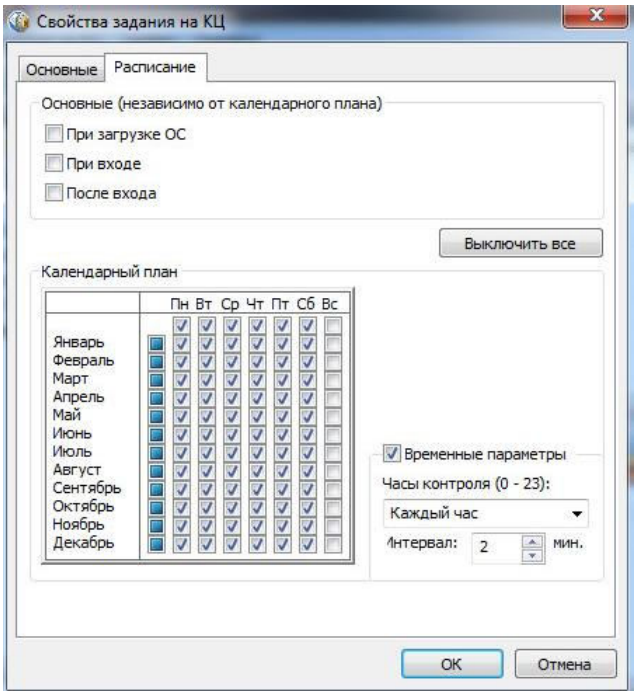
Алгоритм "Полное совпадение" предусматривает возможность восстановления контролируемого объекта в случае нарушения его целостности. Однако при использовании данного алгоритма существенно увеличивается объем базы данных, поскольку эталонным значением для контроля является копия объекта.



- перейдите на вкладку "Расписание" и в таблице "Календарный план" установите все отметки в верхней строке "Пн" – "Сб";
- в поле "Временные параметры" установите флажок, в поле "Часы контроля" выберите "Каждый час" и укажите интервал "2 мин.". Проверка

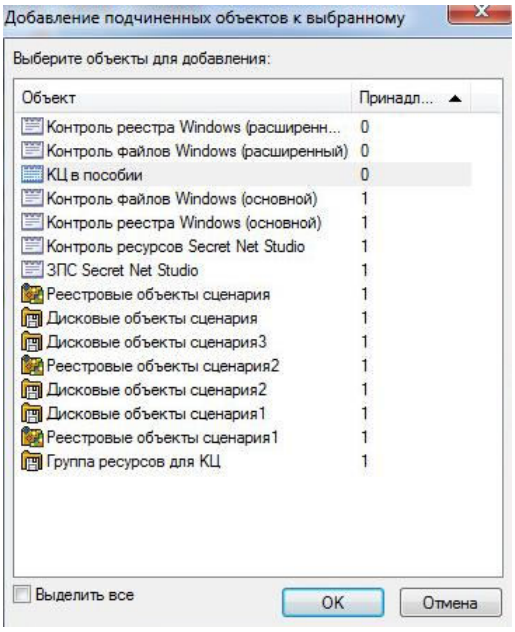
целостности ресурса будет проводиться в заданные дни каждый час с интервалом 2 минуты.

Подробнее об установке параметров расписания см. в руководстве администратора по настройке и эксплуатации Secret Net Studio.

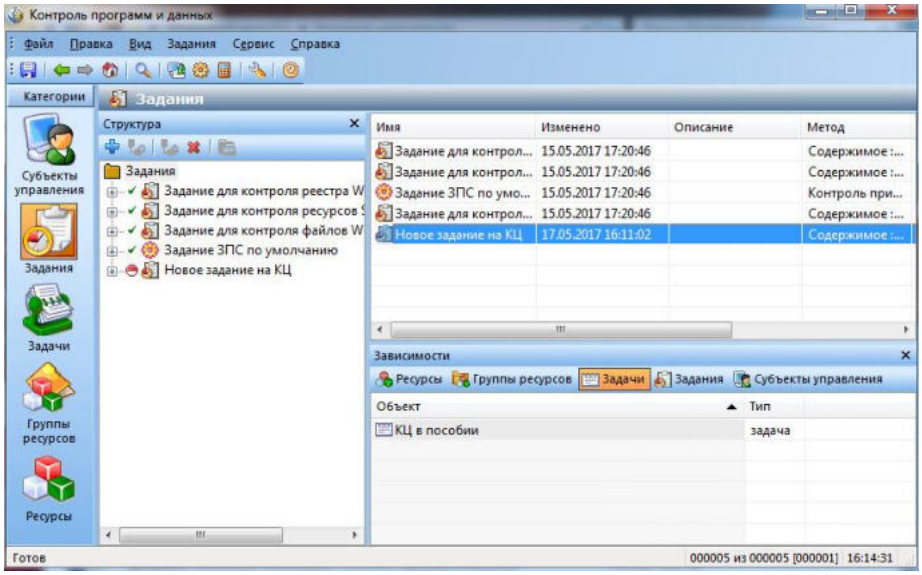


8. Нажмите кнопку "ОК". В панели "Задания" сформируется новое задание "Новое задание на КЦ". Добавьте в созданное задание задачу "КЦ в пособии". Для этого:

- в окне "Контроль программ и данных" для экземпляра задания "Новое задание на КЦ" вызовите контекстное меню и выберите опцию "Добавить задачи/группы / Существующие". Откроется диалоговое окно;

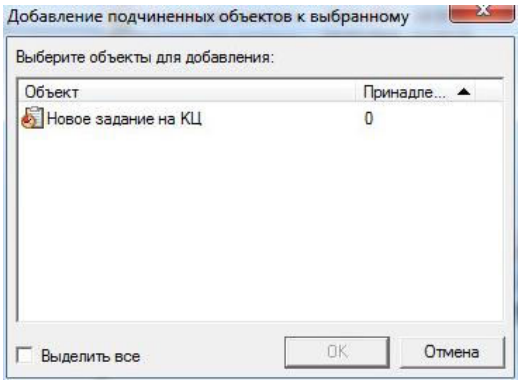


- выберите задачу "КЦ в пособии" и нажмите кнопку "ОК". Вы вернулись в окно "Контроль программ и данных" и добавили задачу в задание.

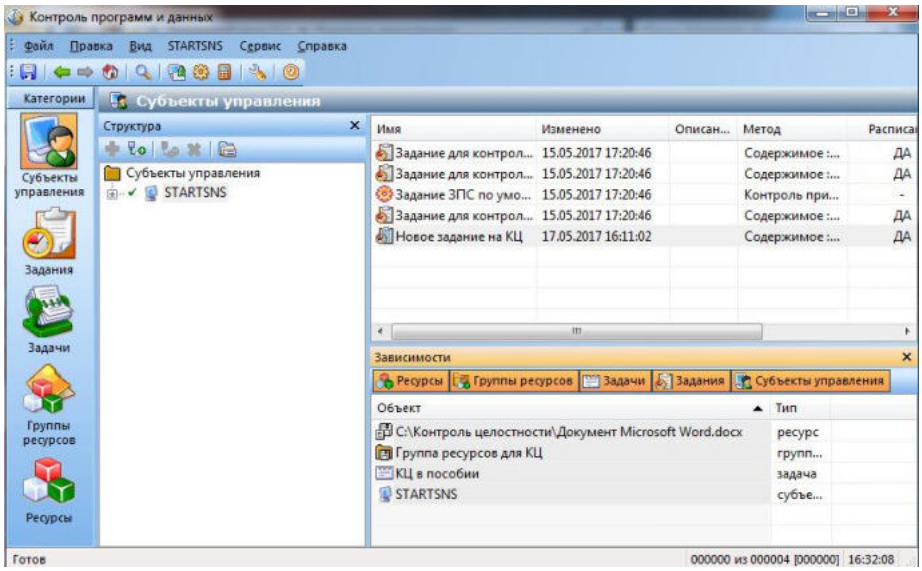


9. Укажите субъект управления, на котором будет выполняться контроль целостности, т.е. выберите компьютер и добавьте к нему сформированное задание – при установке связи заданий контроля целостности с субъектами "Компьютер" или "Группа" (компьютеров) включается действие механизма КЦ. Для этого:

- в окне "Контроль программ и данных" выберите категорию "Субъекты управления" и для компьютера StartSNS из контекстного меню выберите опцию "Добавить задания / Существующие". Откроется диалоговое окно добавления объектов;

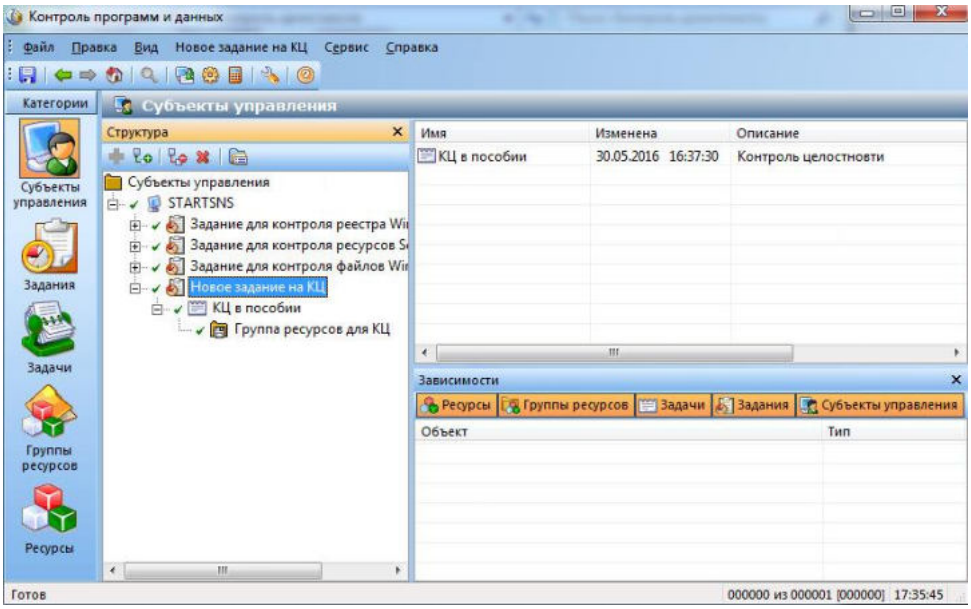


- выберите задание "Новое задание на КЦ" и нажмите кнопку "ОК". Задание добавлено субъекту.

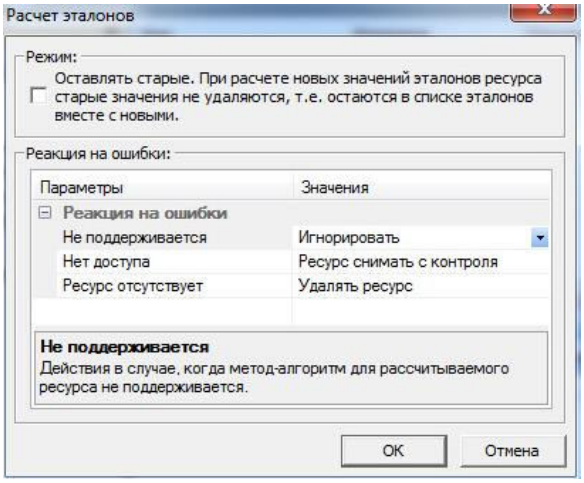


10. Проведите расчет эталонов для входящих в задания контролируемых ресурсов. Для этого сделайте следующее:

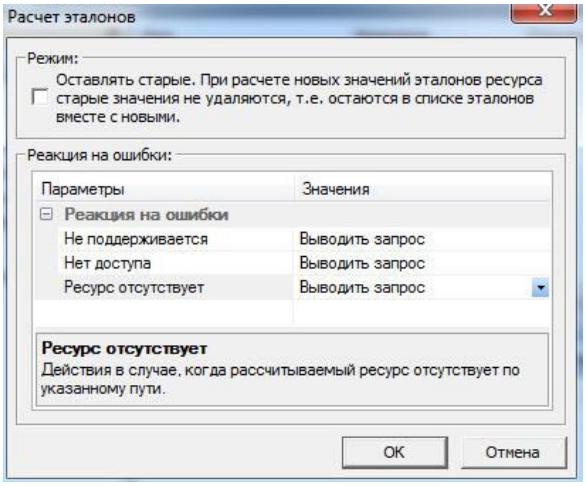
- в панели "Структура" разверните структуру субъекта управления "StartSNS", найдите и выделите задание "Новое задание на КЦ";



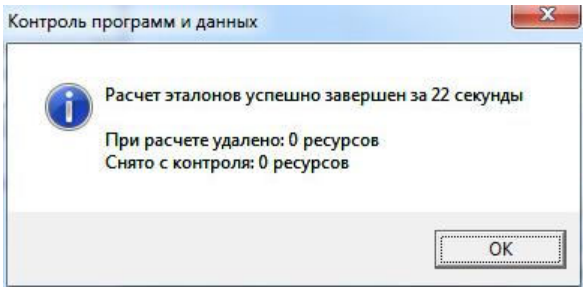
- в главном меню выберите опцию "Сервис / Эталоны / Расчет". Откроется диалоговое окно "Расчет эталонов";



- в разделе "Реакция на ошибки" установите для всех пунктов значение "Выводить запрос" (система будет выводить соответствующее сообщение и запрос на выполнение последующих действий);



- нажмите кнопку "ОК". В диалоговом окне подтверждения сохранения изменений нажмите кнопку "Да" и дождитесь окончания процесса расчета эталонов для ресурсов;



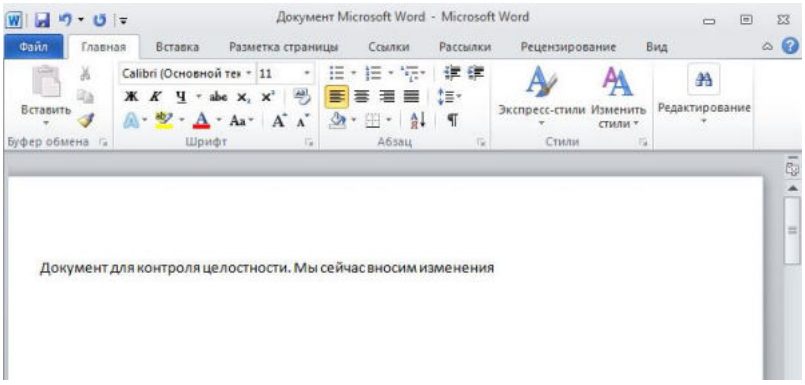
- после завершения расчета в окне информационного сообщения нажмите кнопку "ОК". Вы вернетесь в окно программы "Контроль программ и данных".

11. Контроль целостности настроен.

Как было описано в общем порядке настройки механизма КЦ (см. раздел "Контроль целостности ресурсов" главы 2), перед началом эксплуатации механизма КЦ можно выполнить проверку корректности параметров заданий. В связи с тем что в данной лабораторной работе было сформировано достаточно простое задание, такая проверка здесь проводиться не будет. Отметим лишь, что для ее начала используется команда "Запуск задания" из меню "Сервис".

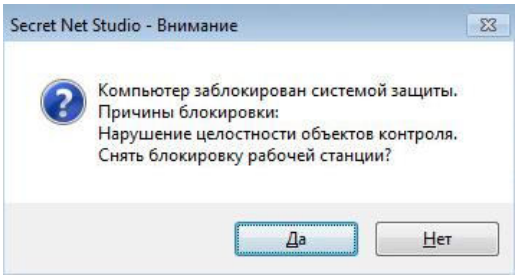
Далее проверяется работа механизма контроля целостности. Завершите работу программы "Контроль программ и данных", перезагрузите ВМ и авторизуйтесь под учетной записью "user1" (Иванов Иван Иванович).

12. Откройте файл "C:\Контроль целостности\Документ Microsoft Word.docx", внесите произвольные изменения, а затем сохраните и закройте документ.



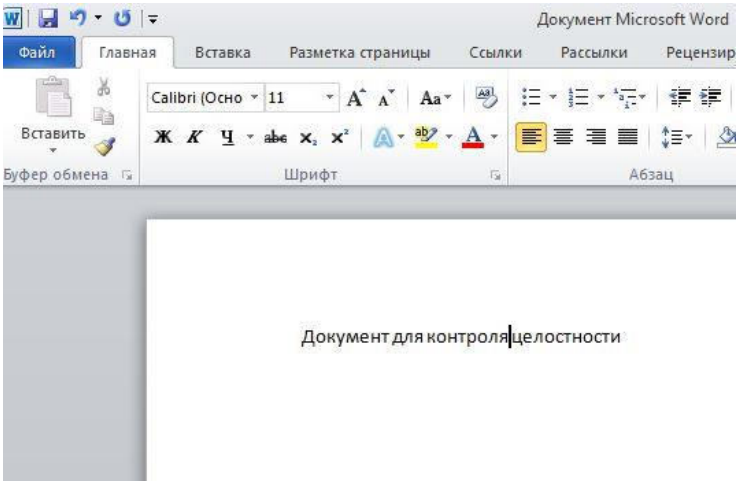
13. Подождите указанное в расписании контроля целостности время (см. п. 7, последний подпункт). Компьютер должен заблокироваться системой защиты Secret Net Studio.

14. Войдите в систему под учетной записью "adminsns". В диалоговом окне ознакомьтесь с запросом на снятие блокировки.

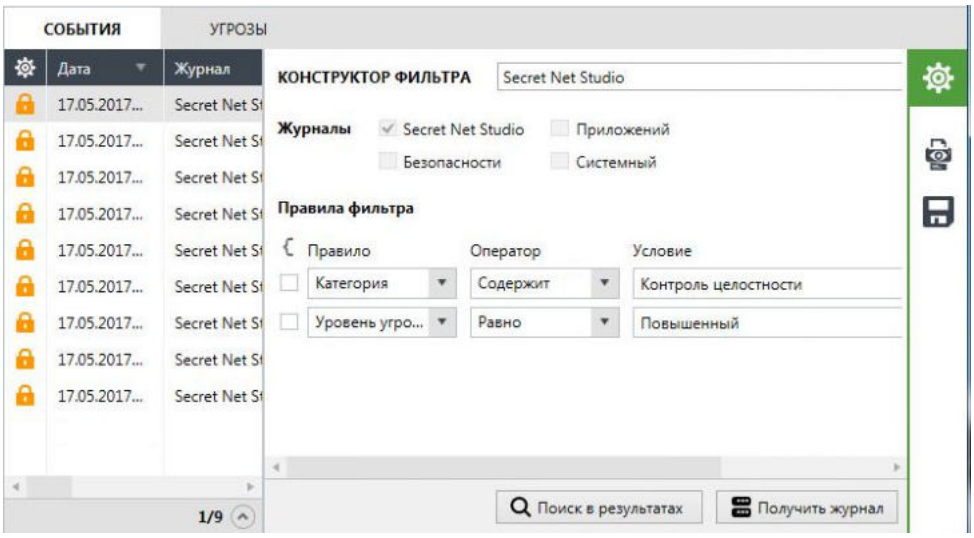


15. Нажмите кнопку "Да", снимите блокировку и дождитесь окончания загрузки ОС.

16. Проверьте целостность файла "C:\Контроль целостности\Документ Microsoft Word.docx". Для этого откройте данный файл и убедитесь, что он восстановлен.



17. В программе управления в локальном режиме откройте журнал событий Secret Net Studio. Найдите и ознакомьтесь с записями категории "Контроль целостности" с уровнем угрозы "Повышенный".



18. Проведена начальная настройка механизма КЦ и проверена его работа на примере контроля целостности текстового файла. Выполнение лабораторной работы завершено.

Лабораторная работа №3 "Централизованное ведение журналов в Secret Net Studio"

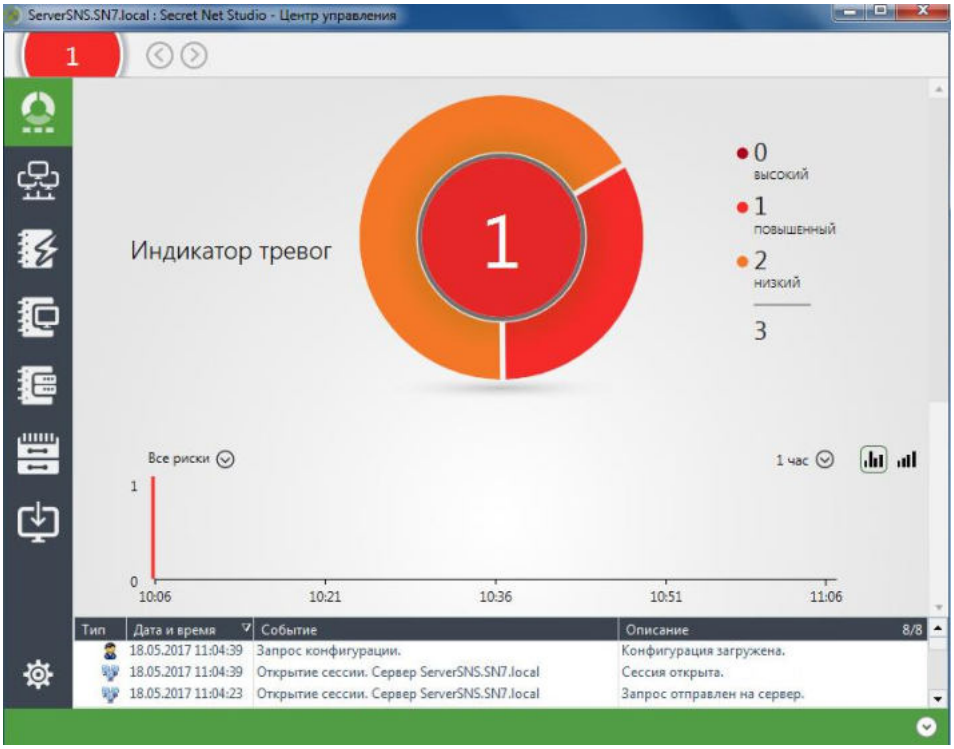
В данной лабораторной работе рассматривается проведение важных операций по ведению журналов в SNS (см. раздел "Настройка аудита в системе" главы 2):

- обработка событий тревоги (квитирование);
- сбор локальных журналов Secret Net Studio с защищаемых компьютеров в БД СБ;
- централизованная настройка на защищаемых компьютерах параметров локальных политик и регистрации определенных событий в журнале SNS;
- настройка поиска угроз и просмотра сведений об угрозах.

1. Откройте консоль ВМ ARM2 и убедитесь, что вы авторизованы в системе под учетной записью "dadminsns1" (пароль "P@ssw0rd").
2. Запустите программу управления: "Пуск → Все программы → Код Безопасности → Secret Net Studio → Центр управления" и подключитесь к серверу безопасности ServerSNS.SN7.local. В окне программы управления вы увидите

панель "Начало", которая отображает сведения об общем состоянии защищенности системы.

Программа управления предоставляет возможность контролировать и управлять состоянием и параметрами работы компьютеров, на которых установлено клиентское ПО системы Secret Net Studio в сетевом режиме, а также централизованно управлять параметрами групповых политик.

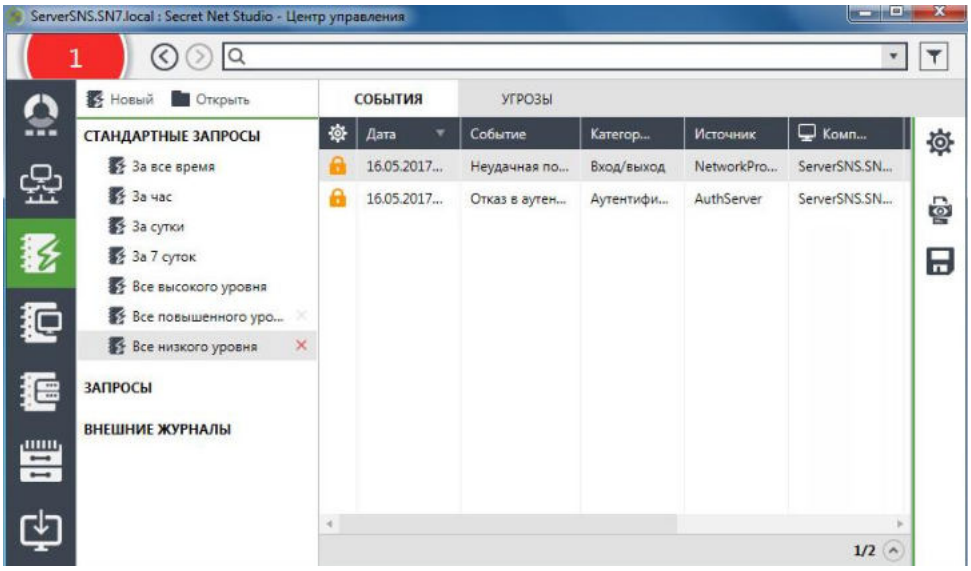


3. Ознакомьтесь с элементами панели "Начало":

- в центре панели – круговой индикатор тревог, внутренняя часть которого окрашена в соответствии с наивысшим уровнем актуальных на данный момент угроз в системе и содержит число этих событий. Внешняя часть круга – диаграмма, отражающая соотношение имеющихся событий тревоги разного уровня;
- справа от индикатора отображается количество по уровням угроз актуальных событий тревоги в системе. События тревог от подчиненных клиентов и СБ поступают в реальном времени;
- ниже индикатора тревог расположен график распределения на интервале времени зарегистрированных событий тревоги. Для выбора нужного интервала используйте поле с раскрывающимся списком 1 час в правом верхнем углу графика, а для настройки отображения событий тревоги в зависимости от их уровня – поле с раскрывающимся списком Все риски в левом верхнем углу графика;
- числа на круговом индикаторе и в перечне справа от него являются гиперссылками, нажатие на которые позволяет посмотреть информацию о данных событиях в журнале тревог.

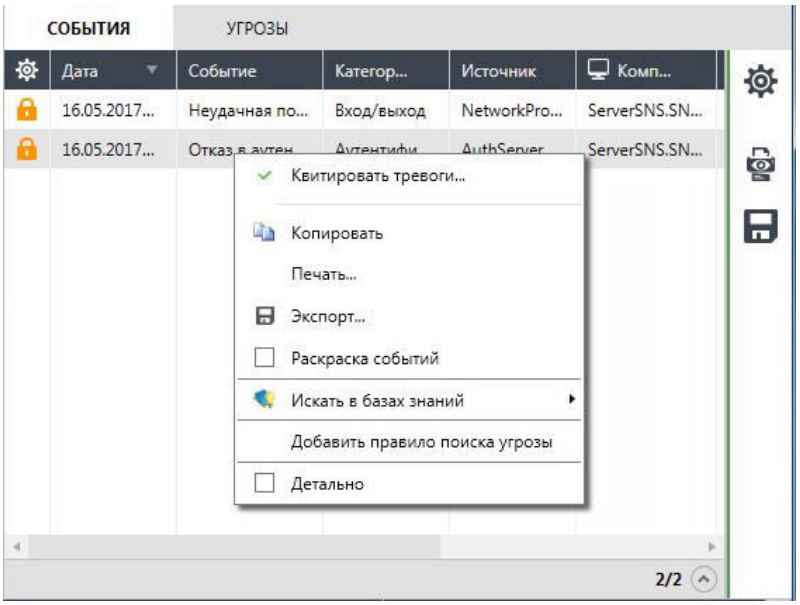
4. Обратите внимание на панель "События системы", расположенную в нижней части окна программы управления. Она отображает информацию о происходящих событиях, о выполняемых командах или запросах пользователя и пр.

5. Щелкните на любом числовом индикаторе – вы перейдете в журнал тревог. При этом автоматически сформируется и выполнится запрос на вывод событий тревог выбранного уровня (высокого, повышенного или низкого), после чего в панели событий появится запись о получении журнала тревог.

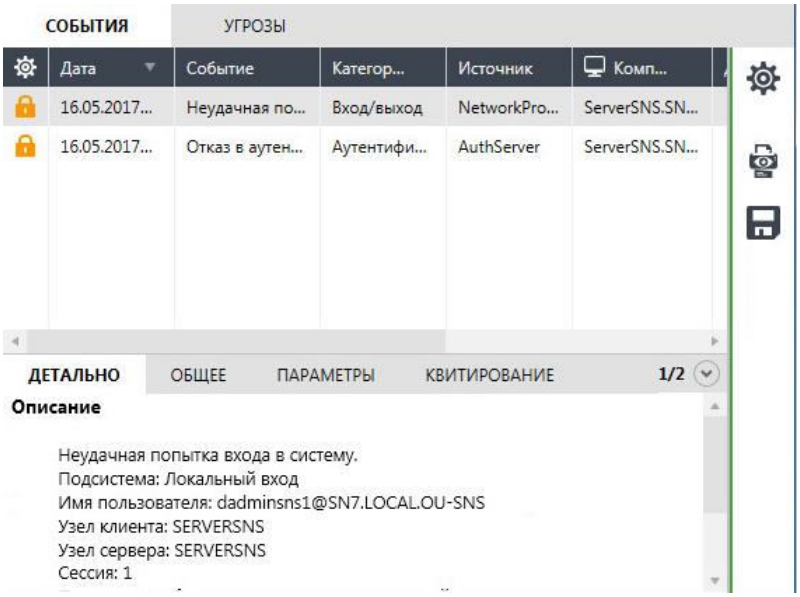


При получении уведомлений о произошедших событиях тревоги программа управления путем подачи различных визуальных сигналов незамедлительно оповещает об этом администратора безопасности.

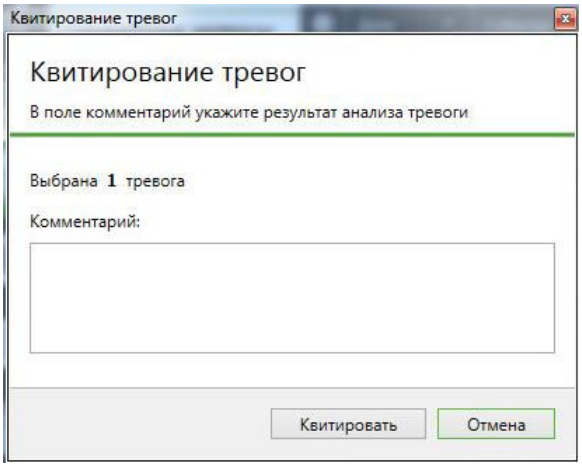
6. Выделите любое событие в журнале тревоги, вызовите его контекстное меню правой кнопкой мыши и ознакомьтесь с некоторыми возможными операциями над событиями:



- "Детально" – отображение подробного описания событий.



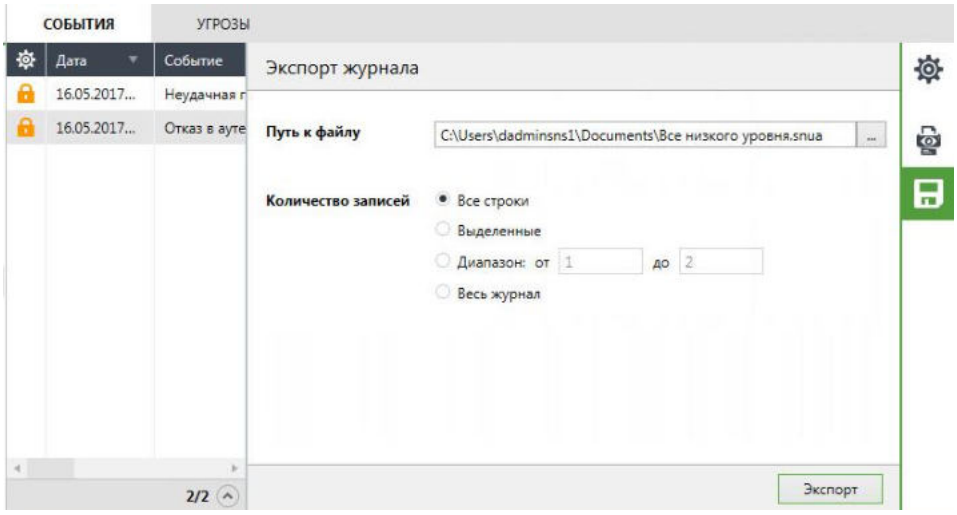
- "Квитировать тревоги". При этом администратор может ввести текстовый комментарий с описанием причин и принятых мер, и этот комментарий будет сохранен в системе вместе с признаком квитирования события. Информация о самом событии тревоги не удаляется из журнала. В дальнейшем по журналу событий тревоги можно определить, кто, когда и как отреагировал на произошедшие события. После квитирования всех полученных от компьютера событий для этого компьютера сбрасывается признак тревоги.



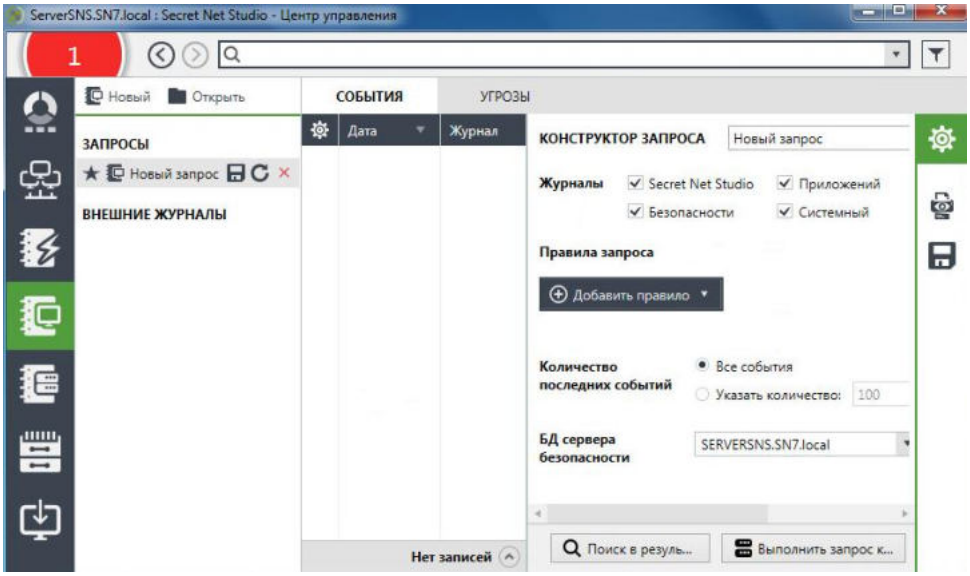
Квитировать можно отдельное событие или группу событий тревоги, предварительно выделив их с помощью клавиш [Ctrl] или [Shift].

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

- "Экспорт". Позволяет экспортировать (сохранять) записи текущего запроса в файлы специальных форматов: *.snua – записи журнала событий тревоги; *.snlog – записи журнала станций; *.snsrv – записи журнала сервера безопасности. Эта операция может также выполняться с помощью кнопки "Экспорт журнала" , расположенной в правой части окна;



7. В панели навигации нажмите кнопку "Журнал станций"  , сформируйте общий запрос на показ записей из всех журналов и убедитесь, что результат его будет пустым.



Журнал станций – это объединенный журнал компьютеров, который предназначен для централизованного хранения содержимого локальных журналов (журнал Secret Net Studio и штатные журналы ОС Windows), поступивших с защищаемых компьютеров.

Пустой результат запроса означает, что в базе данных сервера безопасности нет полученных с защищаемых компьютеров записей, которые удовлетворяют заданным в запросе правилам отбора.

8. В панели навигации откройте панель "Компьютеры"  . Она содержит средства администрирования и управления компьютерами. В текущем представлении на диаграмме отображаются домены, организационные подразделения, серверы безопасности и группы компьютеров, подчиненные серверам безопасности в соответствующих подразделениях.
9. Ознакомьтесь с некоторыми значками в диаграмме управления:

 – сервер безопасности, с которым установлено соединение (сервер подключения);

 – количество открытых на компьютерах сессий работы пользователей. Цветной фон обозначает сессию локального администратора;

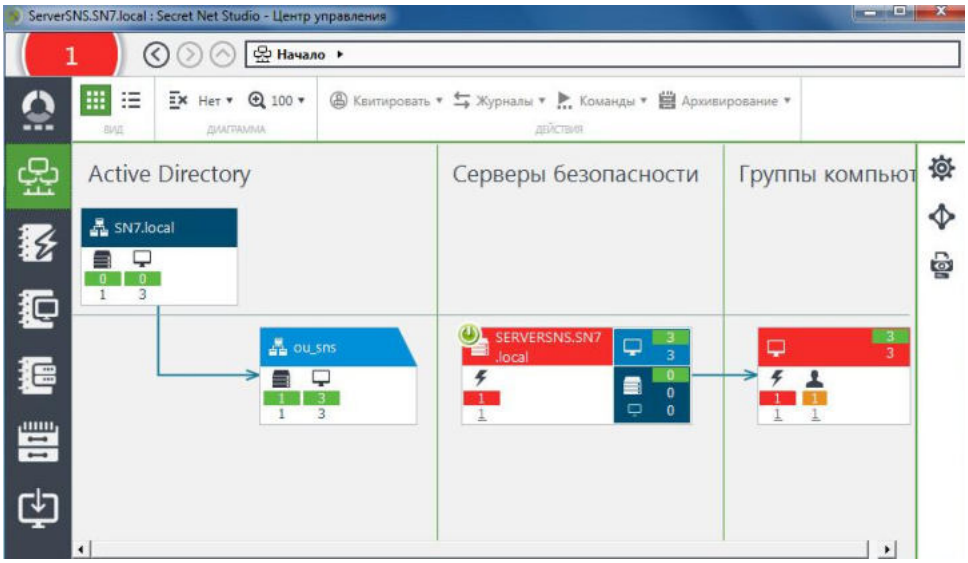
4 – счетчик зарегистрированных событий, ожидающих квитирования (подтверждение приема) администратором безопасности. Максимальное числовое значение счетчика – 999. В случае превышения ограничения счетчик отображает значение "99+";

– на компьютере (компьютерах) действует фильтр событий тревоги;

– зафиксирована ошибка при проверке лицензии;

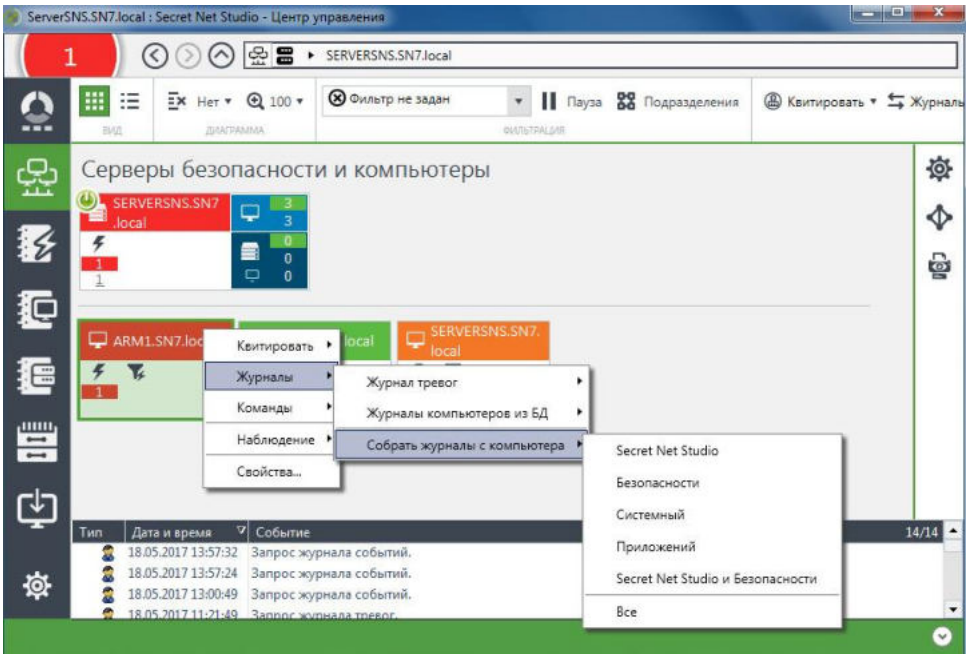
– БД сервера безопасности переполнена;

– учетная запись компьютера отключена.



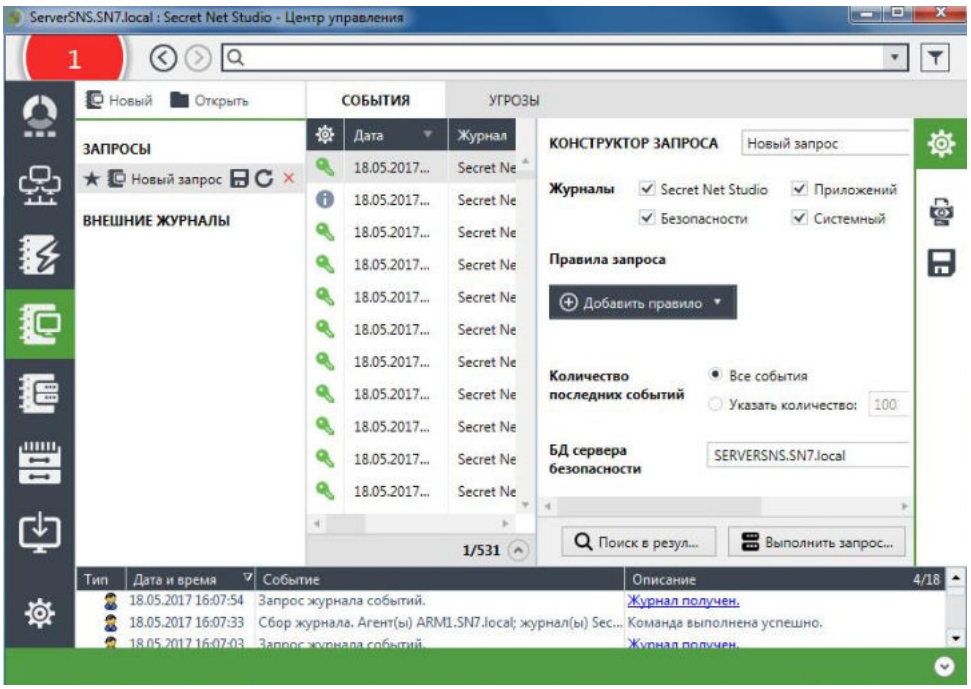
10. Проведите процедуру сбора журналов с компьютера ARM1. Для этого:

- в диаграмме управления раскройте двойным щелчком группу компьютеров. Обратите внимание, что при этом выбираются (помечаются) все содержащиеся в данной группе компьютеры;
- выберите плитку компьютера ARM1. Правой кнопкой мыши вызовите ее контекстное меню и выберите опцию: "Журналы / Собрать журналы с компьютера / Все";

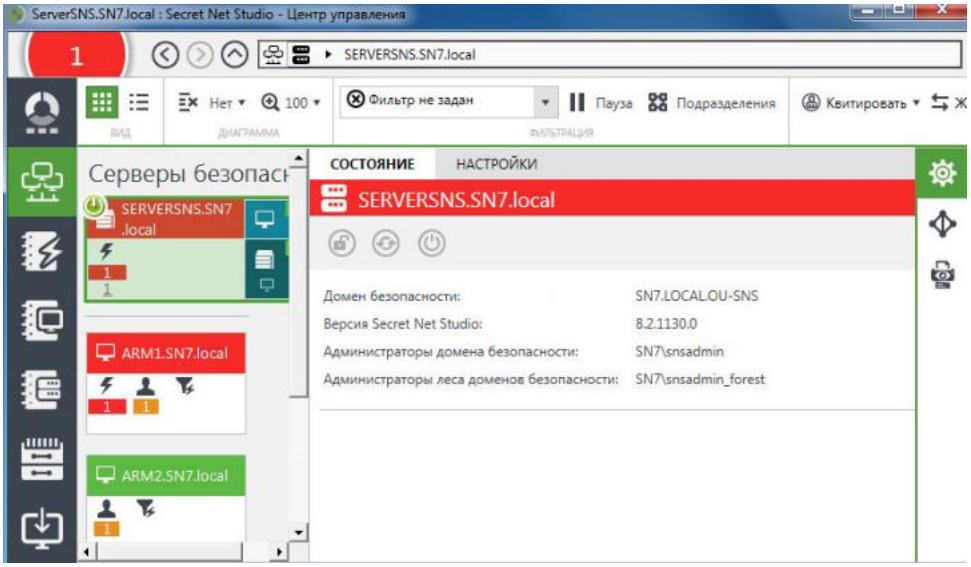


- обратите внимание на сообщение о сборе журнала в панели событий системы и дождитесь завершения операции сбора;

- после завершения операции сбора в поле "Описание" этого события появится отметка "Команда выполнена успешно". На панели навигации нажмите кнопку "Журнал станций"  и повторите выполнение запроса, который вы сформировали в п. 7 данной лабораторной работы (см. выше);
- дождитесь завершения операции и ознакомьтесь с результатами. Поскольку мы провели процедуру сбора журналов, в БД сервера безопасности теперь есть записи, полученные с защищаемых компьютеров.

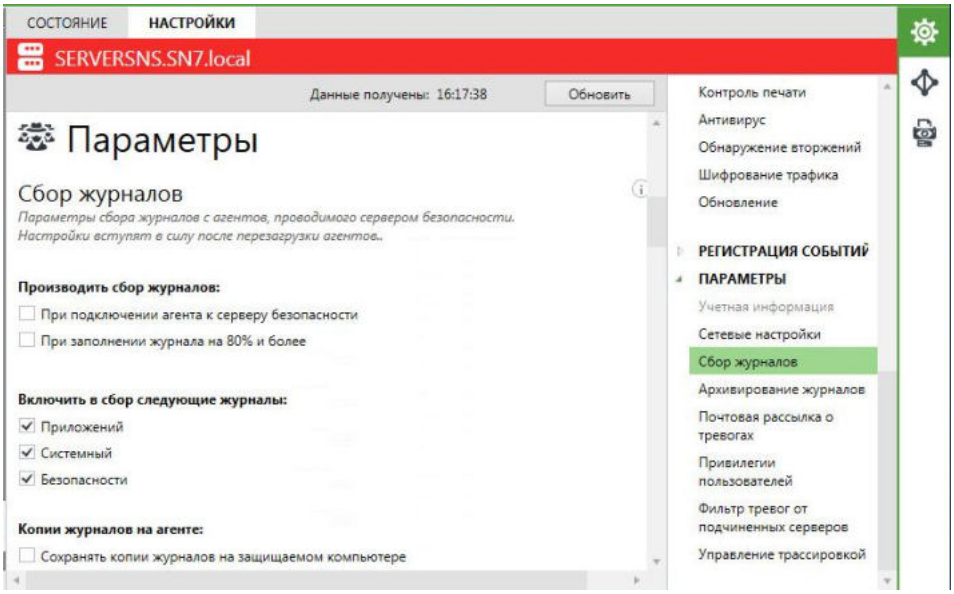


11. Ознакомьтесь с возможностью централизованной настройки параметров передачи локальных журналов в БД СБ. Для этого в панели навигации откройте панель "Компьютеры"  , в диаграмме управления выберите элемент сервера безопасности и, используя опцию "Свойства" из контекстного меню сервера или кнопку "Свойства"  в правой части окна, раскройте окно его свойств.



12. В открывшейся панели свойств элемента сервера безопасности переключитесь на вкладку "Настройки". Если на этой вкладке появится кнопка "Загрузить настройки", нажмите ее, чтобы загрузить параметры настроек выбранного объекта.

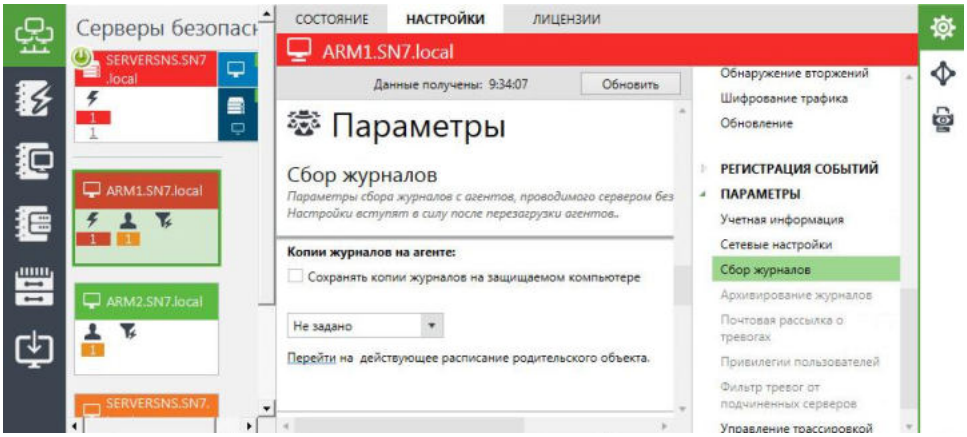
    В правой части окна раскройте раздел "Параметры" и выберите группу параметров "Сбор журналов", которая содержит параметры передачи локальных журналов на сервер безопасности.



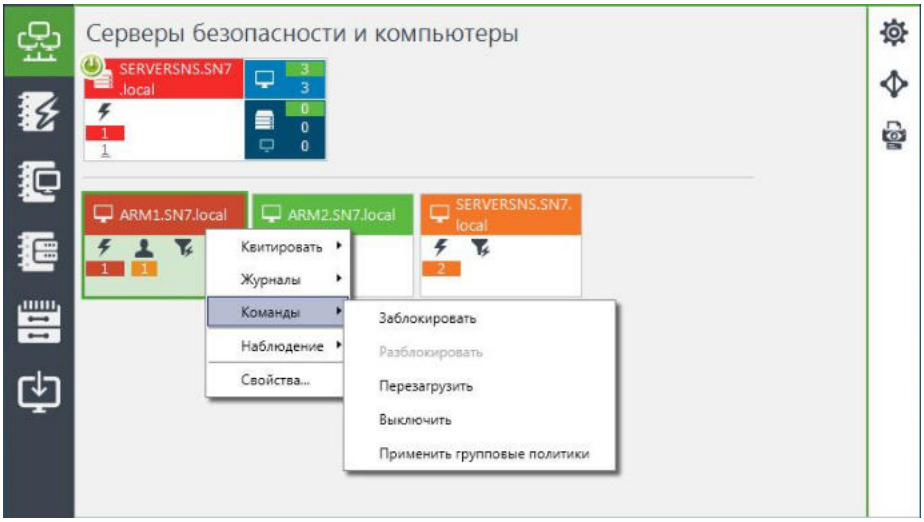
13. Параметры сбора локальных журналов, заданные для сервера безопасности, относятся ко всем компьютерам, которые подчинены этому серверу. Как отмечалось в главе 2, на отдельных компьютерах можно настроить индивидуальные параметры, которые будут иметь более высокий приоритет по сравнению с заданными на СБ параметрами. Установите следующие параметры сбора локальных журналов:
    - в группе "Производить сбор журналов" установите флажок в поле "При подключении агента к серверу безопасности";
    - обратите внимание на поле "Сохранять копии журналов на защищаемом компьютере" – его следует использовать, если требуется оставлять на рабочих станциях копии содержимого локальных журналов после их передачи на сервер безопасности. Эти копии сохраняются на компьютере в виде evt-файлов в подкаталоге \OmsAgentEvtCopy, расположенном в каталоге установки клиента. Обработка и удаление данных файлов должна выполняться администратором;
    - в группе "Включить в сбор следующие журналы" снимите флажок в поле "Системный".
14. Нажмите кнопку "Применить" и дождитесь завершения процедуры сохранения параметров. Обратите внимание, что в панели событий системы появилась соответствующая запись о сохранении конфигурации.

15. На панели "Компьютеры"  выберите плитку компьютера ARM1, на вкладке "Настройка" раскройте раздел "Параметры" и выберите группу параметров "Сбор журналов". В данном режиме можно настроить индивидуальные локальные настройки сбора журналов для компьютера ARM1, которые будут иметь более высокий приоритет по сравнению с заданными на СБ параметрами.

    Убедитесь, что в раскрывающемся списке выбора расписания установлено "Не задано" и выберите ссылку "Перейти на действующее расписание родительского объекта". Вы снова вернетесь к установленным для СБ настройкам сбора журналов.



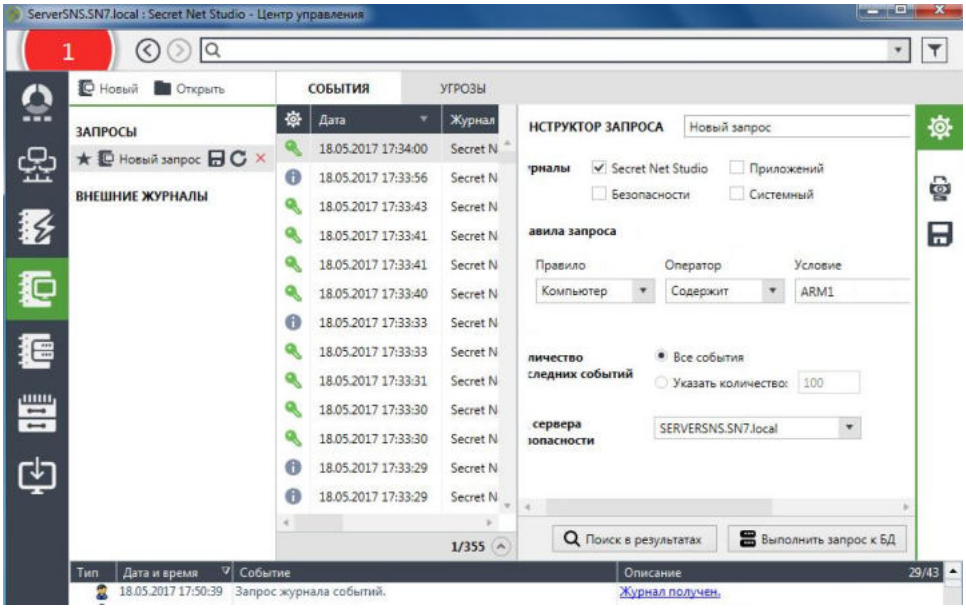
16. Используя кнопку "Свойства"  , закройте панель свойств и вернитесь к интерфейсу диаграммы управления. Вызовите контекстное меню компьютера ARM1 и выберите опцию "Команды / Перезагрузить". В диалоговом окне подтверждения перезагрузки нажмите кнопку "Да". Дождитесь завершения перезагрузки и авторизуйтесь на ВМ компьютера ARM1 под учетной записью "dadminsns1".



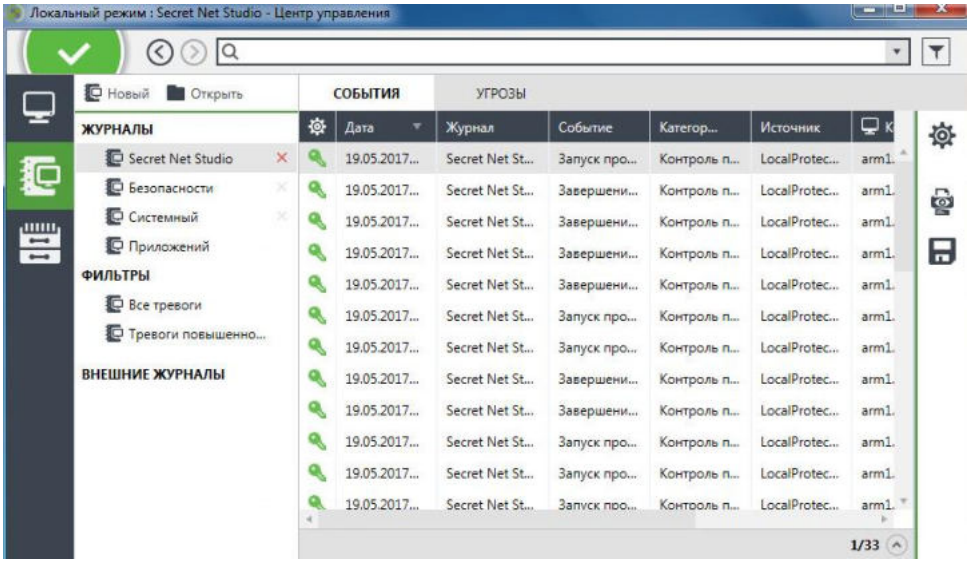
17. Обратите внимание, что в панели событий системы появились записи об успешной перезагрузке и авторизации пользователя в системе.

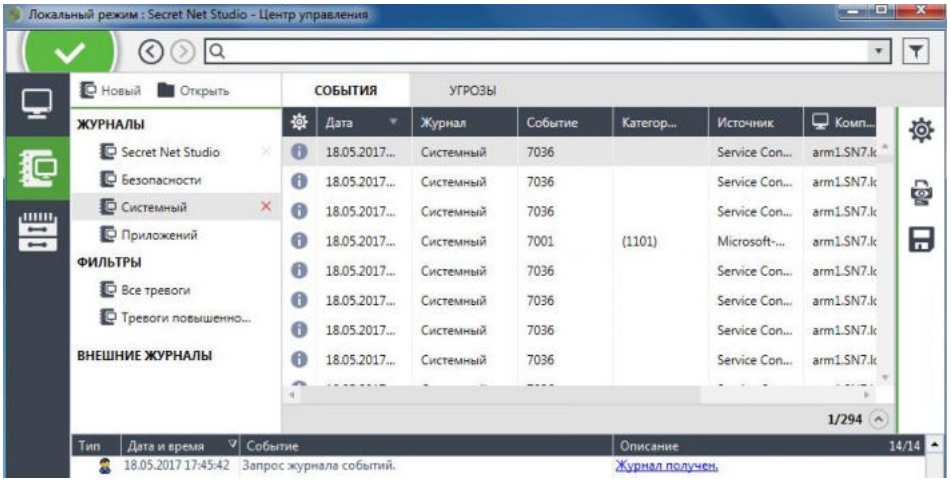
18. Используя описание п. 7 данной лабораторной работы (см. выше), раскройте "Журнал станций", сформируйте соответствующий запрос и убедитесь, что после перезагрузки защищаемого компьютера ARM1 и подключения агента к СБ содержимое локальных журналов, кроме системного, было передано с ARM1 в БД СБ. Обратите внимание на панель событий системы, в которой отражены события о запросе журнала с пометкой о получении в поле "Описание".

Примечание. Параметры расписания, заданные для сервера безопасности, не применяются на защищаемых компьютерах с индивидуально настроенными расписаниями передачи журналов.



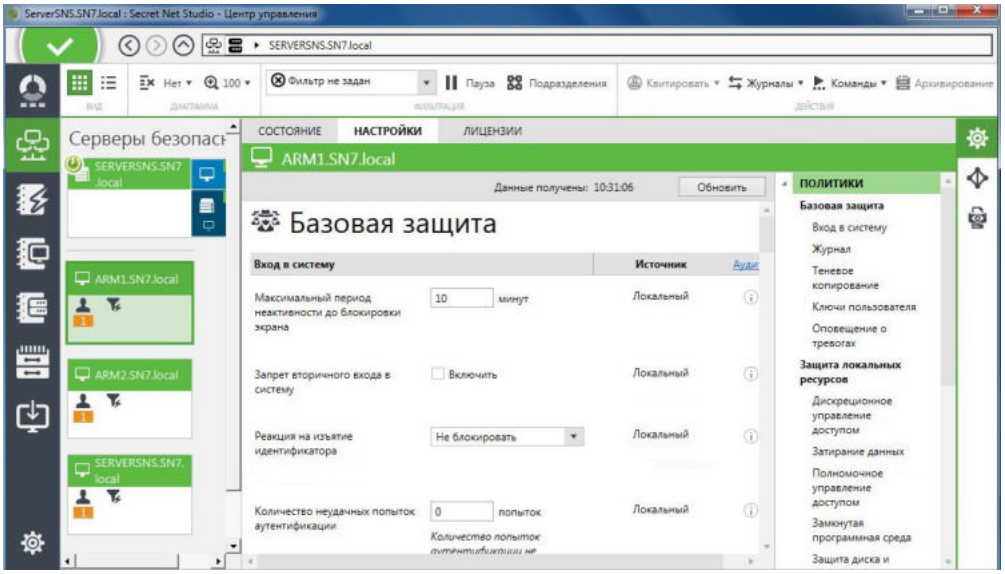
19. Переключитесь в окно ВМ ARM1, запустите программу "Локальный центр управления", откройте панель "Журнал станций" и с помощью соответствующих запросов убедитесь, что после перезапуска были переданы в БД СБ и соответственно очищены все локальные журналы, кроме системного.



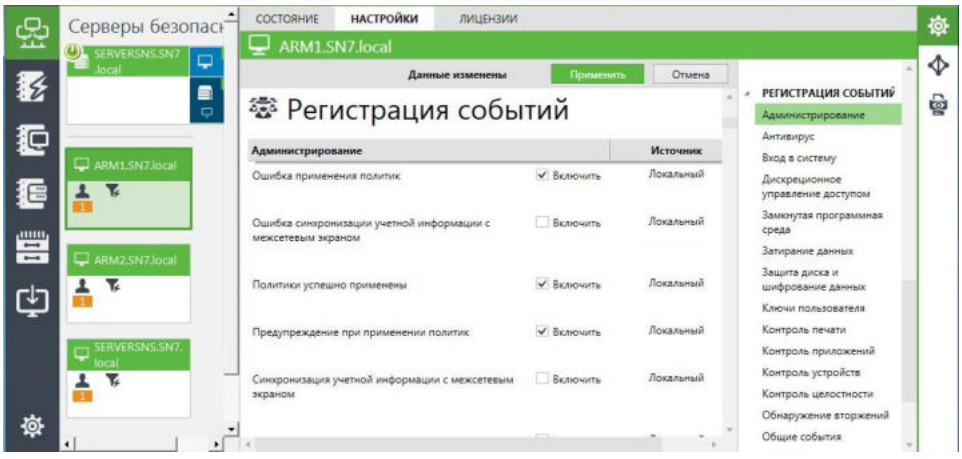


Подробнее об обработке событий журнала тревог и других журналов см. в руководстве администратора по централизованному управлению, мониторингу и аудиту.

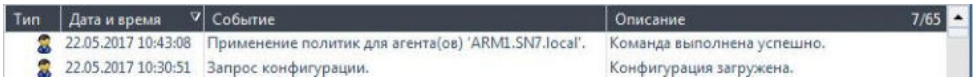
20. Операции квитирования тревог и сбора локальных журналов рассмотрены. Далее будет проиллюстрирован пример централизованной настройки на защищаемых компьютерах параметров локальных политик и регистрации определенных событий в журнале Secret Net Studio. В окне консоли BM ARM2, в программе управления на панели "Компьютеры" с помощью кнопки "Свойства"  откройте панель свойств компьютера ARM1 и выберите вкладку "Настройки".



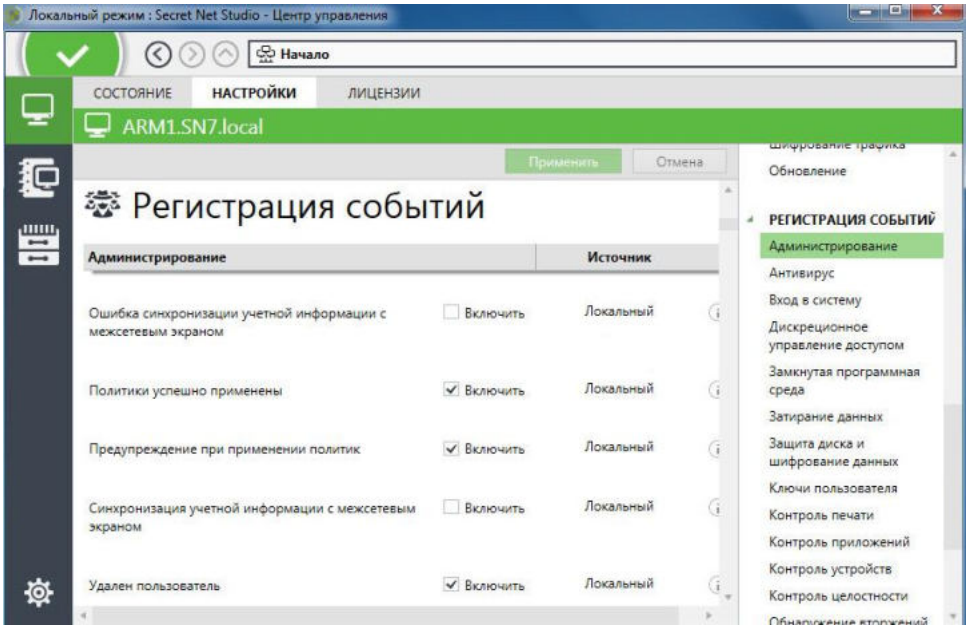
21. В лабораторной работе №1 данной главы уже рассматривалась автономная настройка на отдельном компьютере параметров раздела "Регистрация событий" и группы "Политики / Базовая защита". Теперь будет показано управление этими настройками в сетевом режиме. В группе "Регистрация событий / Администрирование" найдите и отключите параметры "Ошибка синхронизации учетной информации с межсетевым экраном" и "Синхронизация учетной информации с межсетевым экраном".



22. На панели инструментов нажмите кнопку "Применить"  , дождитесь появления в панели событий системы записей об успешном выполнении команды и изменении локальных политик на агенте.

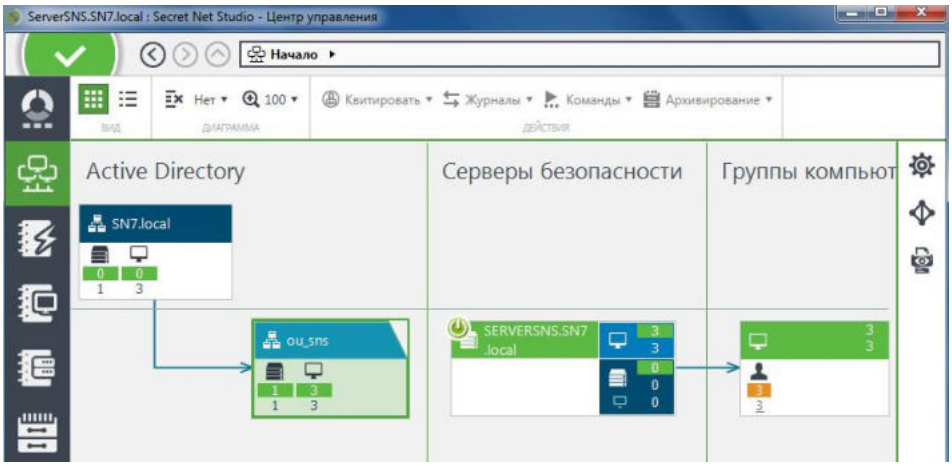


23. Откройте консоль BM ARM1 под учетной записью "dadminsns1" и запустите программу "Локальный центр управления". На панели "Компьютер" перейдите на вкладку "Настройки", разверните группу параметров "Регистрация событий / Администрирование" и убедитесь, что регистрация событий "Ошибка синхронизации учетной информации с межсетевым экраном" и "Синхронизация учетной информации с межсетевым экраном" отключена.

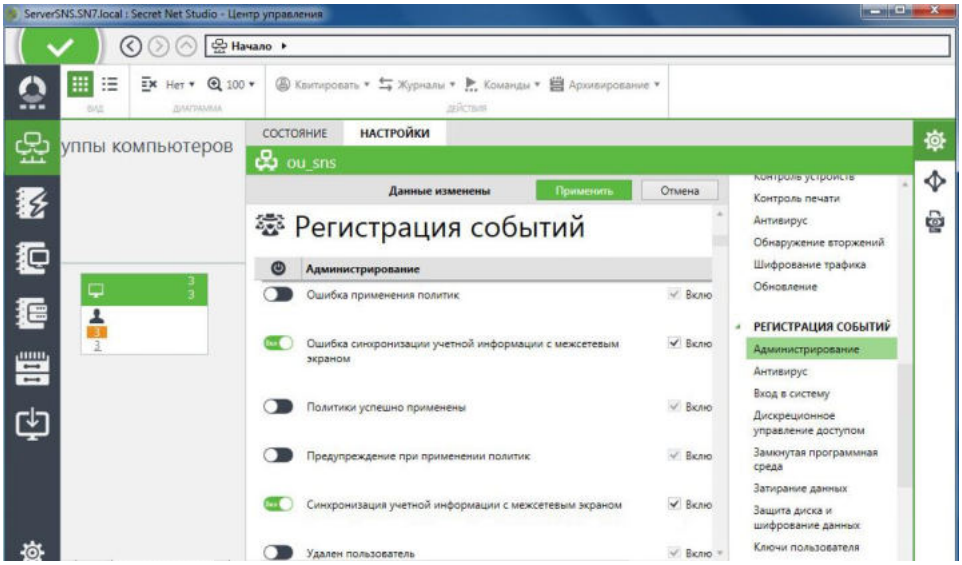


24. Теперь изменим данные параметры для всего домена безопасности, т.е. в нашем случае для подразделения "ou_sns":

- переключитесь в окно консоли ВМ ARM2, в программе управления на панели "Компьютеры" с помощью кнопки "Свойства"  сверните панель свойств компьютера ARM1 и вернитесь к диаграмме управления в режиме отображения списков компьютеров;
- в панели навигации в верхней части окна нажмите кнопку "Вверх на один уровень"  и перейдите в режим общей начальной структуры. Обратите внимание, что в данном режиме отображаются домены, организационные подразделения, серверы безопасности и группы компьютеров, подчиненные серверам безопасности в соответствующих подразделениях;

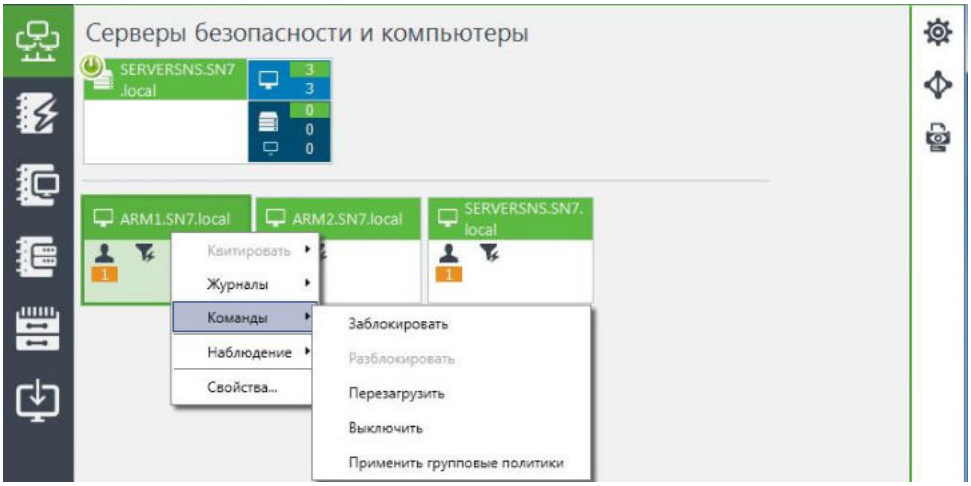


- выберите организационное подразделение "ou_sns", на которое был спроецирован домен безопасности, и с помощью кнопки "Свойства"  откройте панель свойств. Если появится кнопка "Загрузить настройки", нажмите ее, чтобы загрузить параметры настроек выбранного объекта;
- на вкладке "Настройка" с помощью значка  включите в группе "Регистрация событий / Администрирование" параметры "Ошибка синхронизации учетной информации с межсетевым экраном" и "Синхронизация учетной информации с межсетевым экраном";



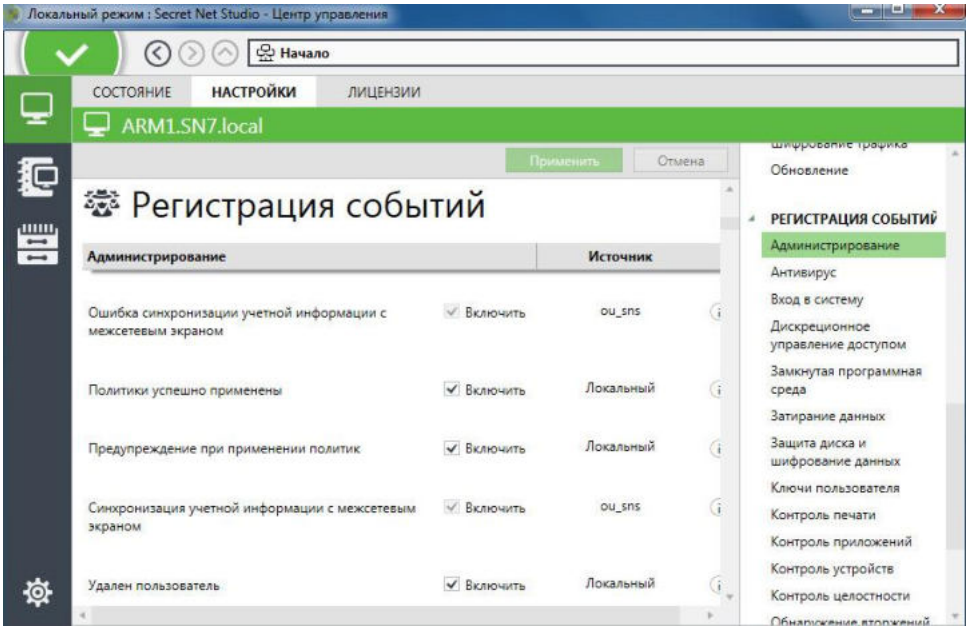
- на панели инструментов нажмите кнопку "Применить" Применить, дождитесь появления в панели событий системы записи об успешном сохранении конфигурации и применении политик.

25. С помощью кнопки "Свойства" закройте окно свойств организационного подразделения, в диаграмме управления двойным щелчком выберите группу компьютеров, раскройте контекстное меню компьютера ARM1 и выберите опцию "Команды / Применить групповые политики".



26. Обратите внимание на сообщение в панели событий об успешном применении групповых политик.

27. Перейдите в окно консоли ВМ ARM1 и в программе управления в локальном режиме убедитесь, что регистрация событий "Ошибка синхронизации учетной информации с межсетевым экраном" и "Синхронизация учетной информации с межсетевым экраном" включена на уровне организационного подразделения и в локальном режиме не изменяется.



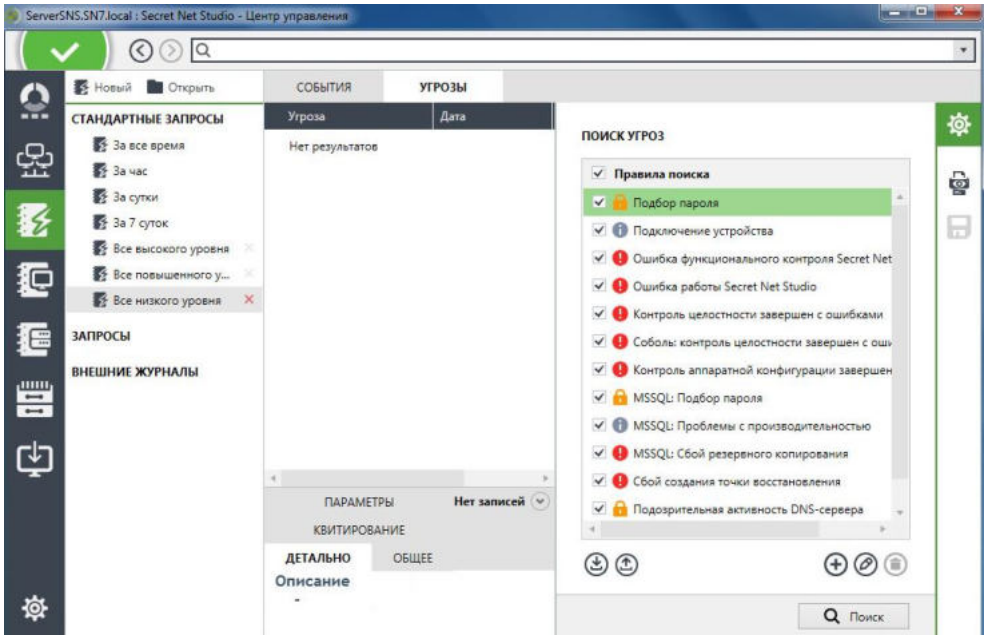
Параметры политик, заданные для корневого сервера безопасности, имеют наивысший приоритет и применяются на всех компьютерах, которые находятся в непосредственном или транзитивном подчинении.

По умолчанию параметры заданы только в локальной политике. Для большинства параметров локальной политики изменение значений возможно как централизованно в программе управления, так и локально на защищаемом компьютере. При этом изменить в локальной политике значение, заданное политикой другого уровня, невозможно. Сведения о политике, определяющей значение параметра, представлены в локальной политике в колонке "Источник".

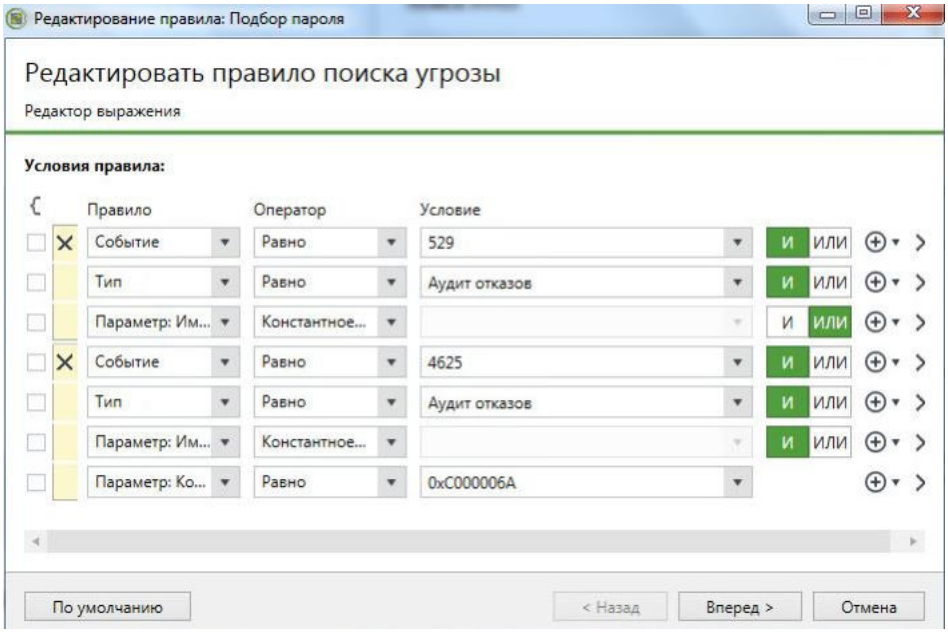
28. Ознакомьтесь с настройками поиска событий угроз и проведите просмотр списка угроз, полученного в результате анализа загруженных записей журналов. Еще раз отметим, что режим просмотра угроз предназначен для предоставления администратору или аудитору наиболее важной для них информации из журналов, а сами события угроз представляют собой сжатые или разъясняющие сведения о зарегистрированных событиях (например, событиях с признаками подбора пароля).

Для настройки поиска событий угроз выполните следующие действия:

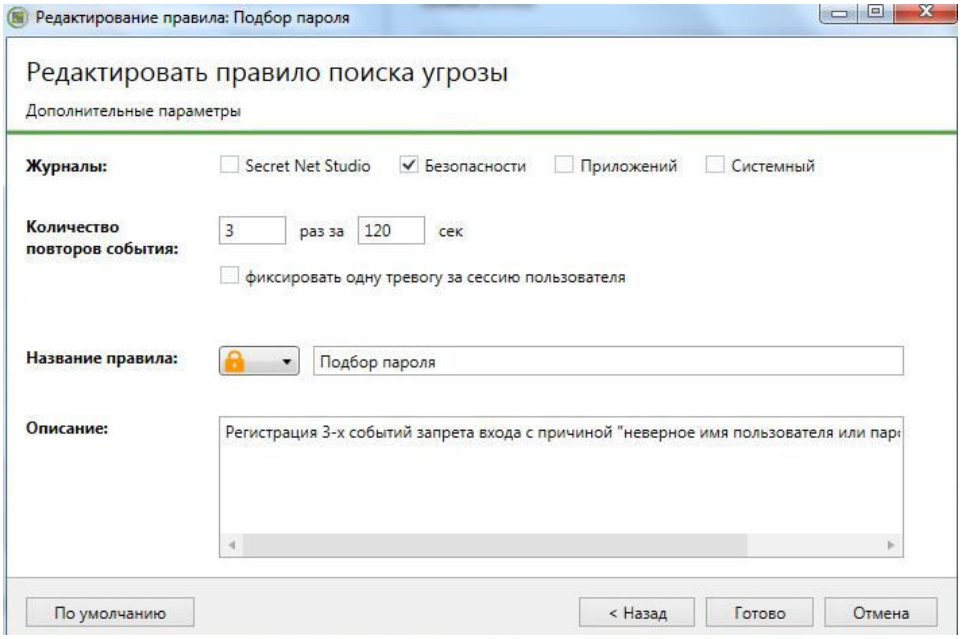
- в панели навигации нажмите кнопку "Журнал тревог"  , в области отображения сведений переключитесь на вкладку "Угрозы" и в верхней части панели настройки вывода сведений (справа от области отображения сведений) нажмите кнопку "Запрос"  . На экране появится панель настройки параметров поиска угроз, содержащая предустановленные по умолчанию правила общего характера, которые нельзя удалять, но можно изменять;



- просмотрите полученный список. Убедитесь, что выбрано правило поиска "Подбор пароля" и под списком правил справа нажмите кнопку "Редактировать правило угрозы"  . Откроется диалоговое окно "Редактирование правила: …", где можно изменить список условий, которым должны удовлетворять записи для соответствия данному событию угрозы;



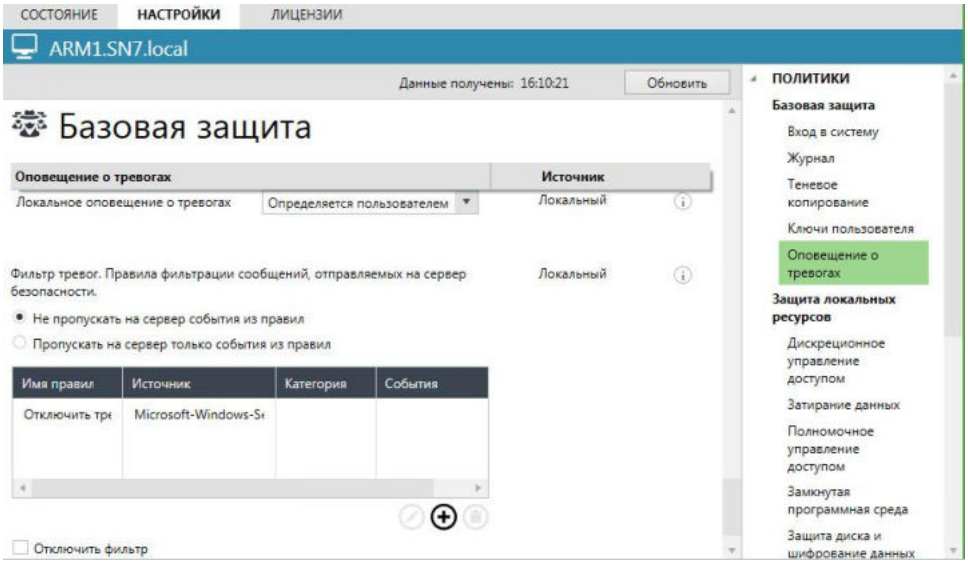
- просмотрите список условий выбранного правила. Обычно список содержит несколько связанных между собой выражений. Связь формируется с помощью логически операторов И / ИЛИ или значка группировки (кнопка с фигурной скобкой над списком). Группировка позволяет задать обязательное совпадение заданных значений для полей (например, "Тип", "Событие" и "Параметр: Имя пользователя"), чтобы при анализе не рассматривались записи, у которых хотя бы одно из значений в указанных полях не совпадает с заданным;
- нажмите кнопку "Вперед". На данном шаге мастера можно установить дополнительные параметры правила: выбрать журналы, записи которых будут рассматриваться при анализе, для отслеживания повторяющихся событий указать количество повторов в интервале времени, а также выбрать режим сжатия в поле "фиксировать одну тревогу за сессию пользователя", чтобы при выявлении нескольких одинаковых событий за сеанс работы пользователя в журнале формировать только одну запись;



- обратите внимание, что по умолчанию для формирования события тревоги и соответствующей угрозы задано 3 попытки ввода пароля. Нажмите кнопку "Отмена", чтобы не сохранять изменений в выбранном правиле. Самостоятельно просмотрите условия и параметры поиска других правил, например, "Контроль целостности завершен с ошибками".

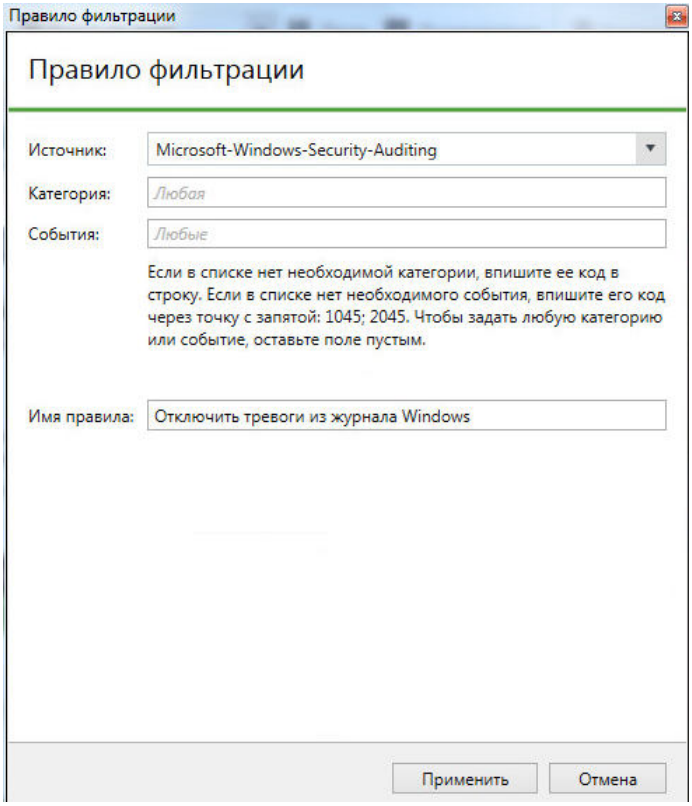
29. Перед просмотром списка угроз ознакомьтесь с возможностью установки непосредственно на защищаемых компьютерах фильтра передачи уведомлений о событиях тревоги. Для этого:

- в панели навигации переключитесь на панель "Компьютеры", выберите компьютер ARM1, раскройте панель его свойств и на вкладке "Настройки" разверните группу "Политики / Базовая защита / Оповещение о тревогах", параметры которой позволяют ограничить непосредственно на защищаемых компьютерах передачу на СБ уведомлений о событиях тревоги;



- с помощью значка–кнопки ⓘ ознакомьтесь с описанием параметров выбранной политики и обратите внимание, что по умолчанию заданы значения: "Локальное оповещение о тревогах" – "Определяется пользователем", "Фильтр тревог. Правила фильтрации сообщений …" – "Не пропускать на сервер события из правил". В заданных настройках фильтр не пропускает уведомления о событиях тревоги, которые удовлетворяют условиям правил в таблице;

- если в таблице присутствует запись от источника "Microsoft-Windows-Security-Auditing", выберите ее и под таблицей нажмите кнопку "Редактировать" . Откроется диалоговое окно для настройки параметров выбранного правила;

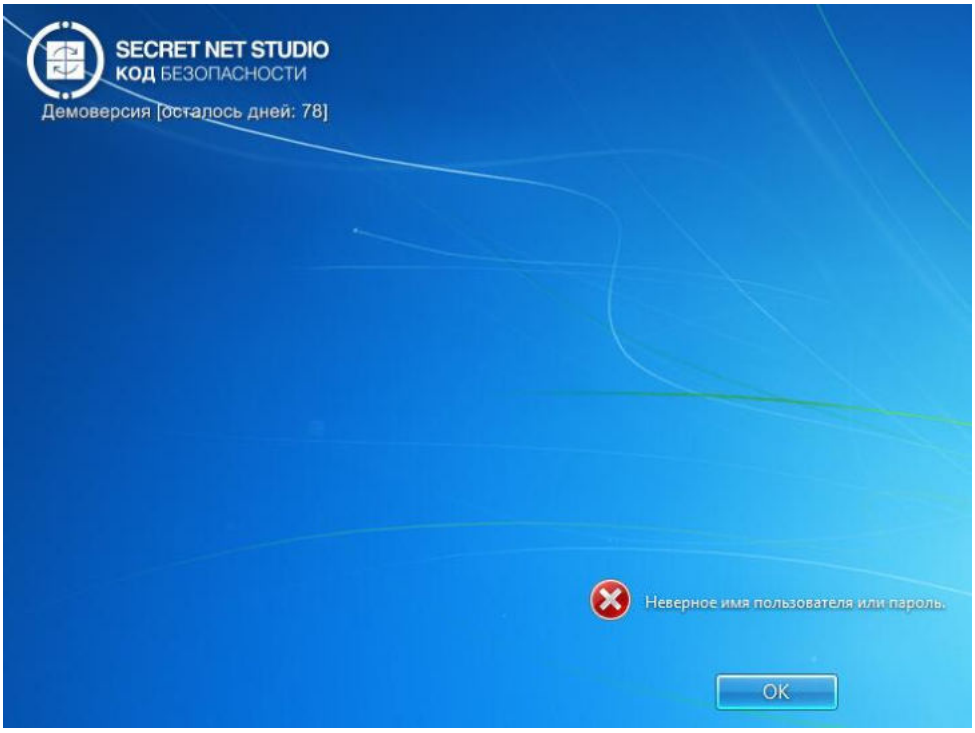


- примите к сведению, что параметры правил фильтрации уведомлений подробно описаны в руководстве администратора по централизованному управлению, мониторингу и аудиту SNS:
  - "Источник" – имя компонента/подсистемы–источника события;
  - "Категория" – числовой код категории событий;
  - "Событие" – числовые идентификаторы событий;
- в диалоговом окне "Правило фильтрации" нажмите кнопку "Отмена". В параметрах группы политик "Оповещение о тревогах" установите переключатель "Отключить фильтр" и в верхней части вкладки "Настройки" нажмите кнопку "Применить".

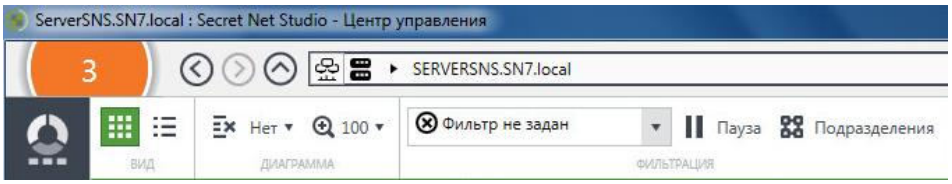
> **Примечание.** Не включайте инверсный режим "Пропускать на сервер только события из правил" при пустом списке правил. Иначе фильтр не пропустит ни одно событие тревоги.

30. Просмотрите сформированный на основе сделанных настроек (пп. 27–29) список угроз. Для этого:

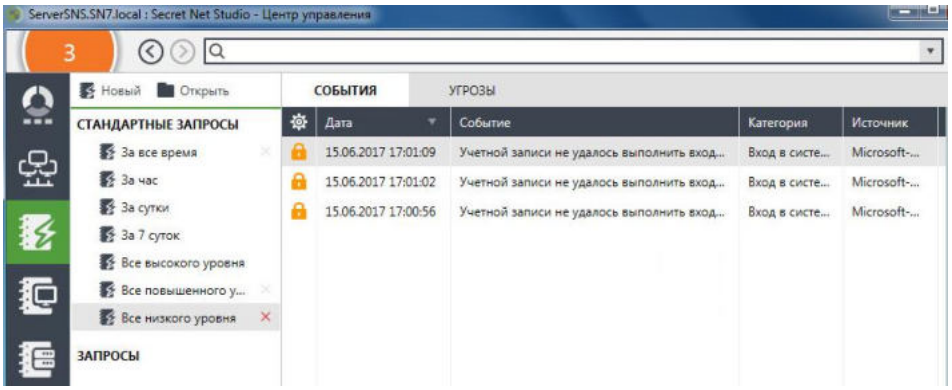
- используя описание п. 6, проведите квитирование всех имеющихся событий тревоги и убедитесь, что журнал тревог теперь пуст;
- убедитесь, что с момента сохранения сделанных в п. 45 настроек прошло необходимое время для их применения на защищаемом компьютере (4–6 мин.);
- переключитесь в окно ВМ ARM1 и переавторизуйтесь под УЗ dadminsns1, указав три раза неправильный пароль;



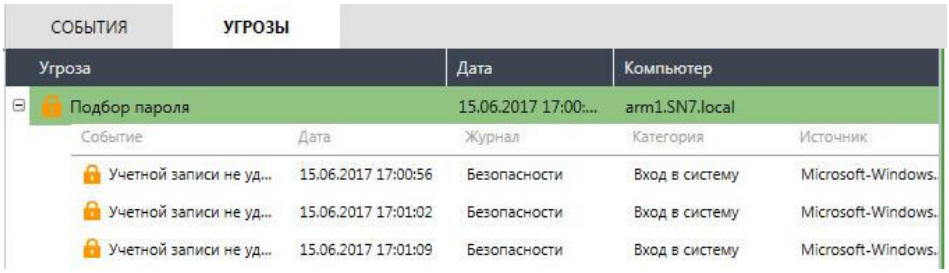
- убедитесь, что с момента сохранения сделанных в п. 45 настроек прошло необходимое время для их применения на защищаемом компьютере (4–6 мин.);
- переключитесь в окно ARM2. Обратите внимание на изменившийся числовой показатель индикатора тревог в левом верхнем углу окна – он показывает количество зарегистрированных событий тревоги;



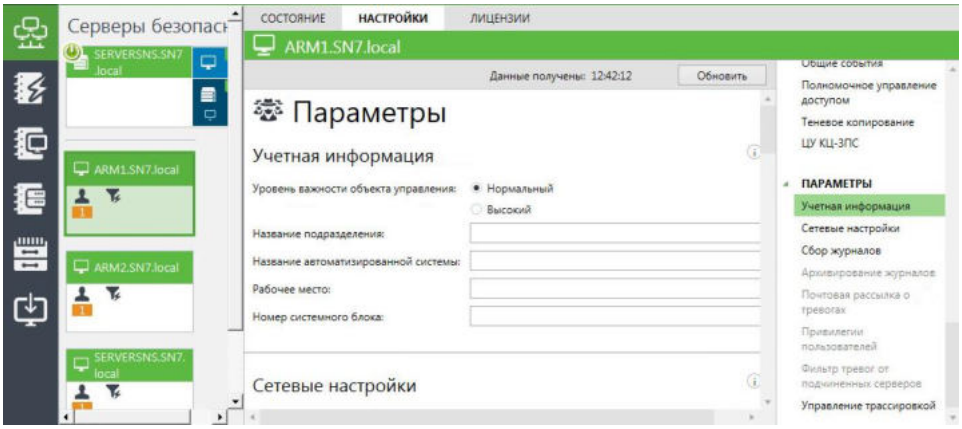
- щелкните на этом числовом индикаторе. Откроется панель "Журнал тревог", в которой вы увидите зарегистрированные события тревоги, полученные с компьютера ARM1;



- переключитесь на вкладку "Угрозы" и убедитесь, что на основании зарегистрированных событий была сформирована одна угроза "Подбор пароля";



31. На панели "Компьютеры" выберите в диаграмме управления элемент компьютера ARM1, раскройте панель его свойств и на вкладке "Настройки" разверните группу "Параметры / Учетная информация", которая содержит сведения о компьютере, которые могут использоваться администратором для идентификации данного компьютера при работе с системой Secret Net Studio.

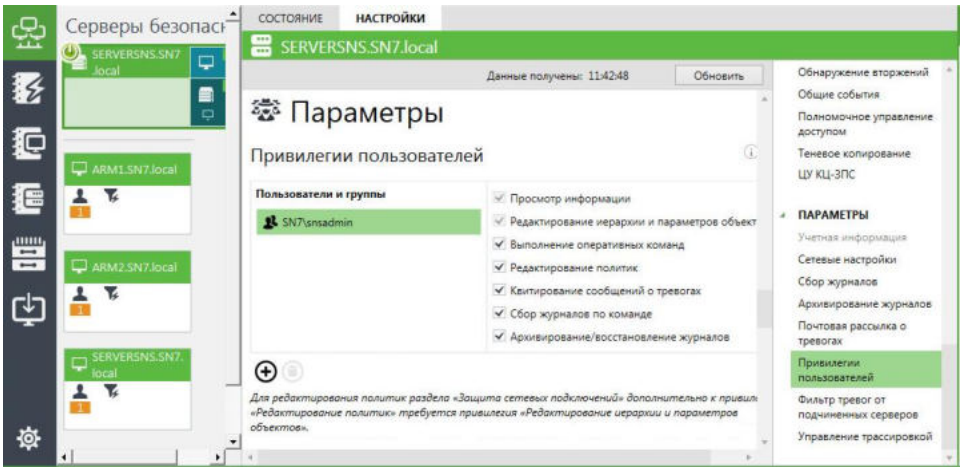


Обратите внимание, что при редактировании учетной информации можно указать уровень важности объекта, который определяет присваиваемый уровень для событий тревоги, а также ввести данные о компьютере, которые будут использоваться при построении отчетов. Эти данные можно редактировать как централизованно, так и локально на защищаемом компьютере.

Установите для компьютера ARM2 уровень важности "высокий" и примените изменения.

32. На вкладке "Настройки" откройте группу "Параметры / Привилегии пользователей", которая доступна только при выборе СБ и предназначена для настройки привилегий пользователей для работы с программой управления.

С помощью кнопки (i) ознакомьтесь с кратким описанием привилегий.



Обратите внимание, что по умолчанию все перечисленные привилегии предоставлены пользователям, входящим в группу администраторов домена безопасности. При необходимости привилегии можно назначить и другим учетным записям, исключая привилегию "Редактирование иерархии и параметров объектов" – данная привилегия в обязательном порядке предоставляется только для группы администраторов домена безопасности.

33. Рассмотрен ряд важных операций по ведению журналов в Secret Net Studio. Останьтесь в текущем окне.

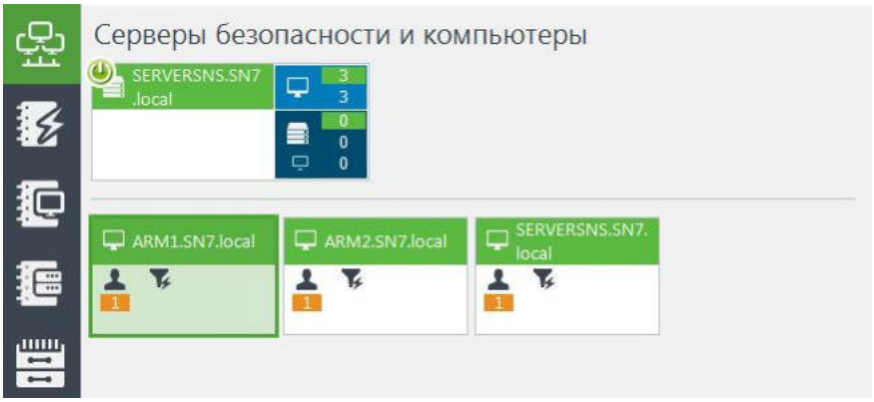
Выполнение лабораторной работы завершено.

Лабораторная работа №4 "Управление подчинением защищаемых компьютеров серверу безопасности SNS"

В этой лабораторной работе рассматривается:

- внесение изменений в структуру оперативного управления на примере выведения (добавления) защищаемого компьютера из (в) подчинения серверу безопасности;
- возможность смены режима функционирования клиента – из автономного режима в сетевой и обратно.

1. Рассмотрим пример внесения изменений в структуру оперативного управления. Перейдите в окно консоли ВМ ARM2, в программе управления на панели "Компьютеры"  нажмите кнопку "Свойства"  . Панель свойств компьютера ARM1 свернется, и вы вернетесь к диаграмме управления. Обратите внимание, что в данном представлении верхняя часть диаграммы содержит выбранный СБ (с его подчиненными серверами, если они есть), а нижняя – компьютеры, непосредственно подчиненные выбранному серверу.

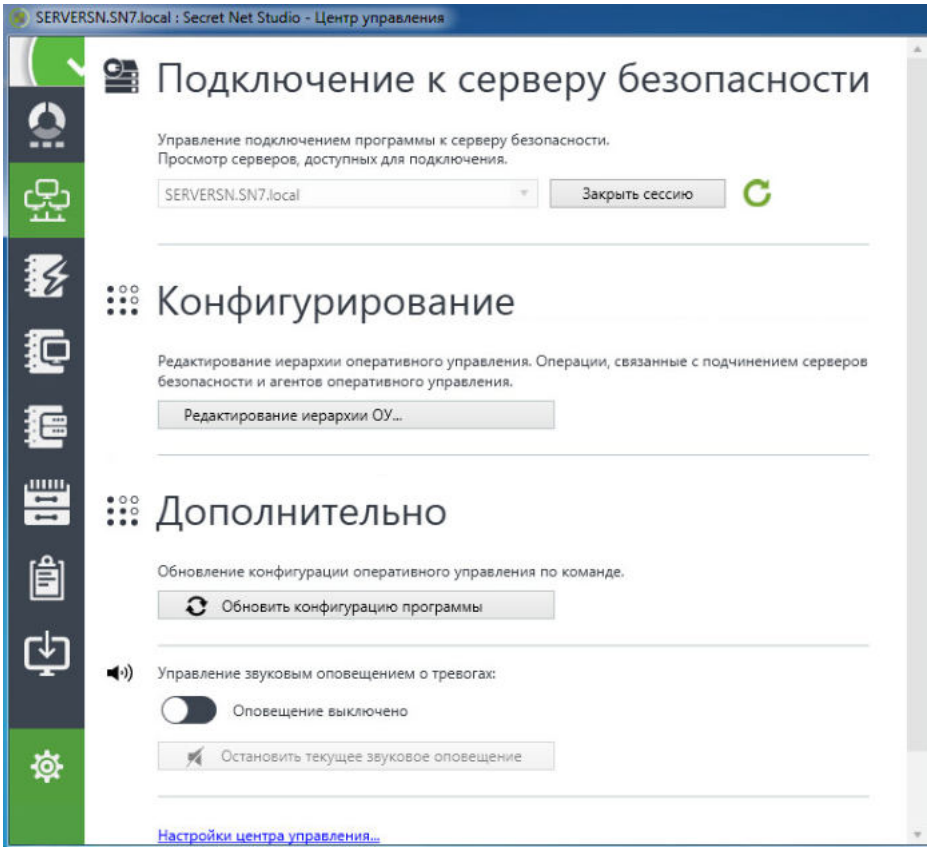


Если при установке серверов безопасности и клиентов выполнялось их подчинение СБ, эти компьютеры будут включены в структуру оперативного управления (ОУ). Структура ОУ считается сформированной на достаточном уровне, если все защищаемые компьютеры присутствуют в ней и подчинены серверам безопасности.

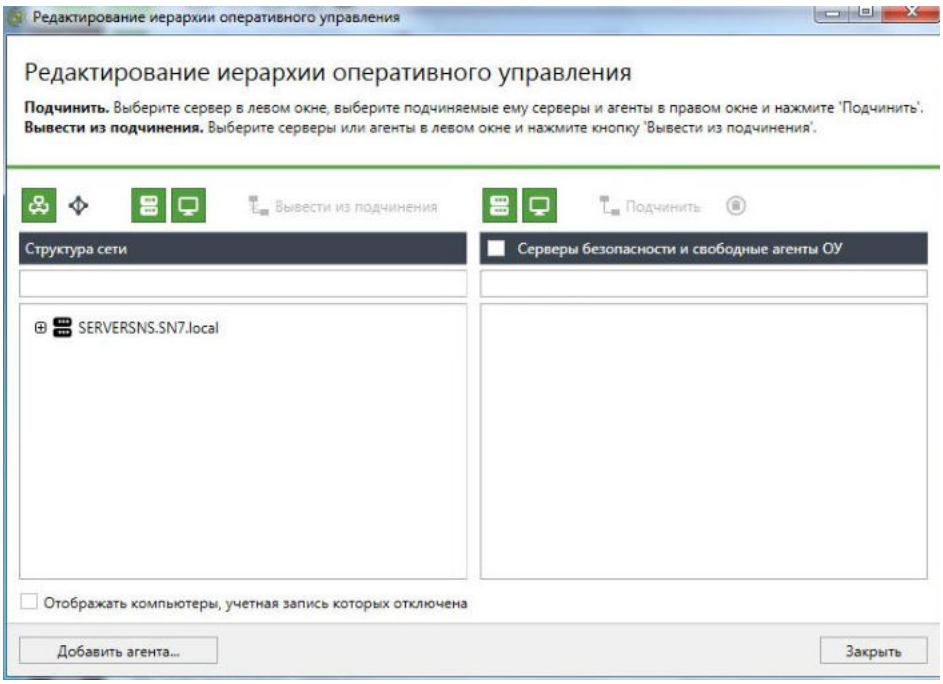
2. Изменения в структуре ОУ (добавление или исключение из нее защищаемых объектов) могут выполняться автоматически, при установке или удалении ПО системы Secret Net Studio на компьютерах. При необходимости в программе управления можно вручную вносить нужные изменения в сформированную структуру ОУ. Например, изменять отношения подчинения между СБ или подчинять защищаемые компьютеры другим серверам. Переподчинение объектов (например, при пересмотре сетевой структуры) требует предварительного вывода их из подчинения текущим СБ.

В качестве примера проведения изменений в структуре ОУ выведите компьютер ARM1 из подчинения серверу ServerSNS. Для этого:

- в нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки"  . На экране появится панель инструментов настройки и конфигурирования;



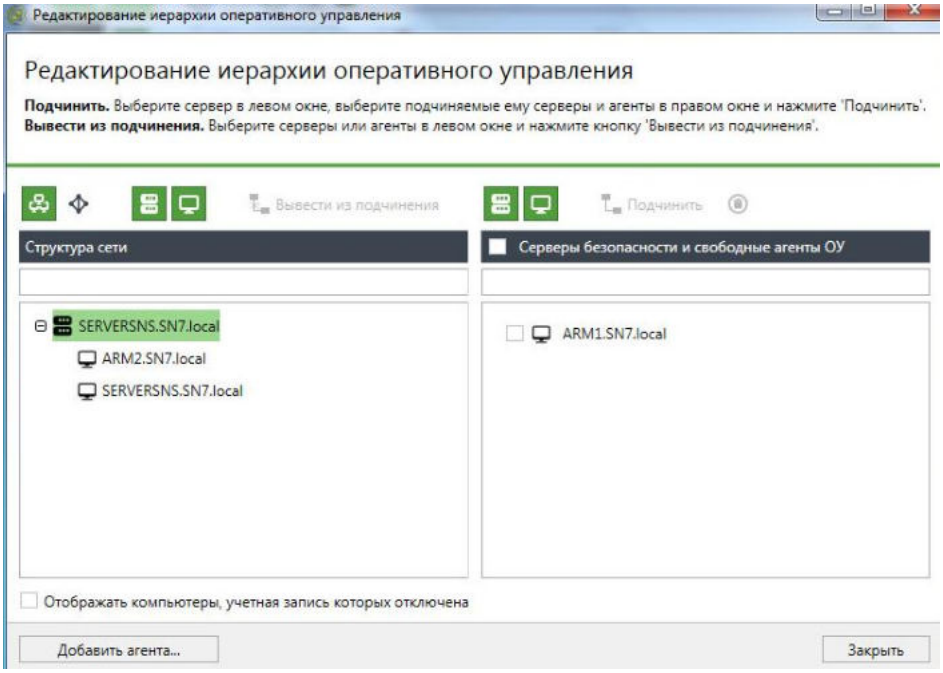
- в разделе "Конфигурирование" нажмите кнопку "Редактирование иерархии ОУ" Редактирование иерархии ОУ... . На экране появится диалоговое окно, в левой части которого представлена текущая структура объектов управления, а в правой – список защищаемых компьютеров и серверов безопасности, доступных для подчинения выбранному серверу;



Обратите внимание, что при необходимости с помощью кнопок и текстового поля для поиска, расположенных над списками объектов, а также переключателя "Отображать компьютеры, учетная запись которых отключена" можно фильтровать списки объектов по типу, контексту или по состоянию учетной записи.

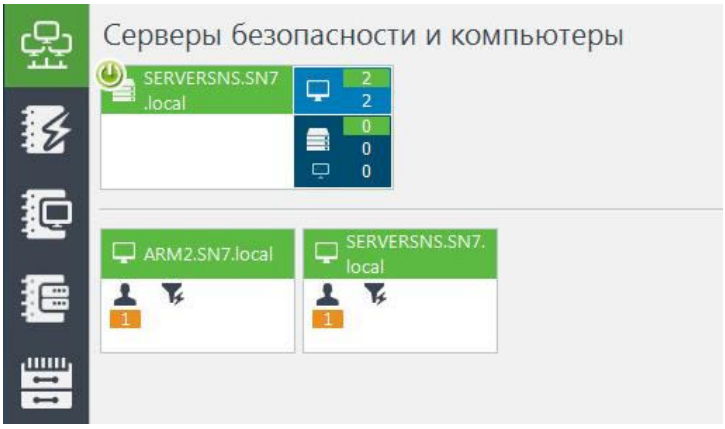
- слева в списке "Структура сети" разверните структуру сервера безопасности, выберите компьютер ARM1 и нажмите кнопку "Вывести из подчинения" 

. В появившемся диалоговом окне запроса подтвердите выполнение операции. Выбранный объект перестанет отображаться в списке "Структура сети" и будет перемещен в список свободных агентов относительно выбранного СБ.



Примечание. При выводе объекта из подчинения текущему СБ этот объект становится свободным. Свободный компьютер в дальнейшем необходимо подчинить СБ. Если из подчинения выведен сервер безопасности, то он может продолжать функционировать в качестве независимого объекта управления.

3. Закройте диалоговое окно "Редактирование иерархии оперативного управления" и вернитесь в программу управления к диаграмме управления в режиме отображения списков компьютеров. Обратите внимание, что выведенный из подчинения компьютер не представлен в структуре после обновления конфигурации.



4. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки"  и, используя описание п. 2 данной лабораторной работы, восстановите подчинение компьютера ARM1 серверу ServerSNS.

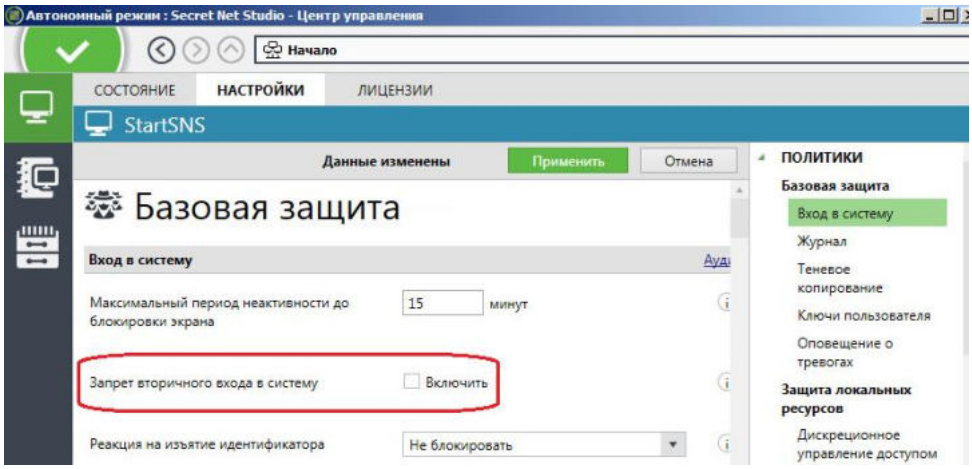
Убедитесь, что компьютер ARM1 появился в диаграмме управления.

Примечание. В реальной работе можно добавить в качестве объекта структуры ОУ любой компьютер, зарегистрированный в Active Directory. Если домен безопасности сформирован на базе вложенного контейнера Active Directory (в организационном подразделении), перед добавлением в структуру ОУ компьютеры следует переместить в этот контейнер, используя штатные средства администрирования AD.

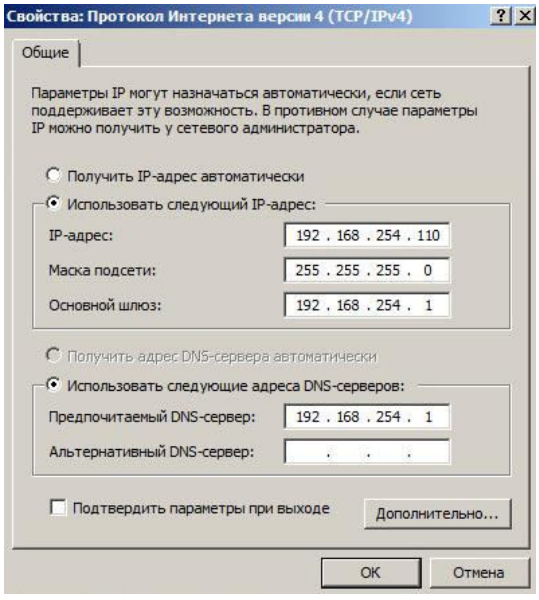
5. Далее будет проиллюстрирована возможность смены режима функционирования клиента Secret Net Studio из автономного в сетевой и обратно на примере компьютера StartSNS. Данная операция доступна только в локальном режиме работы программы управления.

Перед изменением режима работы клиента на компьютере StartSNS проведите на нем необходимые настройки:

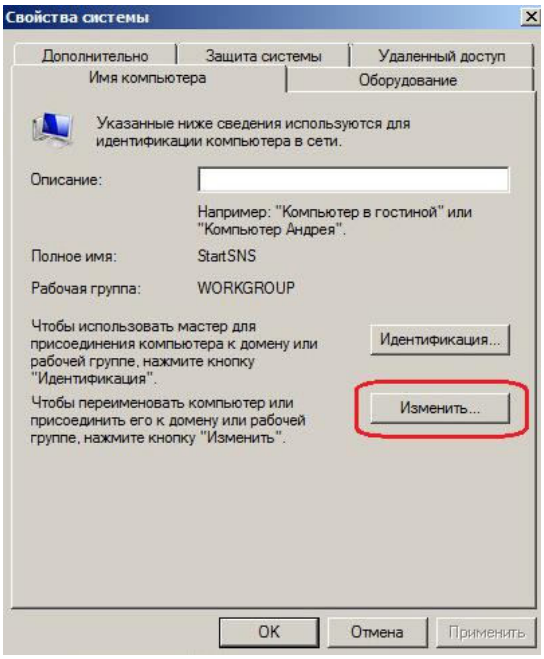
- откройте окно консоли BM StartSNS и в программе управления в группе настроек "Политики / Базовая защита / "Вход в систему" отключите параметр "Запрет вторичного входа в систему", а затем нажмите кнопку "Применить" Применить;

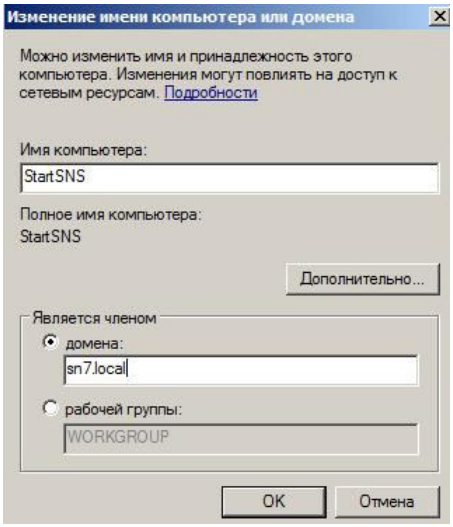


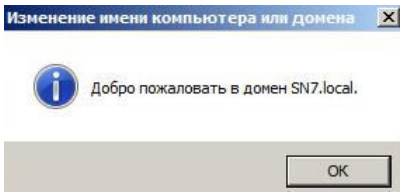
- чтобы изменения вступили в силу, перезагрузите BM StartSNS и авторизуйтесь под учетной записью **adminsns / P@ssw0rd**;
- через Панель управления установите следующие параметры сетевого соединения:
  - отключите протокол IPv6;
  - "IP-адрес" – **192.168.254.110**;
  - "Маска подсети" – **255.255.255.0**;
  - "Основной шлюз" / "Предпочитаемый DNS-сервер" – **192.168.254.1**;



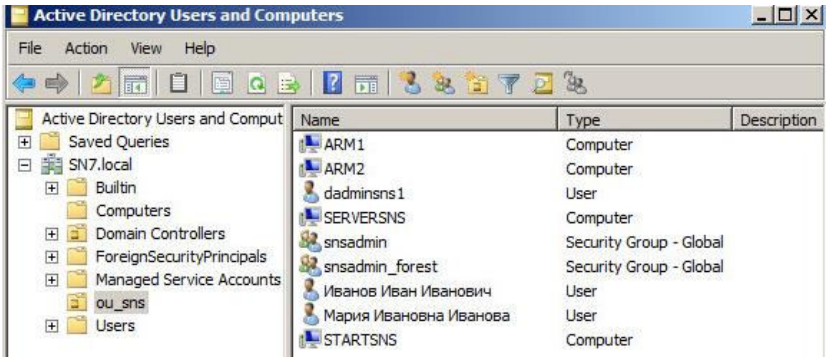
- через окно свойств компьютера введите ВМ StartSNS в домен sn7.local, указав реквизиты администратора домена **Администратор / P@ssw0rd**, перезагрузите ОС и авторизуйтесь под учетной записью администратора домена;



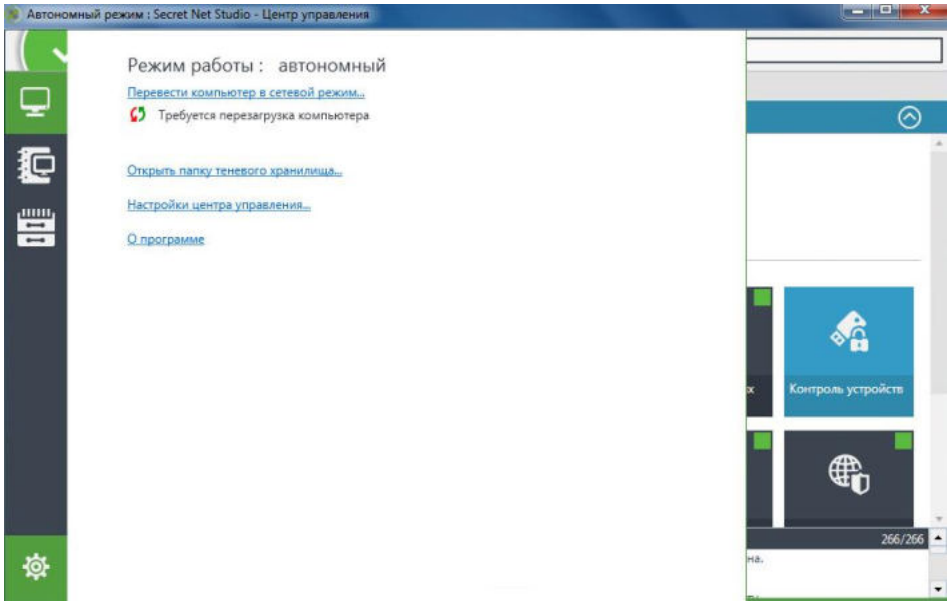




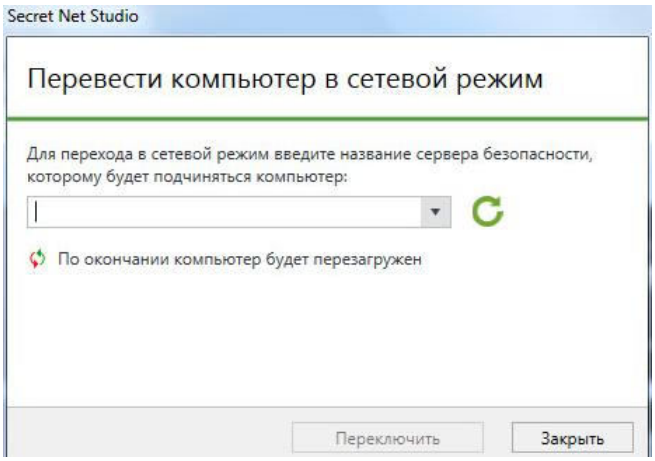
- включите доменную группу "snsadmin" в группу локальных администраторов компьютера StartSNS, а затем переавторизуйтесь под учетной записью "dadminsns1";
- переключитесь в окно консоли контроллера домена DC, откройте оснастку "Active Directory Users and Computers" и переместите в подразделение "ou_sns" компьютер StartSNS.



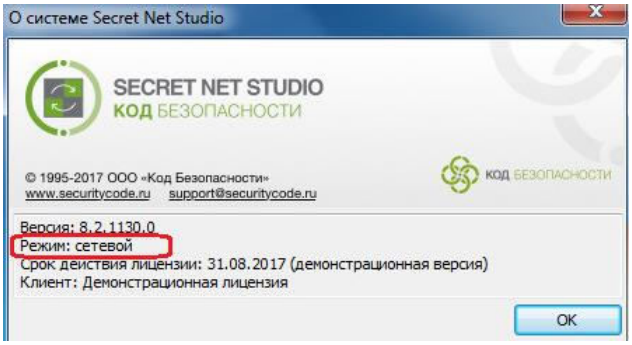
6. Измените на компьютере StartSNS режим функционирования клиента Secret Net Studio из автономного в сетевой. Для этого:
   - запустите локальный центр управления и откройте панель "Настройки"  . Обратите внимание, что в верхней части открывшейся панели указан текущий режим работы – "автономный";



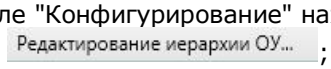
   - нажмите кнопку-ссылку "Перевести компьютер в сетевой режим". Откроется окно перехода в сетевой режим и поиска СБ;

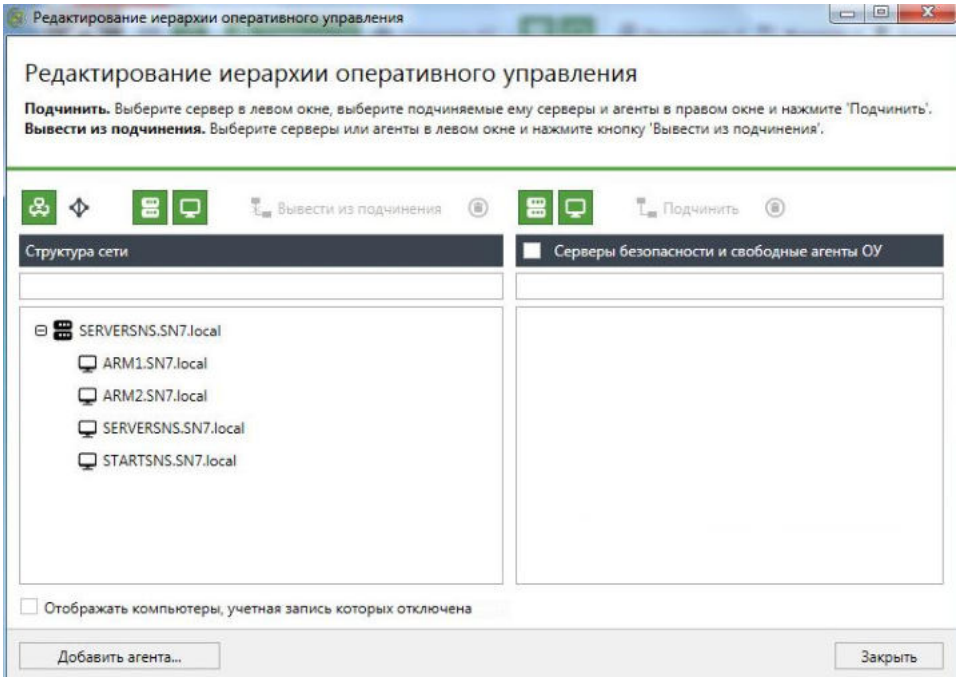


   - справа от поля ввода названия сервера нажмите кнопку "Поиск сервера безопасности" и после появления в данном поле имени "ServerSNS.SN7.local" нажмите кнопку "Переключить";
   - дождитесь завершения настройки компьютера для работы в сетевом режиме, перезагрузите ОС и авторизуйтесь под учетной записью "dadminsns1". Теперь на ВМ StartSNS клиент Secret Net Studio работает в сетевом режиме. Убедитесь в этом – в области трея Windows раскройте контекстное меню значка Secret Net Studio, выберите опцию "О системе", ознакомьтесь с представленной информацией, а затем закройте окно.

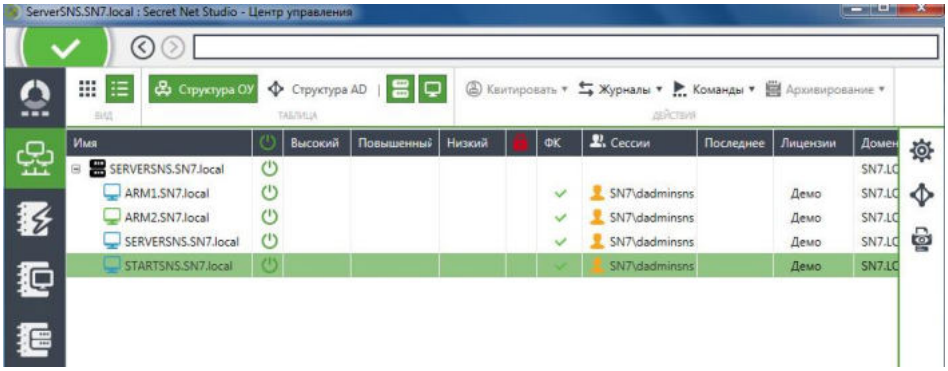


7. Убедитесь, что значок компьютера StartSNS появился в структуре оперативного управления СБ ServerSNS. Для этого:

- переключитесь в окно ВМ ARM2, в окне программы управления в нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки"  , в появившейся панели настройки и конфигурирования в разделе "Конфигурирование" нажмите кнопку "Редактирование иерархии ОУ"  ;
- в левой части открывшегося диалогового окна разверните структуру объекта сервера безопасности и убедитесь, что в нее добавлен компьютер StartSNS;



- закройте диалоговое окно "Редактирование иерархии оперативного управления" и откройте диаграмму управления в режиме отображения списков компьютеров. Обратите внимание, что компьютер StartSNS также представлен в структуре.



Теперь для данного компьютера будут действовать централизованно заданные администратором безопасности настройки и политики защиты Secret Net Studio.

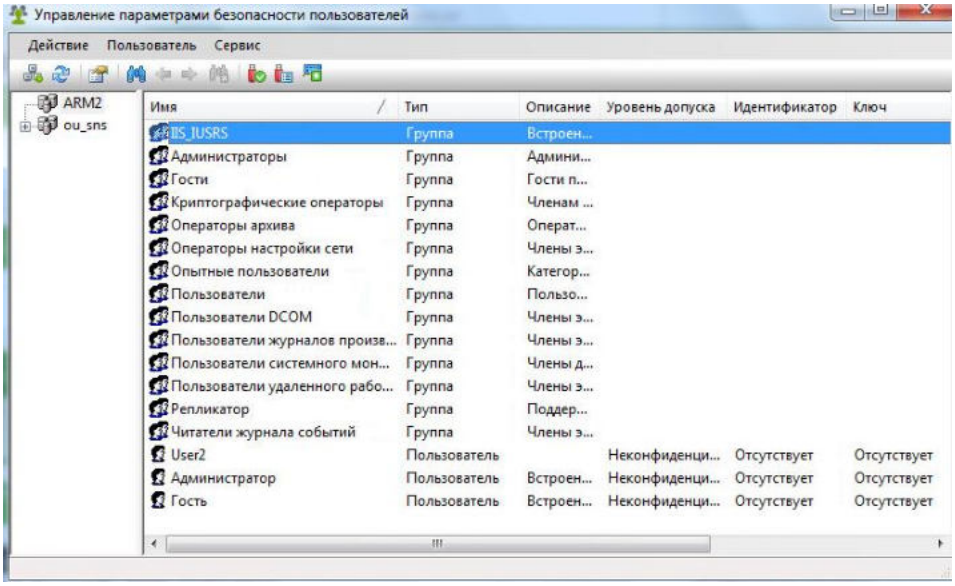
8. Самостоятельно. Используя описание пп. 5–6 выведите компьютер StartSNS из подчинения серверу безопасности, переключив сетевой режим работы клиента SNS обратно в автономный, в оснастке "Active Directory Users and Computers" переместите в папку "Computers" компьютер StartSNS и выведите его из домена SN7.local, а затем отключите на нем сетевой интерфейс.
9. Мы рассмотрели возможности управления подчинением защищаемых компьютеров серверу безопасности SNS. Останьтесь в текущем окне.

   Выполнение лабораторной работы завершено.

Лабораторная работа №5 "Работа с электронными идентификаторами"

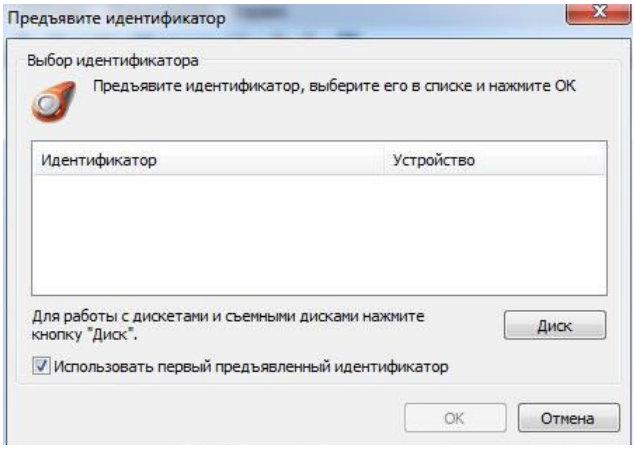
В данной лабораторной работе рассматривается порядок работы с электронными идентификаторами в централизованном режиме Secret Net Studio. Поскольку на лабораторном стенде не установлен ПАК "Соболь" или другой вид идентификатора, будет использоваться USB-флеш-накопитель в качестве примера идентификатора DS199x и для доступа к диалоговым окнам интерфейса генерации ключей ЦУ ПАК "Соболь".

1. На ВМ ARM2 под учетной записью "dadminsns1" подключите USB-флеш-накопитель.
2. Запустите программу "Управление пользователями": "Пуск / Все программы / Код безопасности / Secret Net Studio / Управление пользователями". Она предназначена для настройки параметров работы пользователей в системе защиты и позволяет выполнять действия как с доменными пользователями, так и с локальными.



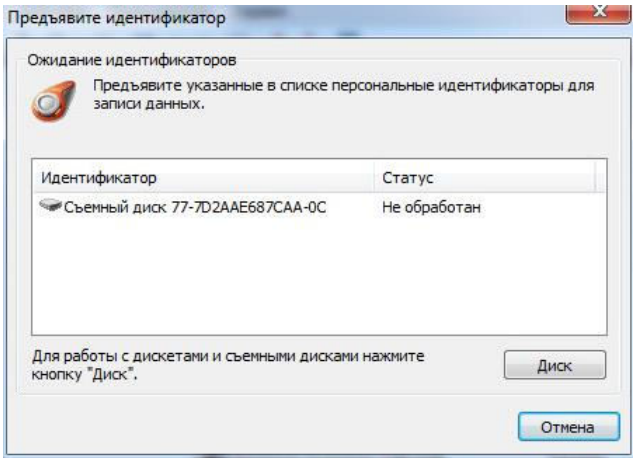
Обратите внимание, что интерфейс программы реализован аналогично стандартной оснастке ОС Windows "Active Directory – пользователи и компьютеры". В левой части окна отображается список контейнеров (текущий компьютер и структура разделов и организационных подразделений домена), а в правой – список пользователей в выбранном контейнере, представленный в виде таблицы со сведениями об уровнях допуска пользователей, наличии идентификаторов и ключей для усиленной аутентификации. Для централизованного управления по умолчанию в программу загружается структура текущего домена.

3. В главном меню выберите опцию "Сервис / Инициализация идентификатора" – откроется диалоговое окно.

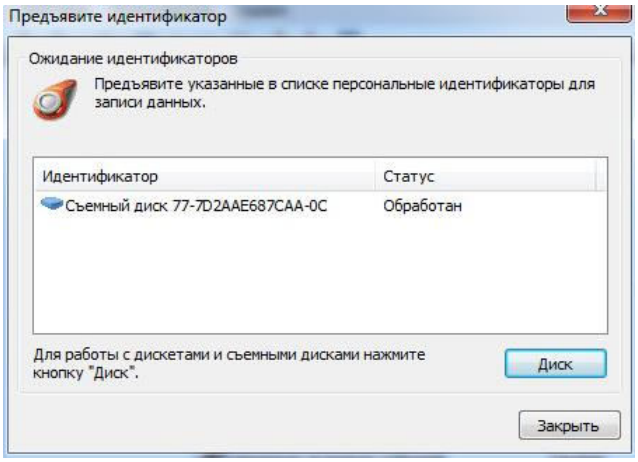


Данная операция предполагает форматирование, обеспечивающее возможность использования идентификатора в системе Secret Net Studio. Инициализация требуется, когда в персональном идентификаторе по каким-либо причинам была нарушена или отсутствует структура данных.

4. Нажмите кнопку "Диск" и дождитесь появления в списке новой записи с наименованием сменного носителя со статусом "Не обработан".



5. Выберите в списке запись необработанного носителя и еще раз нажмите кнопку "Диск". Дождитесь появления статуса "Обработан".



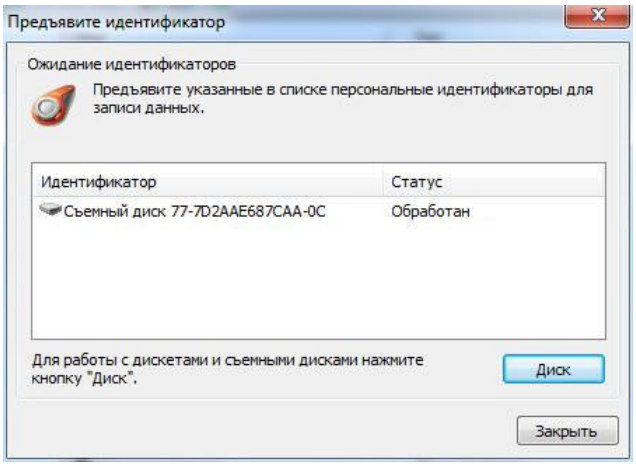
6. Нажмите кнопку "Закрыть". Ознакомьтесь с сообщением в информационном диалоговом окне и нажмите кнопку "ОК". Инициализация идентификатора произведена.

   Описанный выше порядок действий аналогичен для всех видов идентификаторов.

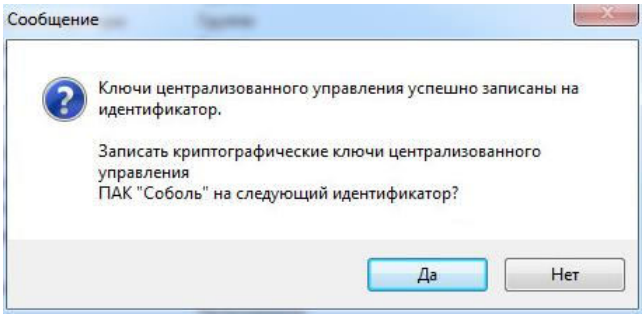
7. Теперь рассмотрим алгоритм создания ключей ЦУ ПАК "Соболь". В главном меню окна "Управление параметрами безопасности пользователей" выберите

опцию "Сервис / Генерация ключей ЦУ ПАК "Соболь". Откроется уже знакомое окно предъявления идентификатора.

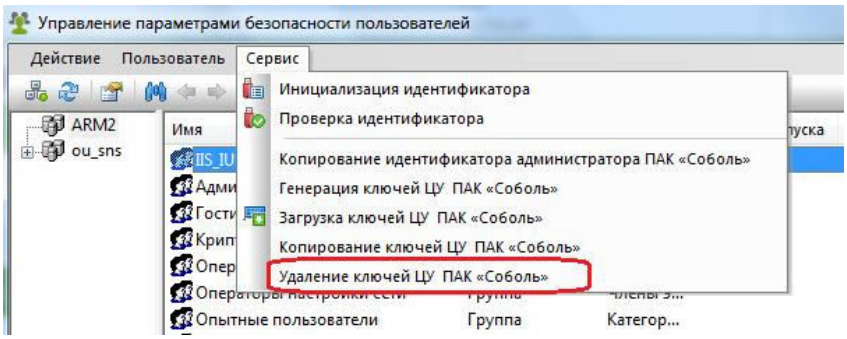
8. Нажмите кнопку "Диск", выберите запись съемного диска со статусом "Не обработан" и еще раз нажмите кнопку "Диск". Убедитесь, что в поле "Статус" значение изменилось на "Обработан".



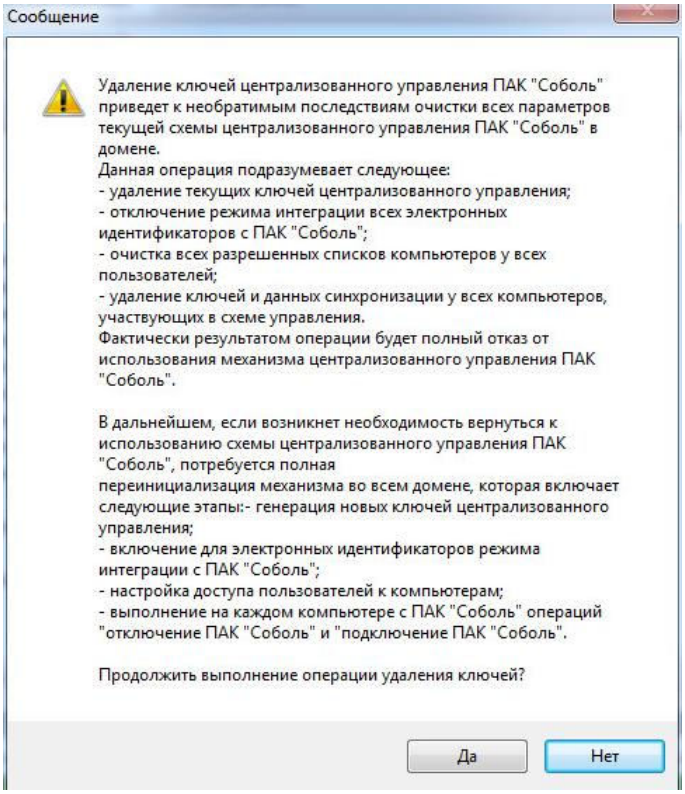
9. Нажмите кнопку "Закрыть". Обратите внимание, что в диалоговом окне "Сообщение" можно сразу сделать копию ключей ЦУ и записать их на еще один идентификатор. Нажмите кнопку "Нет".



10. В окне "Управление параметрами безопасности пользователей" в главном меню выберите опцию "Сервис" и обратите внимание, что в меню стал доступен пункт "Удаление ключей ЦУ ПАК "Соболь". Данная операция приводит к необратимым последствиям, после которых все процедуры, связанные с инициализацией, придется проделывать заново на всех компьютерах системы.

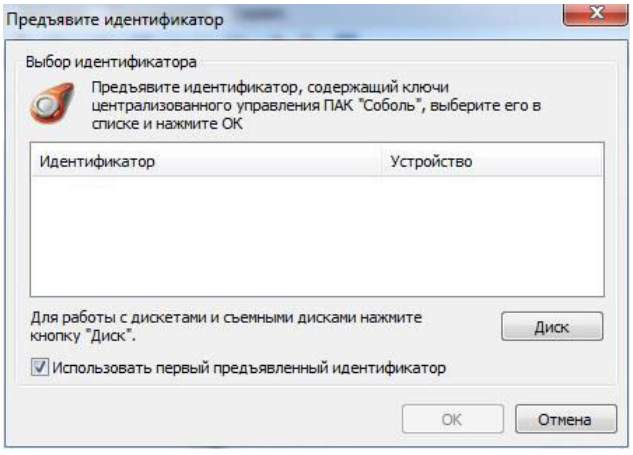


11. В главном меню выберите опцию "Сервис / Удаление ключей ЦУ ПАК "Соболь" и внимательно прочитайте текст сообщения.

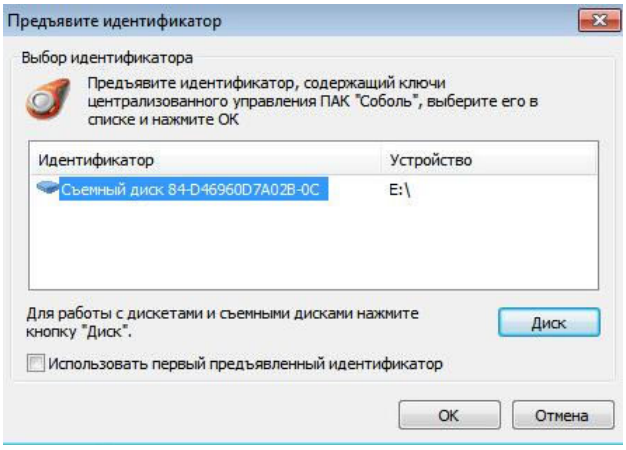


12. Нажмите кнопку "Нет". После того как были сформированы ключи ЦУ ПАК "Соболь", они автоматически загружены в ПУ Secret Net Studio. Если закрыть окно "Управление параметрами безопасности пользователей", они выгружаются и для возможности управления параметрами пользователей их необходимо загрузить заново.

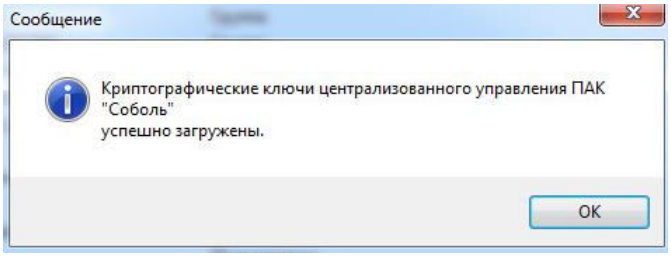
13. Закройте программу "Управление пользователями" и запустите ее вновь. В главном меню выберите опцию "Сервис / Загрузка ключей ЦУ ПАК "Соболь" – откроется диалоговое окно предъявления идентификатора.



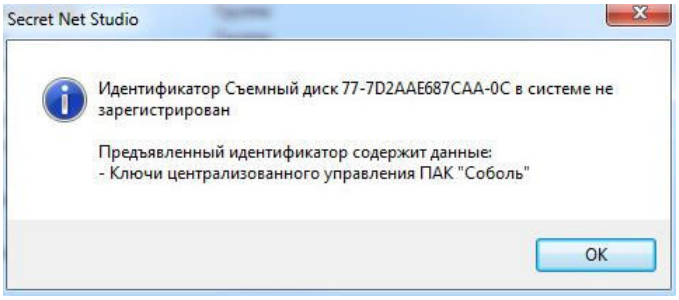
14. Снимите галочку в поле "Использовать первый предъявленный идентификатор", чтобы процесс был "видимым". Нажмите кнопку "Диск", выберите идентификатор и нажмите кнопку "ОК".



15. В диалоговом окне ознакомьтесь с текстом информационного сообщения о загрузке ключей и нажмите кнопку "ОК".



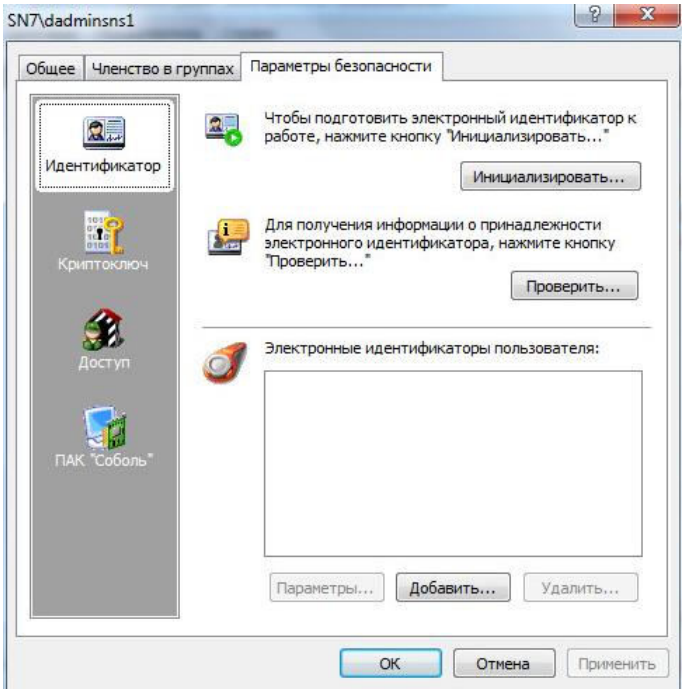
16. Теперь рассмотрим порядок проверки идентификатора. В главном меню окна "Управление параметрами безопасности пользователей" выберите опцию "Сервис / Проверка идентификатора". В диалоговом окне предъявления идентификатора с помощью кнопки "Диск" выберите идентификатор и нажмите кнопку "ОК". Появится диалоговое окно с информационным сообщением.



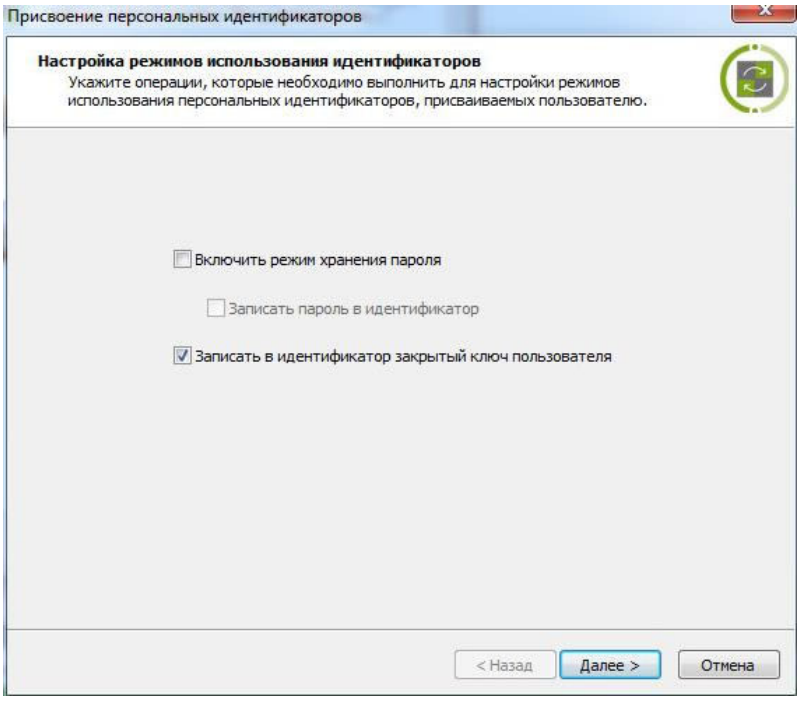
17. Прочитайте сообщение Secret Net Studio о том, что идентификатор в системе не зарегистрирован – это означает, что он не присвоен ни одному из пользователей домена безопасности. Нажмите кнопку "ОК".

18. Далее рассмотрим порядок присвоения идентификатора пользователю. В окне "Управление параметрами безопасности пользователей" раскройте структуру домена безопасности "ou_sns", выберите запись пользователя "dadminsns1" и из ее контекстного меню выберите опцию "Свойства".

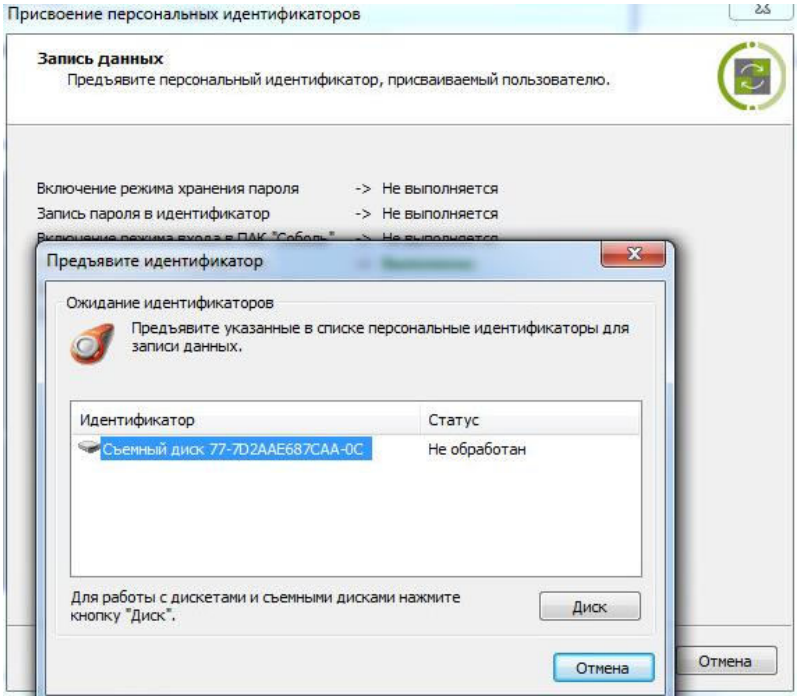
19. В открывшемся диалоговом окне перейдите на вкладку "Параметры безопасности".



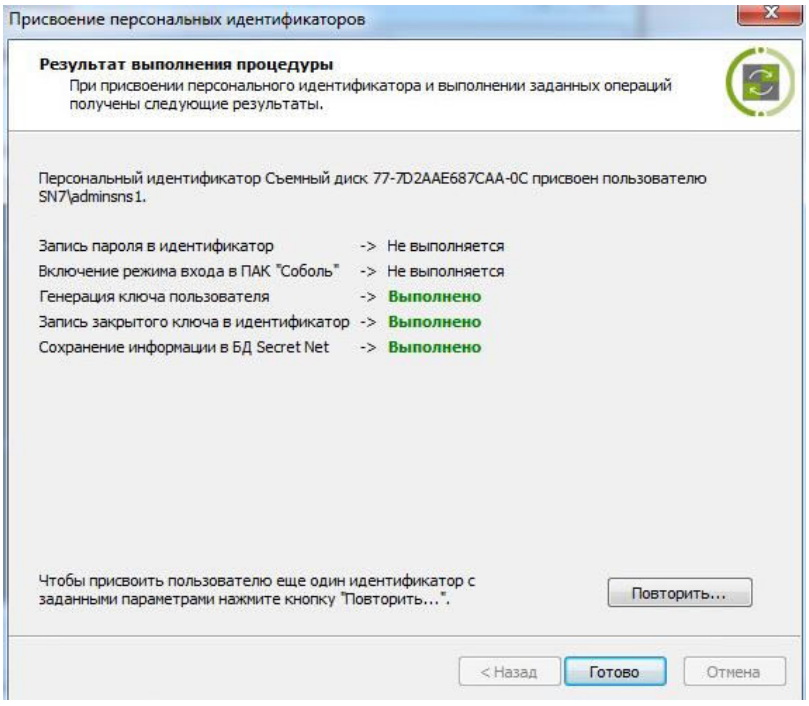
20. В категории настроек "Идентификатор" нажмите кнопку "Добавить". Откроется диалоговое окно "Присвоение персональных идентификаторов". Установите флажок в поле "Записать в идентификатор закрытый ключ пользователя" и нажмите кнопку "Далее".



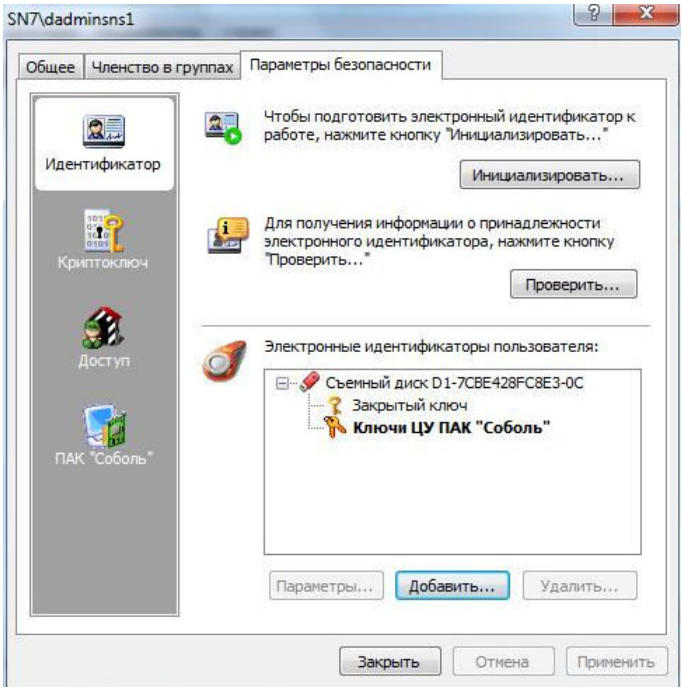
21. В процессе записи данных система запросит предъявление идентификатора. В диалоговом окне "Предъявите идентификатор" нажмите кнопку "Диск".



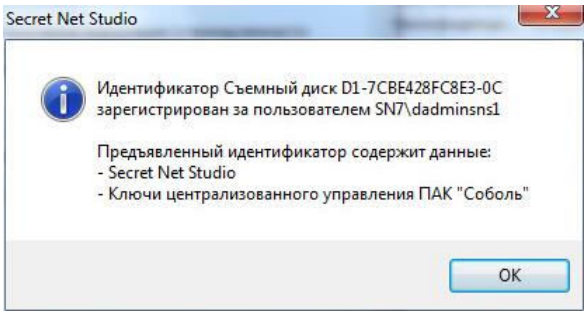
22. Выберите запись идентификатора со статусом "Не обработан" и еще раз нажмите кнопку "Диск". После изменения значения поля "Статус" на "Обработан" нажмите кнопку "Закрыть" и ознакомьтесь с результатом выполнения процедуры присвоения персонального идентификатора.



23. Нажмите кнопку "Готово". Обратите внимание на появившиеся записи в поле "Электронные идентификаторы пользователя".

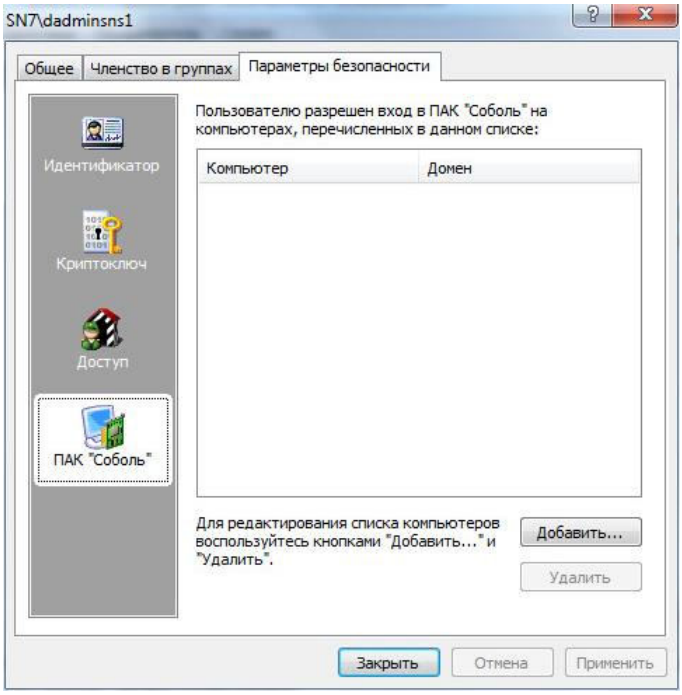


24. Нажмите кнопку "Проверить". С помощью кнопки "Диск" выберите идентификатор и после завершения проверки ознакомьтесь с информационным сообщением Secret Net Studio. Идентификатор зарегистрирован за пользователем "dadminsns1" и содержит данные Secret Net Studio и ключи централизованного управления ПАК "Соболь".

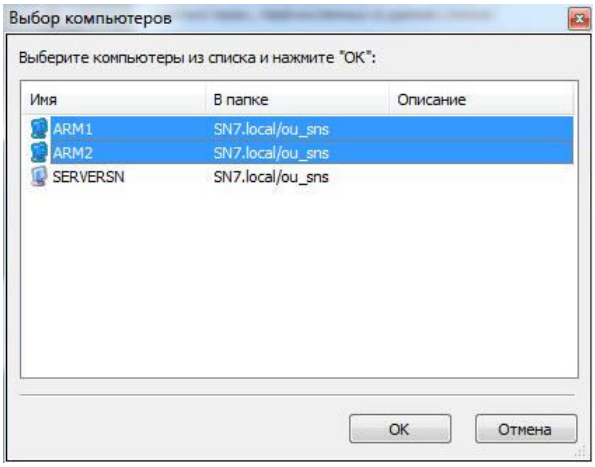


25. В окне информационного сообщения нажмите кнопку "ОК". Идентификатор присвоен пользователю и результат проверен.

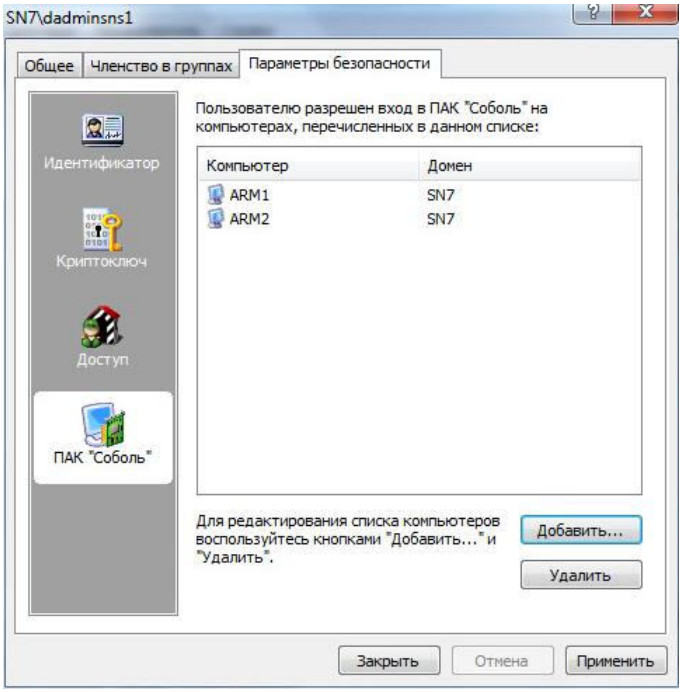
26. Рассмотрим действия администратора для передачи данных о пользователе и его идентификаторе в ПАК "Соболь" на конкретные компьютеры домена. На вкладке "Параметры безопасности" выберите категорию настроек "ПАК "Соболь".



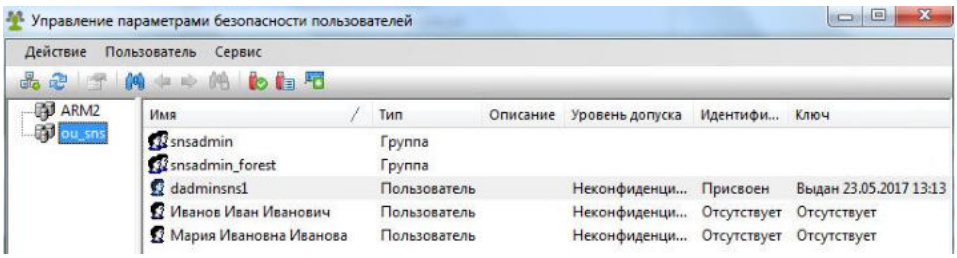
27. Нажмите кнопку "Добавить". В открывшемся диалоговом окне "Выбор компьютеров" с помощью клавиши [Ctrl] выберите из списка компьютеры ARM1 и ARM2 и нажмите кнопку "ОК".



28. Вы вернулись на вкладку "Параметры безопасности" окна свойств учетной записи "dadminsns1". Обратите внимание, что выбранные компьютеры появились в списке разрешенных для данного пользователя.



29. В окне свойств учетной записи "dadminsns1" нажмите кнопку "Применить", а затем – кнопку "ОК". Если бы ПАК "Соболь" был установлен на компьютерах ARM1 и ARM2, а в качестве идентификатора использовался бы идентификатор типа DS1995 – выполненные действия привели бы к регистрации данного пользователя в ПАК "Соболь" на этих компьютерах.



30. Закройте окно программы "Управление параметрами безопасности пользователей". Выполнение лабораторной работы завершено.

Контрольные вопросы

1. Какие программные модули и защитные механизмы входят в компонент базовой защиты?
2. Какие средства используются в Secret Net Studio для управления механизмами защиты а) в централизованном режиме, б) в локальном режиме?
3. Какие из настроек в соответствии с концепцией управления безопасностью Secret Net Studio имеют приоритет – локальные или групповые политики?
4. Какие из политик, заданные для защищаемых компьютеров в программе "Центр управления", имеют более высокий приоритет – политики для объекта домена в структуре оперативного управления или политики сервера безопасности, которому подчинены эти компьютеры?
5. В чем заключается различие между стандартным и усиленным режимами аутентификации пользователя в Secret Net Studio?
6. Почему не рекомендуется смена администратором пароля пользователя через стандартные оснастки Windows, если в Secret Net Studio включен режим усиленной аутентификации по паролю?
7. Для чего используется административный режим входа в систему? Как он активируется и выключается?
8. Какие персональные идентификаторы можно использовать в Secret Net Studio?

9. При действующих по умолчанию настройках регистрации в журнале Secret Net Studio событий запуска и завершения приложений (процессов) регистрируются только события, относящиеся к работе запущенных пользователем приложений, либо регистрируются все процессы системы – как пользовательские, так и системные? Почему?
10. Целостность (неизменность содержания) каких ресурсов можно контролировать подсистемой контроля целостности Secret Net Studio?
11. Какие категории объектов включает в себя МД КЦ-ЗПС? Кратко опишите их назначение.
12. Какое ПО и в каких режимах используется для построения МД КЦ-ЗПС?
13. Какой формат данных используется для хранения записей о событиях в локальном журнале Secret Net Studio?
14. Могут ли защитные подсистемы Secret Net Studio регистрировать сведения о событиях в штатных журналах ОС Windows?
15. В каких случаях происходит очистка локальных журналов Secret Net Studio?
16. Какие события считаются событиями тревоги? Как администратор должен обрабатывать эти события?
17. Как в Secret Net Studio называется подтверждение администратором безопасности получения информации о событии тревоги с описанием принятых мер?
18. Где хранятся записи журналов станций, собранных на сервере безопасности с защищаемых компьютеров?
19. Каким образом после развертывания в сети средств защиты Secret Net Studio можно произвести переподчинение защищаемых компьютеров от одного сервера безопасности к другому либо просто вывести компьютер из подчинения серверу безопасности?
20. Какие предварительные настройки следует выполнить на защищаемом компьютере с установленным автономным клиентом Secret Net Studio для переключения его работы в сетевой режим?

Глава 3
Настройка и применение компонентов локальной защиты Secret Net Studio

В этой и последующих главах приводится более детальное описание дополнительных компонентов защиты SNS, которые могут подключаться по отдельности (см. схему лицензирования на рис. 1 и структуру клиента на рис. 2).

Эта глава посвящена настройке и применению некоторых из подсистем защиты, входящих в состав отдельно лицензируемых компонентов:

- "средство защиты информации от несанкционированного доступа" (СЗИ от НСД) включает в себя следующие подсистемы:
  - контроль устройств;
  - контроль печати;
  - замкнутая программная среда;
  - полномочное управление доступом;
  - дискреционное управление доступом;
  - затирание данных;
- "защита дисков и шифрование контейнеров" включает в себя следующие подсистемы:
  - защита информации на локальных дисках;
  - шифрование контейнеров.

Далее рассматриваются подсистемы защиты в порядке, в котором они перечислены: сначала описываются подсистемы лицензируемого компонента "СЗИ от НСД", а затем – компонента "защита дисков и шифрование контейнеров".

Контроль устройств

Для защиты доступа к устройствам компьютера используются следующие взаимосвязанные механизмы:

- механизм контроля подключения и изменения устройств – предназначен для обнаружения и реагирования на изменение аппаратной конфигурации компьютера, а также для поддержания в актуальном состоянии списка устройств компьютера;
- механизм разграничения доступа к устройствам – выполняет разграничение доступа пользователей к устройствам из актуального списка, сформированного механизмом контроля подключения и изменения устройств.

Список устройств представляет множество установленных или подключаемых к защищаемым компьютерам устройств, организованных по иерархической схеме. Отдельные устройства группируются в классы, которые, в свою очередь, включаются в группы. Группы являются элементами объединения верхнего уровня, и их количество фиксировано – см. табл. 3.

Табл. 3. Группы и классы устройств

Группа	Класс	Описание
Локальные устройства	Последовательные порты. Параллельные порты. Сменные диски. Оптические диски. Физические диски. Процессоры. Оперативная память. Системная плата. Аппаратная поддержка. Программно реализованные диски	Фиксированные устройства компьютера, для которых не предполагается ограничивать подключение
Устройства USB	Сетевые платы и модемы. Интерфейсные устройства. Сканеры и цифровые фотоаппараты. Принтеры. Устройства хранения. Bluetooth-адаптеры. Сотовые телефоны. Электронные идентификаторы и считыватели. Прочие	Устройства, подключаемые к шине

Группа	Класс	Описание
Устройства PCMCIA	Последовательные порты и модемы. Параллельные порты. Устройства хранения. Сетевые платы. Прочие	Устройства, подключаемые к шине
Устройства IEEE1394	Устройства хранения. Принтеры. Сканеры и цифровые фотоаппараты. Сетевые устройства. Цифровые видеокамеры. Прочие	Устройства, подключаемые к шине
Устройства Secure Digital	Карточки памяти	Устройства, подключаемые к шине
Сеть	Соединение Ethernet. Беспроводное соединение (WiFi). Соединение Bluetooth. Соединение 1394 (FireWire). Инфракрасное соединение (IrDA)	Устройства, являющиеся сетевыми интерфейсами (адаптеры). Если сетевым интерфейсом является нефиксированное подключаемое устройство, то оно может также присутствовать и в другой группе. Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве сетевого интерфейса

Некоторые классы допускают дополнительное разбиение устройств по моделям, которые объединяют устройства с одинаковыми идентификационными кодами, присвоенными производителем. В списке устройств присутствуют предопределенные модели, например, модели электронных идентификаторов. Также в список можно добавлять модели на основе имеющихся устройств, если в этих устройствах производителем были указаны идентификационные коды. В дальнейшем при обнаружении нового устройства с такими же идентификационными кодами это устройство автоматически будет добавлено в качестве экземпляра к той же модели. За счет этого можно управлять одинаковыми устройствами без необходимости настройки параметров каждого из них по отдельности.

Для объектов каждого уровня (группа, класс, модель, устройство) определен набор параметров, с помощью которых настраиваются механизмы контроля подключения и изменения устройств, разграничения доступа к устройствам, теневого копирования и полномочного управления доступом.

Список устройств на компьютере создается при первой загрузке ОС сразу после установки клиентского ПО системы Secret Net Studio и принимается как эталонная конфигурация компьютера. Он хранится в локальной базе данных системы Secret Net Studio и загружается в локальной политике.

Для централизованного управления можно создать список устройств в групповой политике. После создания список устройств состоит из групп, классов и предопределенных моделей устройств. При необходимости в него можно добавить и конкретные устройства.

Вариант централизованного управления устройствами на уровне их групп и классов является предпочтительным, когда требуется обеспечить общие принципы контроля устройств на защищаемых компьютерах и нет необходимости централизованной настройки для отдельных устройств. Администратору безопасности достаточно настроить параметры использования для групп и классов (а также и моделей устройств, если они предусмотрены для класса) в нужных групповых политиках (о принципе наследования политик см. в разделе "Организация управления системой защиты" главы 2).

В отличие от централизованного локальное управление на уровне конкретных устройств применяется, если требуется установить особые параметры использования конкретных устройств на отдельном компьютере.

В рамках групповой или локальной политики права доступа к каждому объекту, а также параметры контроля устройств определяются в соответствии с правилами наследования или явного задания параметров. Параметры могут быть заданы для групп, классов, моделей или конкретных устройств. При этом может использоваться принцип наследования параметров от вышестоящих элементов иерархии в списке. Явно заданные параметры имеют приоритет перед наследу-

емыми от старших элементов иерархии. Например, если для устройства явно заданы особые параметры доступа, они будут применяться независимо от того, какие параметры заданы для класса и группы.

По умолчанию после установки системы защиты в локальной политике заданы следующие правила использования устройств, которые распространяются на всех пользователей компьютера:

- для групп "Локальные устройства" и "Сеть" включен режим контроля "Устройство постоянно подключено к компьютеру". Для остальных групп включен режим "Подключение устройства разрешено";
- для всех обнаруженных жестких дисков, а также сменных и оптических дисков включен режим контроля "Устройство постоянно подключено к компьютеру" с дополнительным параметром "Блокировать компьютер при изменении устройства". При этом для классов, к которым относятся такие устройства, включен режим "Подключение устройства разрешено";
- для устройств с возможностью разграничения доступа предоставлен полный доступ трем стандартным группам пользователей: "Система", "Администраторы" и "Все";
- теневое копирование отключено для всех устройств;
- для устройств с возможностью назначения категории конфиденциальности включен режим доступа "Устройство доступно без учета категории конфиденциальности";
- для сетевых интерфейсов разрешено функционирование независимо от уровней конфиденциальности сессий в режиме контроля потоков механизма полномочного управления доступом;
- регистрируются все события категорий "Контроль аппаратной конфигурации" и "Разграничение доступа к устройствам";
- разрешается использование локальных устройств и ресурсов в терминальных сессиях.

Чтобы пользователь мог подключать к компьютеру только разрешенные к использованию устройства, настройку системы рекомендуется выполнить следующим образом:

1. После установки системы защиты администратор безопасности последовательно подключает к компьютеру все устройства, планируемые к использованию. На этом этапе устройства регистрируются в системе, и для них или копируются разрешающие права доступа и параметры контроля от вышестоящих объектов (моделей, классов и групп), или настраиваются особые параметры (например, назначаются нужные категории конфиденциальности). После этого наследование прав на эти устройства отключается.
2. По завершении регистрации устройств администратор отключает разрешающие права для соответствующих моделей, классов и групп (например, для группы "Устройства Secure Digital"). Это приведет к тому, что пользователь сможет подключать только устройства, зарегистрированные на шаге 1. Подключение других устройств будет запрещено.

> **Пояснение.** По запросу пользователя о необходимости разрешения использования имеющегося у него устройства (например, USB-флеш-накопителя) администратор безопасности предлагает подключить это устройство к компьютеру на рабочем месте пользователя. После подключения устройства, даже если оно будет запрещено к использованию, сведения о нем появятся в списке устройств локальной политики. Администратор на своем рабочем месте в программе управления загружает параметры локальной политики соответствующего агента и выполняет необходимые действия для разрешения использования устройства.

Функцию теневого копирования можно включить для всех устройств, подключаемых к системе в качестве дисков, следующих видов:

- подключаемые сменные диски;
- дисководы гибких дисков;
- дисководы оптических дисков с функцией записи.

Практическое применение подсистемы контроля устройств рассматривается в соответствующей лабораторной работе (см. ниже).

Контроль печати

Настройка параметров использования принтеров осуществляется в отдельном списке "Принтеры". Если администратор не задавал для принтеров никаких специальных параметров, при печати на любые принтеры будут применяться установки по умолчанию.

Представленные в списке принтеров печатающие устройства могут также присутствовать и в списке устройств (см. предыдущий раздел). Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве принтера.

Список принтеров создается на компьютере сразу после установки клиентского ПО системы Secret Net Studio, представляется в локальной политике и хранится в локальной базе данных системы Secret Net Studio. Для централизованного управления можно создать список принтеров в групповой политике.

Изначально список принтеров состоит из одного элемента – "Настройки по умолчанию". Заданные для этого элемента параметры использования применяются ко всем принтерам, кроме тех, которые явно присутствуют в списке.

Процедуры загрузки списка принтеров при работе с программой управления в централизованном и локальном режимах выполняются аналогично.

После установки системы защиты в локальной политике по умолчанию будут заданы следующие правила использования принтеров, которые распространяются на всех пользователей компьютера:

- к принтерам предоставлен доступ стандартным группам пользователей: "Система", "Все" и "Все пакеты приложений";
- теневое копирование отключено для всех принтеров;
- для принтеров разрешена печать документов любой категории конфиденциальности;
- разрешается использование локальных принтеров в терминальных сессиях.

Чтобы пользователь мог печатать только на разрешенных к использованию администратором безопасности принтерах, настройку системы рекомендуется выполнить следующим образом:

1. После установки системы защиты SNS администратор последовательно добавляет на компьютер все принтеры, которые планируется использовать. Подключение к одним и тем же принтерам может выполняться различными способами – например, если принтер (физическое устройство) установлен как локальный и как сетевой с IP-адресом. В этом случае для корректной идентификации и разграничения доступа к таким принтерам, необходимо выполнить процедуру установки (добавления) принтера для каждого способа подключения.
2. По завершении установки принтеров администратор формирует список принтеров, который должен содержать элементы, соответствующие используемым принтерам, и в том числе отдельные элементы для различных способов подключения. При этом для элемента "Настройки по умолчанию" нужно установить запрет печати для всех пользователей и включить ограничение печати документов всех категорий конфиденциальности. Для остальных элементов списка принтеров устанавливаются необходимые права доступа пользователей и ограничения печати конфиденциальных документов. После этого пользователи не будут иметь возможность распечатывать документы в обход механизмов защиты на тех принтерах, которые они могут установить самостоятельно.
3. В дальнейшем при необходимости разрешить печать на новый принтер (или на тот же принтер, подключаемый другим способом) администратор может сам выполнить его установку, после чего добавить в список нужной политики и настроить параметры использования.

Для централизованного управления параметрами принтеров могут использоваться групповые политики доменов, организационных подразделений и серверов безопасности.

По умолчанию в групповых политиках отсутствуют списки принтеров. Поэтому для реализации централизованного управления необходимо создать список принтеров в нужной групповой политике.

При включенном режиме маркировки в распечатываемые документы автоматически добавляются специальные маркеры (грифы), содержащие учетные сведения для печати. Маркер – это особая форма со сведениями о распечатанном документе (например, когда распечатан, кем, сколько страниц), который обычно располагается в колонтитулах или на полях страниц. В системе маркер представлен как набор шаблонов, являющихся макетами определенных страниц документа: первой, последней, промежуточных и пр. В шаблонах заданы области расположения атрибутов со сведениями.

При печати документа происходит наложение макетов страниц из соответствующих шаблонов, и в результате на печатаемых листах вместе с содержимым документа выводятся относящиеся к маркеру сведения, которые печатаются независимо от расположения на листе текста самого документа.

Маркеры могут применяться для печати документов любой категории конфиденциальности, в том числе неконфиденциальных. При этом допускается использовать несколько маркеров для одной категории, чтобы пользователь мог самостоятельно выбирать нужный из числа предусмотренных.

По умолчанию в системе задан набор маркеров с предопределенными шаблонами и атрибутами. При необходимости можно настроить маркировку в соответствии с действующими в организации требованиями оформления.

Внимание! На компьютерах одного домена безопасности должны применяться одинаковые параметры использования маркеров, которые рекомендуется задать в общей групповой политике.

Более подробное описание подсистемы контроля печати вы найдете в руководстве администратора по настройке и эксплуатации локальной защиты.

Практическое применение процедур централизованной и локальной настройки рассматривается в соответствующей лабораторной работе.

Замкнутая программная среда

Как уже отмечалось в главе 1 (см. раздел "Механизмы защиты Secret Net Studio и принципы их работы" / "Замкнутая программная среда"), механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале регистрируются события тревоги. Настройка механизмов КЦ и ЗПС может осуществляться совместно в программе "Контроль программ и данных", и при этом используется единая модель данных, которая была описана в главе 2 (см. раздел "Контроль целостности ресурсов"). Поэтому для файлов, включенных в перечень ЗПС, можно установить и режим контроля целостности.

Модель данных для механизма ЗПС можно сформировать на основе сведений о запускавшихся программах из журнала Secret Net Studio. При централизованном управлении администратору безопасности (или аудитору) с помощью программы управления необходимо создать файл журнала в evtx- или snlog- формате, содержащий выборку записей за интересующий период. Затем этот файл с помощью программы управления КЦ-ЗПС в централизованном режиме импортируется в базу данных КЦ-ЗПС. При использовании программы "Контроль программ и данных" в локальном режиме сведения о запускавшихся программах можно загрузить непосредственно из локального журнала. Далее на основании этих данных формируются задания ЗПС для субъектов.

Поскольку модель данных, методы ее формирования и синхронизации были описаны в соответствующем разделе, посвященном контролю целостности ресурсов (см. главу 2), перейдем к порядку настройки механизма ЗПС. В качестве основного метода настройки предлагается подход с максимальным использованием автоматических средств – мастера моделей данных и генератора задач.

Поскольку порядок настройки механизма ЗПС аналогичен порядку настройки КЦ, здесь остановимся только на отличиях.

1. Подготовка к построению модели данных. На этом этапе проводится анализ размещения ПО и данных на защищаемых компьютерах, а также разрабатываются требования к настройке КЦ и ЗПС.

2. Построение фрагмента модели данных по умолчанию – только при формировании новой модели с нуля.

3. Добавление задач в модель данных. В модель данных добавляются описания задач (прикладное и системное ПО, наборы файлов данных и т.д.) для использования в ЗПС.

Если МД ЗПС формируется на основе данных журнала Secret Net Studio, то чтобы собрать нужные сведения, пользователям разрешается запускать любые приложения, и записи о запусках регистрируются в журнале. На это отводится некоторый период времени.

По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных.

Примечание. Источником при добавлении задач ЗПС по журналу в централизованном режиме является evtx- или snlog-файл с предварительно экспортированными сведениями из журнала.

4. Добавление заданий и включение в них задач. В модель данных добавляются все необходимые задания ЗПС и в них включаются задачи.

5. Подготовка ЗПС к использованию. Субъектам назначаются задания ЗПС. Для того чтобы ресурсы контролировались механизмом ЗПС, они должны быть специально подготовлены – иметь признак "выполняемый". На данном этапе администратору безопасности нужно выполнить следующие действия:

- отключить контроль ЗПС у привилегированных пользователей (например, администратора) – это снимет ограничения в работе этих пользователей. В Secret Net Studio используется привилегия "Учетные записи, на которые не действуют правила замкнутой программной среды", которая по умолчанию предоставлена группе "Администраторы";
- установить связи субъектов с заданиями ЗПС (то есть назначить субъектам сформированные задания). Задания назначаются субъектам "Компьютер" и "Группа" (в локальном режиме – "Компьютер", "Пользователь" и "Группа пользователей");
- подготовить ресурсы для ЗПС. Чтобы ресурсы контролировались механизмом замкнутой программной среды, они должны иметь признак "выполняемый" и входить в задание ЗПС. Также необходимо выполнить поиск зависимых модулей. В этом случае для каждого ресурса, которому будет установлен признак "выполняемый", будет выполняться поиск в ресурсах компьютера зависимых модулей. Найденные зависимые модули будут добавлены в модель данных в те же группы ресурсов, в которые входят исходные модули. Им также будет присвоен признак "выполняемый".

6. Расчет эталонов. Для всех заданий рассчитываются эталоны (контрольные значения) ресурсов.

7. Включение ЗПС в жестком режиме. В жестком режиме ЗПС возможен запуск только разрешенных программ, библиотек и сценариев. Запуск других ресурсов блокируется, а в журнале Secret Net Studio регистрируются события тревоги. Параметры механизма ЗПС можно задать централизованно или локально. При этом в централизованном режиме доступна возможность задания параметров как для отдельных компьютеров, так и для групп компьютеров. Если заданы разные параметры механизма ЗПС для компьютера и для группы, в которую он входит, – на компьютере будут действовать все включенные параметры этих субъектов (параметры "суммируются"). Например, если для группы включен параметр "Мягкий режим", этот режим будет действовать на компьютере, даже если тот же параметр будет отключен для этого компьютера.

На этапе создания МД, а также в процессе эксплуатации Secret Net Studio в модель можно вносить изменения, необходимость которых, как правило, обусловливается следующими факторами:

- появление новых задач по защите ресурсов;
- обновление программного обеспечения компьютера;
- изменения в задачах (расписание, методы контроля);
- полное или временное снятие задач с контроля.

Ресурс может входить в несколько заданий, и в каждом из них может использоваться свой метод контроля. Кроме того, в зависимости от типа ресурса и метода

контроля могут использоваться разные алгоритмы расчета контрольных значений. Поэтому ресурс может иметь несколько значений эталонов.

Более подробное описание настройки ЗПС вы найдете в руководстве администратора по настройке и эксплуатации локальной защиты.

Практическое применение механизма ЗПС с построением модели данных и внесением в нее изменений рассматривается в соответствующей лабораторной работе (см. ниже).

Полномочное управление доступом

Данный механизм обеспечивает разграничение доступа пользователей к конфиденциальным ресурсам. Его первоначальное описание, состав используемых категорий конфиденциальности и перечень ресурсов, для защиты которых он предназначен, а также базовые принципы использования вы найдете в главе 1 (см. раздел "Механизмы защиты Secret Net Studio и принципы их работы / Полномочное управление доступом"). Здесь приводится ряд особенностей применения полномочного управления доступом.

Для принтеров можно указать категории конфиденциальности документов, разрешенных для печати.

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска.

После установки клиентского ПО системы Secret Net Studio всем каталогам и файлам на локальных дисках компьютера назначается категория "Неконфиденциально" (если ресурсы не имеют ранее присвоенных категорий конфиденциальности). Пользователи могут повышать категории конфиденциальности нужных файлов только в пределах своих уровней допуска. При этом понижать категории конфиденциальности ресурсов, а также повышать категории каталогов разрешено только пользователям, которым предоставлена привилегия на управление категориями конфиденциальности.

Для устройств, которым можно назначить категорию конфиденциальности или выбрать допустимые уровни конфиденциальности сессий, по умолчанию включен режим доступа "Устройство доступно без учета категории конфиденциальности" или "Адаптер доступен всегда". Для принтеров по умолчанию включен режим разрешения печати документов любой категории конфиденциальности. Данные режимы разрешают использование устройств и принтеров независимо от уровня допуска пользователя.

В механизме полномочного управления доступом используется принцип наследования категорий конфиденциальности. Методы наследования различаются в зависимости от типов ресурсов.

Устройства наследуют категорию конфиденциальности от классов, к которым они относятся. При этом для класса разрешено указывать только категорию для общедоступной информации (по умолчанию – "Неконфиденциально") или включить режим доступа "без учета категории конфиденциальности". За счет этого исключается возможность копирования конфиденциальной информации на неразрешенное подключенное устройство (при работе механизма в режиме контроля потоков и отсутствии у пользователя привилегии на вывод конфиденциальной информации).

В соответствии с правилами наследования, при управлении устройствами явно заданные параметры имеют приоритет перед наследуемыми от старших элементов иерархии. Поэтому если для устройства явно назначена категория конфиденциальности, она действует независимо от того, какая категория указана для класса.

Между объектами файловой системы действует метод наследования внутри каталогов, имеющих категорию, отличную от категории для общедоступной информации (по умолчанию – "Неконфиденциально"). Наследование категории конфиденциальности объектов внутри каталога осуществляется в соответствии с установленными признаками наследования в атрибутах этого каталога.

В Secret Net Studio действуют следующие ограничения на присвоение категорий конфиденциальности каталогам:

- нельзя присвоить категорию корневому каталогу жесткого диска;

- не присваивайте категорию, отличную от категории для общедоступной информации (по умолчанию "Неконфиденциально"), системным каталогам, каталогам, в которых размещается прикладное ПО, а также каталогу "Мои документы" и всем подобным ему;
- не присваивайте категорию непосредственно на общедоступный каталог. Используйте для этого вложенные подпапки. Например, если на файл-сервере создан общедоступный каталог "Документы", то для назначения категорий конфиденциальности следует создать в нем подпапки, например, "Секретно", "ДСП" и т.д., которым затем присваивать требуемые категории.

Пользователю разрешается доступ к ресурсу, если его уровень допуска не ниже категории конфиденциальности этого ресурса. Например, пользователю с уровнем допуска "Конфиденциально" разрешается выполнять чтение файлов с категориями "Конфиденциально" и "Неконфиденциально", но запрещено открывать файлы с категорией "Строго конфиденциально". Наивысший уровень допуска предоставляет возможность открывать файлы с любой категорией конфиденциальности.

По умолчанию всем пользователям назначен уровень допуска "Неконфиденциально".

В механизме полномочного управления доступом используются следующие пользовательские привилегии:

- **управление категориями конфиденциальности.** Пользователь с данной привилегией может:
  - изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска;
  - управлять режимом наследования категорий конфиденциальности каталогов;
- **печать конфиденциальных документов** – разрешает пользователю выводить на принтер конфиденциальные документы. Данная привилегия применяется при включенном механизме контроля печати;
- **вывод конфиденциальной информации** – при включенном режиме контроля потоков разрешает пользователю выводить конфиденциальную информацию на внешние носители – сменные диски, для которых включен режим доступа "без учета категории конфиденциальности".

По умолчанию привилегии не назначены и предоставляются администратором безопасности пользователям, уполномоченным управлять конфиденциальностью ресурсов, распечатывать и копировать конфиденциальную информацию.

Режим контроля потоков конфиденциальной информации (по умолчанию отключен) обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации. Если данный режим включен, то:

- возможности использования устройств и доступа к конфиденциальным файлам определяются уровнем конфиденциальности сессии, который устанавливается при входе пользователя в систему;
- пользователи работают с ресурсами компьютера в рамках своих сессий с определенным уровнем конфиденциальности, который устанавливается при входе в систему и не изменяется до окончания сессии.

При выполнении операций с ресурсами их категории конфиденциальности сравниваются с уровнем сессии пользователя. Доступ разрешается, если категория конфиденциальности ресурса ниже или совпадает с уровнем сессии. К ресурсам с более высокой категорией доступ запрещается. Всем создаваемым, скопированным или измененным документам автоматически присваивается категория конфиденциальности, равная уровню сессии.

Общий порядок настройки полномочного управления доступом следующий:

1. В политиках SNS задаются количество и названия категорий конфиденциальности.

Внимание! Чтобы избежать конфликтов в названиях категорий конфиденциальности, их количество и названия должны быть заданы в одной общей групповой политике, которая применяется на защищаемых компьютерах (политике домена, политике OU или сервера безопасности).

2. Каждому пользователю назначаются уровни допуска и привилегии вывода конфиденциальной информации и/или управления категориями конфиденциальности.

3. Ресурсам (устройствам, каталогам и файлам на дисках) присваиваются категории конфиденциальности. При этом категории можно назначать индивидуально каждому ресурсу либо группе, классу или модели в списке устройств.
4. Определяется и задается перечень регистрируемых событий, связанных с работой механизма полномочного управления доступом.
5. Настраивается при необходимости и включается маркировка печати.
6. Настраивается при необходимости использование принтеров. Можно ограничить использование принтеров для печати документов, которым присвоены определенные категории конфиденциальности. Также предусмотрена возможность настройки прав пользователей для печати документов.
7. Включается при необходимости режим контроля потоков. При этом требуется выполнить локально на компьютере дополнительную настройку в отдельной программе настройки подсистемы полномочного управления доступом для режима контроля потоков.

Более детальное описание настройки и использования механизма полномочного управления доступом вы найдете в руководстве администратора по настройке и эксплуатации локальной защиты, а также в документе с комментариями к выпущенной версии продукта (Release Notes).

Практическое применение данного механизма рассматривается в соответствующей лабораторной работе (см. ниже).

Дискреционное управление доступом к каталогам и файлам

Первоначальное описание и принципы применения этого механизма были приведены в главе 1 (см. соответствующий подраздел в разделе "Механизмы защиты Secret Net Studio и принципы их работы"). При настройке дискреционного разграничения доступа к каталогам и файлам выполняются действия:

1. Предоставление привилегии для изменения прав доступа на любых ресурсах, что дает возможность привилегированным пользователям изменять права доступа на любых каталогах и файлах локальных дисков независимо от установленных прав доступа к самим ресурсам. Она, в частности, позволяет назначить администраторов ресурсов, которые в дальнейшем смогут настраивать права доступа к ресурсам для остальных пользователей. По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в группу локальных администраторов.
2. Назначение администраторов ресурсов, которые могут изменять права доступа других пользователей к определенным каталогам и файлам на локальных дисках. Администратором ресурса считается пользователь, для которого установлено разрешение на операцию "Изменение прав доступа" в параметрах доступа к ресурсу.
3. Настройка регистрации событий и аудита операций с ресурсами – для отслеживания произошедших событий, связанных с работой механизма.

В Secret Net Studio действуют следующие ограничения на использование дискреционного разграничения доступа к каталогам:

- невозможно управление параметрами дискреционного доступа для корневого каталога жесткого диска;
- не применяйте параметры дискреционного разграничения доступа непосредственно на общедоступный каталог. Используйте для этого вложенные подпапки. Например, если требуется разграничить доступ пользователей к сетевым папкам на файловом сервере, создайте общедоступный каталог (например, "users"), в котором создайте для пользователей подпапки (например, "Иванов", "Петров" и т.д.) и назначьте им требуемые параметры дискреционного разграничения доступа.

Затирание данных

Первоначальное описание и принципы применения этого механизма на дисках и в оперативной памяти были приведены в главе 1 (см. раздел "Механизмы защиты Secret Net Studio и принципы их работы / Затирание удаляемой информации"). Здесь мы приводим дополнительные сведения о затирании данных при удалении файлов.

Стандартные средства ОС не обеспечивают физического удаления информации при выполнении операций удаления файлов на дисках. Поэтому информация, содержавшаяся в удаленных файлах, может быть восстановлена с использованием специально предназначенных для этого средств. При действии механизма затирания записывается последовательность случайных чисел в область диска, где физически было расположено содержимое удаленного файла.

Для усиления степени защиты запись может быть осуществлена несколько раз подряд (несколько проходов затирания). На практике заведомо достаточно двух проходов затирания данных.

Затирание данных выполняется автоматически при удалении файла с диска или при удалении объекта из оперативной памяти.

В контекстное меню выбранных в Проводнике Windows объектов (файлов или каталогов) добавлена команда "Удалить безвозвратно", которая обеспечивает затирание удаляемых данных. Кроме того, реализовано затирание имен удаляемых файлов и каталогов.

Шифрование данных в криптоконтейнерах

Предоставляемые этим механизмом возможности были описаны в главе 1 (см. соответствующий подраздел в разделе "Механизмы защиты Secret Net Studio и принципы их работы"). Здесь приводятся некоторые особенности его настройки.

В механизме шифрования данных в криптоконтейнерах создание криптоконтейнеров доступно пользователям, которым предоставлена привилегия "Создание криптоконтейнера" и выдан криптографический ключ. По умолчанию данной привилегией обладают пользователи, входящие в группу локальных администраторов и в группу "Пользователи".

Для работы с зашифрованными данными в криптоконтейнерах пользователям необходимо загружать криптографические ключи (ключевую информацию) со своих ключевых носителей. Ключевая информация может храниться в присвоенном пользователю персональном идентификаторе или сменном носителе.

Настройка шифрования выполняется в программе управления в централизованном либо в локальном режиме.

Администратор может настраивать следующие параметры смены ключей, сгенерированных средствами системы Secret Net Studio:

- максимальный срок действия;
- минимальный срок действия;
- время предупреждения об истечении срока действия ключа.

Действие этих параметров распространяется на всех пользователей. По истечении максимального срока действия ключевая информация пользователя становится недействительной. В этом случае пользователь должен сменить ключевую информацию. Смена ключевой информации самим пользователем возможна только по истечении минимального срока действия ключа.

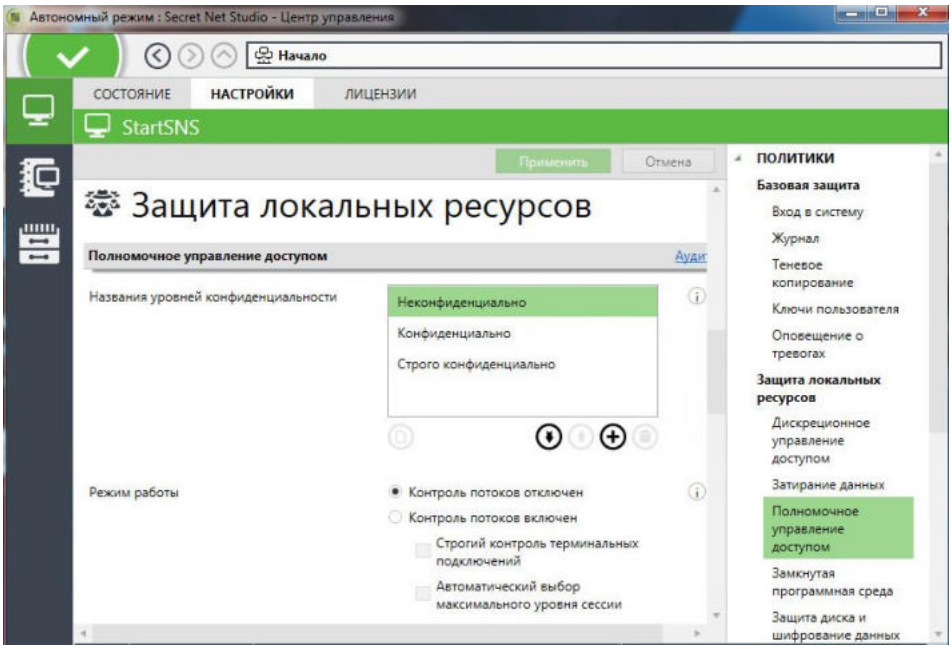
Подробнее о механизме шифрования криптоконтейнеров см. в руководстве администратора по настройке и эксплуатации локальной защиты.

Лабораторная работа №1 "Настройка полномочного управления доступом"

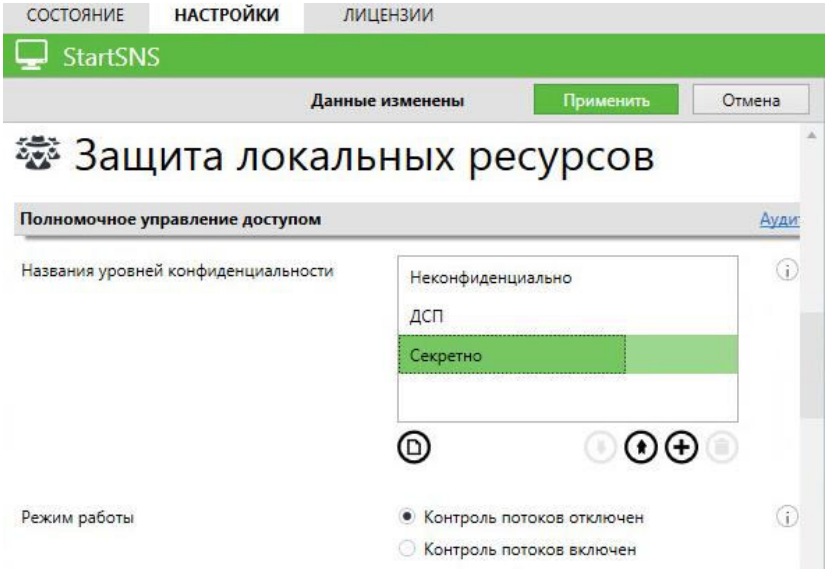
В данной лабораторной работе, следуя порядку настройки механизма полномочного управления доступом, который был описан в соответствующем разделе главы 3, показывается, как система защиты выполняет проверку соответствия уровня допуска пользователя и категории конфиденциальности объекта доступа (каталога или файла).

1. Откройте консоль BM StartSNS и авторизуйтесь под учетной записью "adminsns". Запустите "Локальный центр управления" и раскройте в панель "Компьютер"  .
2. Для первоначальной настройки механизма полномочного управления доступом задайте следующие категории конфиденциальности: "Неконфиденциально", "ДСП" (для служебного пользования), "Секретно". Для этого в

программе управления перейдите на вкладку "Настройки", в разделе "Политики" правой части окна раскройте группу "Защита локальных ресурсов / Полномочное управление доступом" и выполните следующие действия:

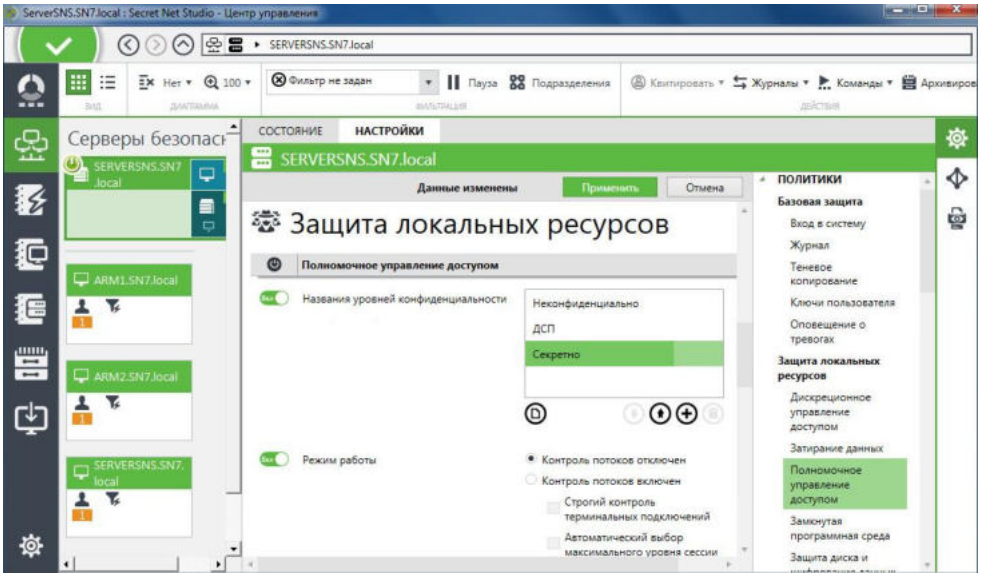


- используя кнопки  , ознакомьтесь с информацией о настройках "Названия уровней конфиденциальности" и "Режим работы". Обратите внимание, что первые три уровня можно только переименовать;
- в поле "Названия уровней конфиденциальности" выберите значение "Конфиденциально" и с помощью клавиши [F2] переименуйте его в "ДСП" (для переименования можно также использовать двойной щелчок);
- аналогично переименуйте "Строго конфиденциально" в "Секретно";
- убедитесь, что в поле "Режим работы" выбран переключатель "Контроль потоков отключен";

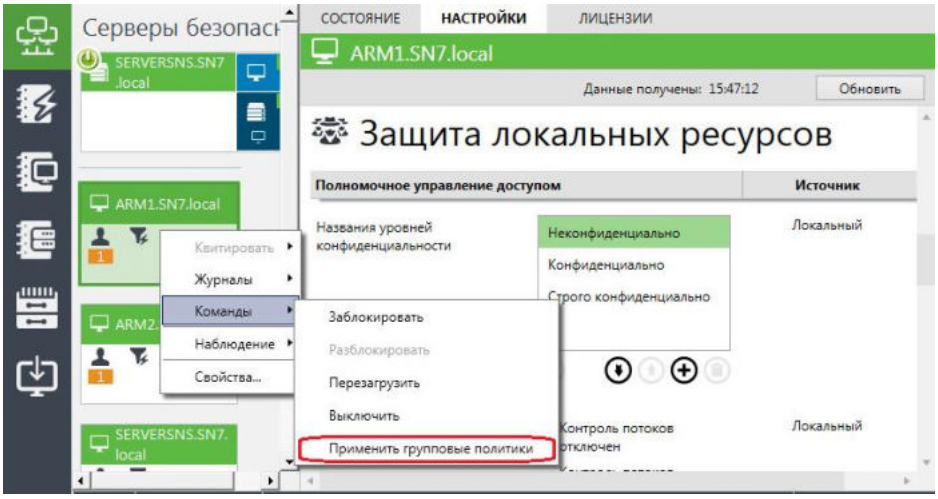


- на вкладке "Настройки" нажмите кнопку "Применить"  и просмотрите появившуюся запись в панели событий системы.

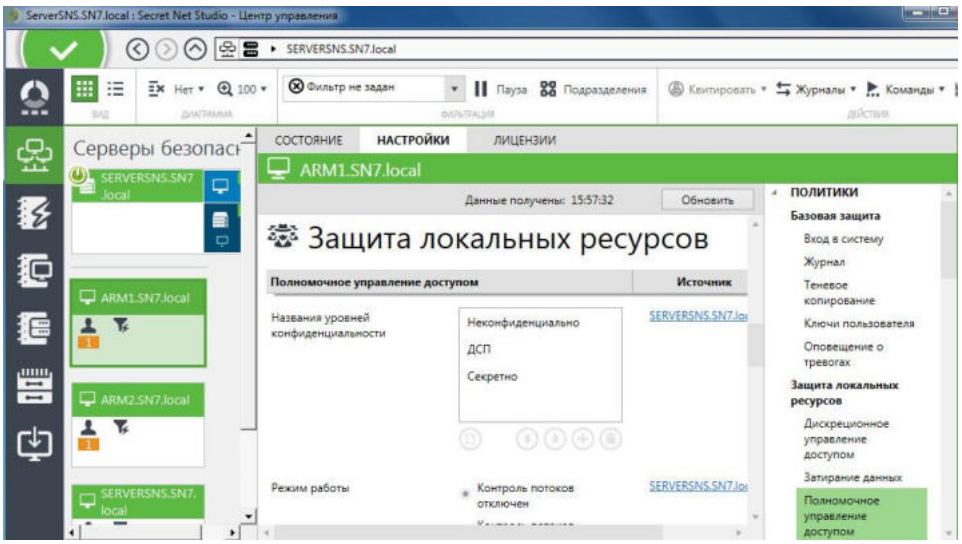
3. Используя описание предыдущего пункта, выполните с рабочего места ARM2 под учетной записью "dadminsns1" аналогичную первоначальную настройку механизма полномочного управления доступом в сетевом варианте для групповых политик сервера подключения ServerSNS.



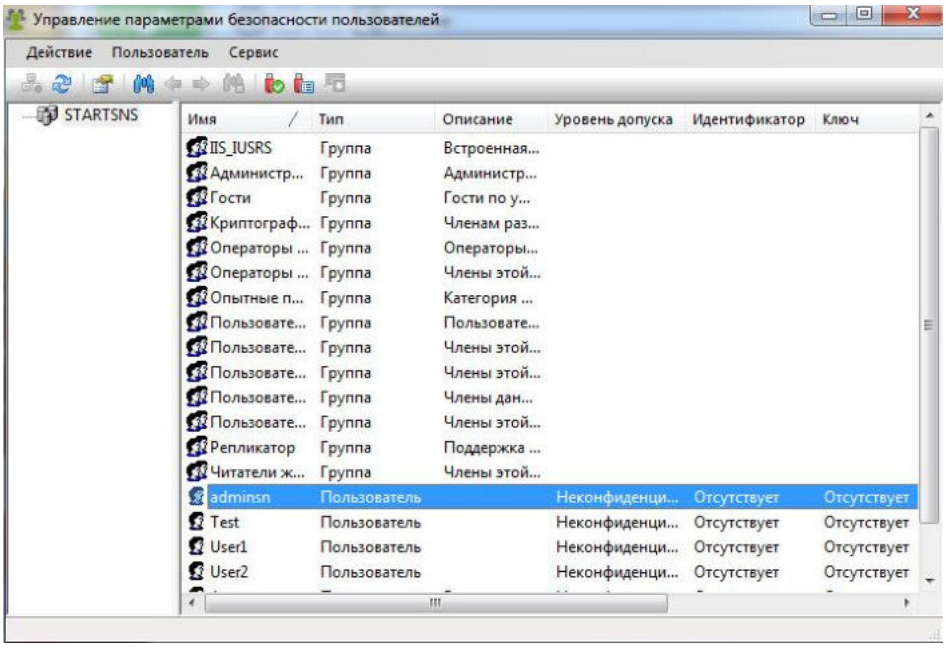
4. Принудительно примените измененные групповые политики для компьютеров ARM1, ARM2 с помощью опции контекстного меню "Команды / Применить групповые политики". Обратите внимание на сообщение в панели событий об успешном применении групповых политик.



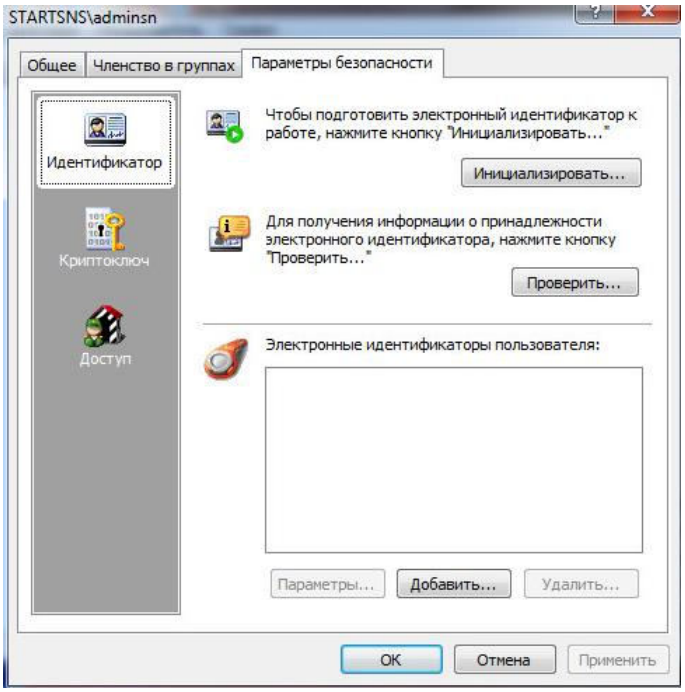
5. Убедитесь, что настроенные групповые политики уровней полномочного управления доступом теперь действуют на защищаемых компьютерах ARM1 и ARM2. Для этого последовательно просмотрите настройки группы политик "Политики / Защита локальных ресурсов / Полномочное управление доступом" каждого из этих компьютеров.



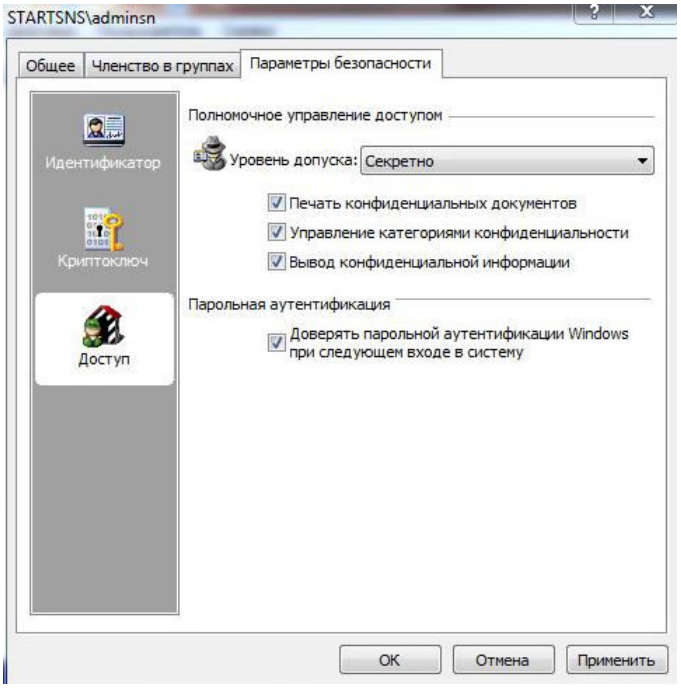
6. Назначьте уровни допуска и привилегии пользователей на компьютере StartSNS. Для этого перейдите в консоль его ВМ и убедитесь, что вы авторизованы под учетной записью "adminsns". Запустите программу "Управление пользователями": "Пуск / Все программы / Код безопасности / Secret Net Studio / Управление пользователями" и выполните следующие действия:



- откройте окно свойств учетной записи администратора "adminsns" и в открывшемся окне перейдите на вкладку "Параметры безопасности";

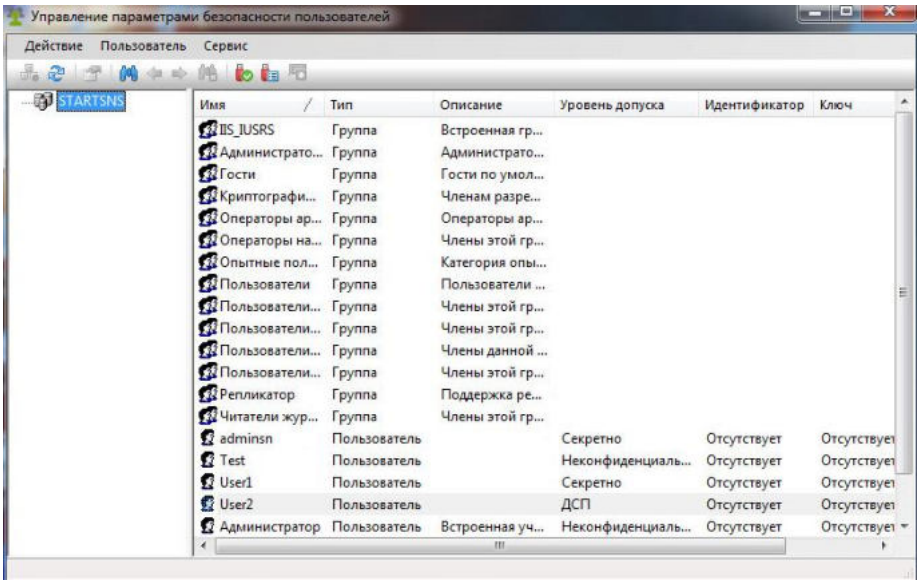


- на вкладке "Параметры безопасности" выберите категорию настроек "Доступ", установите для администратора "adminsns" самый высокий уровень допуска "Секретно", включите все привилегии и нажмите кнопку "ОК";



- аналогично – для пользователей "user1" и "user2" на ВМ StartSNS назначьте уровни доступа согласно таблице и установите все привилегии.

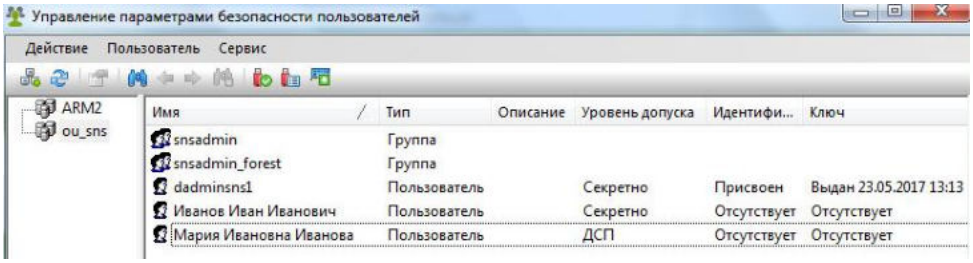
Пользователь	Полное имя	Пароль	Уровень допуска
User1	Иван Иванович Иванов	P@ssw0rd	Секретно
User2	Мария Ивановна Иванова	P@ssw0rd	ДСП



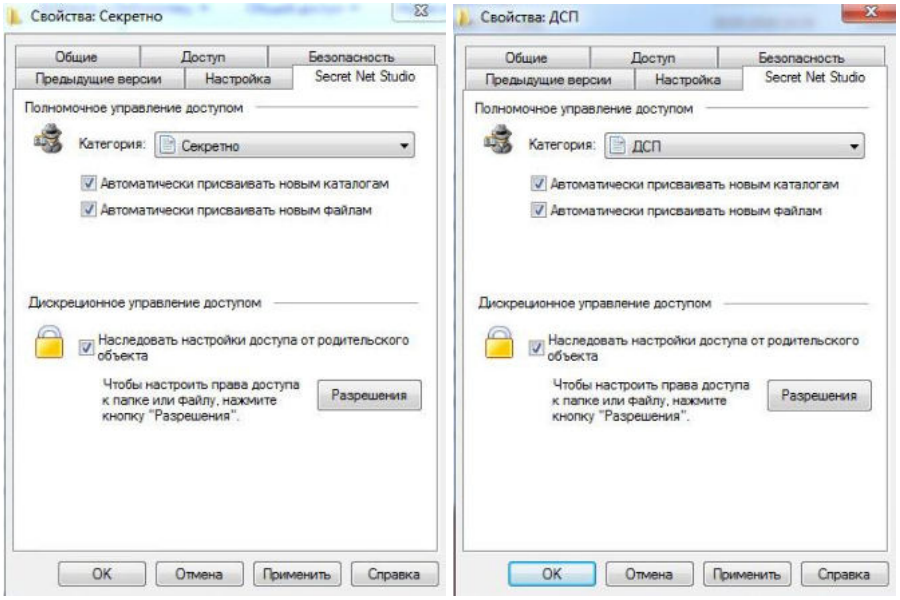
Примечание. Назначенные уровни допуска и привилегии вступят в силу при следующем входе пользователя в систему.

7. Используя описание п. 6, выполните аналогичную настройку уровней доступа и привилегий в сетевом варианте программы "Управление пользователями" с рабочего места ARM2 под учетной записью "dadminsns1" согласно таблице.

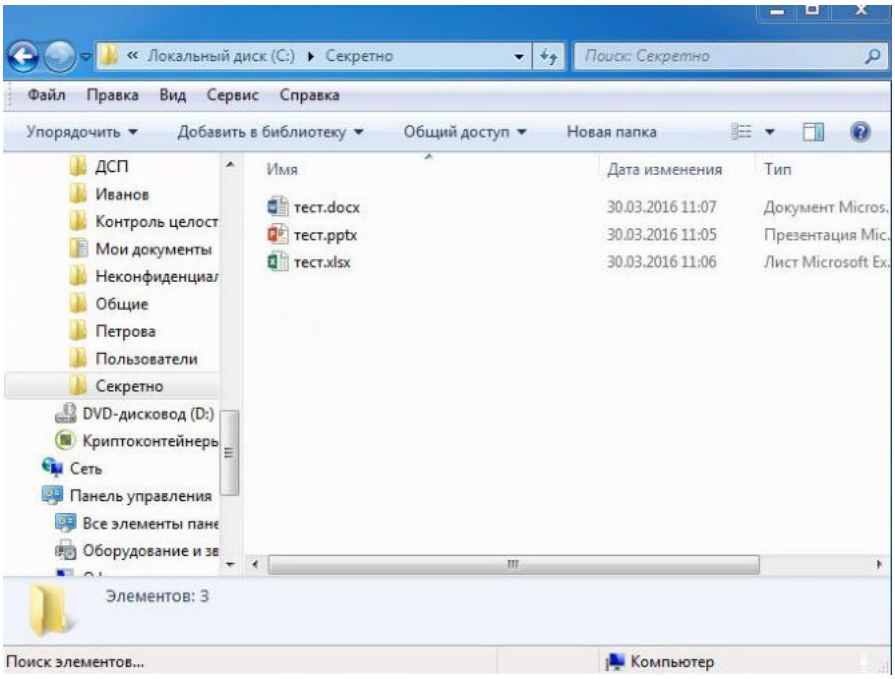
Пользователь	Полное имя	Пароль	Уровень допуска
dadminsns1	dadminsns1	P@ssw0rd	Секретно
User1	Иван Иванович Иванов	P@ssw0rd	Секретно
User2	Мария Ивановна Иванова	P@ssw0rd	ДСП

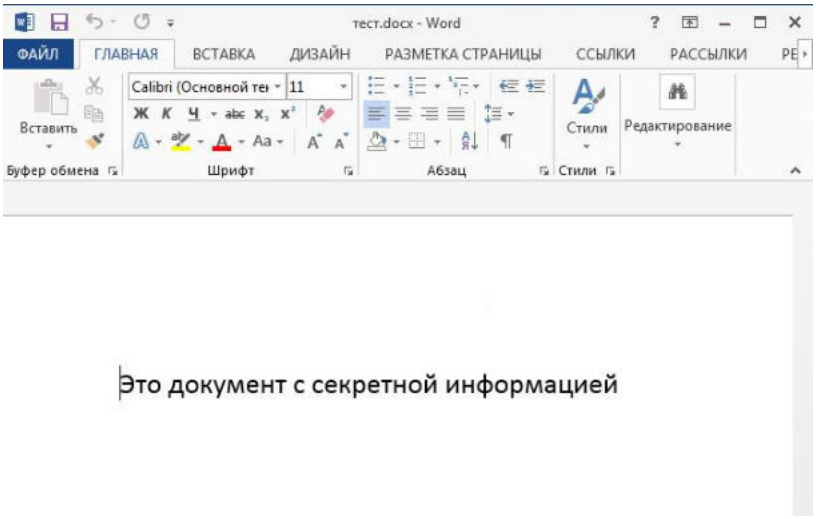


8. В консоли ВМ компьютера StartSNS переавторизуйтесь под учетной записью "adminsns", чтобы назначенный ранее уровень допуска и привилегии вступили в силу, и создайте на диске "C:" папки: "Секретно", "ДСП" и "Неконфиденциально". Выберите для каждой из них в соответствии с названием категорию конфиденциальности.



9. В папке "C:\Секретно" создайте документы форматов Microsoft Word, Microsoft PowerPoint и Microsoft Excel с произвольным содержанием: "тест.docx", "тест.pptx" и "тест.xlsx" соответственно.

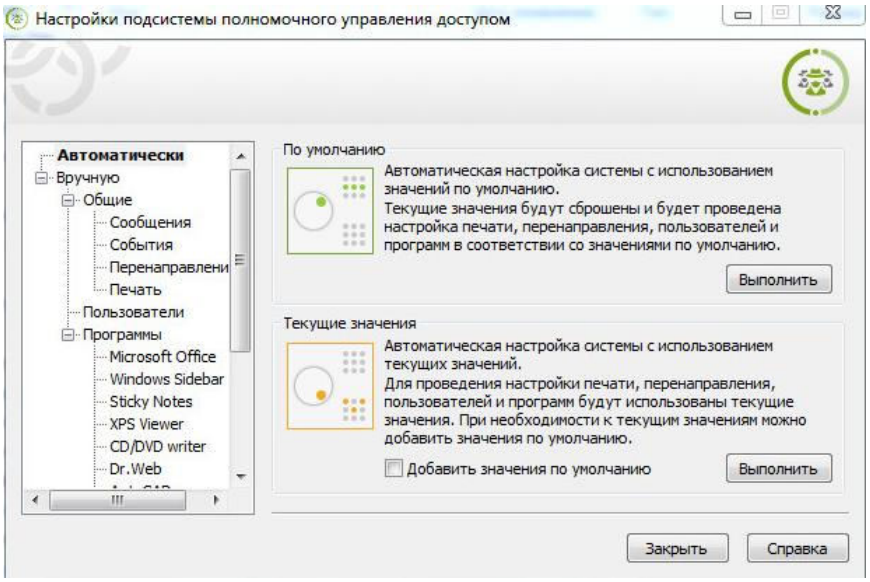




10. Аналогично – в папке "C:\ДСП" создайте документы "тест1.docx", "тест1.pptx" и "тест1.xlsx".

11. Чтобы обеспечить функционирование механизма полномочного управления доступом при включенном режиме контроля потоков, проведите дополнительную настройку локально на компьютере. Подобная настройка должна выполняться перед включением режима контроля потоков, а также в процессе эксплуатации системы при добавлении новых пользователей, программ, принтеров для оптимизации функционирования механизма.

В окне ВМ StartSNS загрузите программу настройки подсистемы полномочного управления доступом: "Пуск / Все программы / Код безопасности / Secret Net Studio / Программа настройки подсистемы полномочного управления доступом".



12. В программе "Настройка подсистемы полномочного управления доступом" реализованы средства как для автоматической настройки, так и для конфигурирования вручную. При автоматической настройке выполняется базовый набор действий, после которых обеспечивается функционирование механизма и совместимость со стандартным и наиболее распространенным программным обеспечением.

Автоматическая настройка со значениями по умолчанию применяется в случае необходимости удалить текущую конфигурацию и вернуть исходные значения параметров. Это может потребоваться, если значения параметров некорректно заданы или удалены, а также при первичной настройке системы с минимально необходимой конфигурацией для функционирования механизма в режиме контроля потоков.

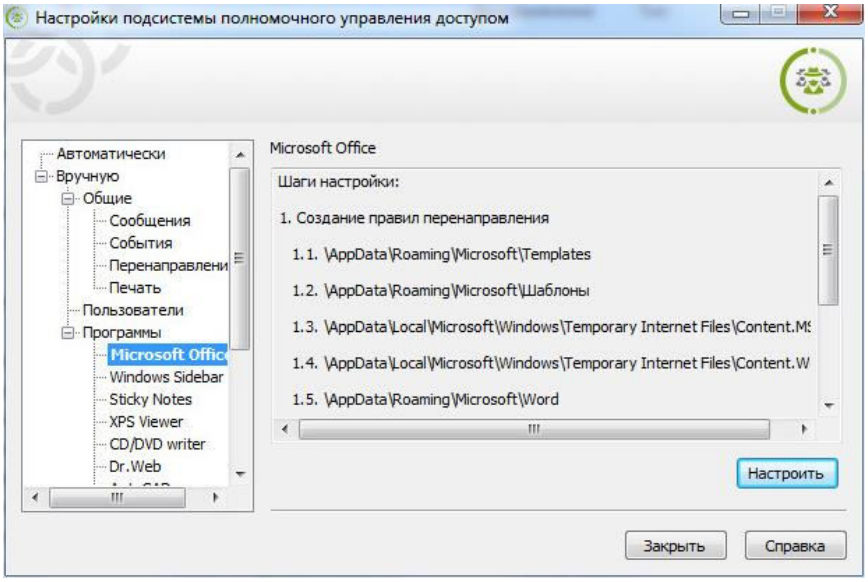
Вариант настройки "Текущие значения" предназначен для повторного применения в системе заданных значений параметров. Это позволяет восстановить настройку системы при сбоях функционирования механизма или при добавлении в систему новых пользователей, программ, принтеров и других объектов, задействованных в механизме полномочного управления доступом и контроля печати. При такой настройке дополнительно к текущим значениям параметров можно добавить исходные значения (значения по умолчанию). При этом текущие значения не удаляются.

Ручная настройка предусмотрена для выполнения специфических действий, например, для обеспечения совместной работы с ПО, которое не входит в список для автоматической настройки. Можно вручную изменять параметры работы механизма полномочного управления доступом и контроля печати, что позволяет обеспечить функционирование с учетом особенностей программной среды компьютера и предпочтений пользователя.

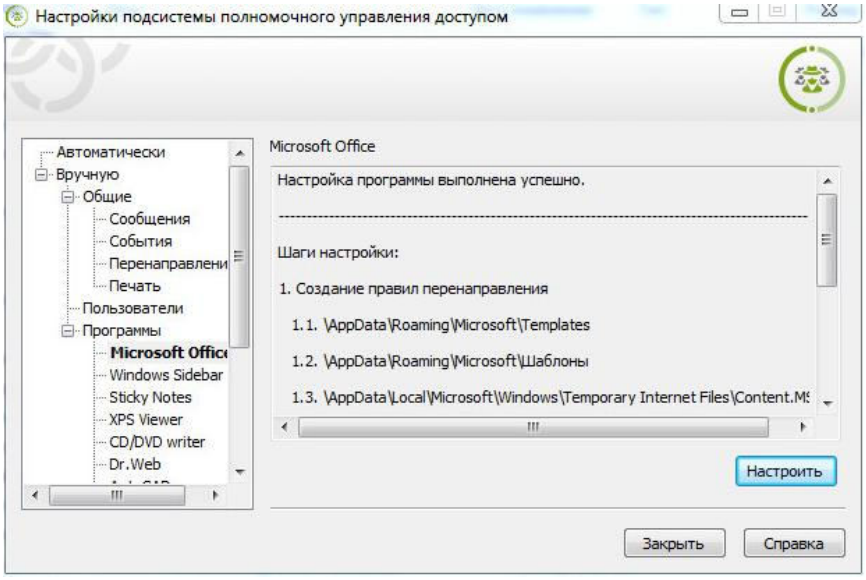
Средства для ручной настройки параметров представлены в следующих основных разделах:

- "Общие" – для настройки общих параметров работы пользователей и приложений;
- "Пользователи" – для настройки параметров, относящихся к профилям пользователей;
- "Программы" – для настройки параметров для приложений.

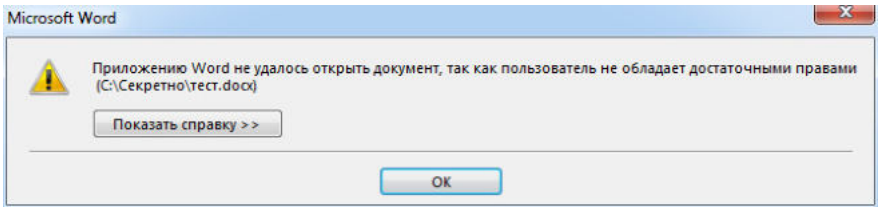
Запустите настройку для программ Microsoft Office. Для этого в разделе настроек выберите "Вручную / Программы / Microsoft Office" и нажмите кнопку "Настроить".



13. Программа проведет настройку перенаправления файлов. Дождитесь завершения этого процесса. После создания правил перенаправления появится окно с информацией об успешном проведении настройки.



14. В окне "Настройка подсистемы полномочного управления доступом" нажмите кнопку "Закрыть". Перезагрузите ОС на ВМ StartSNS и авторизуйтесь под учетной записью "user2 – Иванова Мария Ивановна" с уровнем допуска "ДСП".
15. Сделайте попытку открытия любого файла из папки "C:\Секретно". Поскольку уровень допуска пользователя "user2" ниже, чем уровень конфиденциальности каталога "Секретно" и его содержимого, механизм полномочного управления доступом Secret Net Studio не позволит открыть документ и система выдаст соответствующее сообщение.



16. Переавторизуйтесь на ВМ компьютера StartSNS под учетной записью пользователя "user1 – Иванов Иван Иванович", сделайте аналогичную попытку открытия любого файла из папки "C:\Секретно" и сравните результат.
17. Проведите проверку работы полномочного управления доступом в сетевом варианте. Для этого:
    - переавторизуйтесь на ВМ ServerSNS под учетной записью "dadminsns1" и создайте на диске "C:" общедоступную папку "user_files" с максимальными разрешениями (permissions) на уровне ОС Windows;
    - в папке "user_files" создайте подпапки "Секретно" и "ДСП". Используя описание пп. 8–10, установите для них соответствующий уровень допуска и создайте в них файлы формата .rtf с произвольным содержанием;
    - на ВМ компьютеров ARM1 и ARM2 последовательно переавторизуйтесь под учетной записью "dadminsns1" и, используя описание пп. 11–14, проведите на них локально настройку полномочного управления доступом;
    - на ВМ ARM1 последовательно переавторизуйтесь под учетными записями "user2" и "user1", попробуйте открыть с помощью Microsoft Word файлы из общедоступных папок "user_files\Секретно" и "user_files\ДСП" с компьютера ServerSNS и сравните результат.

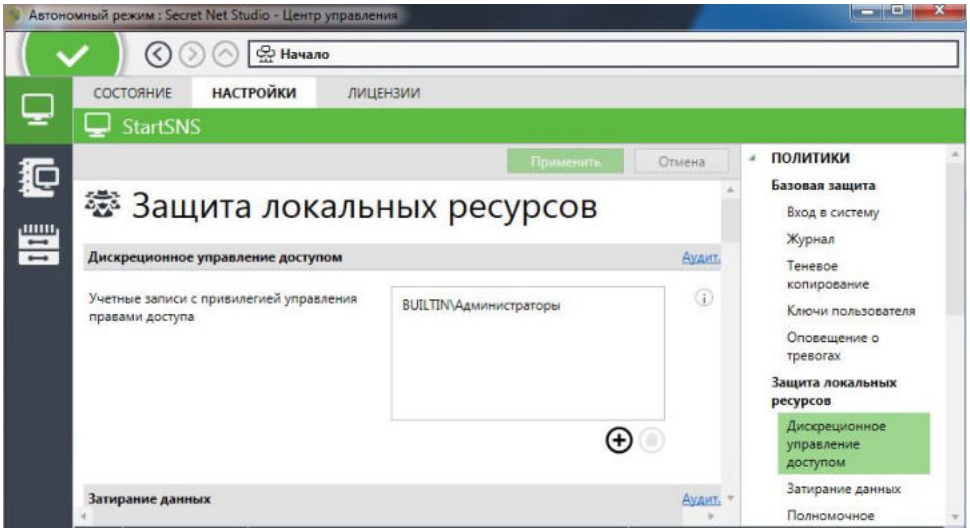
Выполнение лабораторной работы завершено.

Лабораторная работа №2 "Настройка механизма дискреционного управления доступом"

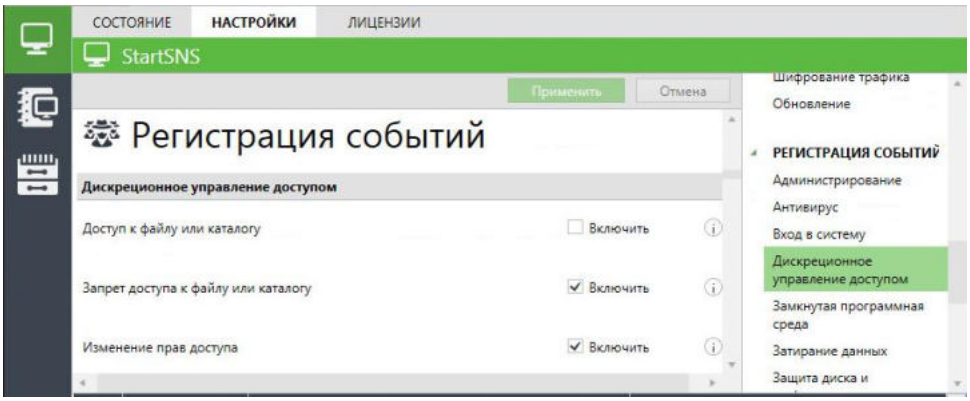
В этой лабораторной работе тестируется работа механизма дискреционного управления доступом на примере текстовых файлов. Действия администратора,

которые следует выполнить при настройке данного инструмента защиты, были описаны в соответствующем разделе главы 3.

1. Переавторизуйтесь на ВМ StartSNS под учетной записью администратора "adminsns".
2. На диске "C:" создайте следующие защищаемые ресурсы:
   - папку "Иванов" и в ней файл произвольного содержания "Доклад.txt";
   - папку "Иванова" и в ней файл произвольного содержания "График.txt";
   - папку "Общие" и в ней файл произвольного содержания "План.txt".
3. Убедитесь, что администратору предоставлены привилегии для изменения прав доступа на любых ресурсах, а также настроена регистрация событий, связанных с доступом к ресурсам. Для этого:
   - загрузите программу "Локальный центр управления", в панели "Компьютер" выберите вкладку "Настройки" и откройте раздел политик "Политики / Защита локальных ресурсов / Дискреционное управление доступом";



   - убедитесь, что в параметре "Учетные записи с привилегией управления правами доступа" выбрана по умолчанию группа локальных администраторов, и с помощью кнопки ⓘ ознакомьтесь с описанием этой настройки. Обратите внимание, что при необходимости, используя кнопку "Добавить" ⊕, можно установить привилегию управления правами доступа для ресурсов другому пользователю или группе пользователей;
   - нажмите кнопку-ссылку "Аудит..." – вы перейдете в раздел настроек "Регистрация событий / Дискреционное управление доступом";



   - с помощью кнопки ⓘ ознакомьтесь с описанием событий. Обратите внимание, что в целях минимизации размера журнала событий факт доступа к файлу или каталогу не регистрируется.

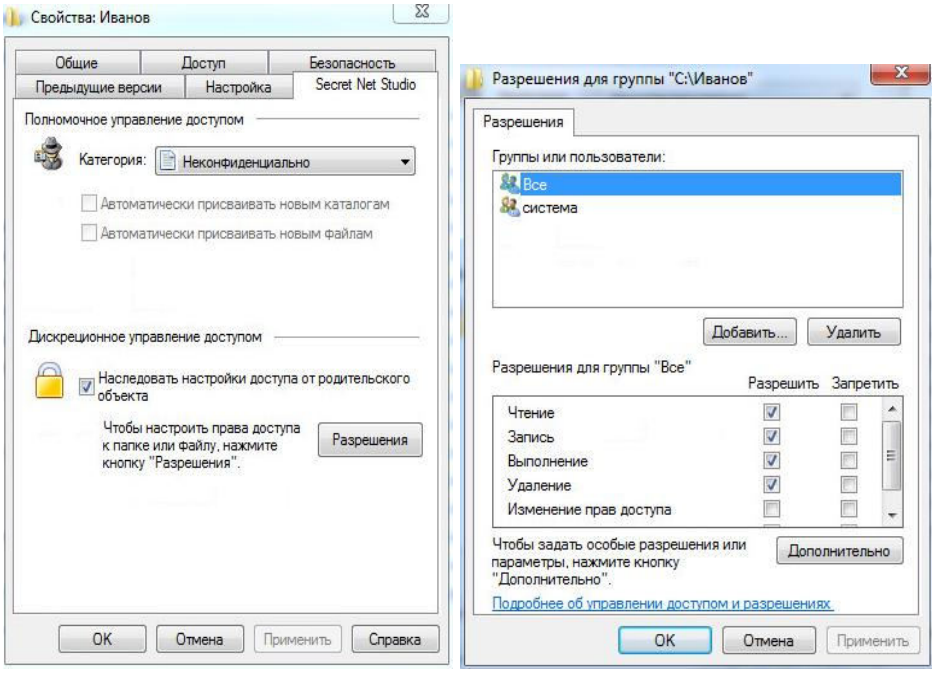
4. Установите права дискреционного доступа для пользователей "user1" и "user2" в соответствии с матрицей доступа, приведенной в таблице.

Пользователи	**Документы**		
	C:\Иванов\ Доклад.txt	**C:\Иванова\ График.txt**	**C:\Общие\ План.txt**
User1	rx	r	Полный доступ
User2	-	rwx	r

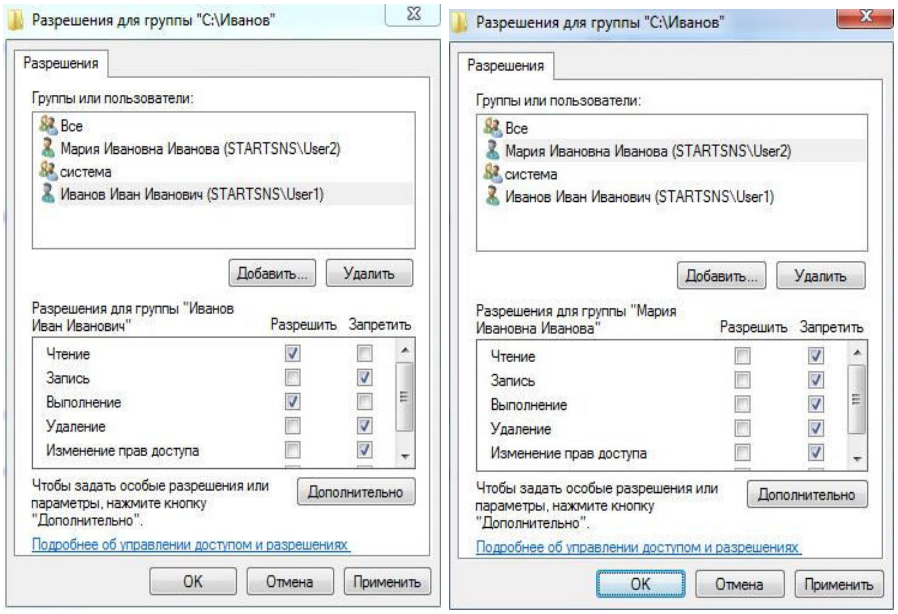
Где r – чтение, w – запись/изменение, d – удаление, x – выполнение.

Для установки прав дискреционного доступа сделайте следующее:

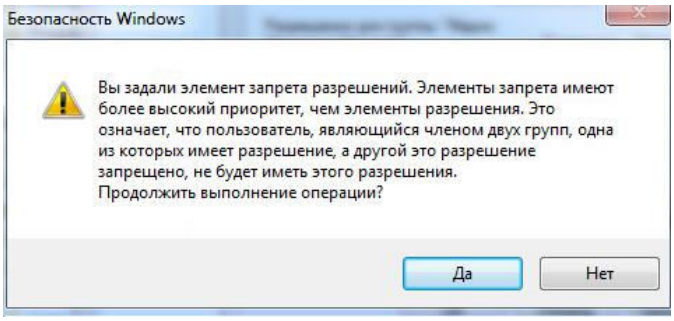
- откройте диалоговое окно "Свойства" для папки, например, "C:\Иванов", и перейдите на вкладку Secret Net Studio. В разделе "Дискреционное управление доступом" снимите галочку в поле "Наследовать…". Откроется диалоговое окно "Разрешения для группы…";



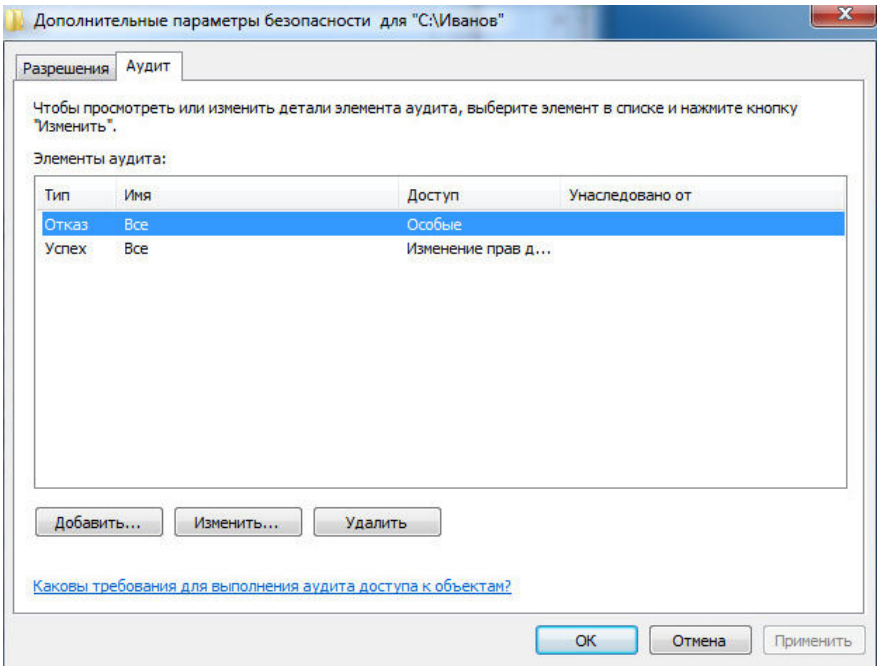
- используя кнопку "Добавить", добавьте пользователей "user1" и "user2" и установите им права доступа в соответствии с таблицей;



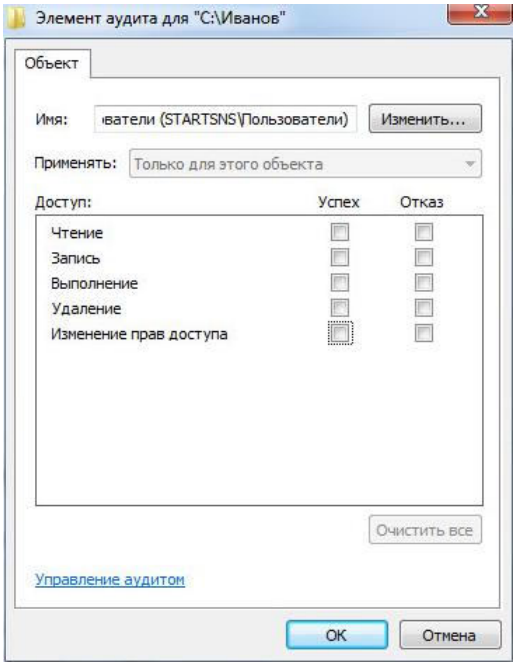
- нажмите кнопку "Применить". Поскольку "user1" и "user2" являются членами группы пользователей компьютера, появится сообщение Windows, предупреждающее, что заданная политика запрета приоритетна. Нажмите кнопку "Да". Доступ для папки "C:\Иванов" задан.



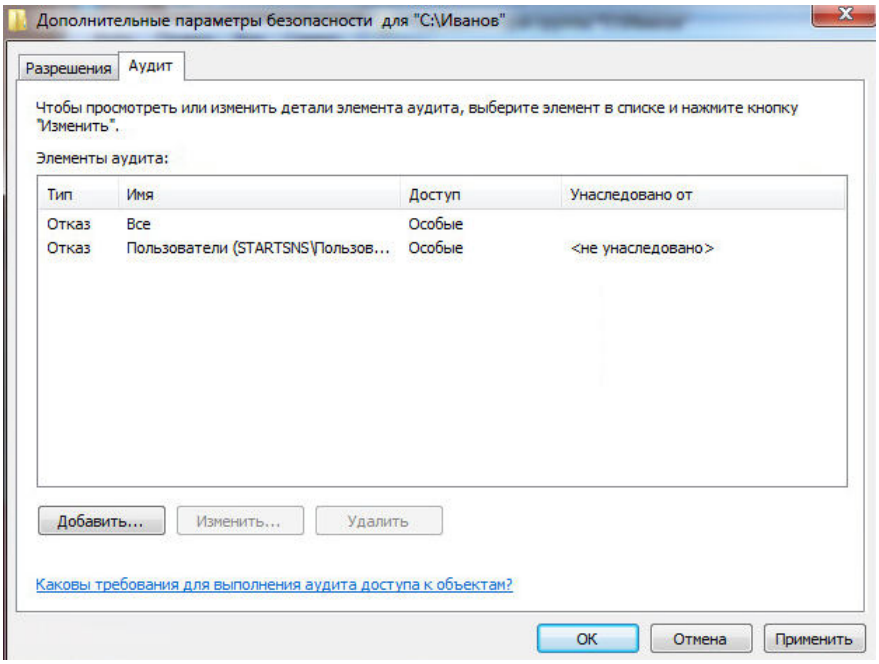
5. Настройте аудит для папки "Иванов" таким образом, чтобы регистрировались только события отказов в доступе. Для этого в окне "Разрешения для группы …" нажмите кнопку "Дополнительно". В открывшемся окне "Дополнительные параметры безопасности…" перейдите на вкладку "Аудит" и сделайте следующее:



- удалите аудит успеха, выбрав в таблице "Элементы аудита" запись "Успех" и нажав кнопку "Удалить";
- добавьте аудит отказа для группы "Пользователи". Для этого нажмите кнопку "Добавить", выберите группу "Пользователи" и нажмите кнопку "ОК". Откроется следующее диалоговое окно "Элементы аудита для…";



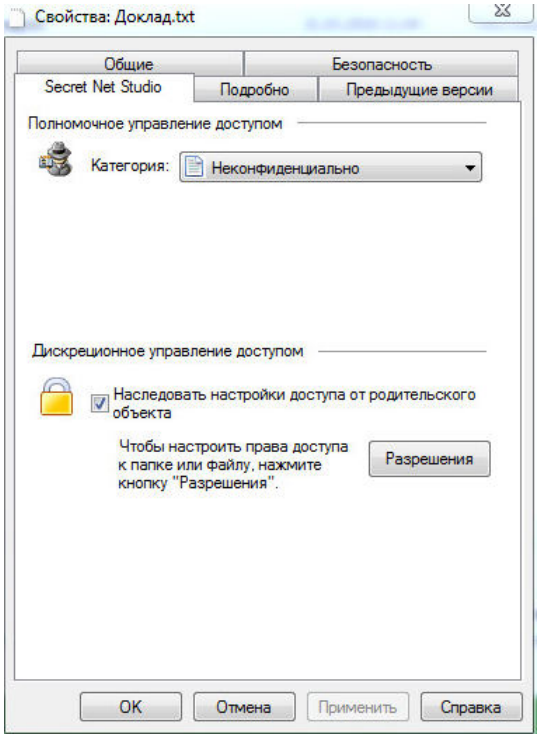
- в колонке "Отказ" установите флажки для всех действий и нажмите кнопку "ОК". Вы вернулись в окно "Дополнительные параметры безопасности...";



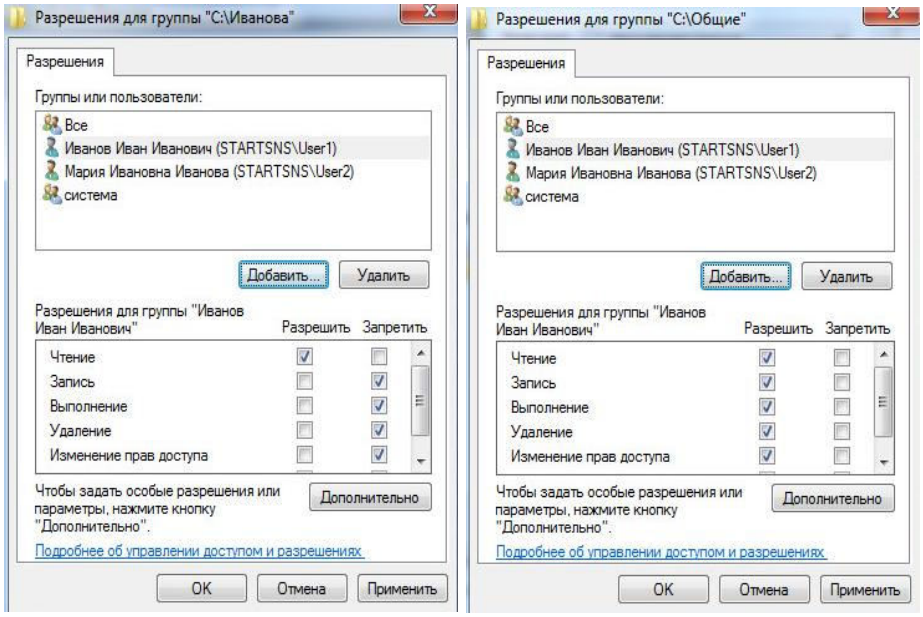
- аудит для папки "Иванов" настроен. Нажмите кнопку "ОК".

6. В окне "Разрешения для группы..." нажмите кнопку "ОК". В окне свойств папки также нажмите кнопку "ОК".

7. Таким образом, мы установили параметры доступа к папке "C:\Иванов" и аудит событий в соответствии с таблицей из п. 4. Откройте папку "C:\Иванов", вызовите окно свойств файла "Доклад.txt", перейдите на вкладку "Secret Net Studio" и убедитесь, что установлен параметр "Наследовать настройки доступа от родительского объекта".

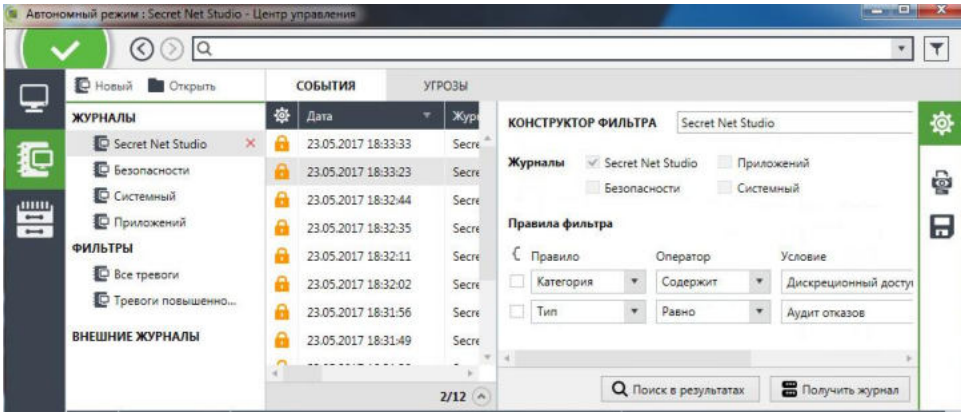


8. Используя описание пп. 4–7, установите в соответствии с матрицей разграничения доступа права доступа и настройку аудита событий для папок "Иванова" и "Общие".



9. На компьютере StartSNS завершите работу локальной программы управления и переавторизуйтесь под учетной записью "user1". Убедитесь, что пользователю "user1", согласно таблице в п. 4, доступны следующие действия с ресурсами: "C:\Иванова\График.txt" – чтение, "C:\Иванов\Доклад.txt" – чтение и выполнение и "C:\Общие\План.txt" – полный доступ.

Откройте журнал Secret Net Studio и просмотрите события категории "Дискреционный доступ" с типом "Аудит отказов" об отказе в выполнении не разрешенных в соответствии с матрицей доступа (см. п. 4) операций с ресурсами.

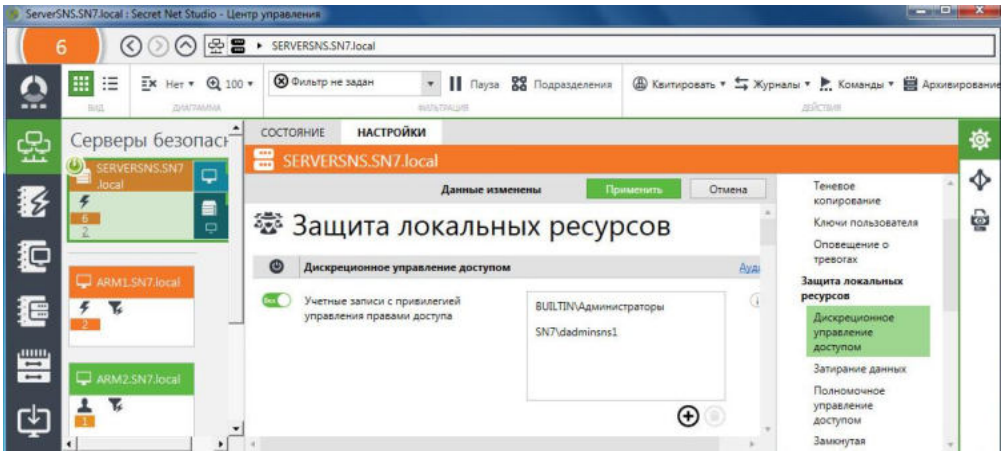


10. Переавторизуйтесь под учетной записью "user2". Убедитесь, что пользователю "user2", согласно таблице в п. 4, доступны следующие действия с ресурсами: "C:\Иванова\График.txt" – чтение, запись и выполнение; "C:\Иванов\Доклад.txt" – доступ запрещен и "C:\Общие\План.txt" – чтение.

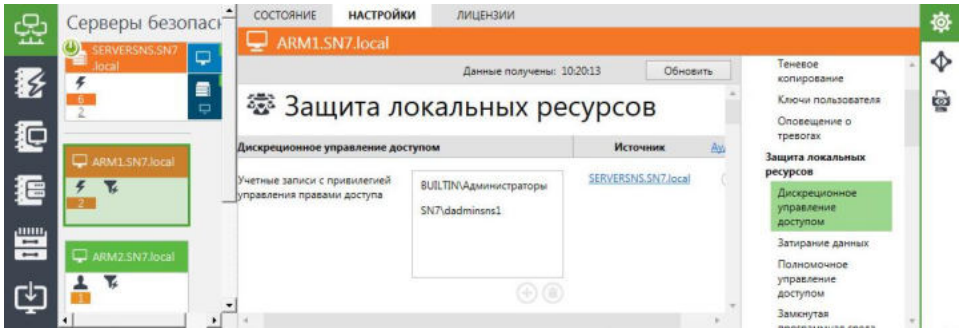
Откройте журнал Secret Net Studio и просмотрите события категории "Дискреционный доступ" об отказе в выполнении не разрешенных в соответствии с матрицей доступа (см. п. 4) операций с ресурсами.

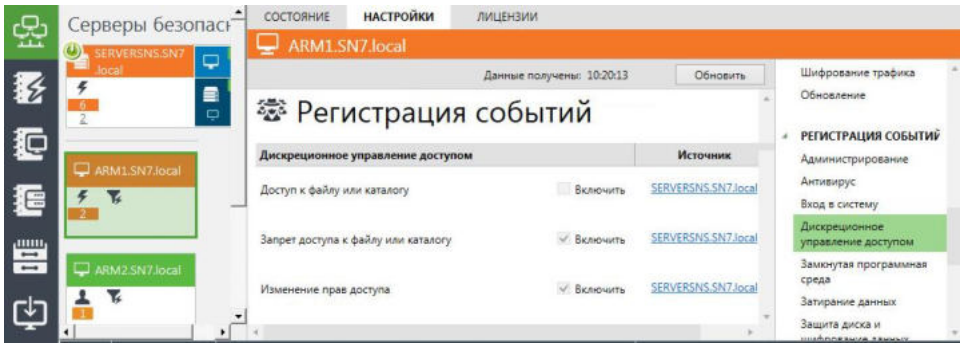
11. Проведите проверку работы дискреционного управления доступом в сетевом варианте. Для этого:

- на ВМ ARM2 откройте программу управления в сетевом режиме, выберите объект сервера безопасности и, используя описание п. 3, включите групповую политику дискреционного управления доступом, добавив привилегию на управление правами доступа группе администраторов домена безопасности "snsadmin", а также включите регистрацию событий дискреционного управления доступом;



- на защищаемых компьютерах ARM1 и ARM2 принудительно примените настроенные на сервере безопасности групповые политики с помощью опции контекстного меню "Команды / Применить групповые политики";





- на ВМ ServerSNS под учетной записью "dadminsns1" в общедоступной папке "C:\user_files" создайте защищаемые ресурсы по аналогии с описанием в п. 2:
  - папку "Иванов" и в ней файл произвольного содержания "Доклад.txt";
  - папку "Иванова" и в ней файл произвольного содержания "График.txt";
  - папку "Общие" и в ней файл произвольного содержания "План.txt".
- распределите для них права дискреционного доступа для пользователей "user1" и "user2" по аналогии с описанием в п. 4 соответственно матрице разграничения доступа;

Пользователи	**Документы**		
	C:\Иванов\ Доклад.txt	**C:\Иванова\ График.txt**	**C:\Общие\ План.txt**
User1	rwx	r	Полный доступ
User2	-	rwx	r

- настройте аудит событий по аналогии с описанием в пп. 4–8;
- на ВМ ARM1 последовательно переавторизуйтесь под учетными записями "user2" и "user1", сделайте попытку доступа к защищаемым ресурсам компьютера ServerSNS, которые вы создали на предыдущем шаге, и сравните результат;
- на ВМ ServerSNS в программе "Локальный центр управления" откройте журнал Secret Net Studio и просмотрите события категории "Дискреционный доступ" с типом "Аудит отказов".

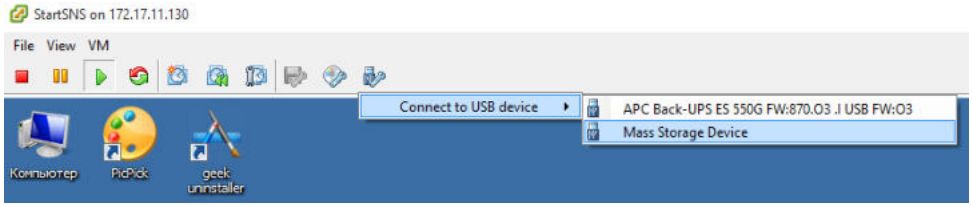
Выполнение лабораторной работы завершено.

Лабораторная работа №3 "Управление доступом к съемным носителям информации"

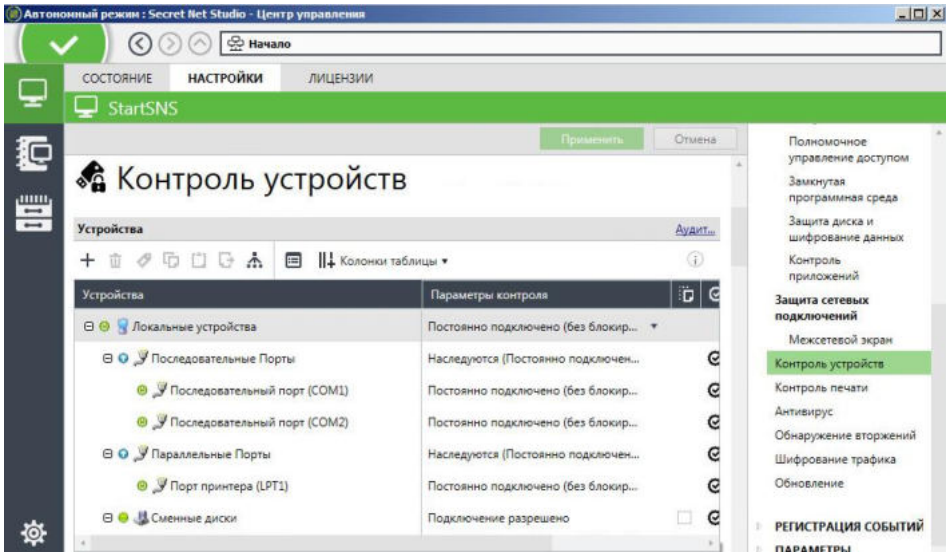
В данной лабораторной работе рассматривается работа механизма управления доступом к подключаемым USB-флеш-накопителям в рамках подсистемы контроля устройств, которая описана в соответствующем разделе главы 3.

Настройку политики контроля устройств можно выполнить либо индивидуально для каждого устройства, либо для модели, класса или группы устройств с использованием принципа наследования параметров.

1. На ВМ StartSNS авторизуйтесь под учетной записью администратора "adminsns".
2. Подключите к ВМ StartSNS USB-флеш-накопитель, который будет использоваться в лабораторной работе в рамках иллюстрации работы подсистемы контроля устройств.



3. Загрузите список устройств, просмотрите сведения о подключенном USB-флеш-накопителе и настройте политики его контроля. Для этого:
   - в программе "Локальный центр управления" на панели свойств компьютера выберите в разделе "Политики" группу "Контроль устройств" и прокрутите содержимое окна к таблице "Устройства";



   - просмотрите список устройств. Обратите внимание, что в него автоматически добавлены все обнаруженные устройства компьютера. Отключенные в данный момент устройства отображаются с зачеркнутыми именами. Для удобства просмотра списка и оперативного получения основных сведений о текущей конфигурации параметров устройств предусмотрены специальные значки статуса:

     – параметры контроля для устройства наследуются от вышестоящего элемента списка устройств;

     – режим контроля для устройства отключен;

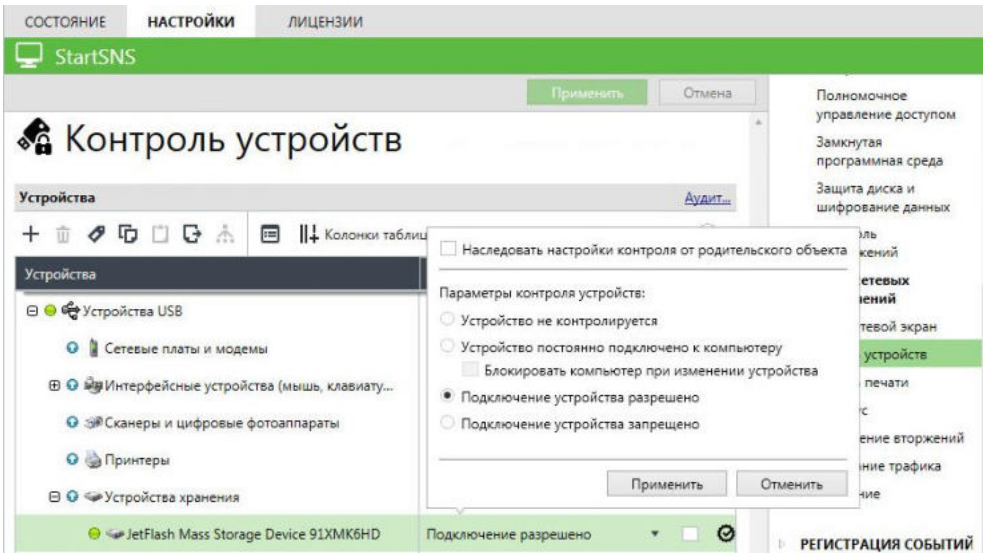
     – включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру;

     – включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать;

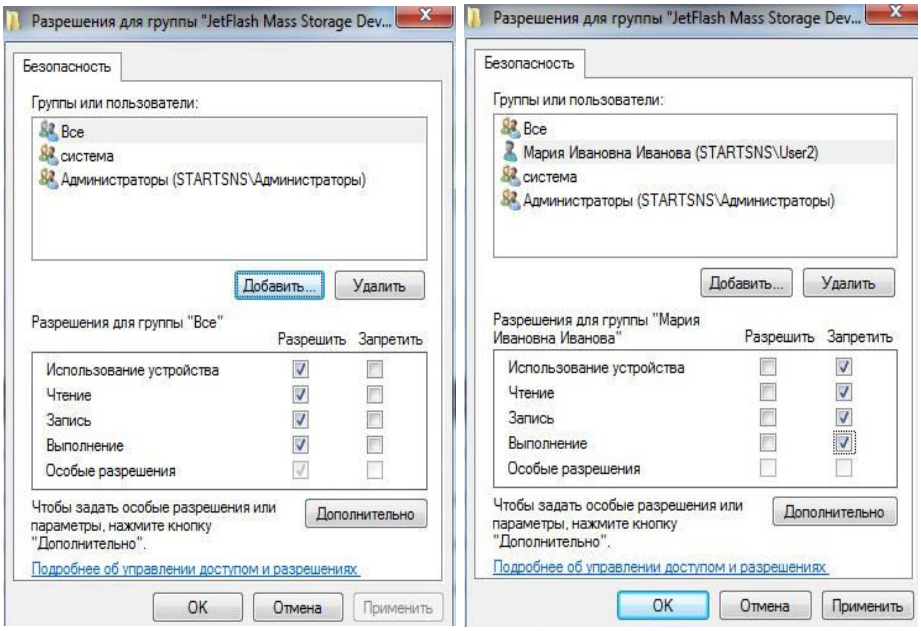
     – включен режим контроля, при котором устройство запрещается подключать к компьютеру;

   - в таблице "Устройства" выберите "Устройства USB / Устройства хранения / <подключенное устройство>" и раскройте поле "Параметры контроля". Убедитесь, что параметр "Подключение устройства разрешено" установлен, а "Наследовать настройки контроля от родительского объекта" – нет.

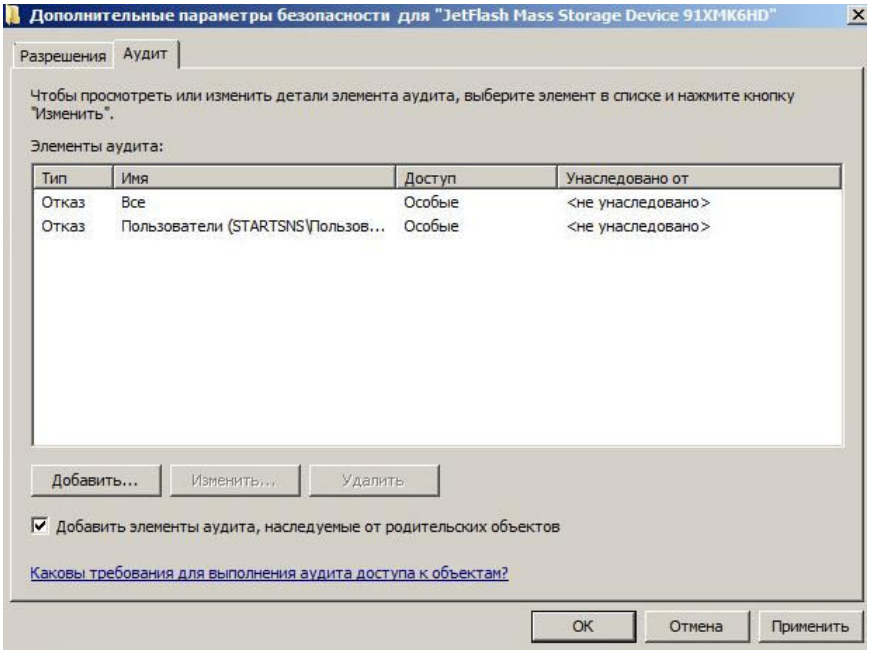
Текущее состояние устройства означает, что включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется. Данное состояние USB-флеш-накопителя нас устраивает;



- закройте поле "Параметры контроля" и справа от него нажмите кнопку "Разрешения" . Откроется диалоговое окно "Разрешения…", которое позволяет задавать параметры доступа к этому устройству. Следует иметь в виду, что настройка разрешений и запретов предусмотрена только для портов, дисков и носителей данных (для системного диска управление разрешениями запрещено);
- в список "Группы или пользователи" добавьте пользователя "user2" и установите ему запрет на работу с подключенным в данный момент (с именно этим) USB-флеш-накопителем;



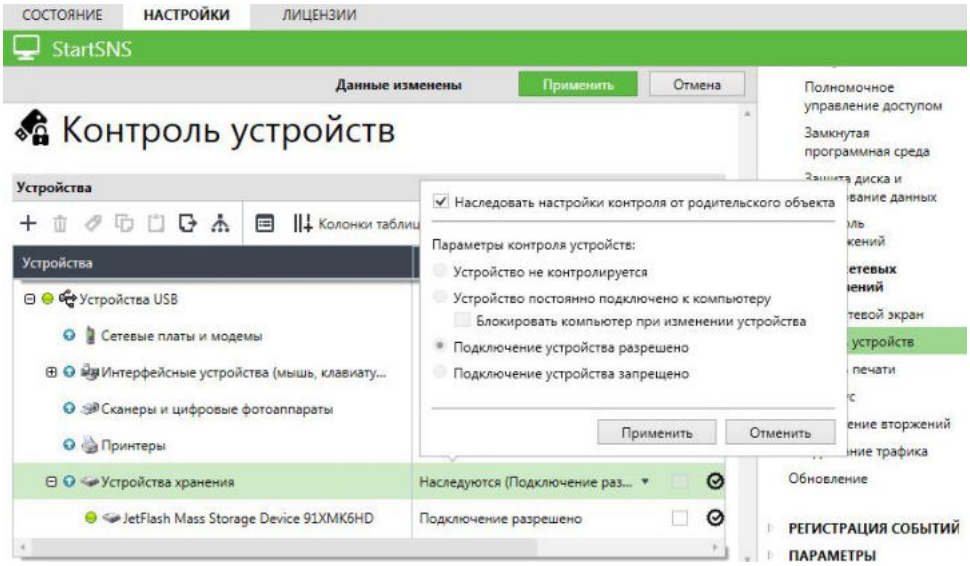
- проведите настройку аудита событий работы с устройством, установив только аудит отказов. Для этого в диалоговом окне "Разрешения…" нажмите кнопку "Дополнительно" и выполните действия, аналогичные описанным в п. 5 предыдущей лабораторной работы;



- политики контроля подключенного USB-флеш-накопителя настроены. Последовательно закройте диалоговые окна "Дополнительные параметры безопасности..." и "Разрешения..." и вернитесь в окно программы управления к перечню параметров "Контроль устройств".

4. Установите запрет всем пользователям на использование незарегистрированных USB-флеш-накопителей (всех, кроме подключенного в настоящий момент). Для этого:

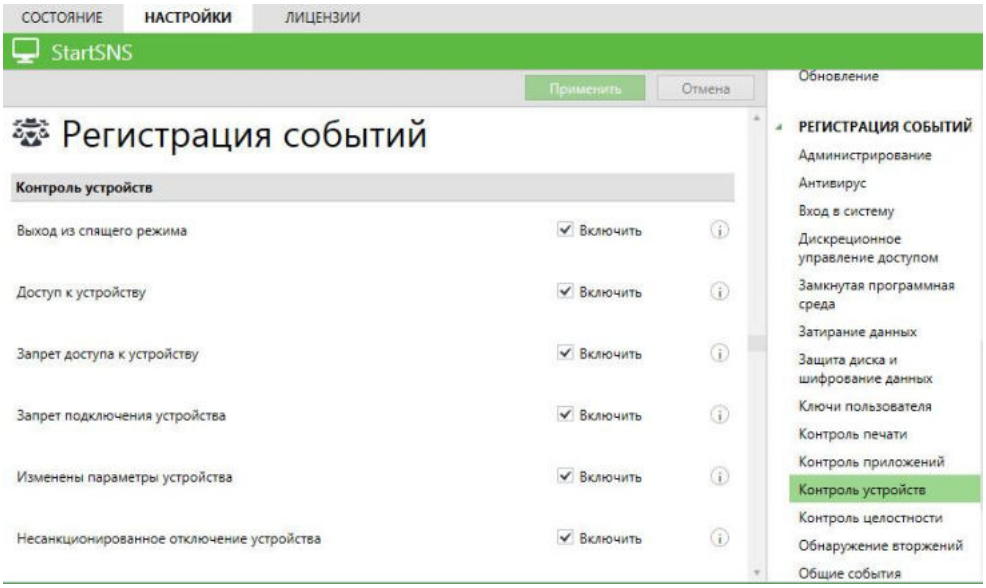
- в таблице "Устройства" выберите: "Устройства USB / Устройства хранения" и раскройте поле "Параметры контроля";



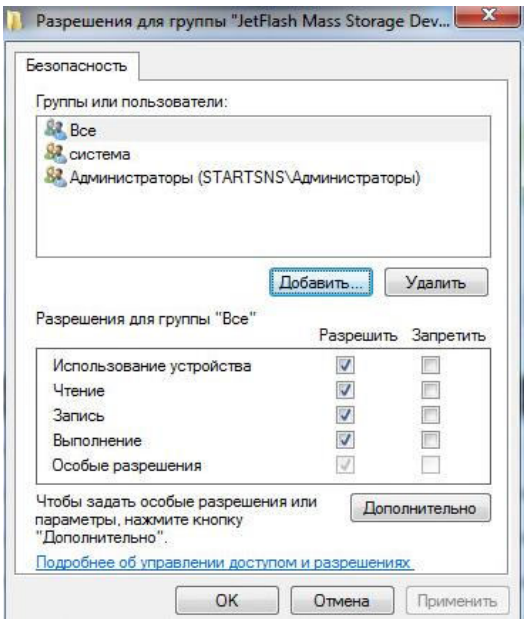
- удалите отметку из поля "Наследовать настройки контроля от родительского объекта" и установите флажок "Подключение устройства запрещено". Нажмите кнопку "Применить";
- на вкладке "Настройки" нажмите кнопку "Применить" Применить. Таким образом, мы запретили всем пользователям использовать незарегистрированные USB-флеш-накопители.

5. Для отслеживания произошедших событий, связанных с работой механизма разграничения доступа к устройствам, следует выполнить настройку регистрации событий. Справа от заголовка группы параметров "Устройства"

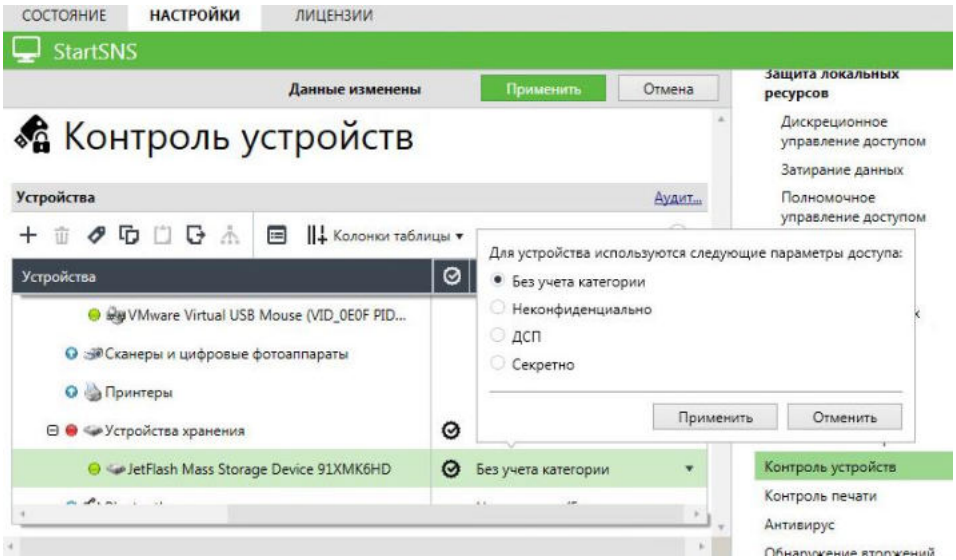
нажмите кнопку-ссылку "Аудит…". Вы переключитесь в раздел настроек "Регистрация событий / Контроль устройств". Используя кнопку , ознакомьтесь с текущим вариантом настроек и измените их на свое усмотрение.



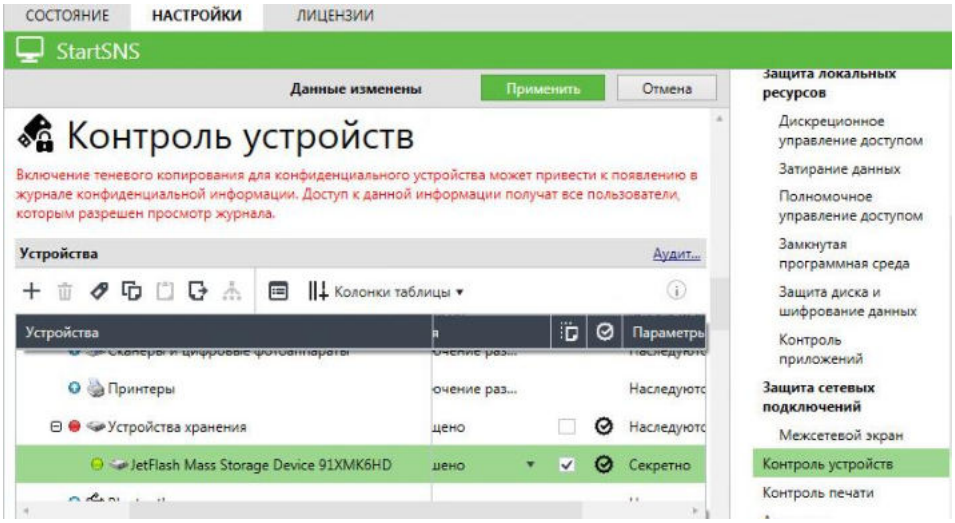
6. На ВМ StartSNS закройте программу управления, переавторизуйтесь под учетной записью пользователя "user2" и сделайте попытку доступа к подключенному в данный момент зарегистрированному USB-флеш-накопителю. Убедитесь, что в доступе отказано.
7. На ВМ StartSNS переавторизуйтесь под учетной записью пользователя "user1" и сделайте попытку доступа к подключенному в данный момент зарегистрированному USB-флеш-накопителю. Убедитесь, что доступ разрешен.
8. Протестируйте возможность разграничения доступа к устройству с помощью механизма полномочного управления доступом, присвоив требуемую категорию конфиденциальности. Для этого:
   - на ВМ StartSNS в программе "Локальный центр управления" на панели свойств компьютера выберите в разделе "Политики" группу параметров "Контроль устройств / Устройства";
   - в таблице "Устройства" выберите "Устройства USB / Устройства хранения / <подключенное устройство>" и справа от него нажмите кнопку "Разрешения" . В открывшемся диалоговом окне "Разрешения…" в списке "Группы или пользователи" удалите запрет на работу с подключенным в данный момент флеш-накопителем для пользователя "user2";



- раскройте поле "Параметры доступа". Текущее значение "Без учета категории" означает, что устройство должно функционировать независимо от уровня допуска пользователя;



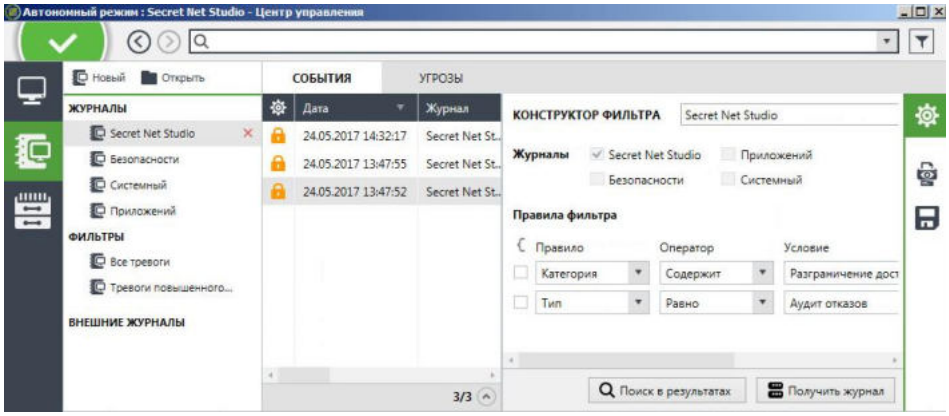
- выберите параметр "Секретно" и нажмите кнопку "Применить" В поле "Теневое копирование" установите флажок. Ознакомьтесь с появившимся над таблицей "Устройства" текстом предупреждения;



- на вкладке "Настройки" нажмите кнопку "Применить" Применить. Закройте программу управления и переавторизуйтесь под учетной записью пользователя "user2". Убедитесь, что в авторизации отказано, поскольку подключено устройство (USB-флеш-накопитель), к которому у пользователя отсутствует доступ, поскольку категория конфиденциальности устройства выше, чем у пользователя.

Подробнее о присвоении категорий конфиденциальности устройствам см. в руководстве администратора по настройке и эксплуатации локальной защиты.

9. Отключите от ВМ StartSNS зарегистрированный USB-флеш-накопитель.
10. Подключите к ВМ StartSNS другой – незарегистрированный – USB-флеш-накопитель и убедитесь, что подсистема контроля устройств Secret Net Studio не позволяет работать с ним всем пользователям.
11. На ВМ StartSNS переавторизуйтесь под учетной записью "adminsns". Откройте журнал Secret Net Studio, просмотрите записи категории "Разграничение доступа к устройствам" с типом "Аудит отказов" о событиях запрета подключения к незарегистрированному USB-флеш-накопителю.

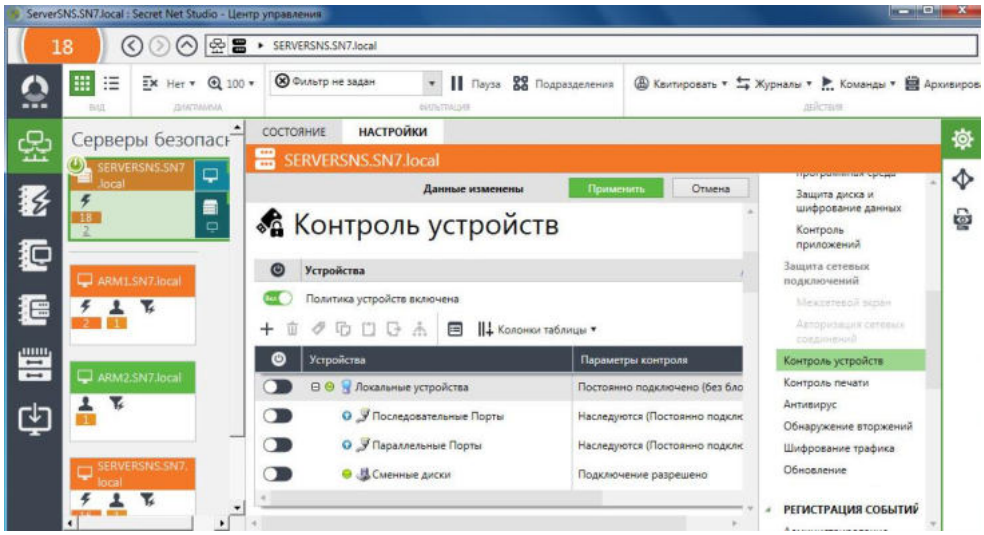


12. На ВМ StartSNS отмените все заданные ограничения на использование USB-флеш-накопителей.

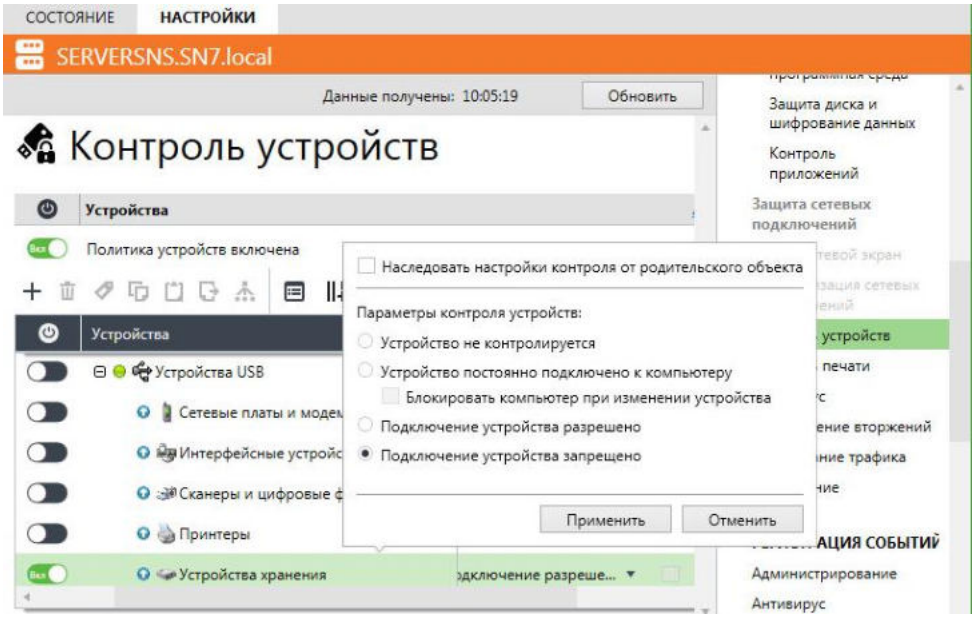
13. Если на нескольких компьютерах требуется применить одинаковые параметры использования конкретных устройств, можно выполнить их настройку в групповой политике. Устройства, к которым нужно настроить доступ, должны быть добавлены в список групповой политики. При этом в список устройств можно добавить сведения об устройствах, подключенных к клиентскому компьютеру.

Проведите настройку механизма разграничения доступа к устройствам в сетевом варианте – сначала запретите подключение любых USB-флеш-накопителей на защищаемых компьютерах, а затем разрешите подключение одного конкретного устройства:

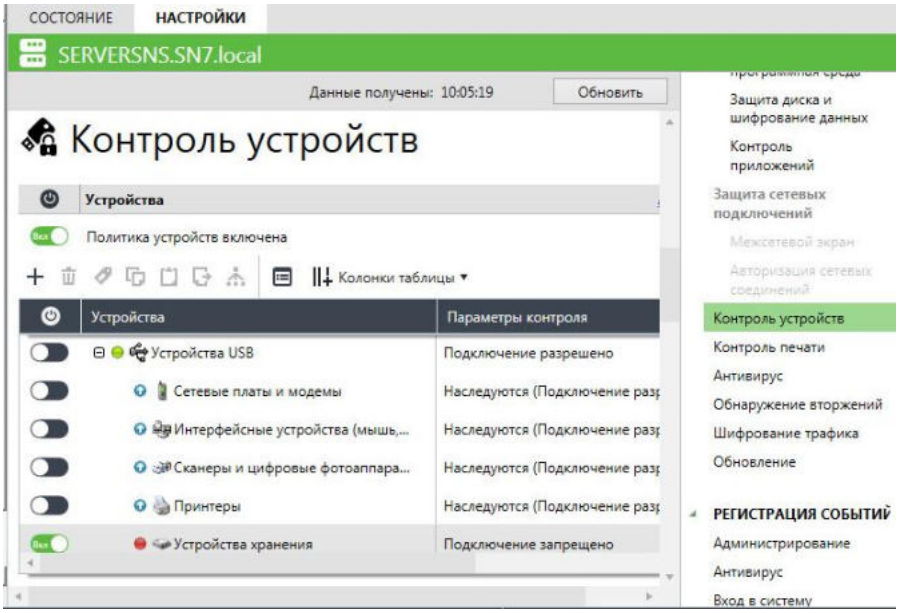
- переключитесь в окно консоли ВМ ARM2. В программе управления в сетевом варианте для объекта сервера безопасности на вкладке "Настройки" включите групповую политику "Контроль устройств";



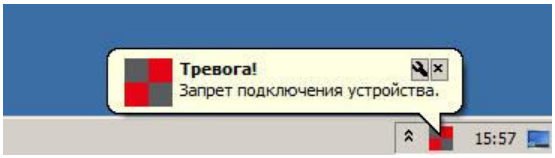
- в таблице "Устройства" включите политику "Устройства USB / Устройства хранения" и примените сделанные изменения;
- в таблице "Устройства" выберите политику "Устройства USB / Устройства хранения", раскройте поле "Параметры контроля", удалите отметку из поля "Наследовать настройки контроля от родительского объекта" и установите флажок "Подключение устройства запрещено";



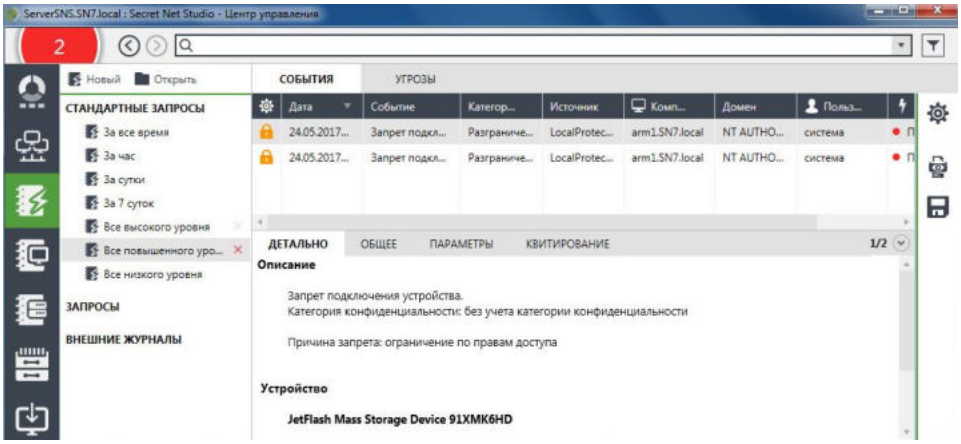
- примените настройки. Таким образом мы запретили всем пользователям подключать любые USB-флеш-накопители;



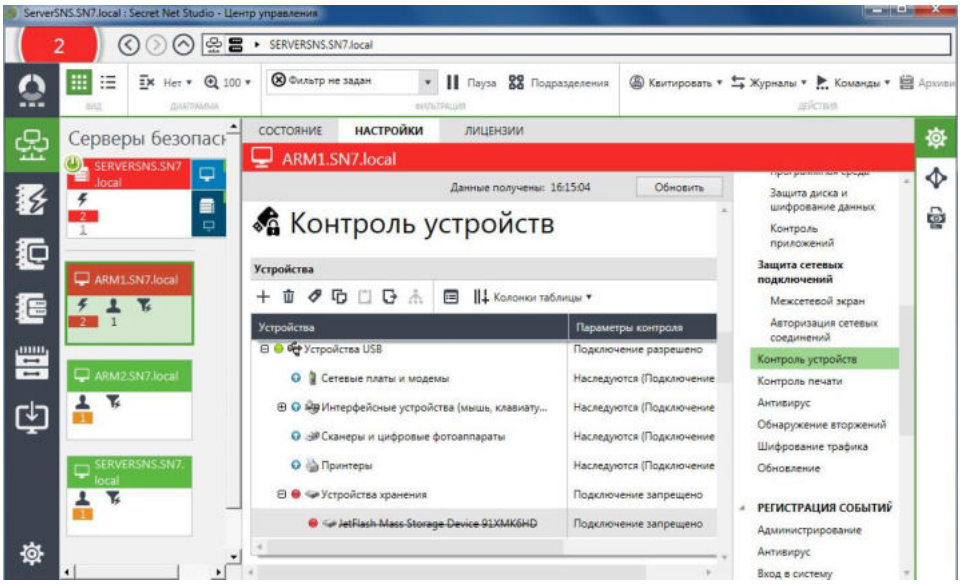
- в программе управления примените групповые политики для объекта ARM1, затем откройте консоль ВМ ARM1, последовательно переавторизуйтесь под учетными записями "user1" и "user2" и убедитесь, что подключение USB-флеш-накопителей запрещено, а системой защиты сгенерировано событие тревоги;



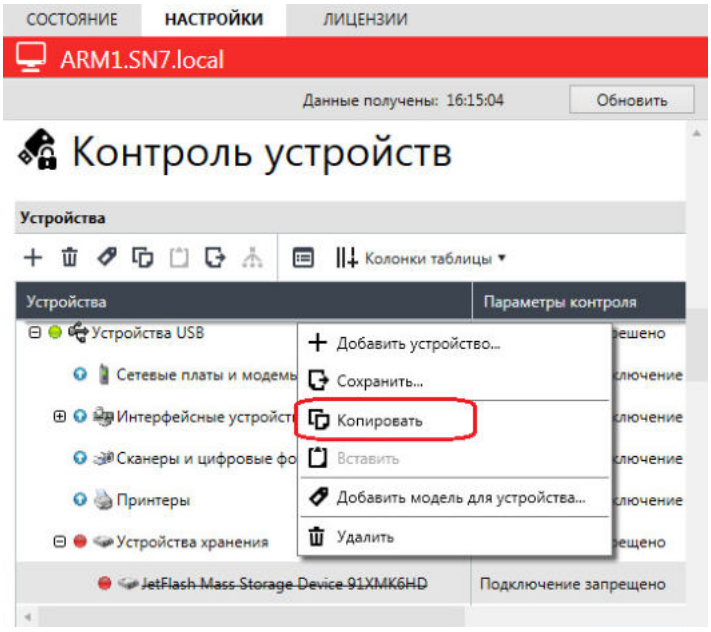
- перейдите в окно консоли ВМ ARM2 и в программе управления откройте "Журналы тревог". В категории "Стандартные запросы" выберите двойным щелчком мыши запрос "Все повышенного уровня" и найдите событие "Запрет подключения устройства" категории "Разграничение доступа к устройствам". Разверните и просмотрите детальные сведения о событии;



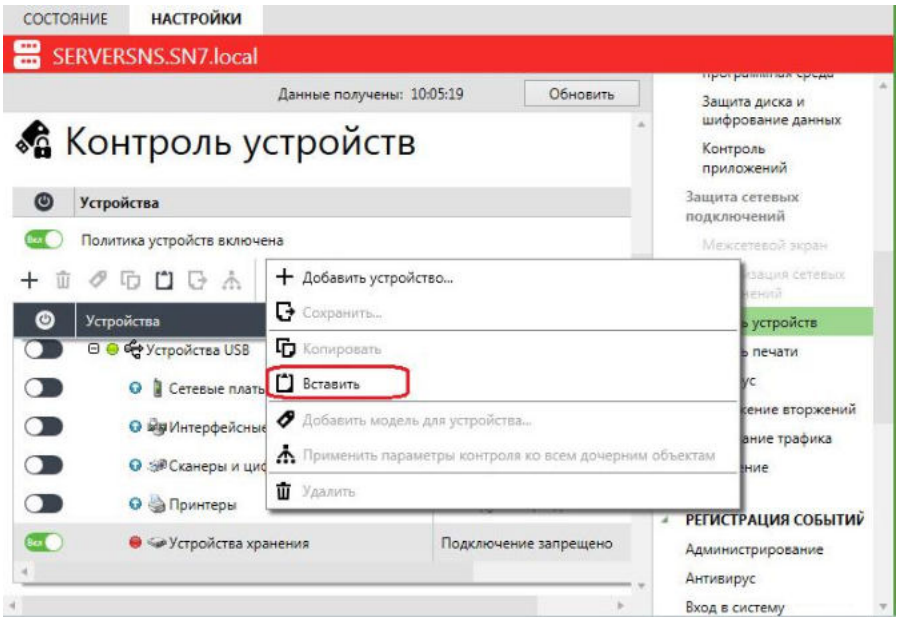
- в программе управления раскройте панель "Компьютеры", выберите объект ARM1, на вкладке "Настройки" панели его свойств раскройте раздел "Контроль устройств" и в таблице "Устройства" выберите запись "Устройства USB / Устройства хранения / <зачеркнутое наименование устройства>" – к этому устройству подключение запрещено;



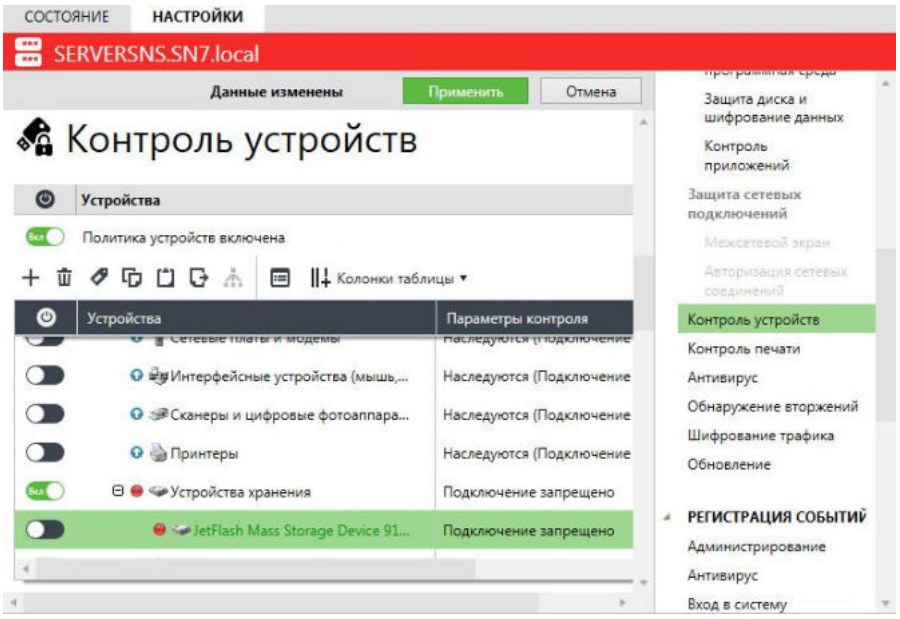
- вызовите контекстное меню этой записи и выберите опцию "Копировать";



- в программе управления перейдите к настройкам политики контроля устройств сервера безопасности. В таблице "Устройства" щелкните правой кнопкой мыши и выберите опцию "Вставить";



- обратите внимание, что в группе "Устройства USB / Устройства хранения" таблицы "Устройства" появилась выделенная зеленым цветом запись с ранее скопированным наименованием из раздела настроек "Контроль устройств" компьютера ARM1;



- используя описание пп. 3 и 4 лабораторной работы, измените параметры доступа к добавленному устройству таким образом, чтобы доступ был разрешен всем пользователям, кроме "user2", а затем примените сделанные настройки;
- в программе управления выберите объект компьютера ARM1 и с помощью опции "Команды / Применить групповые политики" его контекстного меню примените для него групповые политики сервера безопасности.

14. На ВМ ARM1 последовательно переавторизуйтесь под учетными записями "user1" и "user2" и протестируйте возможность подключения USB-флеш-накопителя.

15. Переключитесь в окно ВМ ARM2 и в программе управления отмените все сделанные ограничения на использование USB-флеш-накопителей.

Таким образом, мы рассмотрели примеры настройки механизма управления доступом к подключаемым USB-флеш-накопителям в локальном и сетевом вариантах. Выполнение лабораторной работы завершено.

Лабораторная работа №4 "Настройка механизма замкнутой программной среды"

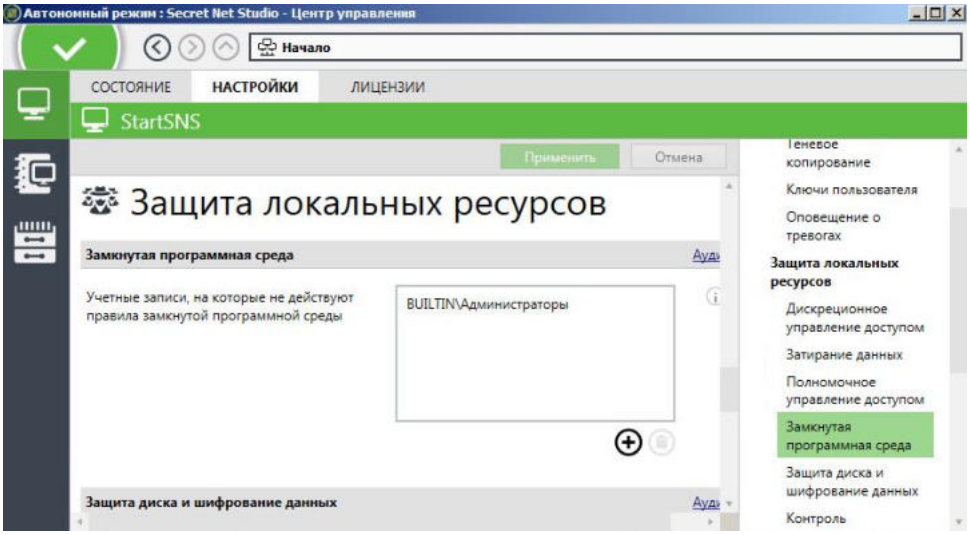
Структура модели данных и порядок настройки механизма ЗПС были описаны в соответствующем разделе главы 3. В данной лабораторной работе проводится создание замкнутой программной среды для пользователей в автономном и сетевом вариантах использования Secret Net Studio на примере организации возможности запуска только ограниченного набора программ: Проводник, MS Wordpad, MS Word, MS Excel, Internet Explorer, Корзина.

Модель ЗПС будет создаваться на основе данных журнала Secret Net Studio. В этом случае, чтобы собрать нужные сведения, пользователям разрешается запускать любые приложения. На это отводится некоторый период времени. Запуск приложений регистрируется в журнале. На время сбора сведений необходимо включить регистрацию всех событий категории "Замкнутая программная среда" на тех компьютерах, на которых ЗПС будет использоваться.

По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных на основе сведений о запускаемых программах из журнала Secret Net Studio. Экспорт сведений в модель данных может выполняться непосредственно из локального журнала Secret Net Studio или из файла, в который предварительно были сохранены записи журнала.

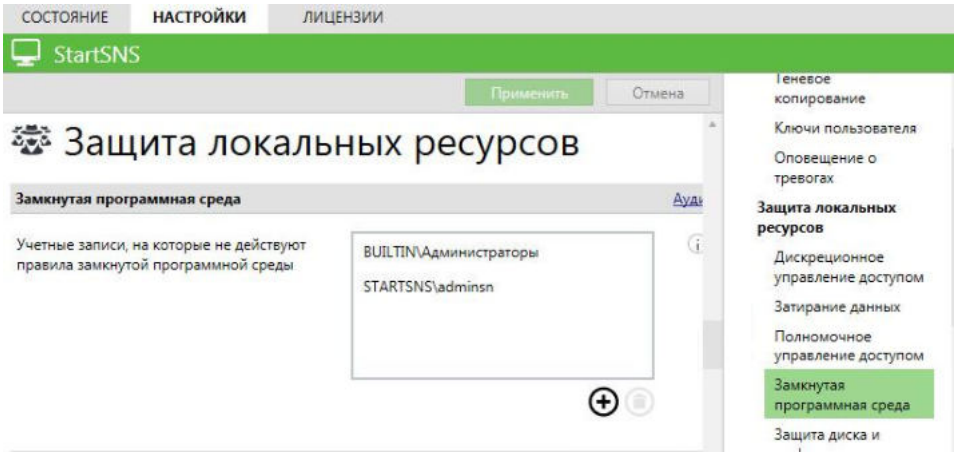
Примечание. Источником добавления задач ЗПС по журналу в централизованном режиме является evtx- или snlog-файл, в который предварительно были экспортированы сведения из журнала.

1. В окне консоли BM StartSNS убедитесь, что вы авторизованы под учетной записью "adminsns". В окне программы управления выберите панель "Компьютер", перейдите на вкладку "Настройки" и раскройте раздел настроек "Политики / Защита локальных ресурсов / Замкнутая программная среда".

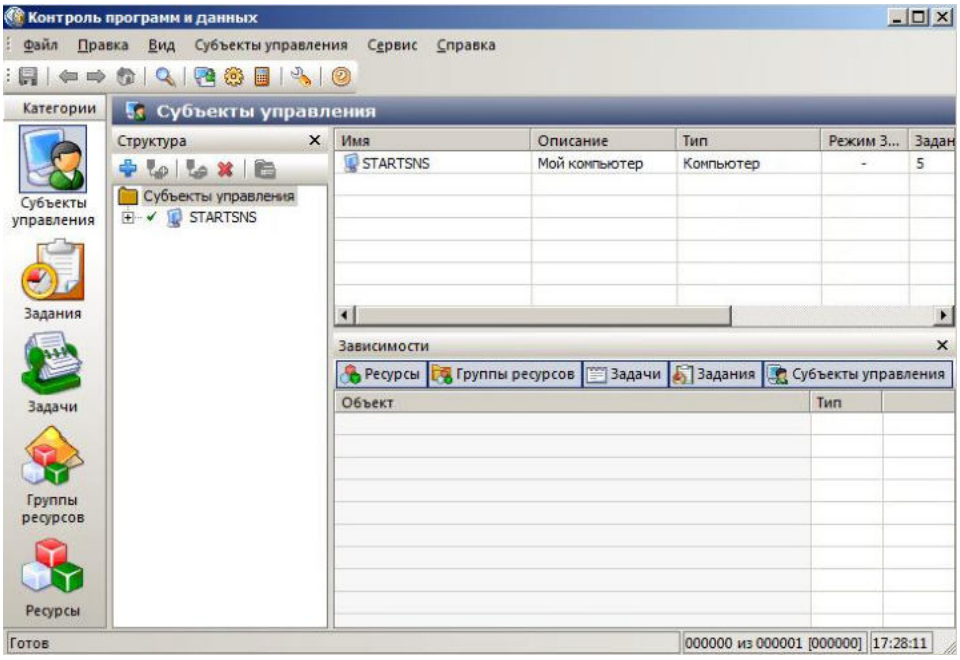


2. Обратите внимание, что в Secret Net Studio используется одна привилегия, связанная с работой ЗПС, – она определяет пользователей, для которых не действуют правила замкнутой программной среды. По умолчанию эта привилегия предоставлена локальной группе "Администраторы".

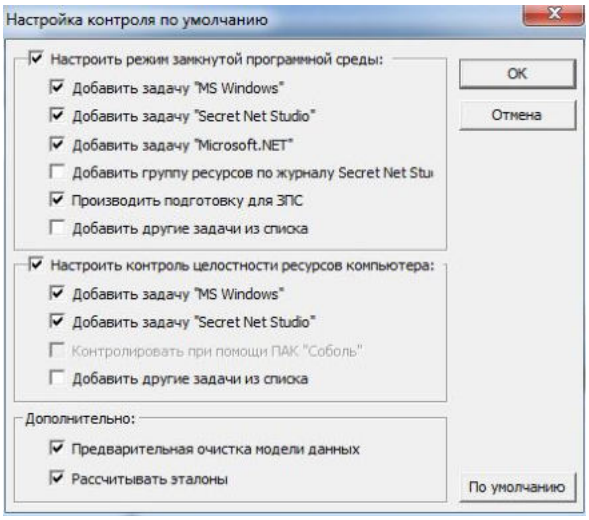
   Добавьте с помощью кнопки "Добавить" ⊕ администратора "adminsns" в группу привилегированных пользователей, а затем сохраните внесенные в политики изменения, используя кнопку "Применить" Применить.



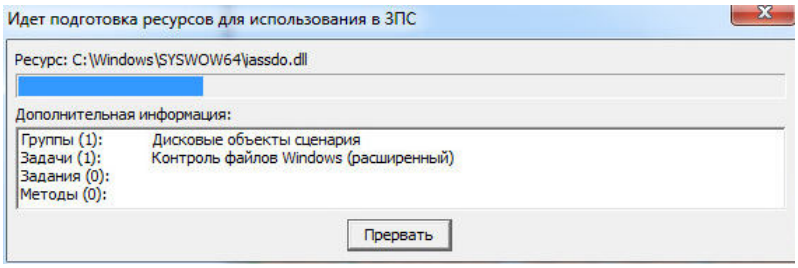
3. Для настройки механизма ЗПС запустите программу "Контроль программ и данных": "Пуск / Все программы / Код Безопасности / Secret Net Studio / Контроль программ и данных".



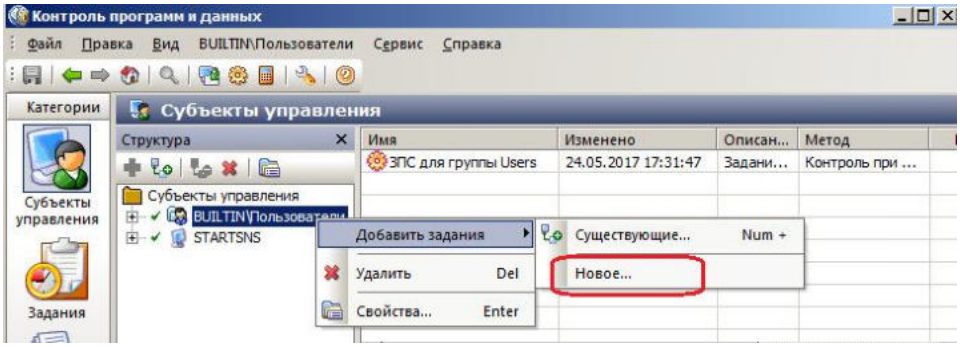
4. Для формирования новой модели данных в главном меню выберите опцию "Файл / Новая модель данных". В открывшемся диалоговом окне "Настройка контроля по умолчанию" установите отметку в поле "Предварительная очистка модели данных".



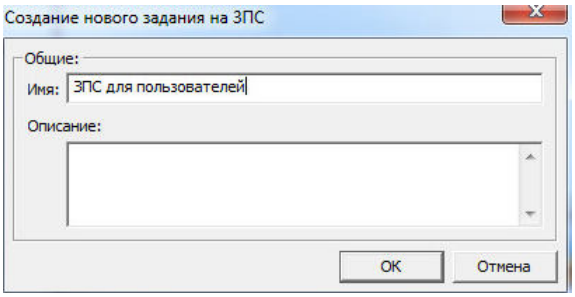
5. Нажмите кнопку "ОК". В диалоговом окне подтверждения нажмите кнопку "Да". Предыдущая модель данных будет удалена, и запустится процедура подготовки ресурсов для использования в ЗПС, по окончании которой автоматически запустится расчет эталонов для ресурсов. Дождитесь его завершения.



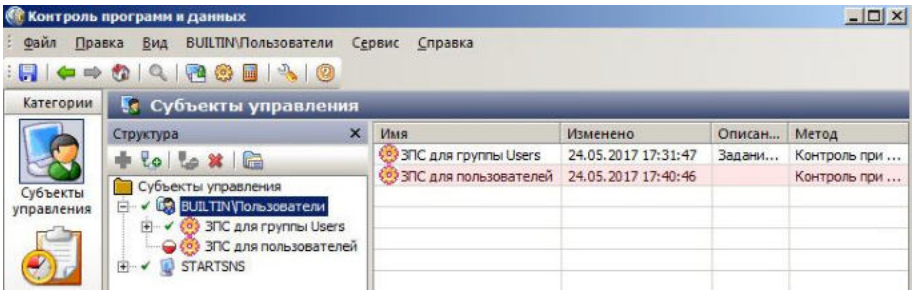
6. После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура объектов. Обратите внимание, что в ней уже содержится сформированное по умолчанию задание, включающее контроль ресурсов самой Secret Net Studio и ОС Windows. Создайте новое задание. Для этого в категории "Субъекты управления" вызовите контекстное меню вновь созданной структуры объектов "BUILTIN\Пользователи" и выберите опцию "Добавить задание / Новое".



7. В открывшемся диалоговом окне введите название **ЗПС для пользователей** и нажмите кнопку "ОК".



8. Обратите внимание, что в окне "Контроль программ и данных" в структуре созданного ранее объекта появилась запись нового задания.



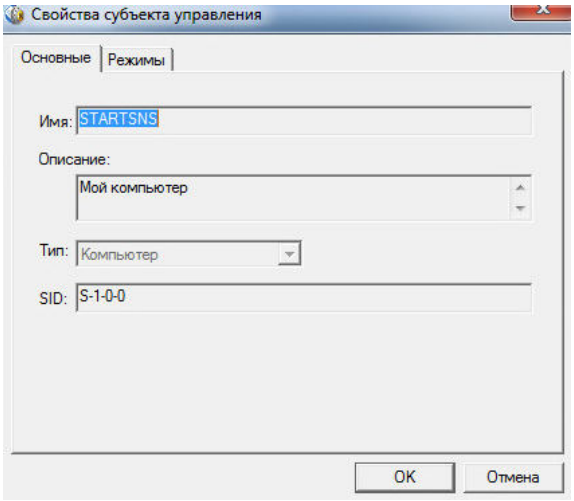
9. Для настройки механизма ЗПС на основе данных журнала Secret Net Studio включите мягкий режим работы ЗПС, в котором пользователю разрешается использовать любые программы. Если при этом запускаются программы, не

входящие в перечень разрешенных, – в журнале Secret Net Studio регистрируются события аудита отказа. Это нужно для того, чтобы, не влияя на работу пользователей, в журнале накопить сведения о возможных ошибках, допущенных при настройке механизма ЗПС, и в последующем их устранить.

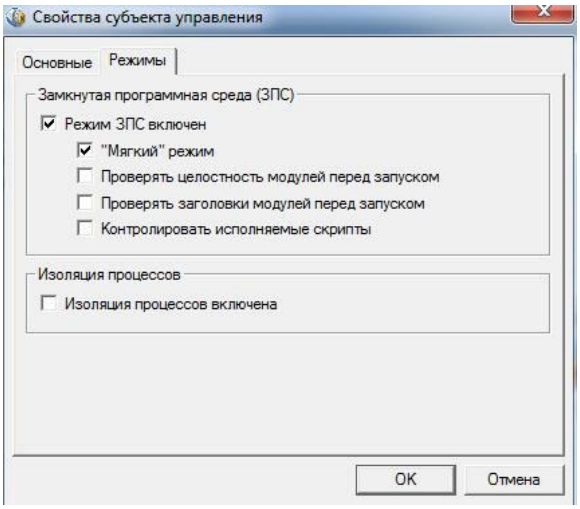
В жестком режиме разрешается запуск только тех программ, которые входят в список разрешенных, а запуск остальных блокируется, и в журнале Secret Net Studio регистрируются события тревоги.

Для включения мягкого режима сделайте следующее:

- в окне "Контроль программ и данных" вызовите контекстное меню субъекта управления "StartSNS" и выберите опцию "Свойства" – откроется диалоговое окно;



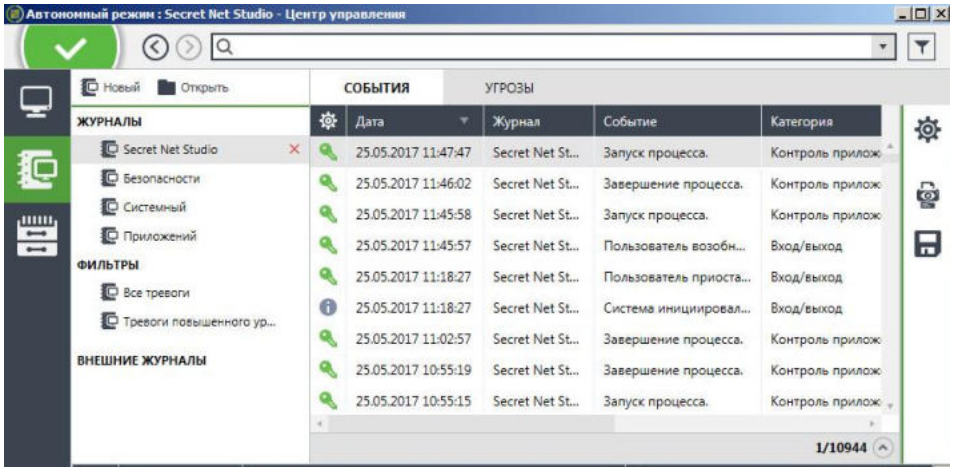
- переключитесь на вкладку "Режимы" и установите отметки в полях: "Режим ЗПС включен" и "Мягкий режим".



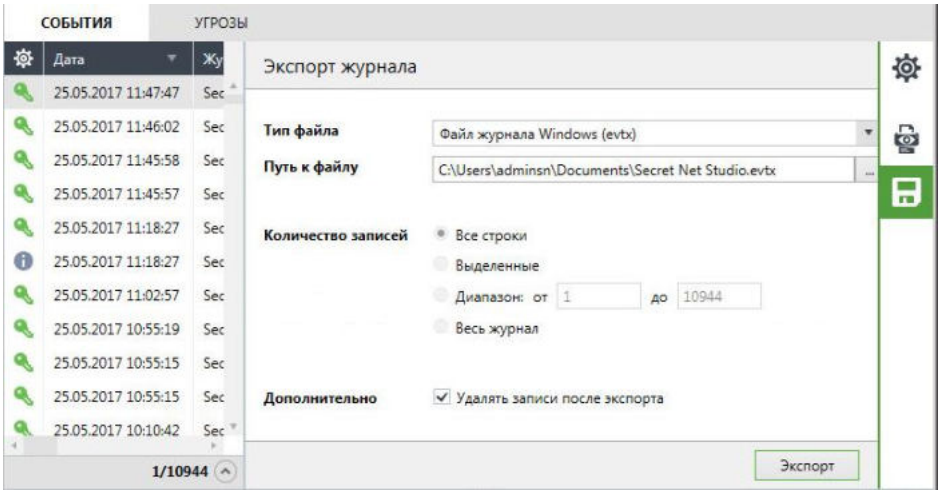
- нажмите кнопку "OK", сохраните модель и перезагрузите ОС на ВМ StartSNS.

10. Авторизуйтесь на ВМ StartSNS под учетной записью "adminsns" и экспортируйте журнал Secret Net Studio во внешний файл, чтобы очистить его. Для этого:

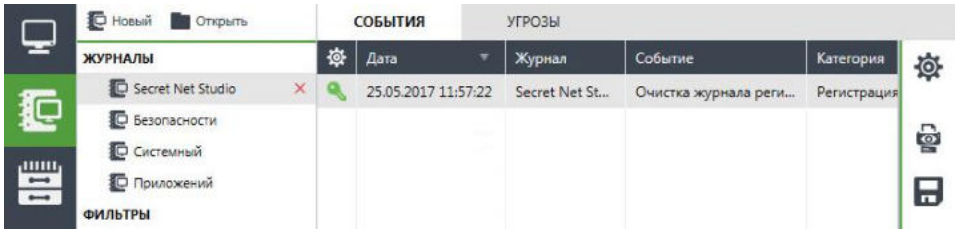
- запустите программу управления в локальном режиме и в панели "Журналы станций" откройте журнал Secret Net Studio;



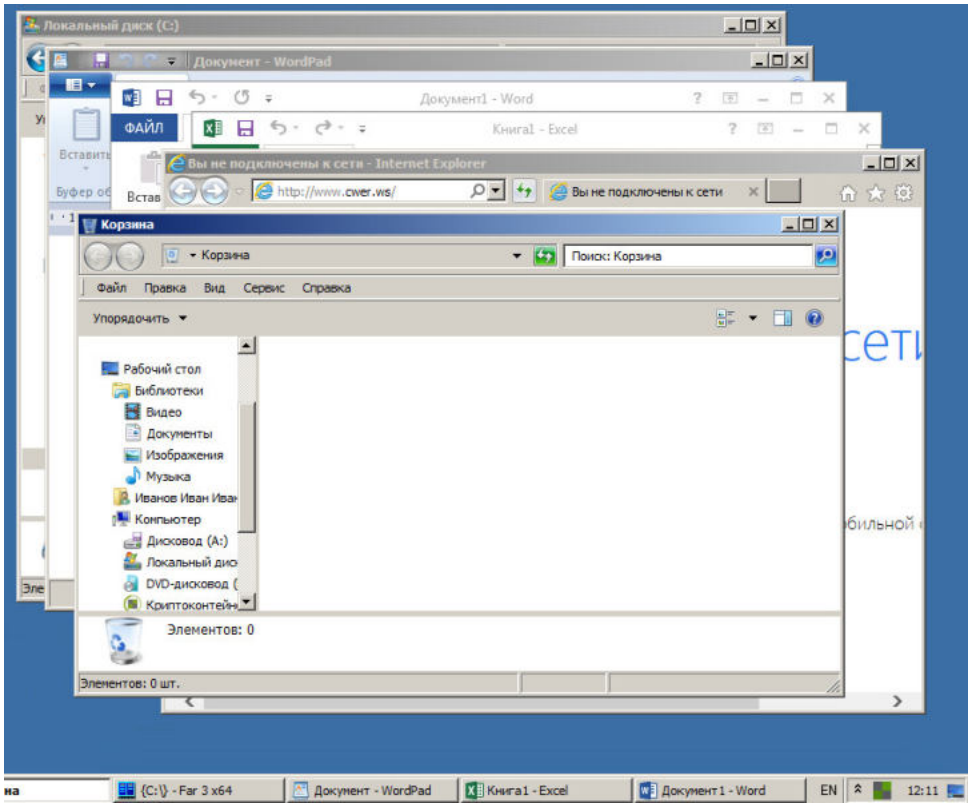
- в правой части окна нажмите кнопку "Экспорт журнала"  и выгрузите журнал Secret Net Studio в файл с произвольным наименованием формата evtx, установив признак очистки журнала при экспорте;



- убедитесь в том, что журнал очищен.



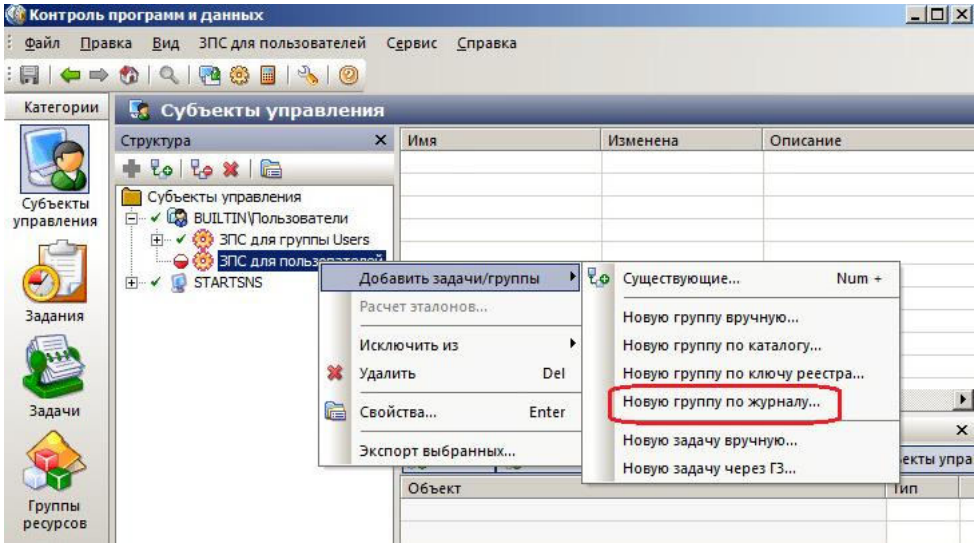
11. Перезагрузите ОС на ВМ StartSNS и авторизуйтесь под учетной записью "user1 – Иванов Иван Иванович". Последовательно запустите все программы, которые будут разрешены в дальнейшем пользователям: Проводник, WordPad, MS Word, MS Excel, Internet Explorer, Корзина.



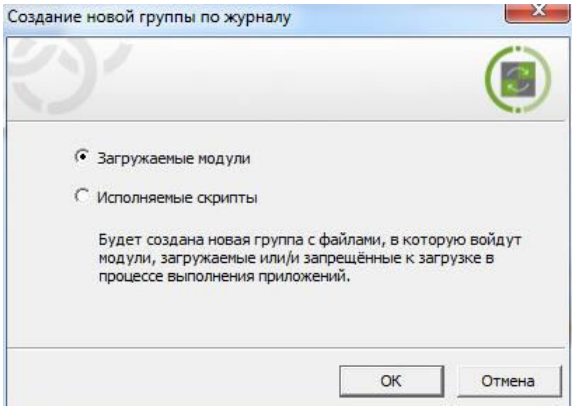
12. Переавторизуйтесь на ВМ StartSNS под учетной записью "adminsns" и откройте программу "Контроль программ и данных".

13. К созданному ранее заданию ЗПС добавьте задачи на основании данных из журнала Secret Net Studio. Для этого:

- выделите запись созданного вами ранее задания "ЗПС для пользователей" и в контекстном меню выберите опцию "Добавить задачи/группы / Новую группу по журналу";

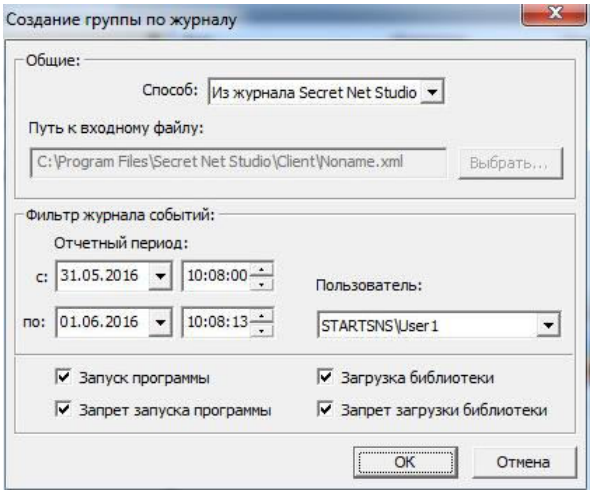


- в открывшемся диалоговом окне выберите переключатель "Загружаемые модули" и нажмите кнопку "ОК".

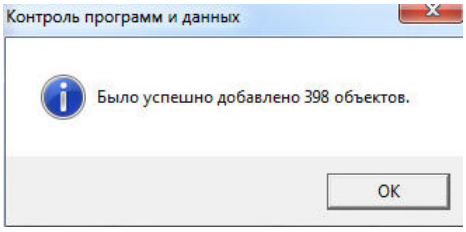


14. В диалоговом окне "Создание группы по журналу" установите следующие параметры:

- "Способ" – "Из журнала Secret Net Studio";
- в поле "Пользователь" нажмите кнопку "Найти" и выберите "user1";
- в поле "Отчетный период" укажите период запуска разрешенных программ для "user1". Поскольку в данной лабораторной работе журнал Secret Net Studio был предварительно очищен, поле "Отчетный период" можно оставить без изменения.

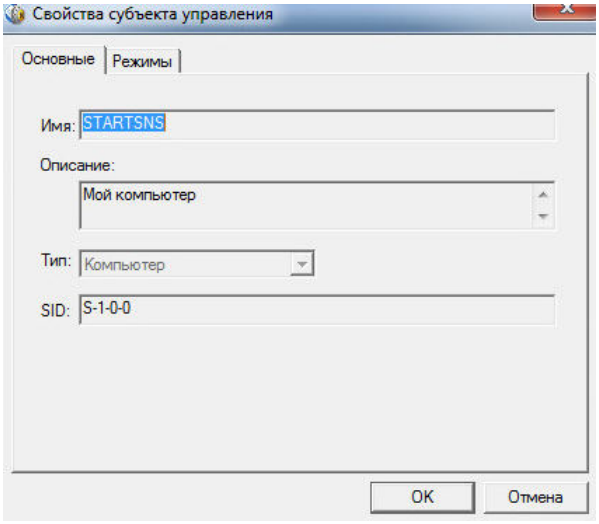


15. Нажмите кнопку "OK" и сохраните сделанные изменения в модели данных.

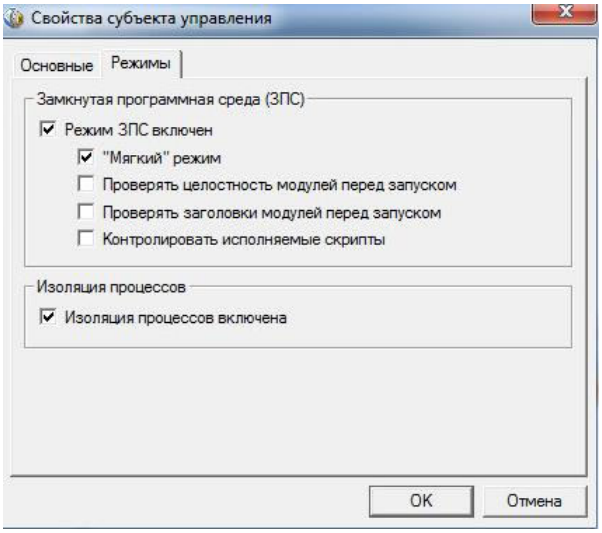


16. Установите запрет обмена данными для приложения WordPad с другими процессами, настроив изоляцию процессов. Для этого:

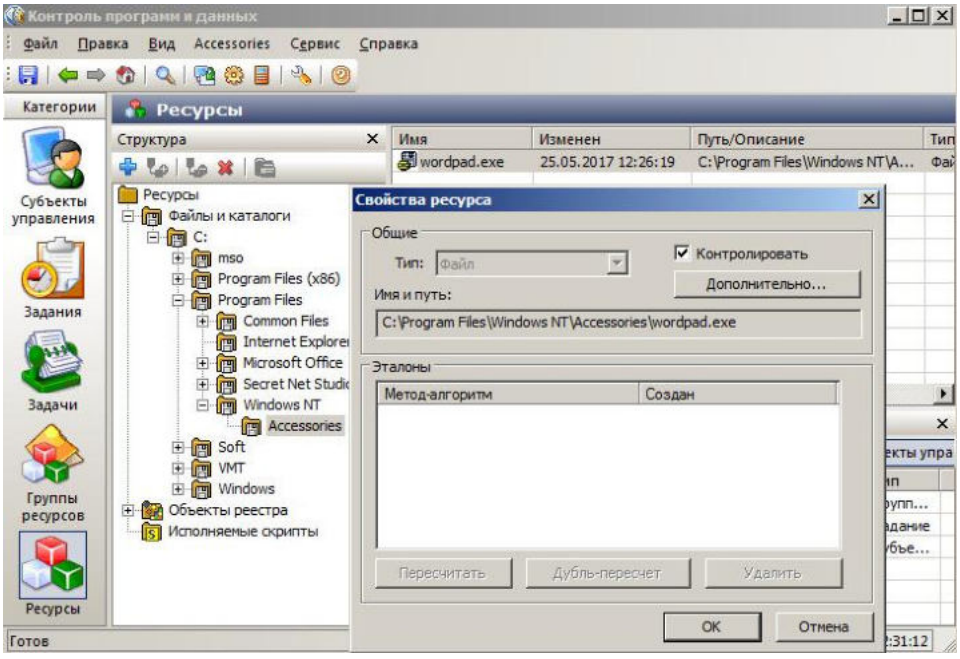
- в окне "Контроль программ и данных" в категории "Субъекты управления" вызовите контекстное меню компьютера StartSNS и выберите опцию "Свойства". Откроется диалоговое окно;



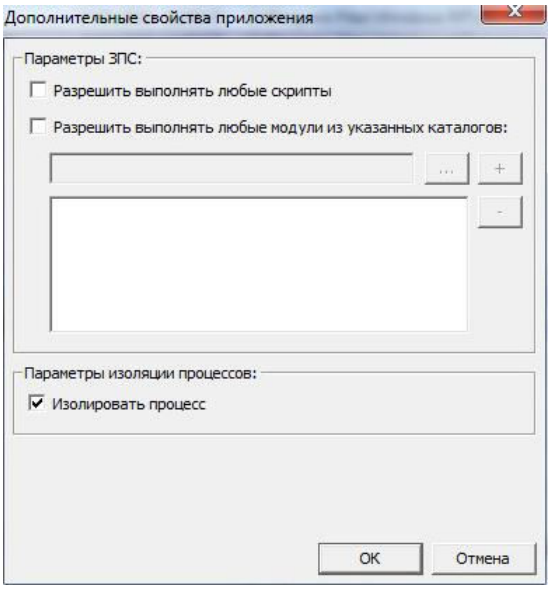
- переключитесь на вкладку "Режимы" и установите отметку в поле "Изоляция процессов включена". Обратите внимание, что механизм изоляции процессов может быть включен независимо от ЗПС;



- нажмите кнопку "ОК". Режим изоляции процессов начнет действовать для выбранного компьютера;
- включите изоляцию для ресурса WordPad. Для этого в окне "Контроль программ и данных" выберите категорию "Ресурсы" и раскройте ветку "Файлы и каталоги / C: / Program files / Windows NT / Accessories". Вызовите контекстное меню файла "wordpad.exe" и выберите опцию "Свойства". Откроется диалоговое окно;



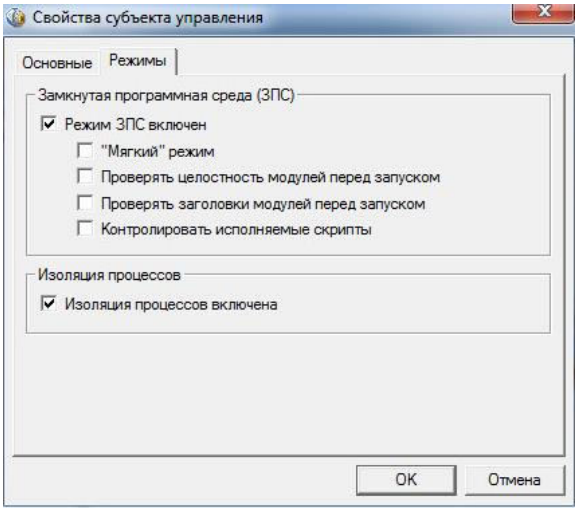
- в диалоговом окне "Свойства ресурса" нажмите кнопку "Дополнительно" – откроется следующее окно. Установите отметку в поле "Изолировать процесс";



- последовательно нажмите кнопку "ОК" в окнах "Дополнительные свойства приложения" и "Свойства ресурса". Изоляция для ресурса WordPad включена и теперь обмен данными для приложения WordPad с другими процессами будет невозможен.

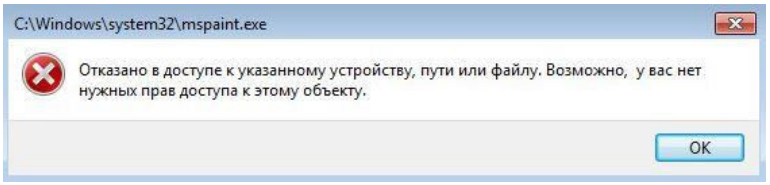
17. Включите жесткий режим для ЗПС. Для этого:

- в окне "Контроль программ и данных" вызовите контекстное меню субъекта управления "StartSNS" и выберите опцию "Свойства". Откроется диалоговое окно;
- переключитесь на вкладку "Режимы" и снимите отметку в поле "Мягкий режим";



- нажмите кнопку "OK" и сохраните модель данных.

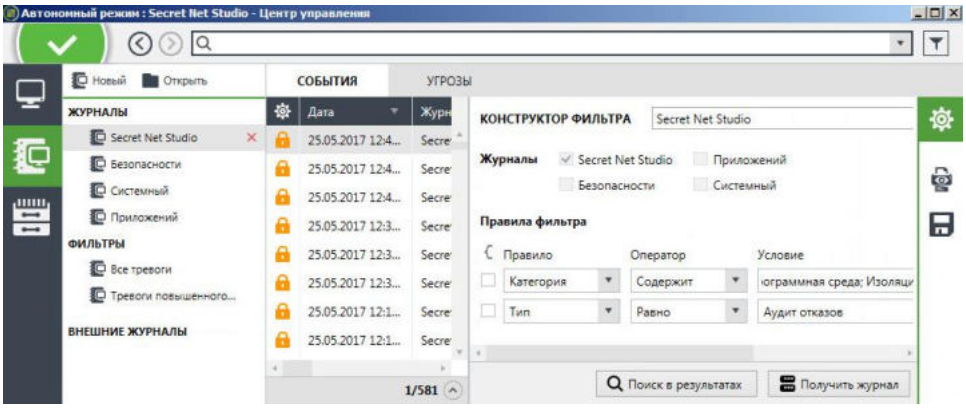
18. Переавторизуйтесь на ВМ StartSNS под учетной записью "user1" и убедитесь, что пользователь может запускать только ограниченный набор программ: Проводник, WordPad, MS Word, MS Excel, Internet Explorer, Корзина. Попытки запуска других программ, например, Paint, блокируются.



19. Убедитесь, что для приложения WordPad работает механизм изоляции процессов и копирование любых данных из окна WordPad в другие приложения невозможно.

20. Переавторизуйтесь на ВМ StartSNS под учетной записью "user2" и убедитесь, что ЗПС работает и для этого пользователя тоже.

21. Переавторизуйтесь на ВМ StartSNS под учетной записью "adminsns", в программе управления откройте журнал Secret Net Studio и просмотрите записи категорий "Замкнутая программная среда" и "Изоляция процессов" с типом "Аудит отказов".



22. Откройте программу "Контроль программ и данных", отключите механизмы ЗПС и изоляции процессов, сохраните изменения и перезагрузите ВМ StartSNS.

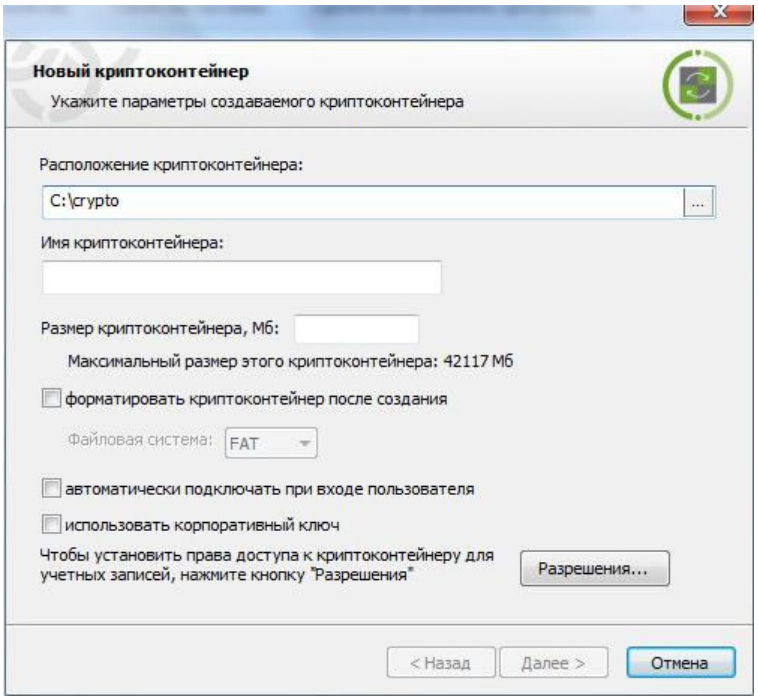
23. Самостоятельно. При наличии свободного времени, руководствуясь описанием данной лабораторной работы и используя в сетевом варианте ПО "Контроль программ и данных" и "Центр управления", проведите аналогичную настройку механизма ЗПС в централизованном варианте для пользователей "user1" и "user2". Помните, что перед добавлением задач по журналу необходимо из него экспортировать сведения в evtx- или snlog-файл.

Выполнение лабораторной работы завершено.

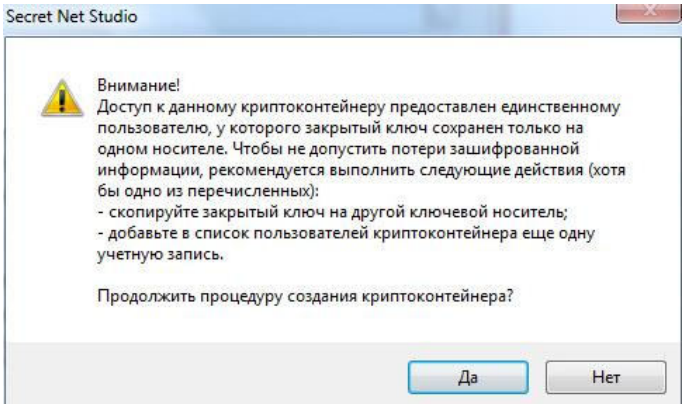
Лабораторная работа №5 "Использование криптоконтейнеров"

В данной лабораторной работе приводится пример использования криптоконтейнера для защиты информации.

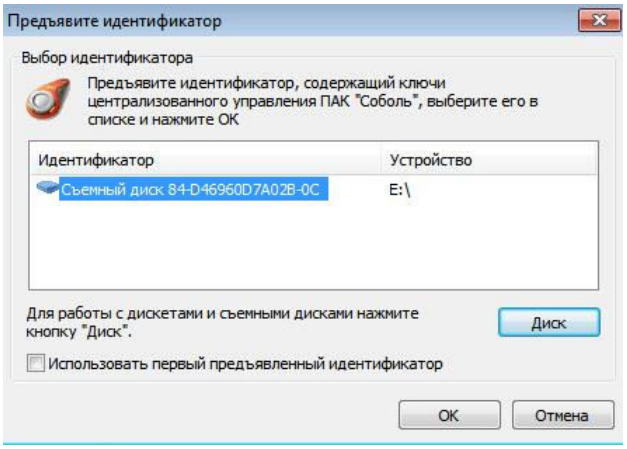
1. Авторизуйтесь на ВМ ARM1 под учетной записью "dadminsns1".
2. Для хранения криптоконтейнера на локальном диске "C:\" создайте папку с произвольным наименованием, например, "C:\crypto".
3. Подключите USB-флеш-накопитель, на котором ранее был создан криптографический ключ (см. лабораторную работу №5 главы 2).
4. Начните создавать контейнер одним из следующих способов:
   - откройте папку "crypto" и в контекстном меню выберите команду "Создать / Криптоконтейнер Secret Net Studio". Откроется диалоговое окно;
   - в окне "Мой компьютер" раскройте системную папку "Криптоконтейнеры Secret Net Studio" и в контекстном меню выберите опцию "Создать". В открывшемся диалоговом окне создания нового контейнера, в поле "Расположение контейнера" укажите "C:\crypto".



5. В диалоговом окне создания нового контейнера укажите следующие параметры:
   - "имя криптоконтейнера" – введите произвольно, например, **info**;
   - "Размер криптоконтейнера, Мб" – **2048**;
   - "автоматически подключать при входе пользователя" – установите отметку;
   - "использовать корпоративный ключ" – установите отметку. В этом случае создается "мастер-ключ", который будет использоваться для доступа к любому криптоконтейнеру, у которого данное поле установлено;
   - нажмите кнопку "Разрешения", в открывшемся диалоговом окне убедитесь, что доступ к создаваемому контейнеру предусмотрен только для текущего пользователя "dadminsns1", а затем закройте окно.
6. Нажмите кнопку "Готово". Откроется диалоговое окно подтверждения создания контейнера. Ознакомьтесь с текстом сообщения.



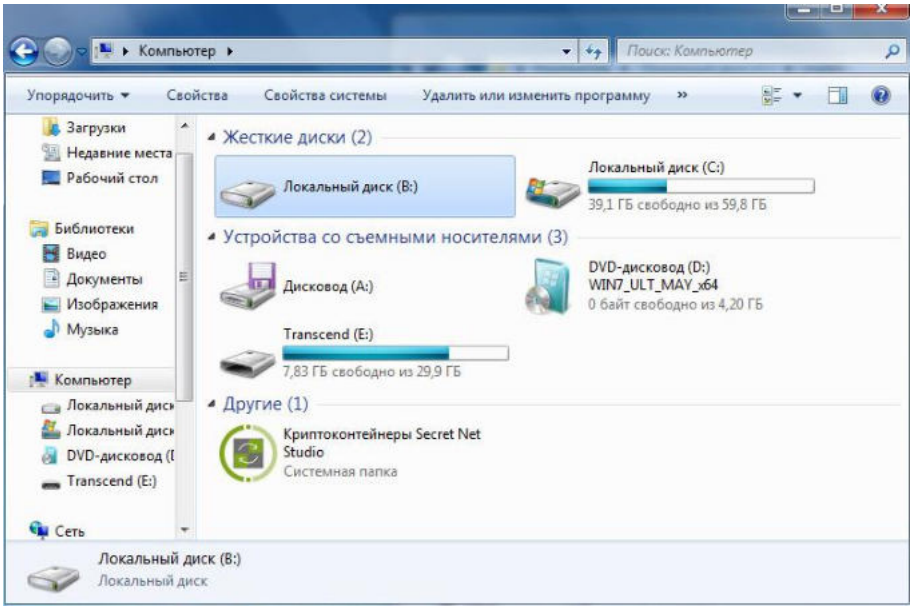
7. Нажмите кнопку "Да". Объект нового контейнера появится в папке. Обратите внимание, что состояние нового контейнера – "Отключен".
8. Для дальнейшей работы с криптоконтейнером необходимо загрузить криптоключ. В области уведомлений на панели задач вызовите контекстное меню значка Secret Net Studio и выберите опцию "Загрузить ключи". В открывшемся диалоговом окне снимите отметку в поле "Использовать первый предъявленный идентификатор" и через кнопку "Диск" выберите ключ.



9. Нажмите кнопку "ОК". Состояние контейнера изменится на "Подключен", и будет назначена буква диска.

Если состояние нового криптоконтейнера изменится на "Не доступен", закройте папку "Криптоконтейнеры Secret Net Studio" и откройте ее вновь.

10. Откройте "Мой компьютер" и убедитесь, что в системе появился новый диск.



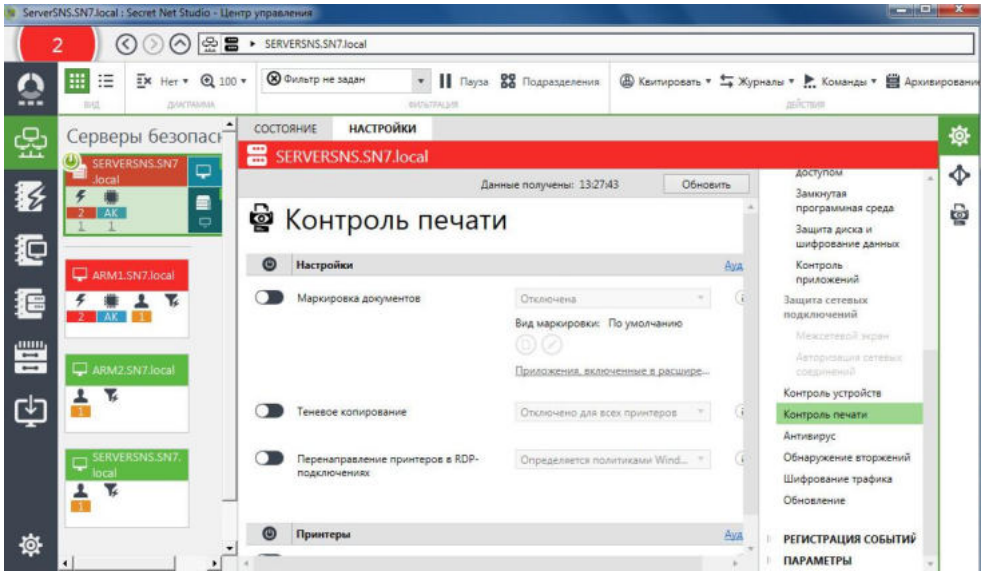
11. Отформатируйте появившийся новый диск в формате NTFS с параметрами по умолчанию. Теперь созданный криптоконтейнер может использоваться как отдельный диск. Создайте на новом диске папку с произвольным наименованием (например, "my docs"), а в папке – документ произвольного содержания с любым наименованием, например, "report".
12. На компьютере ARM1 отключите USB-флеш-накопитель и переавторизуйтесь под учетной записью "user1". Откройте "Мой компьютер" и убедитесь, что для данного пользователя диск криптоконтейнера не смонтировался, и в папке "C:\crypto" доступ к объекту криптоконтейнера невозможен.

    Показана процедура создания криптоконтейнера и его применение. Выполнение лабораторной работы завершено.

Лабораторная работа №6 "Настройка теневого копирования и маркировки при контроле печати"

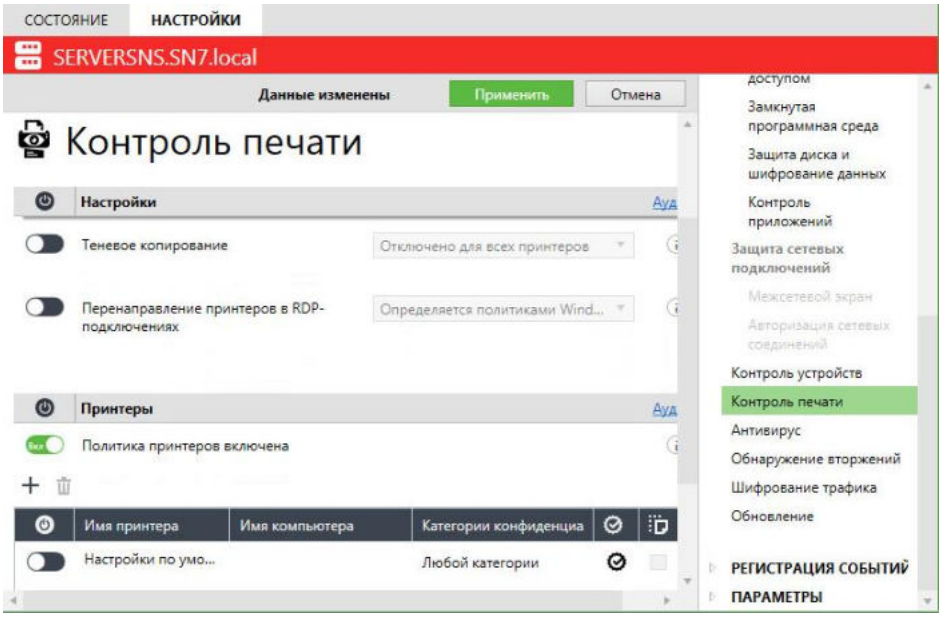
В данной лабораторной работе рассматриваются возможности централизованной настройки механизмов теневого копирования и маркировки в рамках подсистемы контроля печати Secret Net Studio для выводимых на печать документов.

1. Откройте консоль BM ARM2 и в окне программы управления в сетевом режиме на панели "Компьютеры" выберите объект сервера безопасности.
2. Настройте список принтеров в групповой политике. Для этого откройте панель свойств объекта ServerSNS, выберите вкладку "Настройки" и раскройте раздел "Политики / Контроль печати".



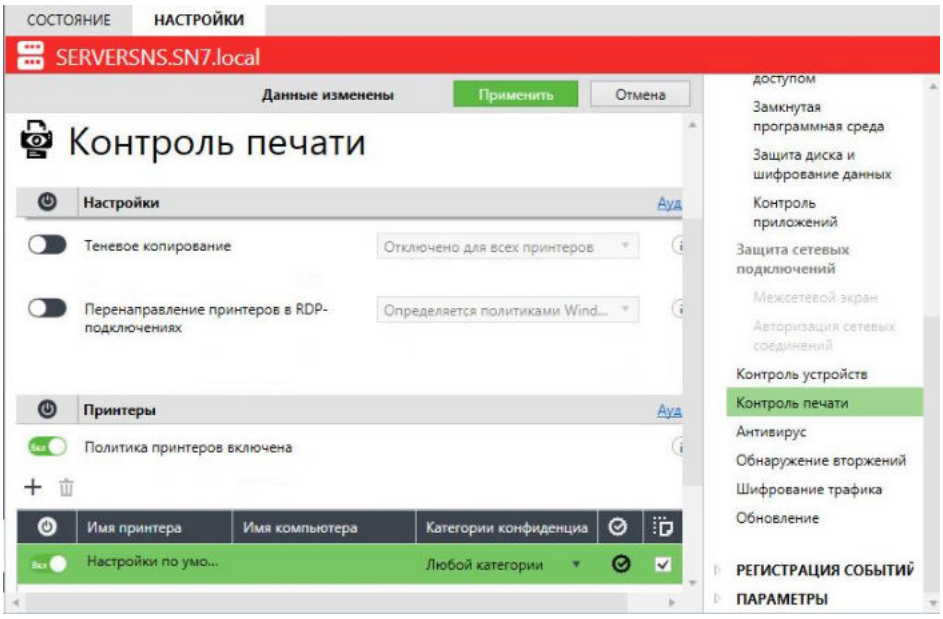
3. Обратите внимание, что в группе "Принтеры" групповая политика принтеров по умолчанию выключена, и список принтеров пуст. Включите эту политику – ниже в таблице появится список принтеров, содержащий единственный элемент "Настройки по умолчанию". Параметры использования принтеров, заданные для этого элемента, применяются ко всем принтерам, кроме тех, которые в явном виде присутствуют в списке принтеров. Явно заданные параметры для конкретных принтеров имеют приоритет перед параметрами элемента "Настройки по умолчанию".

    Используя кнопку ⓘ, внимательно ознакомьтесь с описанием параметров списка принтеров.

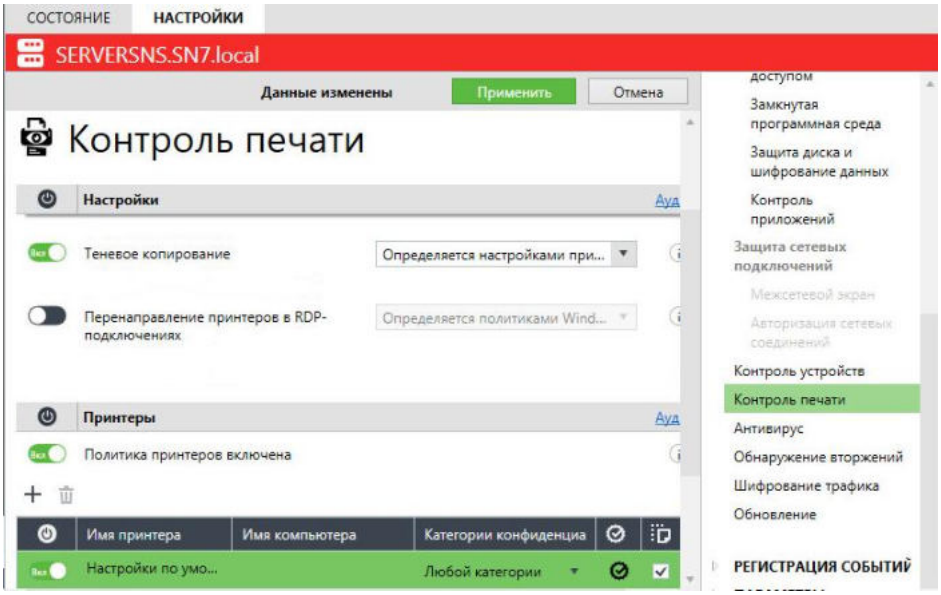


4. Включите политику для принтера "Настройки по умолчанию". Убедитесь, что в графе "Категории конфиденциальности" по умолчанию указано "Любой категории" и установите отметку в поле "Теневое копирование" – для сохранения копий распечатываемых документов.

   Обратите внимание, что при необходимости в ячейке колонки "Разрешения" могут устанавливаться права пользователей для печати документов для конкретных принтеров или для элемента "Настройки по умолчанию".



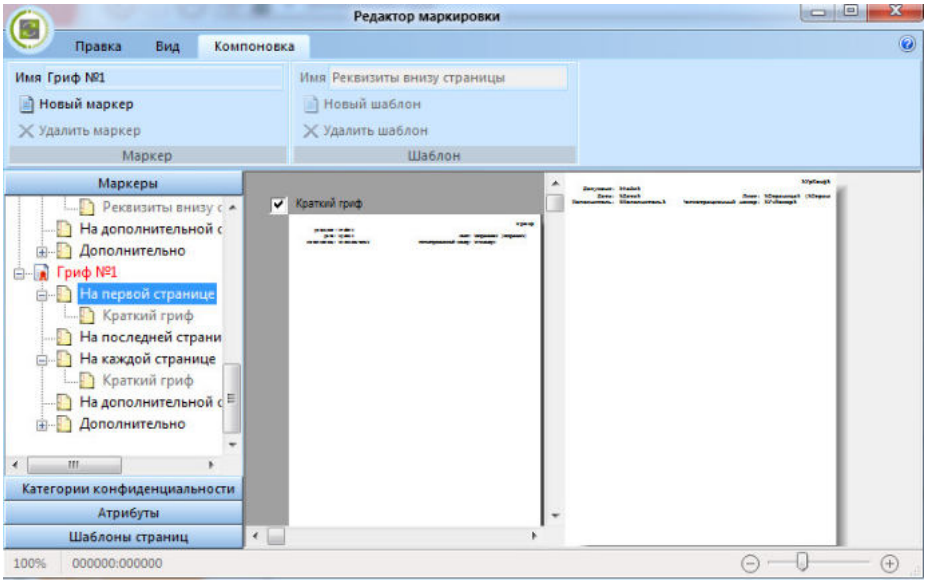
5. Список принтеров в групповой политике настроен. Нажмите кнопку "Применить" Применить .
6. Настройте для принтеров функцию теневого копирования. Для этого:
   - в разделе политик "Политики / Контроль печати" включите групповую политику "Теневое копирование" и с помощью кнопки внимательно ознакомьтесь с ее описанием;
   - измените установленное по умолчанию значение на "Определяется настройками принтера" – настраиваемая функция будет выполняться для принтеров с включенным режимом теневого копирования;



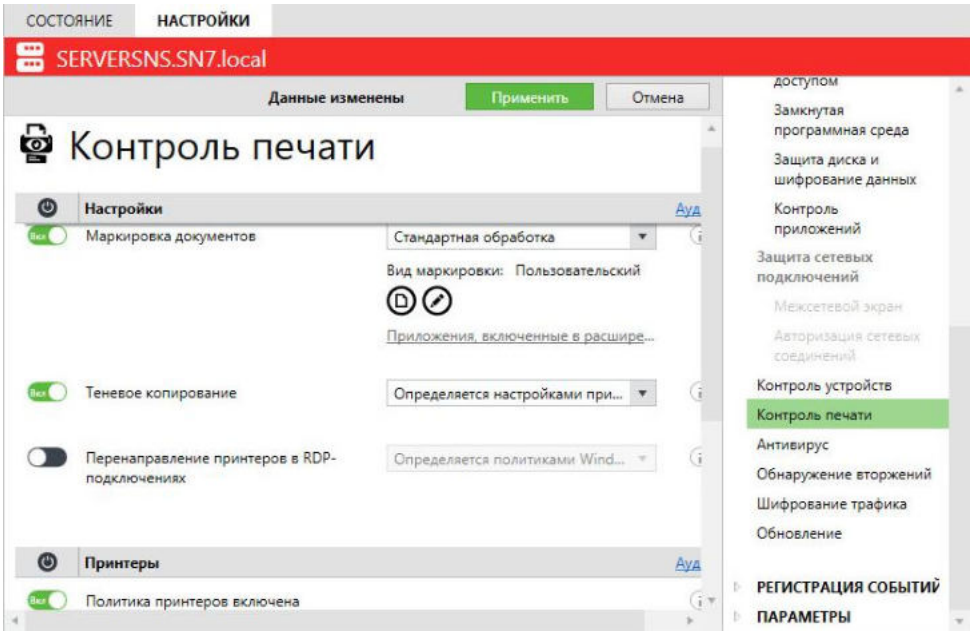
- нажмите кнопку "Применить" Применить .

7. Настройте для принтеров функцию маркировки документов. Для этого:

- в разделе политик "Политики / Контроль печати" включите групповую политику "Маркировка документов" и с помощью кнопки внимательно ознакомьтесь с описанием ее параметров;
- измените установленное по умолчанию значение на "Стандартная обработка" – этот режим может использоваться во всех поддерживаемых приложениях. В данном режиме предпочтительнее печатать документы целиком. При печати фрагмента документа маркер будет содержать сведения только о распечатанных страницах без учета общего количества страниц документа (так как распечатанный фрагмент воспринимается как отдельный документ);
- используя кнопку "Редактировать" , ознакомьтесь с возможностью редактирования заданных грифов маркировки. Выберите краткий гриф для шаблона "Гриф №1";



- обратите внимание, что если в политике "Маркировка документов" выбран параметр "Расширенная обработка", то с помощью кнопки-ссылки "Приложения, включенные в расширенную обработку" можно управлять перечнем приложений, которые будут поддерживать маркировку печатаемых документов;

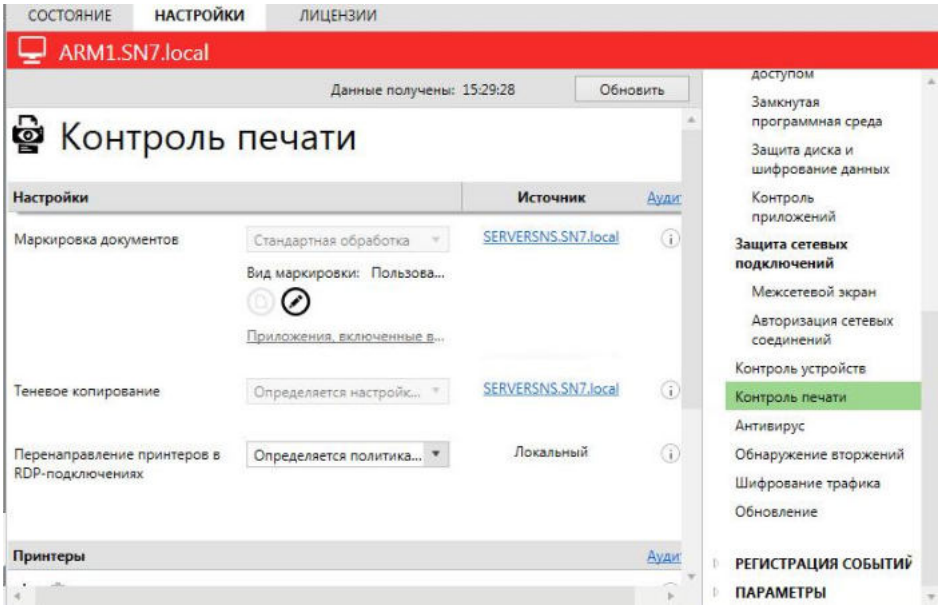


- нажмите кнопку "Применить" Применить .

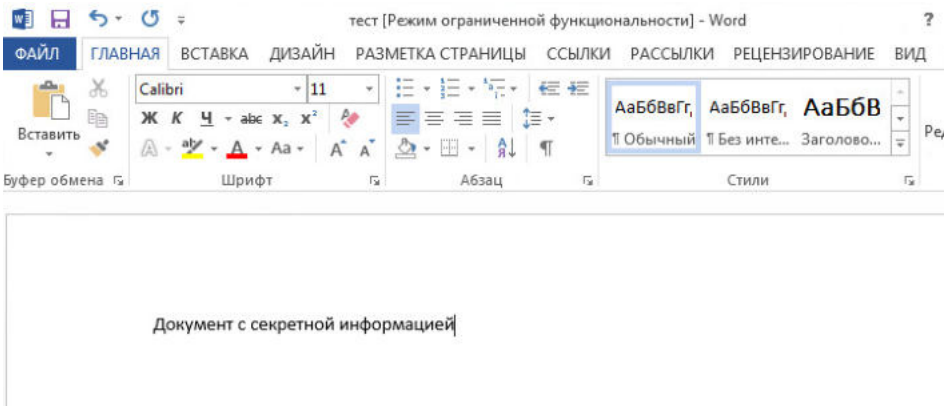
> **Примечание.** Если режим маркировки отключен, регистрация событий печати в журнале Secret Net Studio осуществляется в зависимости от состояния параметра групповой политики, который определяет действие функции теневого копирования для всех принтеров.
>
> Если для параметра "Теневое копирование" указано значение "Определяется настройками принтера", регистрируются события начала и окончания печати документа. При действующем значении "Отключено для всех принтеров" — в журнале регистрируются только события "Печать документа".

8. В окне программы управления в сетевом режиме на панели "Компьютеры" выберите объект ARM1, на вкладке "Настройки" раскройте раздел "Политики / Контроль печати" и убедитесь, что на компьютере ARM1 применяются групповые политики, заданные для сервера безопасности.

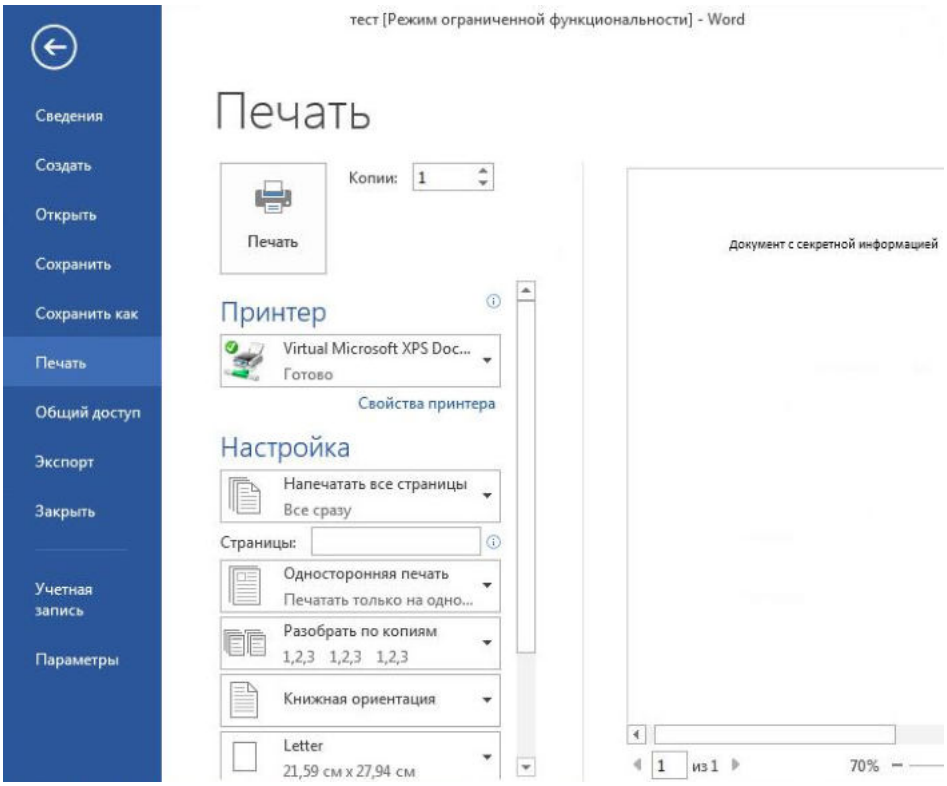
Убедитесь, что то же самое справедливо и для компьютера ARM2.

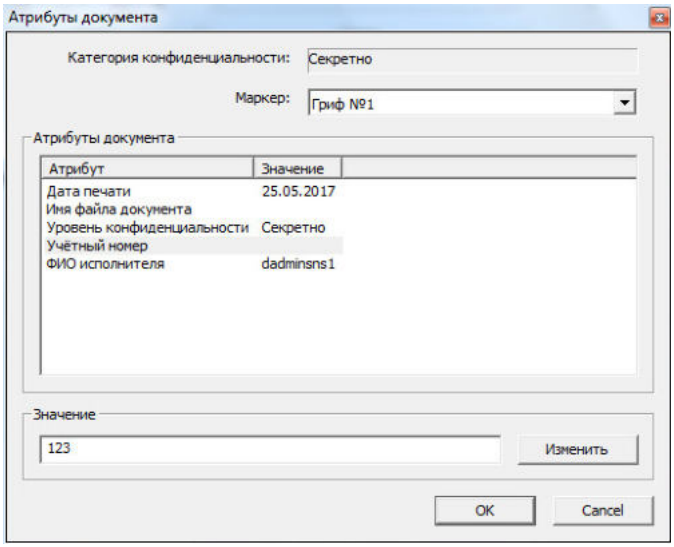


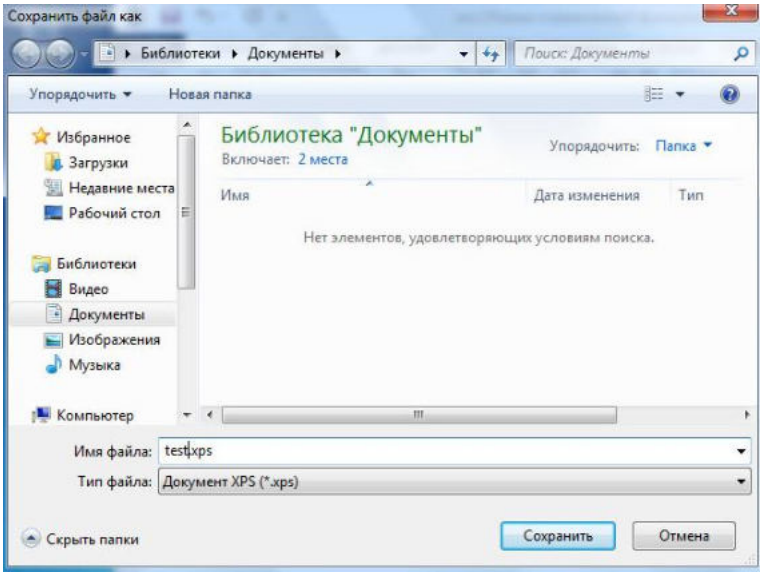
9. Проверьте работу механизмов теневого копирования и маркировки документов при печати. Для этого на ВМ компьютера ARM1 под учетной записью "dadminsns1" откройте любой из документов, которые вы создавали при выполнении лабораторной работы 1 данной главы.



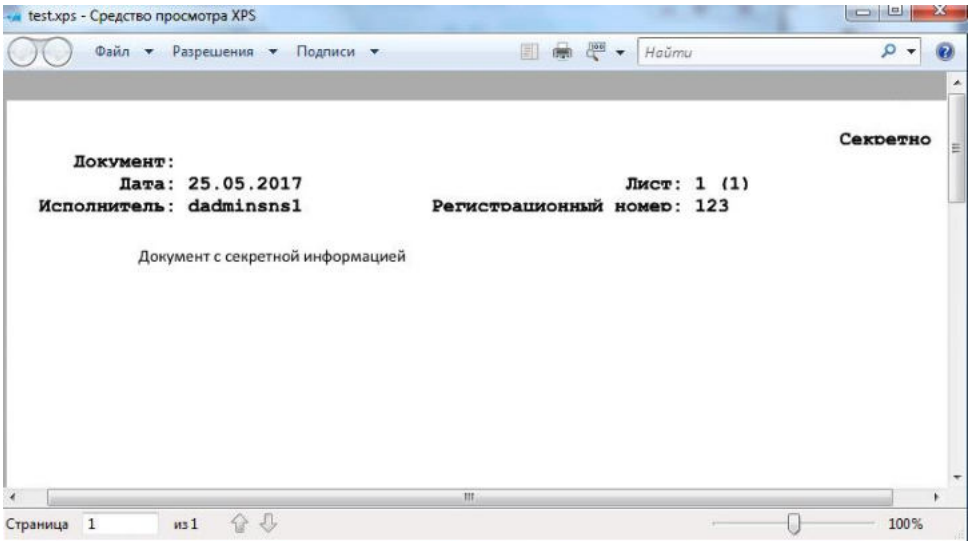
10. Выполните печать документа на установленном по умолчанию виртуальном принтере. В промежуточном диалоговом окне "Атрибуты документа" системы Secret Net Studio введите произвольный учетный номер, а затем сохраните с любым именем файл печати .xps.



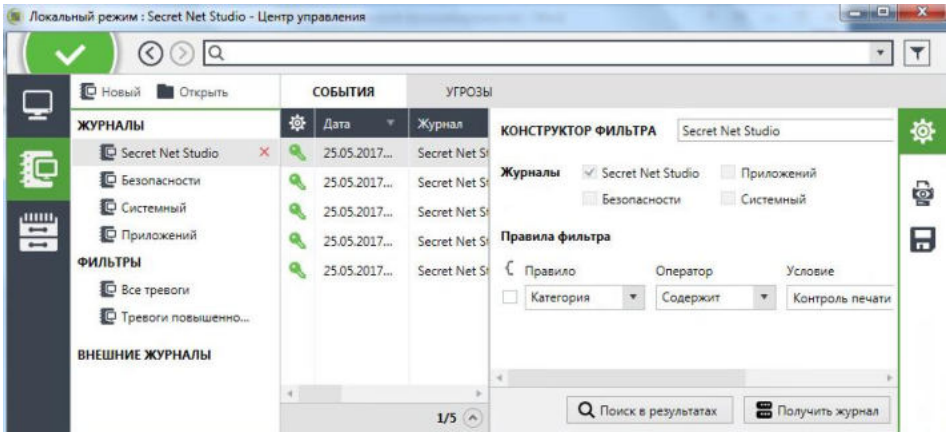




11. Откройте папку, в которую был сохранен xps-файл, просмотрите распечатанный документ и убедитесь в наличии настроенного вами ранее грифа маркировки. Таким образом, маркировка документов проводится в соответствии с заданными ранее параметрами групповой политики.

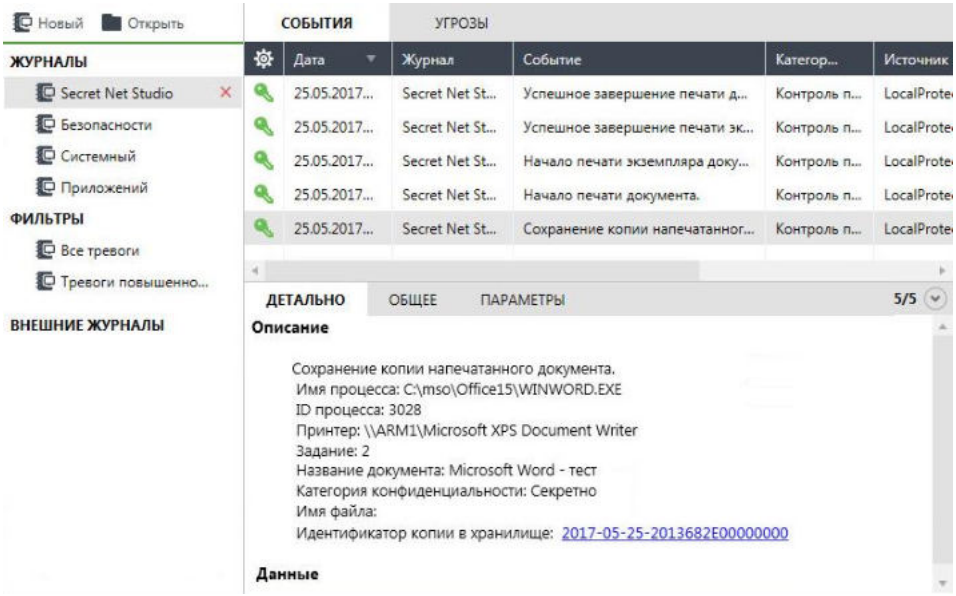


12. Теперь проверьте результат теневого копирования. На ВМ ARM1 откройте программу управления в локальном режиме и в панели "Журналы" сформируйте запрос для отбора записей журнала Secret Net Studio категории "Контроль печати".



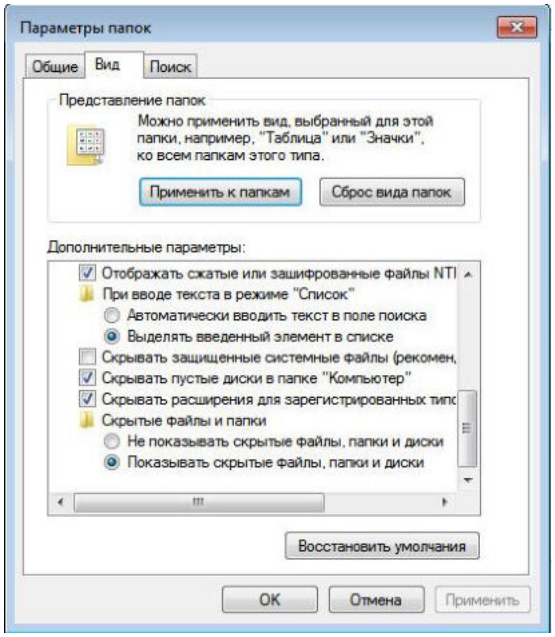
13. Просмотрите полученные записи. Выделите запись "Сохранение копии напечатанного документа". Откройте детальные сведения этой записи и найдите

строку "Идентификатор копии в хранилище" – по этому идентификатору можно найти сохраненную теневую копию документа. Нажмите ссылку в строке "Идентификатор копии в хранилище". Если системная папка "System Volume Information\SnCloneVault\Temp" открылась, то перейдите к п. 15, в противном случае – выполните п. 14.

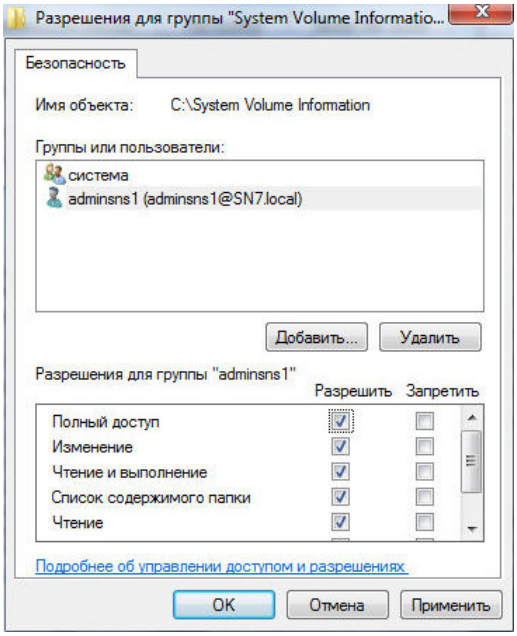


14. Если системный каталог "System Volume Information\SnCloneVault\Temp" не открылся, сделайте предварительные системные настройки:

- установите параметры просмотра скрытых и системных папок и файлов на локальном диске компьютера ARM1 ("Панель управления / Параметры папок");

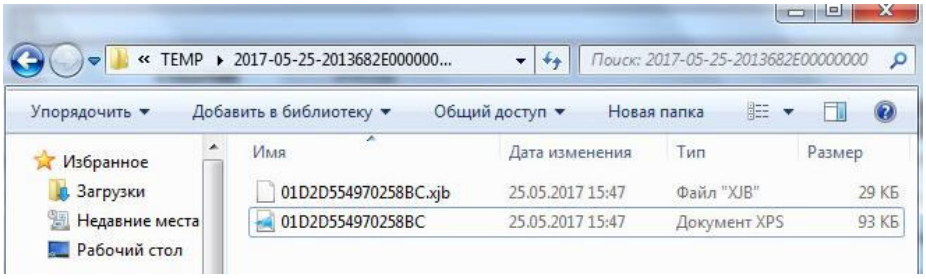


- для каталога "C:\System Volume Information" откройте окно "Свойства" и на вкладке "Безопасность" добавьте в группу пользователей администратора "dadminsns1" и укажите для него разрешение "Полный доступ";



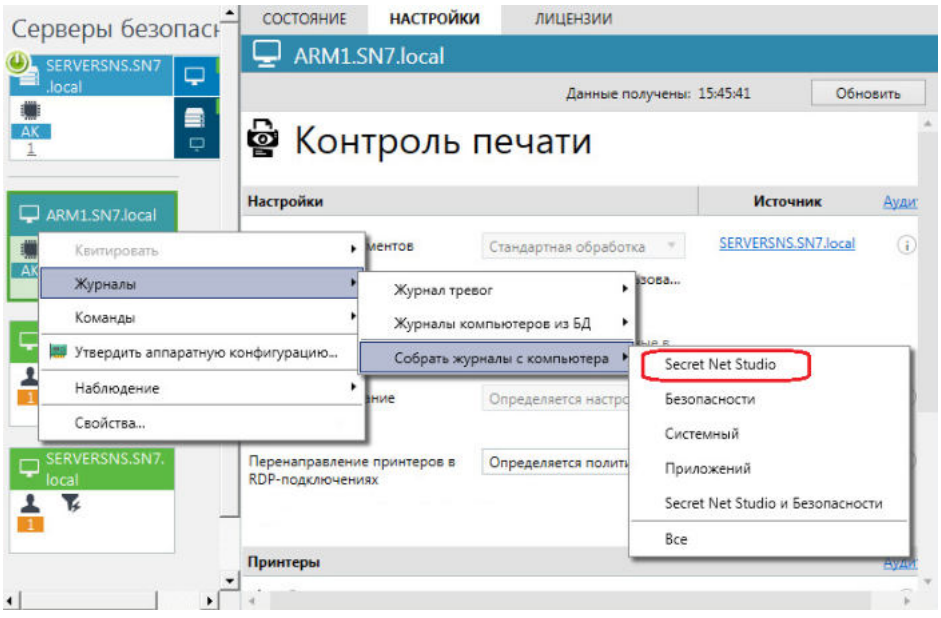
- в программе управления в локальном режиме нажмите ссылку в строке "Идентификатор копии в хранилище". Откроется системная папка "System Volume Information\SnCloneVault\Temp".

15. Откройте папку с идентификатором копии и просмотрите документ теневого копирования.



16. События печати и теневого копирования можно увидеть и в сетевом режиме программы управления, если провести сбор журналов с защищаемых компьютеров.

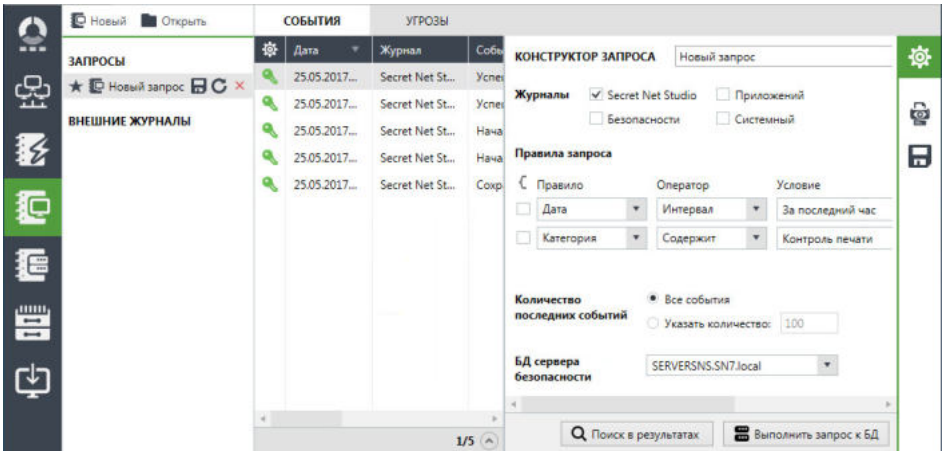
Перейдите в консоль ВМ ARM2. В панели "Компьютеры" вызовите контекстное меню объекта ARM1 и выберите опцию "Журналы / Собрать журналы с компьютеров / Secret Net Studio".



17. Обратите внимание, что в панели событий появится запись об успешном выполнении команды. Напомним, что после передачи в БД сервера безопасности автоматически проводится очистка локальных журналов.

18. Просмотрите полученные записи, свидетельствующие о выполнении теневого копирования. Для этого выберите панель "Журналы станций", сформируйте запрос на отбор записей журнала Secret Net Studio категории "Контроль печати" и просмотрите результат.

    Однако в режиме централизованного управления нельзя просматривать файлы из хранилища теневого копирования. Просмотр теневых копий доступен только локально.



Выполнение лабораторной работы завершено.

Контрольные вопросы

1. Какие подсистемы входят в состав компонента "СЗИ от НСД"?
2. Что такое "список устройств"? По какому принципу организовано хранение объектов в этом списке?
3. Как создается и где сохраняется список устройств на защищаемом компьютере?
4. Для каких видов устройств хранения информации в SNS возможно использовать теневое копирование?
5. Какой инструментарий используется в SNS для управления объектами из списка устройств?
6. В каком журнале регистрируются события категории "Разграничение доступа к устройствам"?
7. Какие ограничения существуют в SNS на применение параметров полномочного и дискреционного управления доступом к каталогам?
8. Как создается и где хранится список принтеров на защищаемом компьютере?
9. Возможно ли в системе защиты SNS централизованное управление параметрами принтеров в рамках доменов, организационных подразделений или серверов безопасности?
10. Какие сведения будут добавляться на листы печатаемого документа при включенном режиме маркировки? Каким образом можно настроить содержание и формат этих сведений в соответствии с действующими в организации требованиями оформления?
11. Для документов каких категорий конфиденциальности возможно применение маркеров при печати?
12. Допустимо ли применение различных параметров использования маркеров на компьютерах в рамках одного домена безопасности?

13. Для каких принтеров будут применяться параметры, заданные в локальной или групповой политике "Настройки по умолчанию" раздела настроек "Политики / Контроль печати / Принтеры"?
14. В каком каталоге и в каком формате сохраняются файлы теневого копирования при печати документов?
15. Каким способом можно просмотреть файлы теневого копирования а) при централизованной работе через "Центр управления", б) при локальной работе через "Локальный центр управления"?
16. В каких журналах и с какой категорией регистрируются события, свидетельствующие о выполнении печати документов и теневого копирования?
17. Какая привилегия, связанная с работой ЗПС, предоставлена в Secret Net Studio группе "Администраторы" по умолчанию?
18. Кому – субъектам или ресурсам – назначаются задания при подготовке к использованию механизма КЦ-ЗПС?
19. В чем различие между мягким и жестким режимами ЗПС? Если для группы компьютеров установлен мягкий режим, а на отдельном компьютере из этой группы параметр "мягкий режим" отключен, то какой режим при этом будет действовать на этом компьютере?
20. Файлы какого формата являются источником данных при добавлении задач ЗПС по журналу в централизованном режиме?
21. Какое количество циклов затирания установлено по умолчанию в Secret Net Studio для механизма затирания данных?

Глава 4
Персональный межсетевой экран

В этой главе мы рассмотрим лицензируемый компонент "персональный межсетевой экран" (ПМЭ), который обеспечивает сетевую защиту и включает в себя следующие подсистемы:

- персональный межсетевой экран – предназначен для защиты серверов и рабочих станций локальной сети от несанкционированного доступа из сети и разграничения сетевого доступа в информационных системах;
- авторизация сетевых соединений и сегментов сети – обеспечивает защиту сетевого взаимодействия между авторизованными абонентами и безопасность обмена данными. Базируется на открытых стандартах протоколов семейства IPsec.

Персональный межсетевой экран

Использование межсетевых экранов (МЭ) является весьма эффективным средством защиты внутреннего периметра корпоративной сети и ее информационных ресурсов. В отличие от традиционных, "периметровых" МЭ, реализованный в SNS распределенный межсетевой экран предназначен именно для защиты информации внутри сети организации, функционирует непосредственно на ее защищаемых объектах (сервер БД, рабочие места руководителей или сотрудников и т.д.) и обеспечивает их защиту от сетевых угроз со стороны внешнего и внутреннего нарушителей.

Механизм защиты МЭ обеспечивает фильтрацию сетевого трафика на сетевом, транспортном и прикладном уровнях. Для этого формируются специальные правила, которые обладают широким диапазоном настроек и позволяют ограничивать сетевые соединения на следующих уровнях:

- пользователи;
- компьютеры;
- группы пользователей (компьютеров);
- параметры соединения – служебные и прикладные протоколы, порты, сетевые интерфейсы, приложения, дни недели, время суток;
- маска фильтра – возможность поиска по фрагменту содержимого пакета.

Для входящего трафика проверка правил производится агентами МЭ на компьютерах – получателях IP-пакетов, для исходящего – на компьютере-отправителе. Реализованы следующие группы правил:

- правила доступа – правила этой группы используются для ограничения доступа к сетевым сервисам защищаемого компьютера. При этом производится процедура аутентификации УЗ отправителей и получателей IP-пакетов, отслеживается ответный трафик (т.е. правила учитывают направление соединения, а не отдельно взятых пакетов, например, соединение от клиента к серверу, а пакет может идти в обратную сторону, так как это ответ сервера на запрос клиента). Для настройки правил используются данные о параметрах соединения с защищаемым компьютером (наименования протоколов, портов TCP/IP и т.п.). В случае необходимости в настройках соединения можно установить параметр "Требовать защищенное соединение", и сетевое соединение по незащищенному каналу устанавливаться не будет (при наличии лицензии на механизм авторизации сетевых соединений);
- прикладные правила – используются для обеспечения фильтрации доступа к общим папкам защищаемого компьютера со всем их содержимым (например, \\server\share), а также сетевых соединений по протоколу Named Pipes. Гранулярное разграничение доступа к подпапкам общих папок (например, \\server\share\folder) данной группой правил не обеспечивается. При использовании этих правил производится процедура аутентификации УЗ, отслеживается ответный трафик. При создании прикладных правил имя общей папки вводится без имени компьютера, на котором она находится (т.е. если сетевой путь к папке – \\server\share, то в правиле следует указать share). При этом в имени можно использовать подстановочные знаки: ? – один сим-

вол и * (звездочка) – несколько символов. Если создать запрещающее правило для учетной записи everyone, в котором в качестве имени общей папки ввести символ *, то для всех пользователей доступ к общим папкам данного компьютера будет запрещен. В этом случае для того, чтобы пользователи имели возможность просматривать список общих папок на данном компьютере, необходимо создать разрешающее правило для общей папки IPC$;

- системные правила – используются для ограничения доступа к защищаемым компьютерам по сетевым протоколам, перечень которых определен в документе RFC 1700 (поддерживаются все IP-based протоколы). При использовании данного вида правил аутентификация отправителей и получателей IP-пакетов не производится, ответный трафик не отслеживается;
- сетевые протоколы – настройки сетевых протоколов используются для управления соединениями на сетевом уровне. С помощью этих настроек можно разрешить или запретить сетевые соединения с защищаемыми компьютерами по следующим протоколам – IPv4, IPv6, Novell IPX, а также некоторым протоколам с устаревшим форматом Ethernet-кадра (LLC, IPX). По умолчанию работа этих протоколов запрещается, за исключением протокола IPv4. Не рекомендуется разрешать доступ по остальным протоколам, так как сетевой трафик по ним не контролируется межсетевым экраном Secret Net Studio. Эти настройки имеют более высокий приоритет, чем правила доступа к сетевым сервисам, прикладные и системные правила. Подробнее о настройке по сетевым протоколам см. в руководстве администратора по настройке и эксплуатации сетевой защиты.

Правила доступа регулируют доступ аутентифицированных и анонимных пользователей к сетевым сервисам защищаемого компьютера. Данные правила имеют более высокий приоритет, чем прикладные, и по умолчанию применяются для всех сетевых интерфейсов компьютера.

По умолчанию правила доступа к объектам обрабатываются в порядке их создания и расположения в таблице правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы.

Системные правила контролируют соединения с данным компьютером по протоколам семейства TCP/IP и имеют более высокий приоритет, чем правила доступа к сетевым сервисам и прикладные правила.

Прикладные правила регулируют доступ аутентифицированных и анонимных пользователей к общим папкам и именованным каналам на данном компьютере. Эти правила имеют минимальный приоритет.

В настройках МЭ предусмотрена также возможность защиты протокола ICMP для организации обмена сообщениями по данному протоколу (по умолчанию отключена).

При изменении правил и их параметров новые настройки вступают в силу в течение 4–6 минут после сохранения изменений.

На этапе ввода системы защиты в эксплуатацию рекомендуется использовать режим обучения, который позволяет составить на основе информации о сетевой активности приложений базовый набор правил доступа, необходимый для функционирования защищаемого компьютера. Если данный режим включен, то разрешается весь сетевой трафик. Для каждого пакета проверяется наличие правила фильтрации (правила с реакцией "по умолчанию" не проверяются). Если правила нет, оно добавляется как разрешающее для каждого из приложений. При этом однотипные правила заменяются одним правилом, включающим в себя все объединенные. Подробнее об использовании режима обучения см. в соответствующем разделе руководства администратора по настройке и эксплуатации сетевой защиты.

Авторизация сетевых соединений

Аутентификация пользователей в Secret Net Studio проводится собственным алгоритмом, основанным на протоколе Kerberos, который нечувствителен к попыткам перехвата паролей и атакам типа "Man in the Middle". С помощью данного механизма удостоверяются субъекты доступа и защищаемые объекты – это предотвращает несанкционированную подмену (имитацию) защищаемой информационной системы с целью осуществления некоторых видов атак.

Механизм аутентификации сетевых соединений выполняет следующие функции:

- авторизация сетевых соединений – добавляет подписи для сетевых пакетов, удовлетворяющих правилам, полученным с сервера управления и авторизации. Осуществляет анализ подписей входящих пакетов и передачу информации в модуль межсетевого экранирования для осуществления фильтрации по правилам;
- контроль неизменности передаваемых сетевых пакетов – позволяет контролировать аутентичность, целостность и конфиденциальность передаваемых данных;
- шифрование трафика – механизм аутентификации сетевых соединений выполняет кодирование трафика.

В Secret Net Studio реализован механизм защиты сетевого взаимодействия между авторизованными абонентами, который базируется на открытых стандартах протоколов семейства IPsec и обеспечивает безопасность обмена данными. В текущей версии используются следующие протоколы:

- протокол AH (Authentication Header) – позволяет гарантировать аутентичность и целостность передаваемых данных каждого IP- пакета и, как следствие, обеспечивает защиту от атак типа "Man in the Middle";
- протокол ESP (Encapsulating Security Payload) – используется для шифрования и контроля целостности передаваемых данных;
- протокол ISAKMP (Internet Security Association and Key Management Protocol) – предназначен для обмена ключами и согласования параметров соединения.

Реализовано несколько режимов настройки. Администратор может для каждого защищаемого компьютера указать индивидуальный режим защиты.

По умолчанию параметры механизма авторизации сетевых соединений настроены следующим образом:

- включен режим подписи пакетов с уровнем подписи "Пакет целиком";
- включен режим защиты от replay-атак;
- сценарий определения пользователя SMB-соединения – от имени учетной записи пользователя.

Защита и целостность передаваемых данных обеспечиваются:

- режимом подписи пакетов – протокол AH в транспортном режиме, алгоритм хэширования HMAC-MD5;
- режимом шифрования и контроля целостности – протокол ESP в транспортном режиме, алгоритм кодирования – AES CBC 128, алгоритм хэширования HMAC-SHA;
- режимом защиты от replay-атак – ISAKMP-ассоциация.

Примечание. В текущей версии системы одновременное использование протоколов AH и ESP не предусмотрено.

В настройках механизма авторизации для определения пользователя SMB-соединения реализованы следующие сценарии:

- от имени учетной записи компьютера;
- от имени учетной записи пользователя – инициатора соединения. При этом для остальных пользователей можно либо разрешить, либо блокировать установленное SMB-соединение.

Деятельность всех пользователей, которым разрешается использовать SMB-соединение, осуществляется от имени инициатора данного соединения. Если инициатор неактивен более 30 секунд, то пользователем соединения считается следующий по порядку пользователь или сервис, которому требуется данное SMB-соединение. При этом действует следующий приоритет предоставления соединений (от низшего к высшему): анонимные пользователи, сервисы, авторизованные пользователи Secret Net Studio.

При реализации сценария, в котором пользователем соединения считается его инициатор, остальным пользователям:

- разрешается пользоваться SMB-соединением – деятельность всех низкоприоритетных абонентов осуществляется от имени высокоприоритетного;

- запрещается пользоваться SMB-соединением – при запросе соединения высокоприоритетным абонентом оно запрещается для низкоприоритетных.

Настройка параметров получения IP-адресов компьютера позволяет средствам сетевой защиты Secret Net Studio идентифицировать компьютер не только по имени, но и по его IP-адресу. Эта возможность может быть использована, например, в случае, если имя компьютера по каким-либо причинам автоматически не преобразуется в IP-адрес.

Подробнее о настройке и использовании механизма авторизации сетевых соединений см. в руководстве администратора по настройке и эксплуатации сетевой защиты.

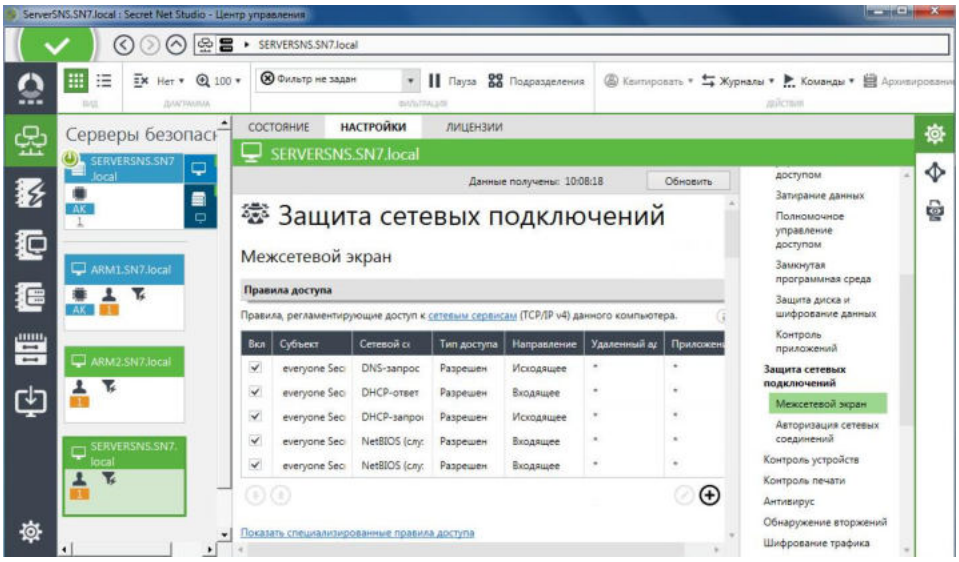
Лабораторная работа №1 "Персональный межсетевой экран"

Настройка межсетевого экрана осуществляется централизованно в программе управления на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров. Программа управления в локальном режиме непосредственно на защищаемом компьютере позволяет только просматривать централизованно заданные настройки.

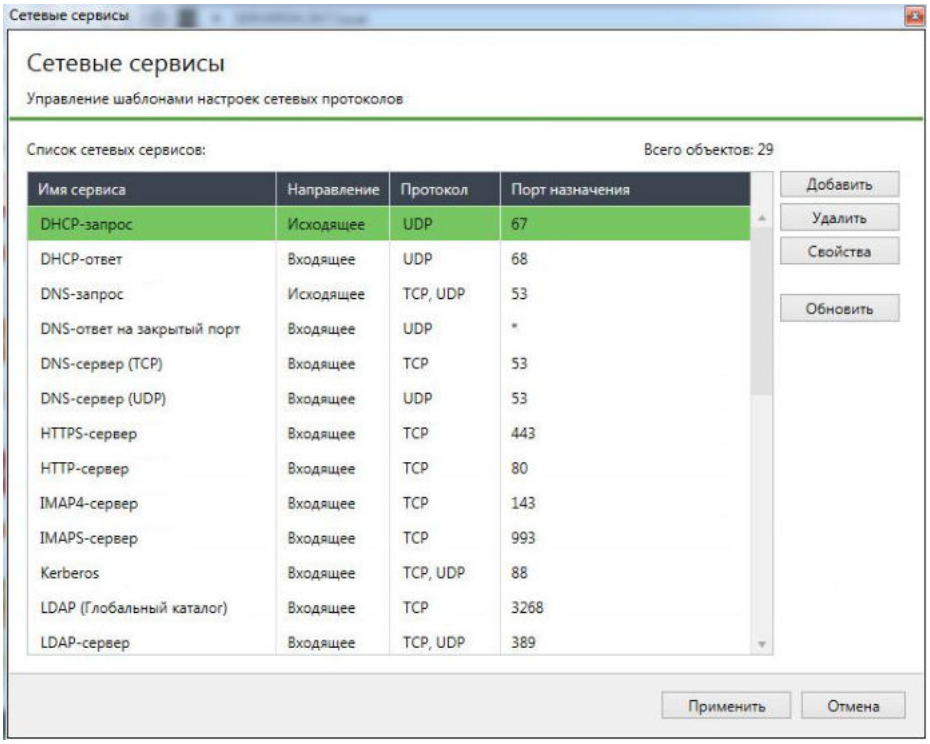
В соответствующем разделе главы 4 описаны группы правил, использующихся для управления доступом, а в данной лабораторной работе рассматриваются некоторые практические примеры их применения.

1. Ознакомьтесь с параметрами настройки политик МЭ. Для этого:

- в окне консоли ВМ ARM2 откройте программу управления в сетевом режиме;
- в панели "Компьютеры" выберите объект ServerSNS, который не помечен значком  и раскройте панель его свойств;
- на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Межсетевой экран" – в средней части экрана появится область настройки выбранных параметров.

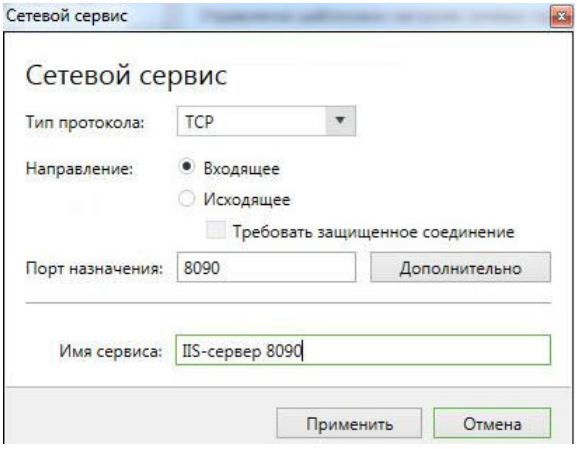


2. Обратите внимание, что первыми в перечне политик следуют правила доступа, которые, как уже отмечалось в главе 4, регулируют доступ пользователей к сетевым сервисам защищаемого компьютера. С помощью кнопки  ознакомьтесь с описанием этой группы политик, а затем нажмите над таблицей правил ссылку сетевых сервисов – откроется диалоговое окно "Сетевые сервисы".



3. Просмотрите список сетевых сервисов – это шаблоны наиболее распространенных настроек сетевых протоколов. Добавьте новый сетевой сервис для доступа к серверу IIS по порту 8090 (в качестве этого сервера будет выступать сервер безопасности). Для этого нажмите кнопку "Добавить" и в открывшемся диалоговом окне заполните следующие параметры:

- "Тип протокола" – TCP;
- "Направление" – "Входящее";
- "Порт назначения" – введите **8090**. При необходимости можно использовать символ "*" – для всех портов или указать диапазон значений;
- "Требовать защищенное соединение" – оставьте пустым, чтобы соединение устанавливалось по незащищенному каналу;
- "Имя сервиса" – введите "IIS-сервер 8090".



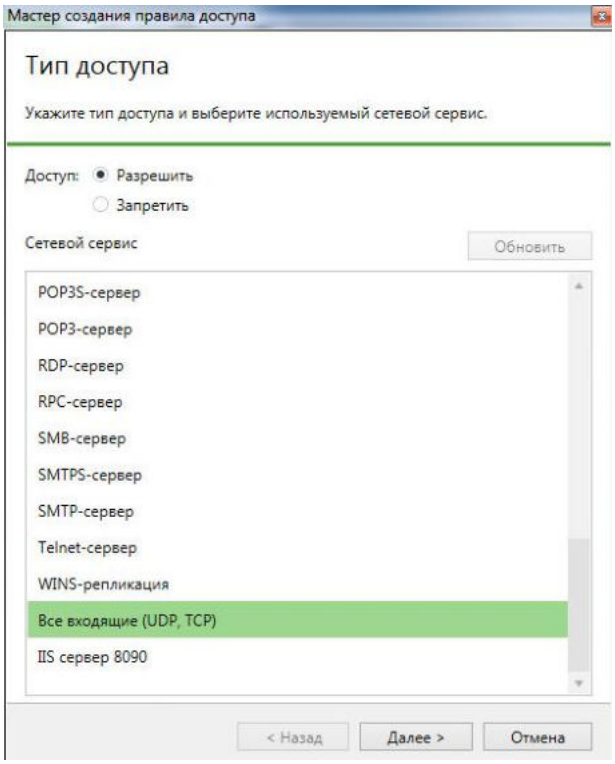
4. Нажмите кнопку "Применить". Запись нового сетевого сервиса появится в диалоговом окне "Сетевые сервисы". Далее для созданного сервиса можно прописать правила фильтрации доступа (см. ниже).

5. Закройте окно "Сетевые сервисы" и вернитесь к перечню политик межсетевого экрана. Добавим запрет RDP-подключения к серверу ServerSNS с компьютера ARM1 (192.168.254.21).

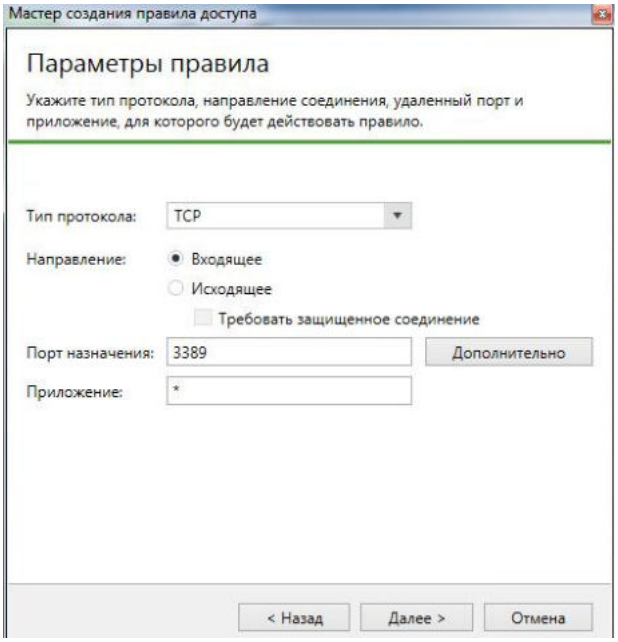
Для дальнейшего выполнения лабораторной работы убедитесь, что RDP-подключение к ServerSNS доступно для всех пользователей с ВМ ARM1 и ARM2. Если это не так, настройте удаленное подключение на сервере.

6. Чтобы добавить новое правило, под таблицей "Правила доступа" нажмите кнопку "Добавить" ⊕. Откроется окно мастера создания правила.

   Обратите внимание, что в списке сетевых сервисов отображаются заданные по умолчанию и добавленные администратором вручную сервисы.



7. Установите параметры: "Доступ" – "Запретить", "Сетевой сервис" – "RDP-сервер". Нажмите кнопку "Далее". На следующем шаге мастера задаются параметры соединения. Их значения по умолчанию соответствуют выбранному на предыдущем шаге сетевому сервису.



   Если необходимо изменить порт, то можно указать нужный номер порта или задать диапазон номеров либо использовать символ "*" (см. п. 3).

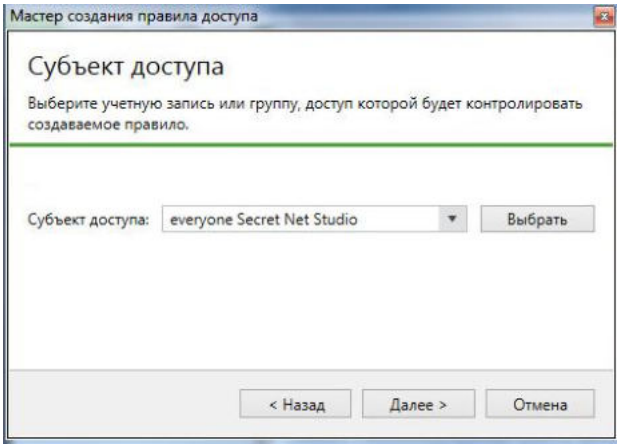
   В поле "Приложение" можно указать путь к исполняемому файлу, для которого действует правило. При этом можно использовать системные переменные Windows. Символ "*" (звездочка) задает действие для всех приложений.

Созданное правило будет анализировать сетевой трафик для приложения, работающего непосредственно на защищаемом компьютере.

Внимание! Для корректной работы правил доступа рекомендуется указывать полный путь к исполняемому файлу приложения.

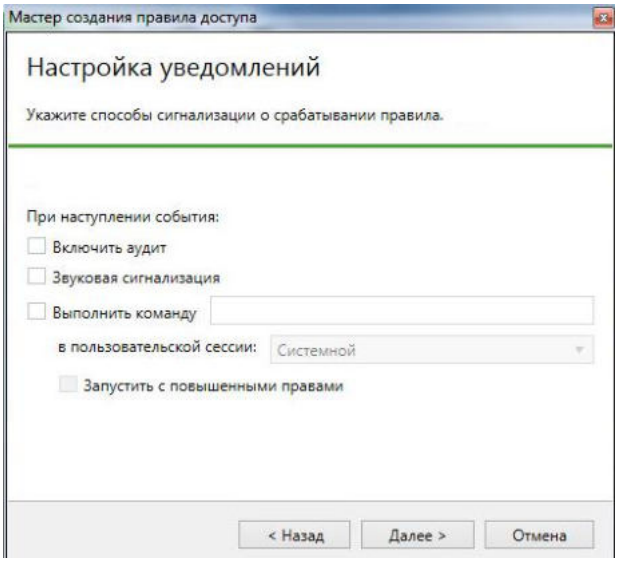
8. Оставьте заданные по умолчанию параметры правила и нажмите кнопку "Далее". На следующем шаге можно выбрать пользователя или группу пользователей, доступ к которой будет контролироваться.

Данная возможность есть только при наличии отдельной лицензии на использование механизма авторизации сетевых соединений. Без такой лицензии в качестве пользователя будет задан “everyone”, т.е. фильтрация трафика будет в режиме обычного МЭ.

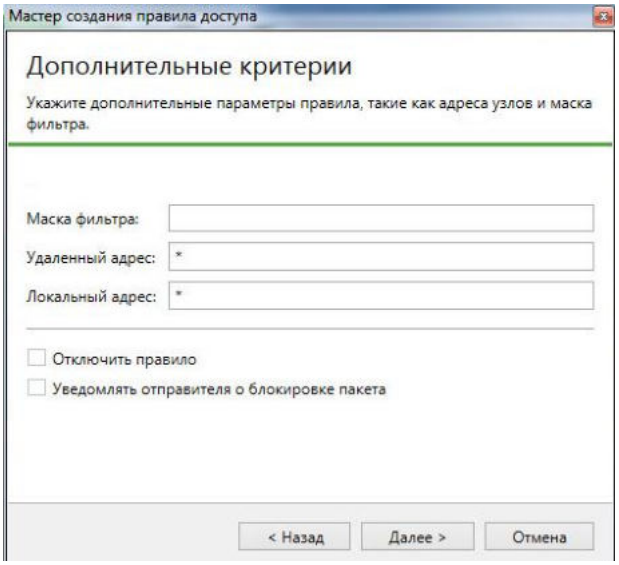


9. Нажмите кнопку "Далее". На этом шаге мастера можно настроить уведомления о срабатывании правила.

Поле "Выполнить команду" оставьте пустым. Оно используется, если на защищаемом компьютере при срабатывании правила требуется автоматически запускать исполняемый файл. Тогда ниже, в текстовом поле следует указать полный путь к исполняемому файлу (с параметром), например, C:\windows\notepad.exe 1.txt.

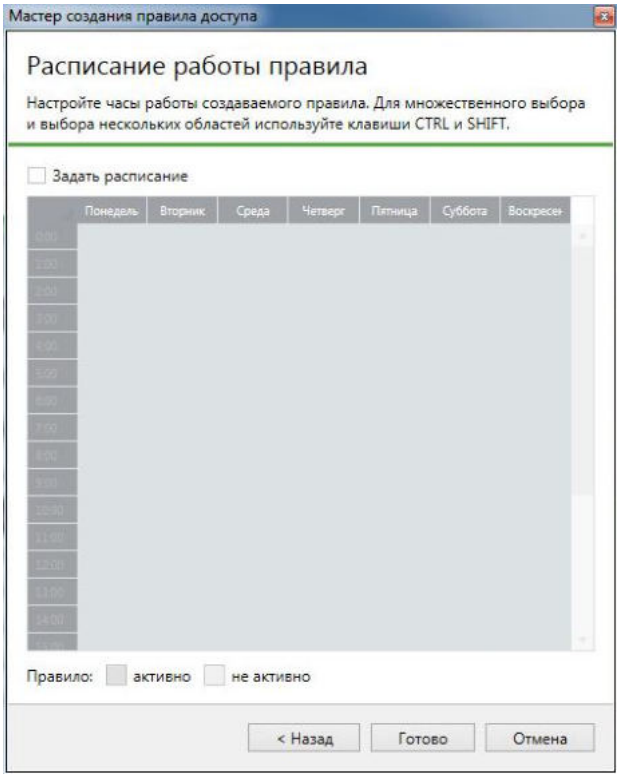


10. Чтобы фиксировать в журнале возникающее при срабатывании правила событие, установите отметку в поле "Включить аудит" и нажмите кнопку "Далее". На следующем шаге настройте дополнительные параметры правила:

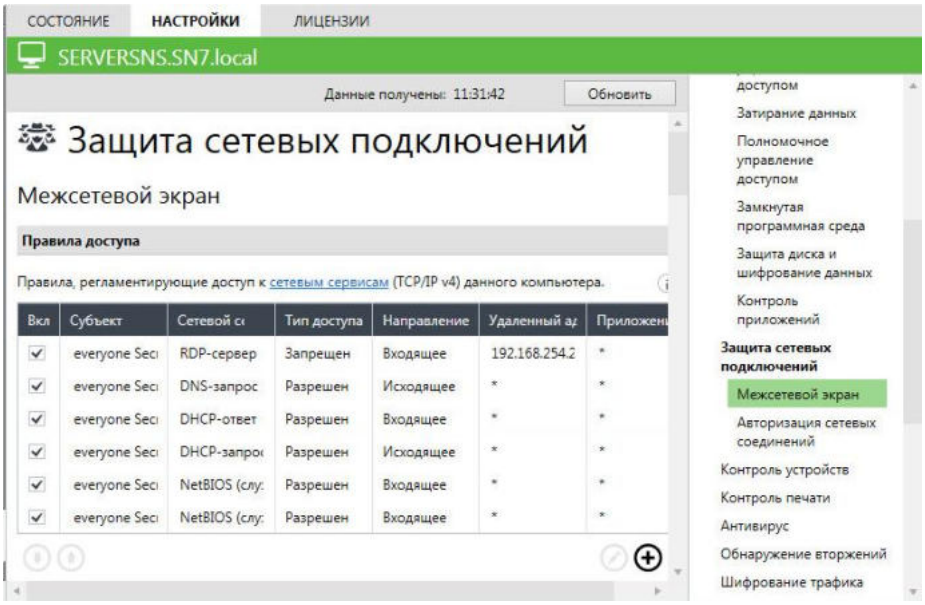


- "Маска фильтра" – оставьте пустым. При необходимости здесь указывается контекст для поиска IP-пакетов. Правилом будут обрабатываться только IP-пакеты, в теле которых содержится введенное значение;
- "Удаленный адрес" – введите IP-адрес компьютера ARM1 – **192.168.254.21**. Символ "*****" задает действие правила для всех адресов. Разделитель ";" используется, если нужно указать несколько диапазонов адресов или подсетей, а сами диапазоны задаются через дефис;
- "Уведомлять отправителя о блокировке IP-пакета" – оставьте пустым. Поле доступно для изменений в правилах с типом доступа "Запретить" и направлением трафика "Входящее". Если отметка установлена, то отправитель получает уведомления о блокировке пакетов. В случае срабатывания правила для протокола TCP будут генерироваться RST-пакеты, для всех остальных протоколов (кроме ICMP, AH, ESP) – пакеты ICMP (тип Destination Unreachable).

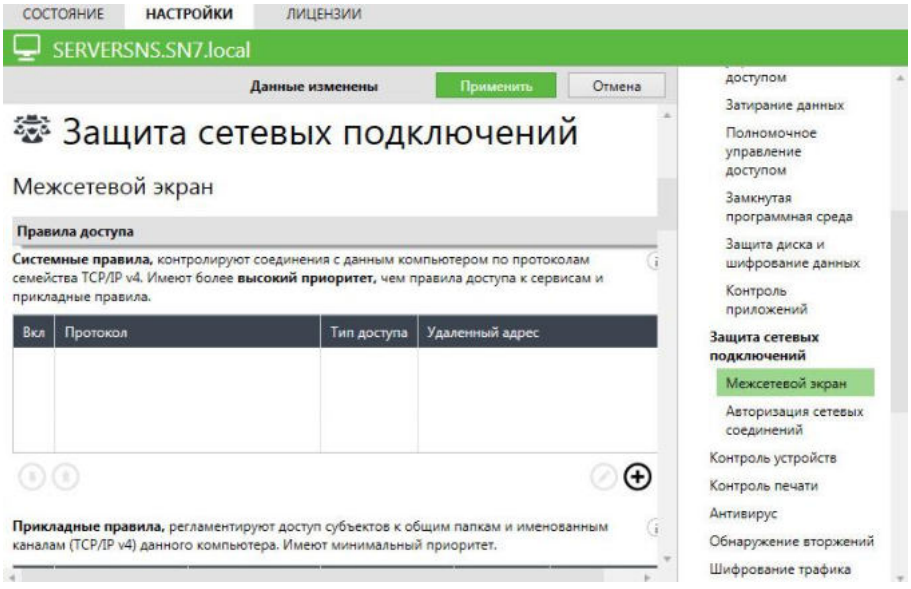
11. Нажмите кнопку "Далее". На завершающем шаге мастера можно настроить расписание работы правила. При этом время работы для правила определяется часовым поясом защищаемого компьютера.



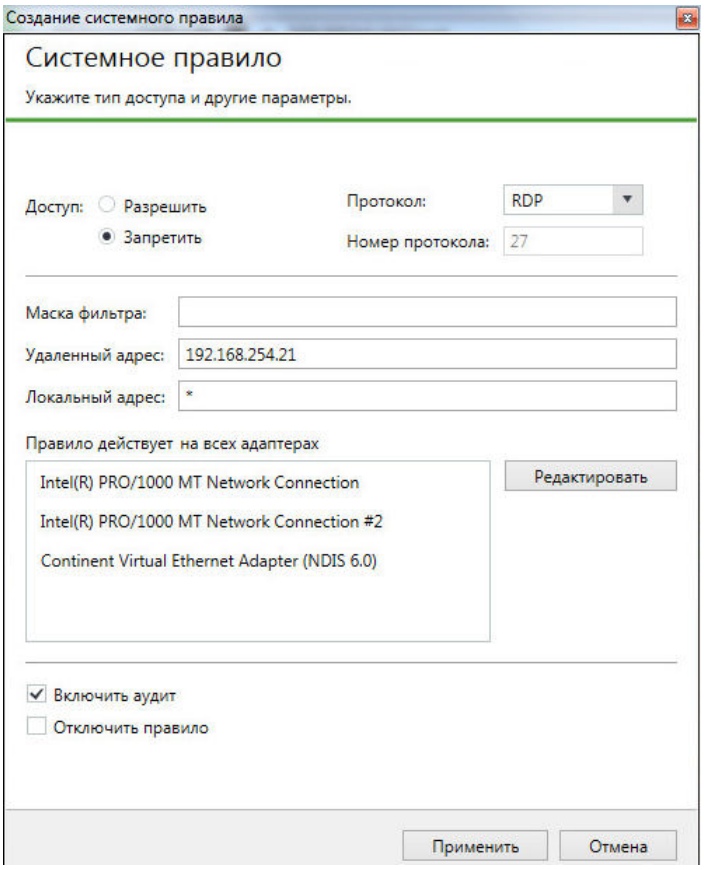
12. Нажмите кнопку "Готово". Правило будет создано и отобразится в списке правил. На вкладке "Настройки" нажмите кнопку "Применить" Применить. Как упоминалось в главе 4, новые настройки вступают в силу в течение 4–6 минут после сохранения изменений, и наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы.



13. Используя описание пп. 6–12, добавьте следующие правила фильтрации доступа для созданного вами ранее сетевого сервиса "IIS-сервер 8090":
    - запретить доступ к порту 8090 клиентам группы Everyone (для всех пользователей) с произвольными IP-адресами;
    - разрешить доступ к порту 8090 клиентам группы Everyone только с одного компьютера ARM2 с IP-адресом 192.168.254.22.
14. С помощью расположенных под таблицей кнопок "Вниз" и "Вверх" установите приоритет разрешающего правила выше, чем запрещающего.
15. На вкладке "Настройки" нажмите кнопку "Применить" Применить. Теперь, если на IIS-сервере создать http веб-узел для порта 8090, доступ к нему будет возможен только с компьютера ARM2. В журнале событий Secret Net Studio будут регистрироваться попытки доступа с IP-адресами отправителя и получателя пакетов.
16. Ознакомьтесь с настройками дополнительных категорий правил. Для этого под таблицей "Правила доступа" нажмите кнопку-ссылку "Показать специализированные правила доступа" и прокрутите перечень настроек политик вниз, чтобы увидеть таблицу "Системные правила".

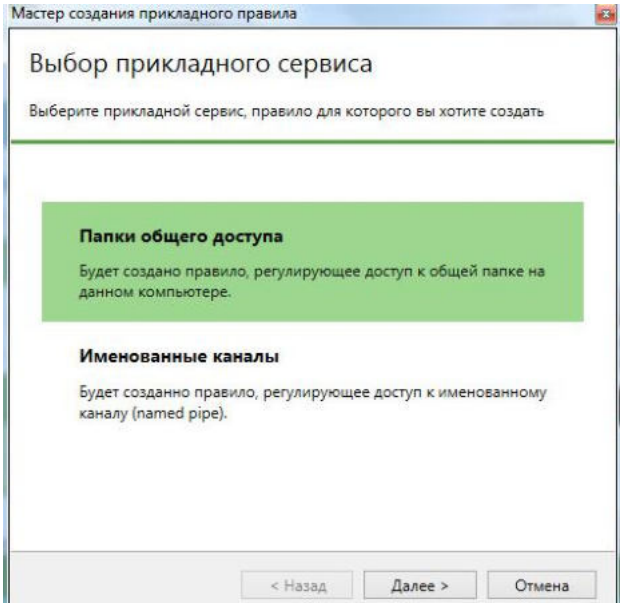


17. Системные правила являются более общими по сравнению с правилами доступа. Ниже на рисунке показан пример настройки рассмотренного выше запрета доступа к серверу ServerSNS по RDP-протоколу.

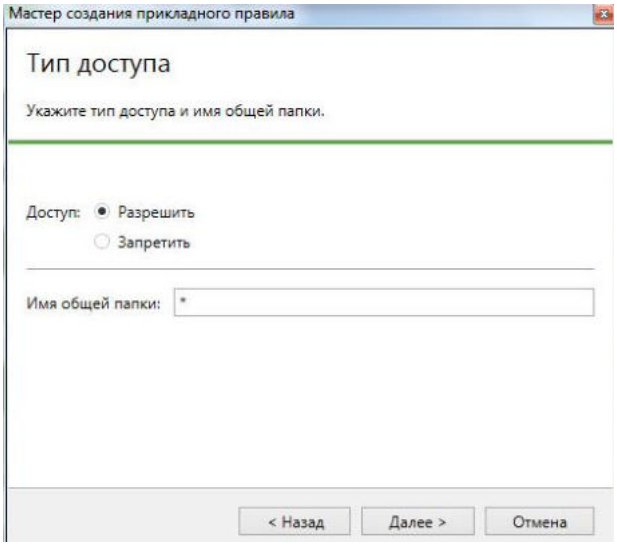


Самостоятельно опишите в качестве примера системных правил созданные вами в пп. 13–14 правила.

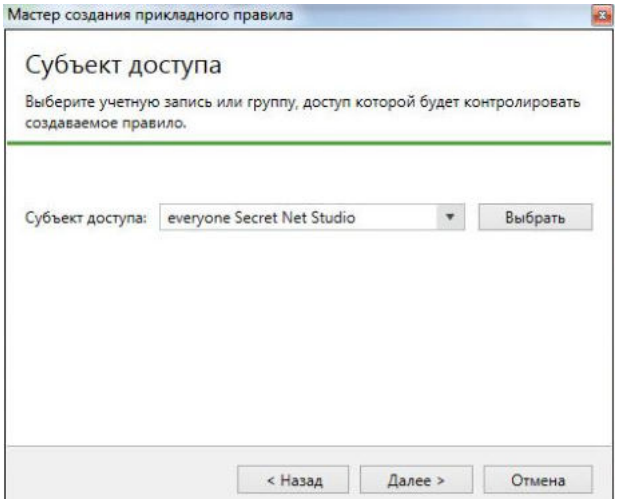
18. Создайте прикладное правило, запрещающее доступ с компьютера ARM1 (192.168.254.21) к общедоступной папке "user_files", расположенной на сервере ServerSNS. Для этого под таблицей "Прикладные правила" нажмите кнопку "Добавить" ⊕ и в окне мастера создания правила выполните следующие настройки:



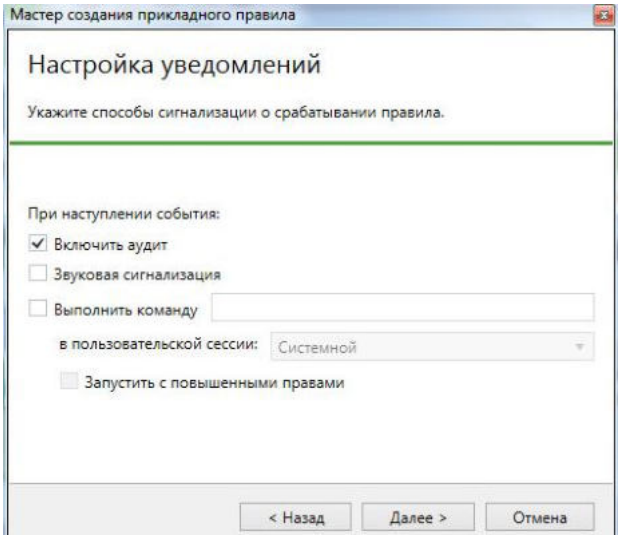
- на начальном шаге выберите сервис "Папки общего доступа" и нажмите кнопку "Далее";



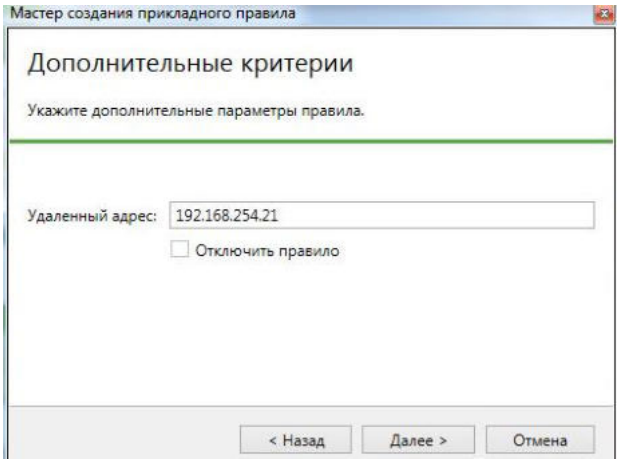
- на следующем шаге установите: "Тип доступа" – "Запретить", "Имя общей папки" – введите **user_files**;
- нажмите кнопку "Далее". На следующем шаге мастера можно выбрать учетные записи, для которых действует правило;



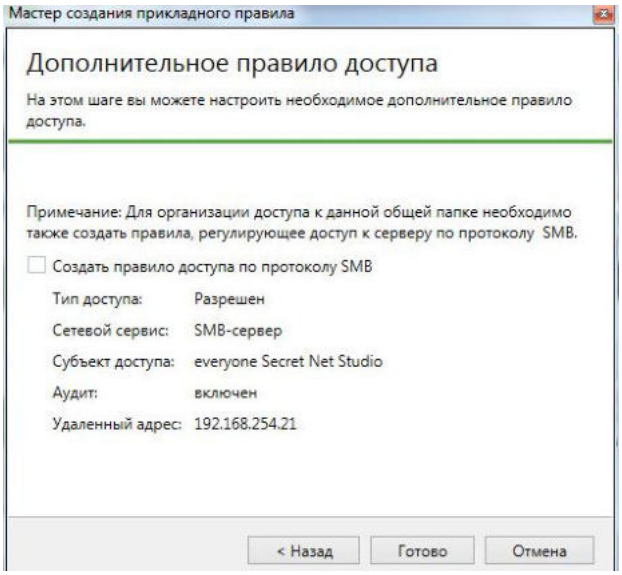
- нажмите кнопку "Далее". На следующем шаге нужно настроить уведомления о срабатывании правила. Выберите поле "Включить аудит";



- нажмите кнопку "Далее". На следующем шаге настраиваются дополнительные параметры. В поле "Удаленный адрес" введите **192.168.254.21** – адрес компьютера ARM1;



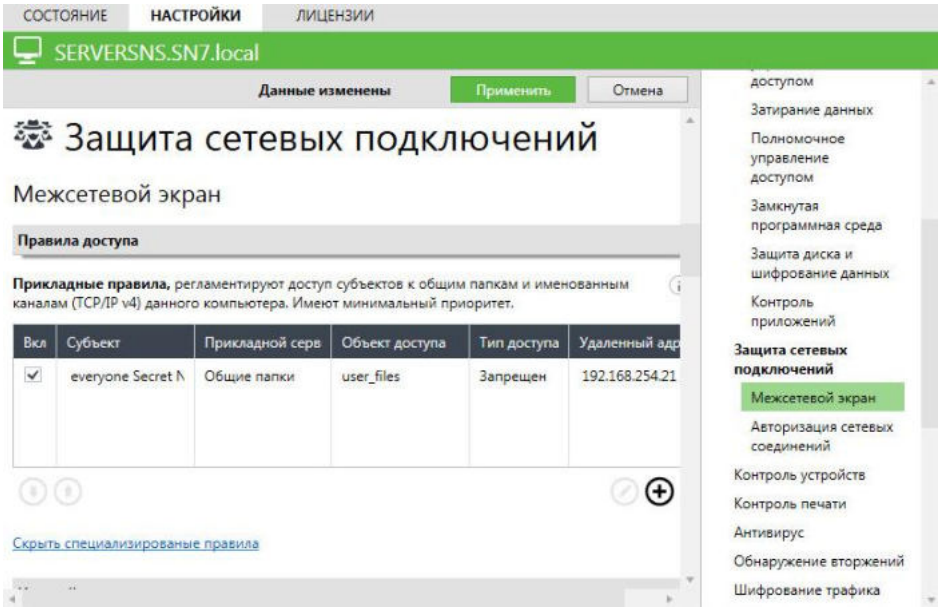
- нажмите кнопку "Далее". На предпоследнем шаге можно настроить расписание. Еще раз нажмите кнопку "Далее" – откроется завершающее окно для создания дополнительного правила доступа;



- установите отметку в поле "Создать правило доступа по протоколу SMB", чтобы создать правило доступа, разрешающее прохождение пакетов по протоколу TCP на порт 445 (и/или 139) для учетной записи (или группы), указанной в прикладном правиле. Это требуется, поскольку для корректной работы прикладных правил необходимо настроить правила прохождения IP-пакетов на транспортном уровне – по протоколу SMB;

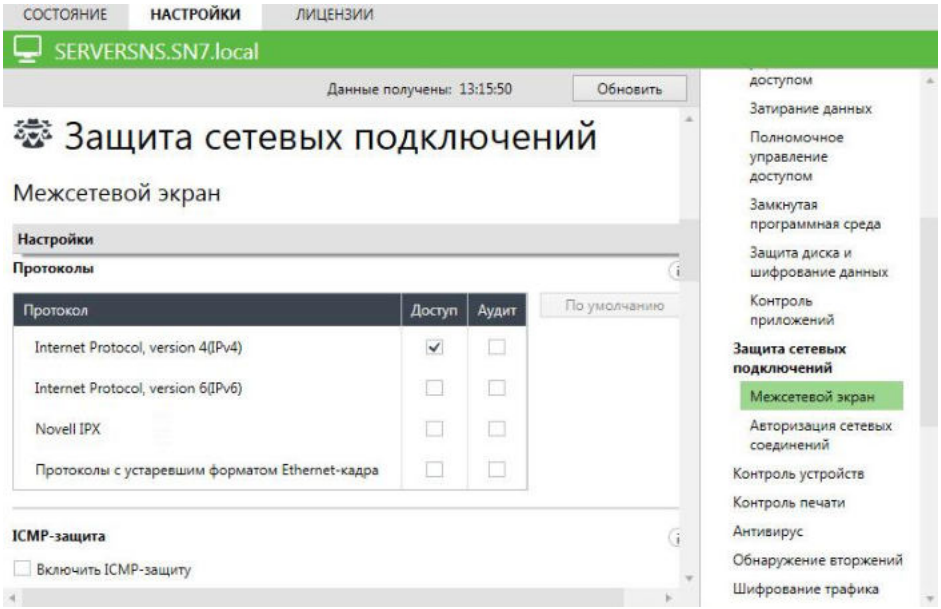
> **Внимание!** Если прохождение пакетов по протоколу SMB запрещается системными правилами или правилами доступа, то прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.

- нажмите кнопку "Готово". В список прикладных правил будет добавлено новое правило. Кроме того, в список правил доступа будет добавлено дополнительное правило, разрешающее использование SMB для учетной записи (группы), указанной в прикладном правиле.

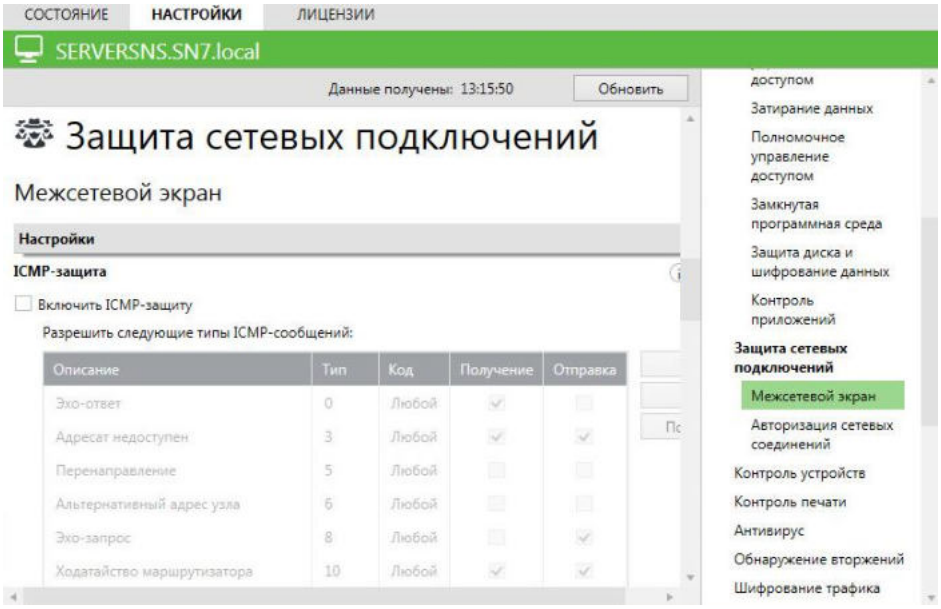


19. На вкладке "Настройки" нажмите кнопку "Применить" Применить. Под таблицей "Прикладные правила" нажмите кнопку-ссылку "Скрыть специализированные правила".

20. В группе настроек "Протоколы" убедитесь, что по умолчанию доступ к защищаемым компьютерам разрешен только по протоколу IPv4. Как указывалось в главе 4, эти настройки имеют более высокий приоритет, чем все рассмотренные выше правила.



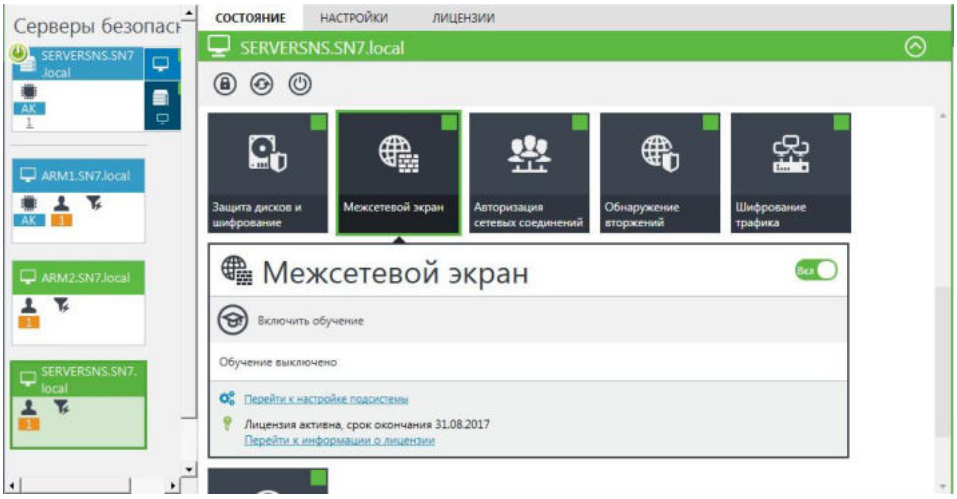
21. Ознакомьтесь с группой настроек "ICMP-защита", которая используется для организации обмена сообщениями по данному протоколу. По умолчанию режим управления пакетами протокола ICMP выключен.



22. Убедитесь, что при выключенной для сервера ServerSNS ICMP-защите с компьютеров ARM1 и ARM2 команда **ping 192.168.254.2** проходит успешно, затем включите ICMP-защиту, нажмите кнопку "Применить" Применить и подождите около 4–6 минут, пока настройки применятся. Повторно используйте команду **ping** и сравните результат.

23. Протестируйте работу созданных вами ранее правил – запрета RDP-подключения к серверу ServerSNS с компьютера ARM1 и запрета обращения к общедоступной папке "user_files" с компьютера ARM1. Просмотрите соответствующие события в локальном журнале Secret Net Studio компьютера ServerSNS (события категории "Проверка ПРД" с типом "Аудит отказов").

24. В программе управления на компьютере ARM2 на панели свойств сервера ServerSNS откройте вкладку "Состояние" и выберите плитку компонента "Межсетевой экран".



Обратите внимание, что данная вкладка позволяет включать/отключать на защищаемом компьютере работу компонента "Межсетевой экран", а также управлять работой режима обучения. Кроме того, с помощью кнопки-ссылки "Перейти к настройке подсистемы" можно перейти к настройке политик межсетевого экрана, с которыми мы познакомились в данной лабораторной работе.

Выполнение лабораторной работы завершено.

Лабораторная работа №2 "Авторизация сетевых соединений"

В данной лабораторной работе рассматриваются некоторые примеры применения механизма авторизации сетевых соединений для обеспечения защищенного

взаимодействия между авторизованными на сервере безопасности Secret Net Studio абонентами (пользователями и компьютерами).

Для установки защищенного соединения необходимо:

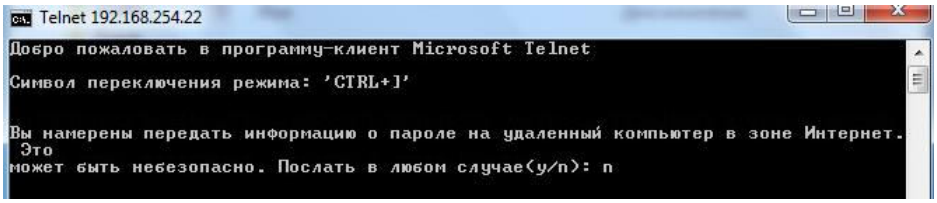
- настроить для удаленного компьютера-получателя правила доступа, необходимые для обмена данными с компьютером-отправителем (авторизация сетевых соединений работает в непосредственном взаимодействии с правилами межсетевого экранирования);
- включить режим подписи или шифрования IP-пакетов на компьютере-отправителе.

При невыполнении одного из этих условий установить защищенное соединение невозможно.

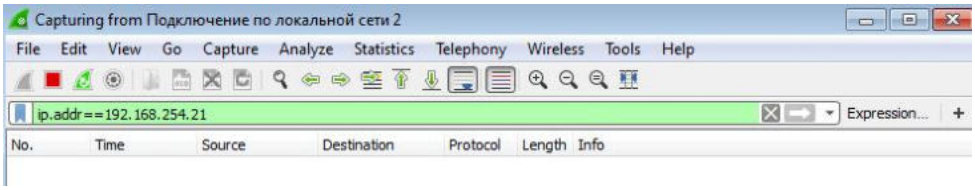
Настройка механизма авторизации сетевых соединений осуществляется централизованно в программе "Центр управления". Программа управления в локальном режиме непосредственно на защищаемом компьютере позволяет только просматривать централизованно заданные параметры.

Внимание! Перед началом выполнения лабораторной работы для проведения анализа сетевого трафика включите BM Sniffer и убедитесь, что ее сетевой интерфейс подключен к виртуальному коммутатору в режиме Promiscouos mode и на ней установлена программа Wireshark.

1. На BM ARM2 в программе управления в сетевом режиме отключите все запрещающие правила, установленные при выполнении предыдущей лабораторной работы.
2. Убедитесь, что при отключенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается открытый трафик. Для этого:
   - на BM ARM1 откройте от имени администратора командную строку и начните подключение по telnet к BM ARM2: **telnet 192.168.254.22** (на запрос передачи пароля введите **n**);

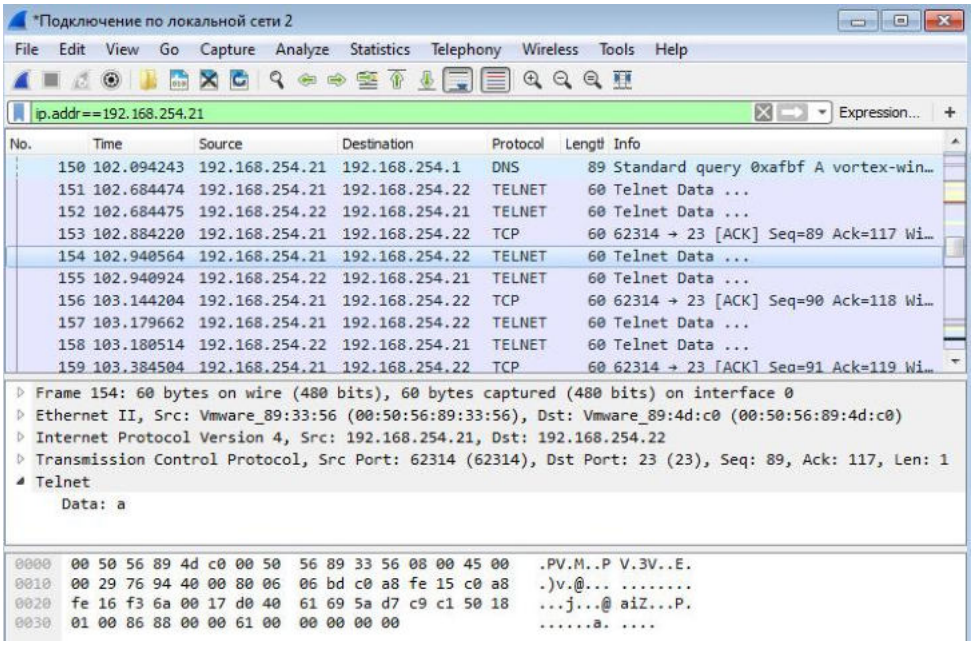


   - переключитесь в окно BM Sniffer, запустите утилиту Wireshark и начните перехват трафика, указав в поле "Apply a display filter" строку фильтра **ip.addr==192.168.254.21**;



   - переключитесь на BM ARM1 и в telnet-сессии последовательно введите: логин **sn7\dadminsns1**, пароль **P@ssw0rd**, а затем – **hostname**, чтобы убедиться в успешном подключении к ARM2;

   - переключитесь в окно BM Sniffer, в окне Wireshark остановите перехват трафика, найдите записи протокола telnet и убедитесь, что при вводе логина и пароля от источника (192.168.254.21) к получателю (192.168.254.22) символы передавались открытым текстом.

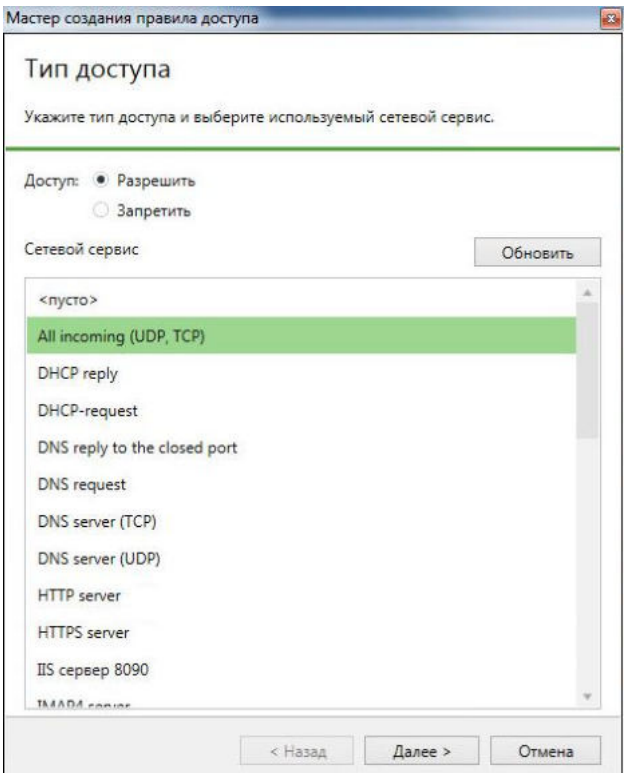


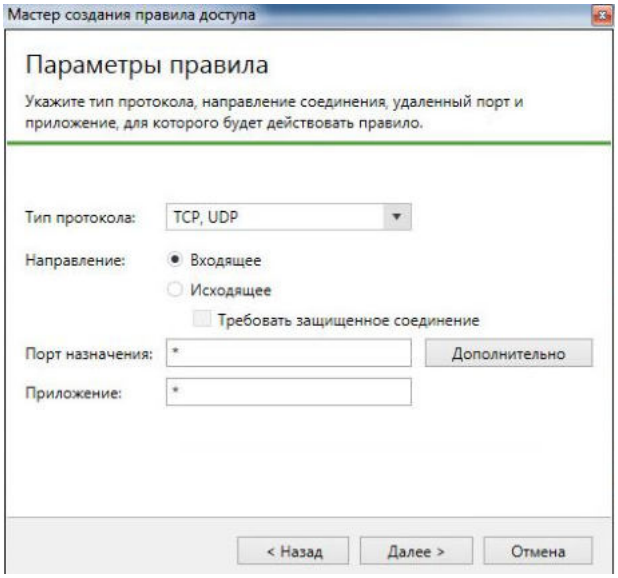
Таким образом, можно констатировать, что при отключенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается не защищенный трафик.

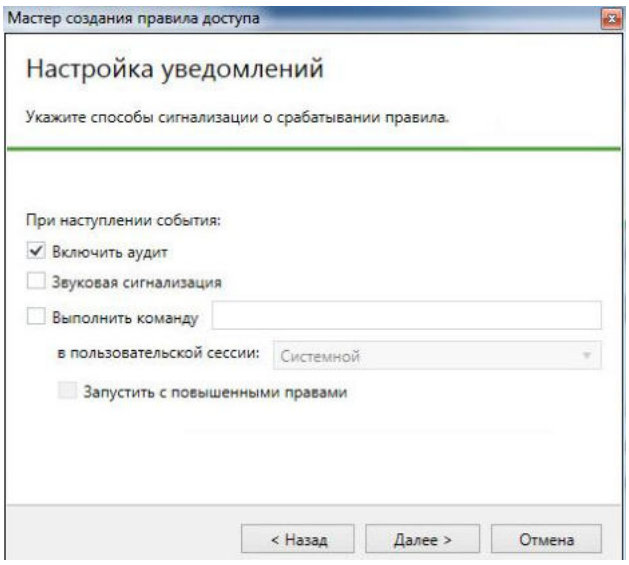
3. Перед установкой защищенного соединения для взаимодействия между компьютерами отправителя и получателя на ВМ ARM2 в программе управления в сетевом режиме настройте правила доступа. Для этого:

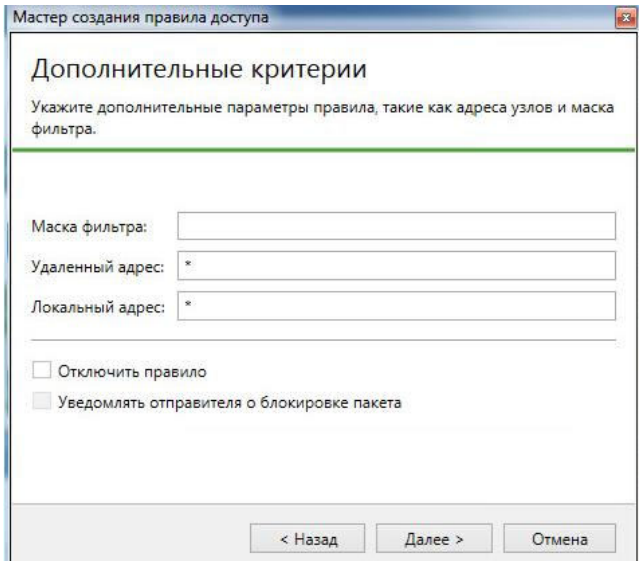
- в панели "Компьютеры" раскройте панель объекта ARM2;
- на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Межсетевой экран" и, используя описание пп. 6–12 предыдущей лабораторной работы, создайте для клиентов группы Everyone разрешающее правило для TCP /UDP – трафика на любой порт с любого удаленного порта.

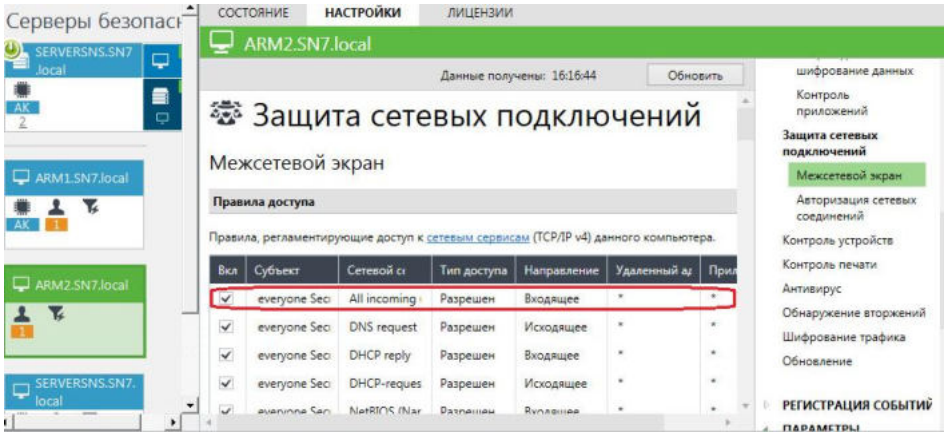
Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
everyone	*	TCP, UDP / any	*	any / any	allow




Мастер создания правила доступа
Параметры правила
Укажите тип протокола, направление соединения, удаленный порт и приложение, для которого будет действовать правило.
Тип протокола:
TCP, UDP
Направление:
Входящее
Исходящее
Требовать защищенное соединение
Порт назначения:
*
Дополнительно
Приложение:
*
< Назад
Далее >
Отмена


Мастер создания правила доступа
Настройка уведомлений
Укажите способы сигнализации о срабатывании правила.
При наступлении события:
Включить аудит
Звуковая сигнализация
Выполнить команду
в пользовательской сессии:
Системной
Запустить с повышенными правами
< Назад
Далее >
Отмена

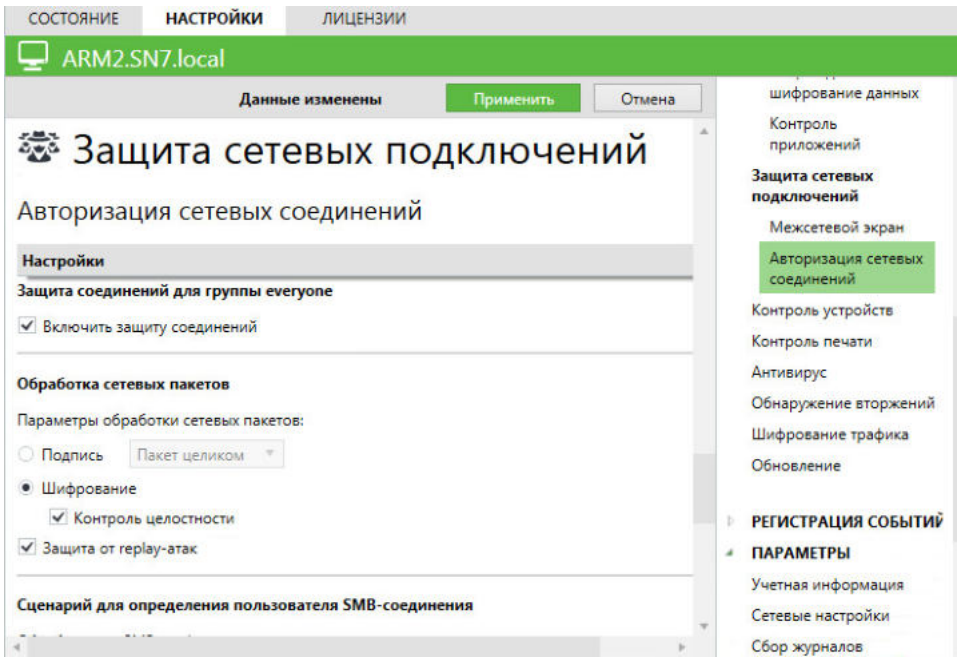

Мастер создания правила доступа
Дополнительные критерии
Укажите дополнительные параметры правила, такие как адреса узлов и маска фильтра.
Маска фильтра:
Удаленный адрес:
*
Локальный адрес:
*
Отключить правило
Уведомлять отправителя о блокировке пакета
< Назад
Далее >
Отмена



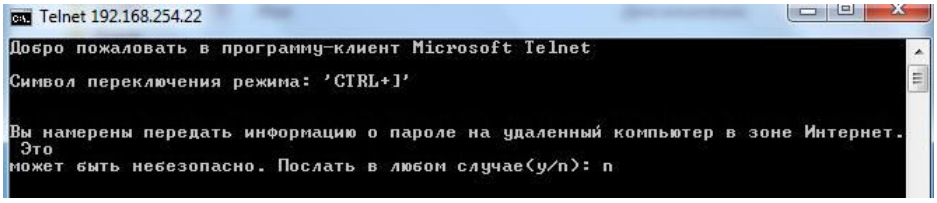
Примечание. Группа Everyone включает в себя пользователей и компьютеры, которые:

- прошли аутентификацию на СБ Secret Net Studio (authenticated Secret Net Studio), т.е. с установленным клиентом SNS;
- не прошли аутентификацию на СБ SNS (anonymous), т.е. либо не установлен клиент SNS, либо имеется проблема сетевого взаимодействия между клиентом и СБ.

4. Настройте режим защиты сетевых соединений между авторизованными клиентами Secret Net Studio. Для этого:
   - для объекта ARM2 на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Авторизация сетевых соединений";
   - в группе настроек "Защита для группы everyone" установите отметку в поле "Включить защиту соединений";
   - в группе настроек "Обработка сетевых пакетов" установите отметку в поле "Шифрование" и убедитесь, что отмечены опции "Контроль целостности" и "Защита от replay-атак";
   - остальные параметры оставьте по умолчанию, примените сделанные настройки и подождите принятое в SNS время (4-6 минут) для их активации.

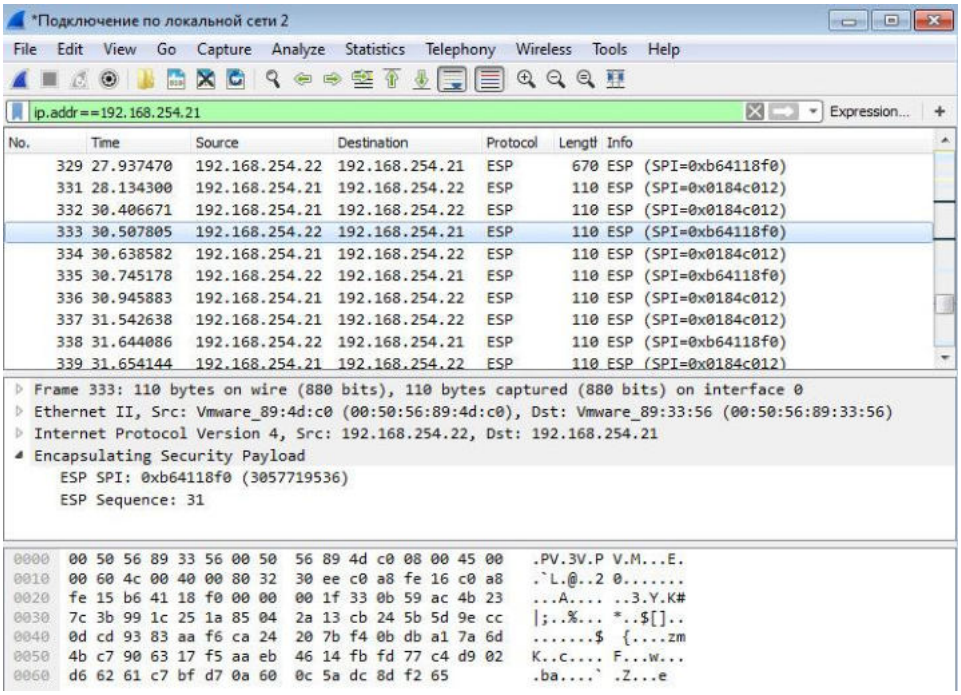


5. Убедитесь, что после включения механизма авторизации сетевых соединений между клиентами SNS передается защищенный трафик. Для этого:
   - на ВМ ARM1 закройте открытое ранее подключение по telnet к ВМ ARM2, используя комбинацию клавиш [Ctrl+]] и команду **quit**:
   - начните новое telnet-подключение к ВМ ARM2: **telnet 192.168.254.22** (на запрос передачи пароля введите **n**);



- переключитесь в окно BM Sniffer и в окне Wireshark начните перехватывать трафик, убедившись, что в поле "Apply a display filter" задан фильтр **ip.addr==192.168.254.21**;
- переключитесь на BM ARM1 и в telnet-сессии последовательно введите: логин **sn7\dadminsns1**, пароль **P@ssw0rd**, а затем – **hostname**, чтобы убедиться в успешном подключении к ARM2;

- переключитесь в окно BM Sniffer, в утилите Wireshark остановите перехват трафика и убедитесь, что после включения защиты соединений от источника (192.168.254.21) к получателю (192.168.254.22) вместо открытого протокола telnet передаются пакеты по ESP-протоколу, который не содержит незашифрованных данных.



Таким образом, можно констатировать, что при включенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается защищенный трафик, который не содержит открытой информации.

6. Переключитесь на BM ARM1 и закройте открытое ранее подключение по telnet к BM ARM2, используя комбинацию клавиш [Ctrl+]] и команду **quit**.

Аналогичный подход может применяться для обеспечения безопасности не только telnet-подключений, но и других сетевых сервисов, которые используются и передают информацию в открытом виде, например, http (обеспечение безопасного подключения клиентов к развернутому в организации веб-серверу).

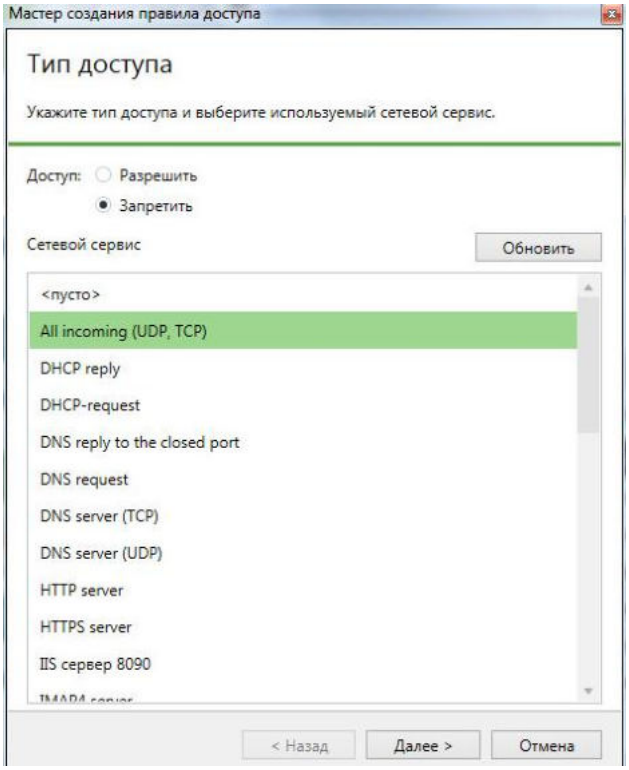
7. Как уже отмечалось выше, механизм авторизации сетевых соединений обеспечивает защиту взаимодействия только между авторизованными на СБ клиентами Secret Net Studio. Если на компьютере пользователя не установлен Secret Net Studio или пользователь по каким-либо причинам не прошел

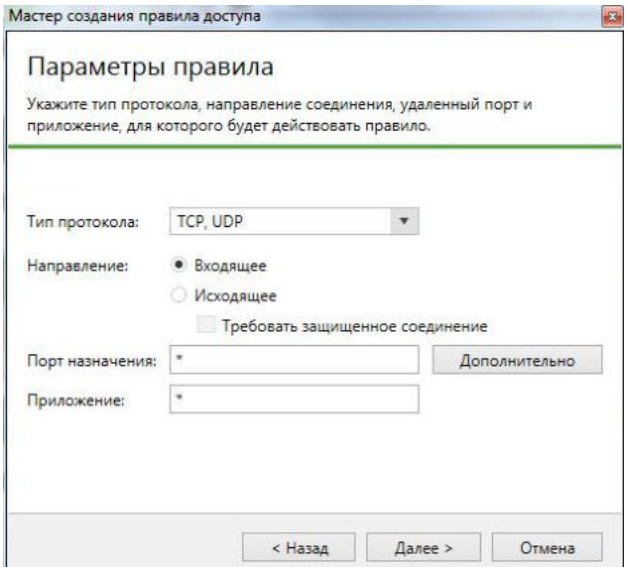
аутентификацию на СБ SNS (anonymous), то трафик между ним и авторизованным клиентом SNS не будет защищаться.

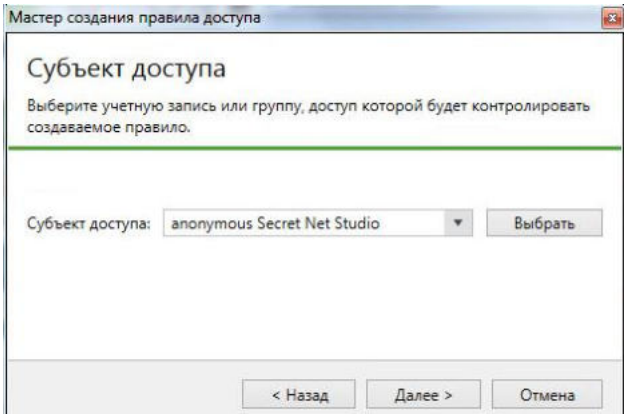
Однако с помощью соответствующих правил межсетевого экранирования администратор может настроить блокировку соединений для неавторизованных на СБ пользователей (anonymous). Для этого:

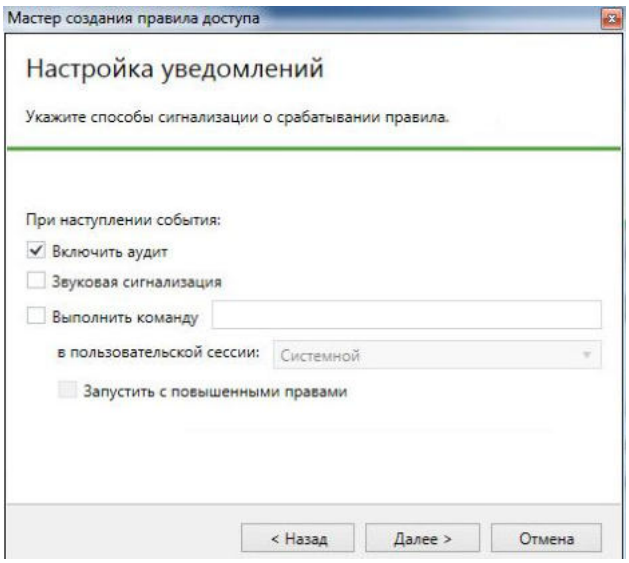
- переключитесь в окно программы управления на ВМ ARM2, в панели "Компьютеры" выберите объект ARM2 и раскройте панель его свойств;
- на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Межсетевой экран" и, используя описание пп. 6–12 предыдущей лабораторной работы, создайте для клиентов группы anonymous запрещающее правило для TCP /UDP–трафика на любой порт с любого удаленного порта.

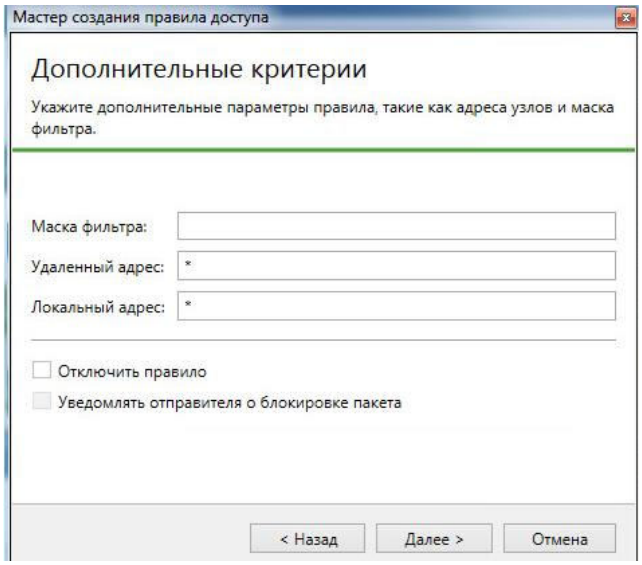
Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
anonymous	*	TCP, UDP / any	*	any / any	deny

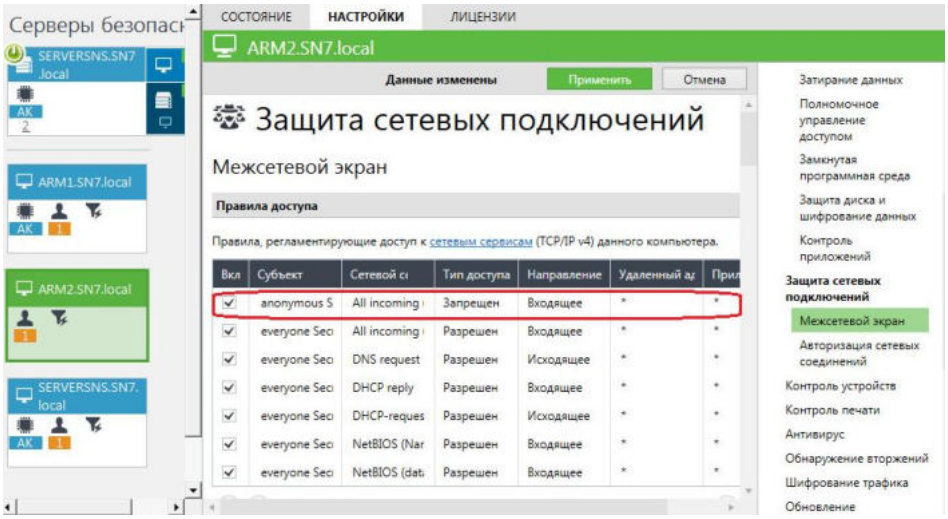





Мастер создания правила доступа
Субъект доступа
Выберите учетную запись или группу, доступ которой будет контролировать создаваемое правило.
Субъект доступа:
anonymous Secret Net Studio
Выбрать
< Назад
Далее >
Отмена


Мастер создания правила доступа
Настройка уведомлений
Укажите способы сигнализации о срабатывании правила.
При наступлении события:
Включить аудит
Звуковая сигнализация
Выполнить команду
в пользовательской сессии:
Системной
Запустить с повышенными правами
< Назад
Далее >
Отмена


Мастер создания правила доступа
Дополнительные критерии
Укажите дополнительные параметры правила, такие как адреса узлов и маска фильтра.
Маска фильтра:
Удаленный адрес:
*
Локальный адрес:
*
Отключить правило
Уведомлять отправителя о блокировке пакета
< Назад
Далее >
Отмена



После применения сделанных изменений сетевое взаимодействие с ARM2 будет возможным только для авторизованных на СБ абонентов.

Если распространить данный подход на всю сетевую инфраструктуру, весь трафик будет изолирован только между клиентами Secret Net Studio.

8. Выключите BM Sniffer. Выполнение лабораторной работы завершено.

Контрольные вопросы

1. В чем заключается особенность функционирования ПМЭ в Secret Net Studio, отличающая его от традиционных, "периметровых" МЭ?
2. Какие группы правил проверки сетевого трафика реализованы в ПМЭ Secret Net Studio?
3. Какая из групп правил проверки сетевого трафика в ПМЭ Secret Net Studio имеет наивысший приоритет? Что регламентируется правилами этой группы?
4. По каким протоколам может ограничиваться доступ к защищаемым ресурсам с помощью системных правил?
5. Какая из групп правил проверки сетевого трафика в ПМЭ Secret Net Studio имеет минимальный приоритет? Что регламентируется правилами этой группы?
6. Каков порядок обработки заданных в параметрах ПМЭ Secret Net Studio правил доступа?
7. Через какой промежуток времени после сохранения изменений вступают в силу новые настройки правил доступа ПМЭ Secret Net Studio?
8. Какой режим работы ПМЭ в Secret Net Studio позволяет составить на основе информации о сетевой активности приложений базовый набор правил доступа, необходимый для функционирования защищаемого компьютера?
9. В чем заключается особенность аутентификации пользователей механизмом авторизации сетевых соединений Secret Net Studio?
10. Какими средствами обеспечивается защита и целостность передаваемых данных в механизме авторизации сетевых соединений?
11. Что необходимо для возможности выбора пользователя или группы пользователей, доступ к которой будет контролироваться при создании нового правила доступа в параметрах настроек политик ПМЭ?
12. Наличие каких правил необходимо для работы прикладных правил доступа к общим папкам на защищаемом компьютере?

Глава 5
Защита от вирусов и вредоносного ПО

В этой главе мы рассмотрим отдельно лицензируемые компоненты Secret Net Studio, обеспечивающие защиту от вирусов и вредоносного ПО (см. рис. 1):

- антивирус – позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ по зарегистрированным в базе сигнатурам. При проверке компьютера проводится сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др., что позволяет обнаружить и заблокировать внешние и внутренние атаки;
- средство обнаружения вторжений – проверяет сетевой трафик, обнаруживает и блокирует внешние и внутренние вторжения, направленные на защищаемый компьютер.

Настройка работы антивируса и СОВ осуществляется либо централизованно в программе "Центр управления" с помощью групповых политик уровня объектов "Домен", "Сервер безопасности" или "Организационная единица", либо непосредственно на защищаемом компьютере через компонент "Локальный центр управления".

Вся информация об активности механизмов антивируса и СОВ регистрируется в журнале Secret Net Studio.

Антивирус

В Secret Net Studio разработаны два компонента антивируса, которые устанавливаются, настраиваются и сопровождаются практически одинаково:

- антивирус (технология ESET) – предназначен для использования в коммерческих организациях, в которых не обрабатываются сведения, составляющие государственную тайну. Данный компонент не проходит процедуру сертификации у регуляторов;
- антивирус – разработан и сертифицирован для применения в системах с защитой гостайны.

Антивирусная защита в SNS обеспечивается реализацией следующих функций:

- постоянная защита – проводит проверку файлов в режиме реального времени и позволяет обнаружить компьютерные вирусы сигнатурными и эвристическими методами при попытках получения доступа к исполняемым файлам, файлам документов, изображений, архивов, а также к скриптам и другим типам потенциально опасных файлов;
- контекстное сканирование – выполняет проверку, запускаемую пользователем из контекстного меню в проводнике Windows;
- сканирование по расписанию – запускает проверку по расписанию, параметры которого настраиваются администратором в программе управления. Пропущенное сканирование по расписанию (например, компьютер был выключен) запускается принудительно после восстановления работы компьютера;
- автоматическая проверка съемных носителей – реализует автоматическую проверку съемных носителей при их подключении к компьютеру;
- список исключений – позволяет составить список файлов, которые не проверяются в режиме реального времени и при сканировании по расписанию. Список исключений действует глобально для всех видов сканирования и не настраивается отдельно для разных режимов;
- выполнение действий при обнаружении вирусов – определяет действие, которое будет выполнено с зараженными объектами: удаление, изолирование (перемещение в карантин), блокировка доступа (только в режиме постоянной защиты), лечение. Выбор реакции на обнаруженные вредоносные программы осуществляется в настройках параметров антивируса;

Примите к сведению, что восстановленные из карантина объекты добавляются в список исключений для всех профилей сканирования (кроме контекстного сканирования). Это необходимо для того, чтобы при сканировании данный объект не попал в карантин повторно.

- обновление антивирусных баз – определяет порядок обновления: либо автоматически в фоновом режиме с сервера обновлений, либо вручную из выбранной директории;
- контроль целостности сигнатур – обеспечивает проверку неизменности базы сигнатур при загрузке службы и при обновлении. При несанкционированном изменении базы создается запись в журнале Secret Net Studio.

Параметры работы антивируса разделены на следующие группы:

- профили режимов сканирования – это набор заранее заданных параметров сканирования, которые будут применены при проверке системы в соответствующем режиме;
- расписание сканирования – определяет время и периодичность проведения проверок в соответствии с заданным профилем сканирования;
- исключения – определяют перечень файлов и каталогов, которые нужно исключить из проверки;
- регистрация событий – определяет уровень регистрации событий в системе защиты.

На защищаемом компьютере программа управления SNS позволяет:

- запускать процедуру сканирования;
- просматривать и управлять содержимым карантина;
- запускать процедуры обновления антивирусных баз.

Помимо средств программы управления реализовано контекстное сканирование выбранных файловых объектов в режиме игнорирования списка исключений. Специальная команда "Проверить на вирусы (игнорировать белый список)" доступна в расширенном контекстном меню каталога или файла для членов локальной группы администраторов. Вызов этого меню осуществляется в Проводнике Windows при нажатой клавише [Shift].

Средство обнаружения вторжений

Обнаружение и предотвращение вторжений обеспечивается в Secret Net Studio реализацией следующих функций:

- детектор сетевых атак – обеспечивает фильтрацию входящего трафика для блокировки внешних атак и обнаружения сканирования портов. Детектор атак функционирует на прикладном уровне модели OSI. Анализ входящих данных производится с помощью изучения поведения;
- сигнатурный анализ – проводит контроль входящего и исходящего трафика на наличие элементов, зарегистрированных в базе решающих правил (БРП). Атакующие компьютеры могут блокироваться на заданный промежуток времени.

Для отдельного компьютера программа управления Secret Net Studio позволяет осуществлять снятие блокировки хостов.

Обновление

Для полноценной защиты компьютеров от вредоносных программ предусмотрена установка следующих обновлений:

- обновление антивирусных баз;
- обновление базы решающих правил.

Обновление антивирусных баз

Для централизованного обновления на защищаемых компьютерах баз антивируса предназначен сервер обновлений – Antivirus Update Server (AVUS). Загрузка обновлений производится с сервера компании "Код Безопасности".

В зависимости от конфигурации и размера защищаемой сети могут использоваться различные схемы размещения сервера обновлений:

- сеть с малым числом рабочих станций – этот вариант рекомендуется использовать, когда в сети не более 5 защищаемых компьютеров. В этом случае в программе "Центр управления" для каждого защищаемого компьютера необходимо настроить функцию обновления антивирусных баз с сервера компании "Код Безопасности";
- сеть с большим числом рабочих станций – этот вариант целесообразно использовать, если в сети более 5 защищаемых компьютеров. В этом случае нужно установить ПО сервера обновлений на выделенном сервере в защищаемой сети, который будет загружать обновления с сервера компании "Код Безопасности" и предоставлять их клиентам в сети и другим серверам обновления в каскадном режиме (см. ниже), не расходуя внешний трафик. В программе управления Secret Net Studio для каждого защищаемого компьютера необходимо настроить функцию обновления антивирусных баз с локального сервера;
- сеть не подключена к интернету – в этом случае необходимо установить отдельный сервер, имеющий доступ к интернету, и установить на нем ПО сервера обновлений. На сервере в закрытой сети также нужно установить ПО сервера обновлений. Сервер обновлений, имеющий доступ к интернету, будет загружать обновления с сервера компании "Код Безопасности" и хранить их. Обновления с этого сервера на сервер в закрытой сети необходимо переносить вручную. В программе управления Secret Net Studio для каждого защищаемого компьютера необходимо настроить функцию обновления антивирусных баз с локального сервера в закрытой сети;
- каскадирование серверов – используется, когда в организации существует, к примеру, несколько подсетей или несколько филиалов. В подобных случаях внутри компании создается каскад серверов, в котором один, корневой, скачивает обновления с сервера компании "Код Безопасности", а остальные, дочерние, скачивают обновления с корневого сервера обновлений или с других дочерних серверов.

Обновление базы решающих правил

База решающих правил (БРП) содержит сигнатуры сетевых атак. При появлении новых сетевых атак формируется обновление базы решающих правил.

Загрузка доступного обновления для БРП выполняется администратором в личном кабинете на сайте компании "Код Безопасности" (http://www.securitycode.ru/).

Чтобы выполнить централизованное обновление БРП, необходимо разместить файл обновления в папке общего доступа, а затем настроить на компьютерах клиентов Secret Net Studio обновление по расписанию из данного каталога.

Лабораторная работа №1 "Настройка антивируса и СОВ"

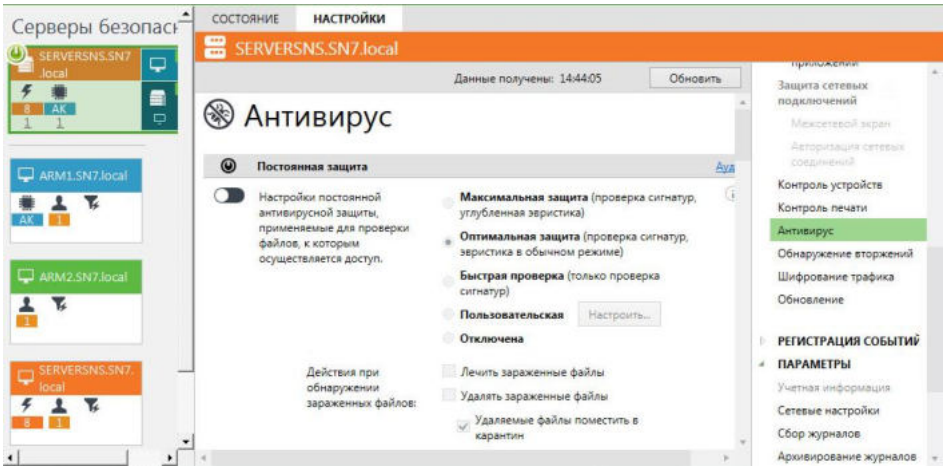
Настройка параметров антивируса и СОВ осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления Secret Net Studio.

В соответствующих разделах главы 5 описаны назначение и функции антивируса и средства обнаружения вторжений, а в данной лабораторной работе мы покажем некоторые способы их настройки и применения.

Внимание! Перед началом выполнения данной лабораторной работы сделайте следующее:

- выключите ВСЕ запрещающие правила, установленные в ходе выполнения лабораторного модуля №4;
- на ВМ ARM2 в программе "Центр управления" на вкладке "Состояние" свойств объекта ARM2 выключите компонент защиты "Межсетевой экран";
- на ВМ ARM1 под учетной записью "dadminsns1" для проведения атак последовательно установите из папки "C:\Distrib\sniff_spoof" следующее ПО: "WinPcap 4.1.3", "ettercap-NG-0.7.3-win32" и "nmap 7.1.2".

1. Ознакомьтесь с параметрами настройки групповых политик антивируса на уровне сервера безопасности. Для этого на компьютере ARM2 в программе "Центр управления" выберите объект сервера подключения ServerSNS и в панели его свойств на вкладке "Настройки" выберите раздел "Политики / Антивирус". В средней части окна появятся параметры настройки групповых политик.



В случае необходимости управления локальными настройками антивируса на защищаемом компьютере нужно выбрать соответствующий объект в программе управления.

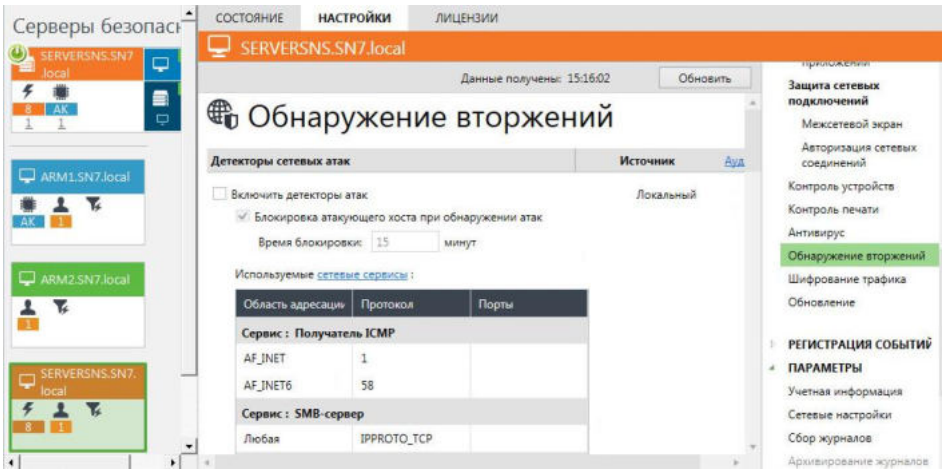
2. Обратите внимание, что первым располагается профиль "Постоянная защита", который определяет параметры сканирования объектов системы в режиме реального времени. Напомним, что описание профилей защиты приведено в соответствующем разделе главы 5.

С помощью кнопки ⓘ ознакомьтесь с описанием профиля "Постоянная защита". Обратите внимание, что если одновременно отмечены пункты "Лечить зараженные файлы" и "Удалять зараженные файлы", то при обнаружении зараженных объектов сначала будет выполнена попытка их лечения, а затем, при неудаче, файлы будут удалены.

При включенном эвристическом анализе ищутся фрагменты кода и программы, имеющие вирусоподобные характеристики, но не зарегистрированные в БД вирусных сигнатур. При обнаружении такого подозрительного файла выполняется оповещение пользователя. Доступны следующие уровни эвристического анализа: "Обычный" (по умолчанию) — глубина эвристики ограничена, низкая вероятность ложных срабатываний, но и вероятность обнаружения неизвестных вирусов не слишком высока; "Углубленный" — высокая вероятность обнаружения неизвестных вирусов, однако и выше вероятность ложных срабатываний.

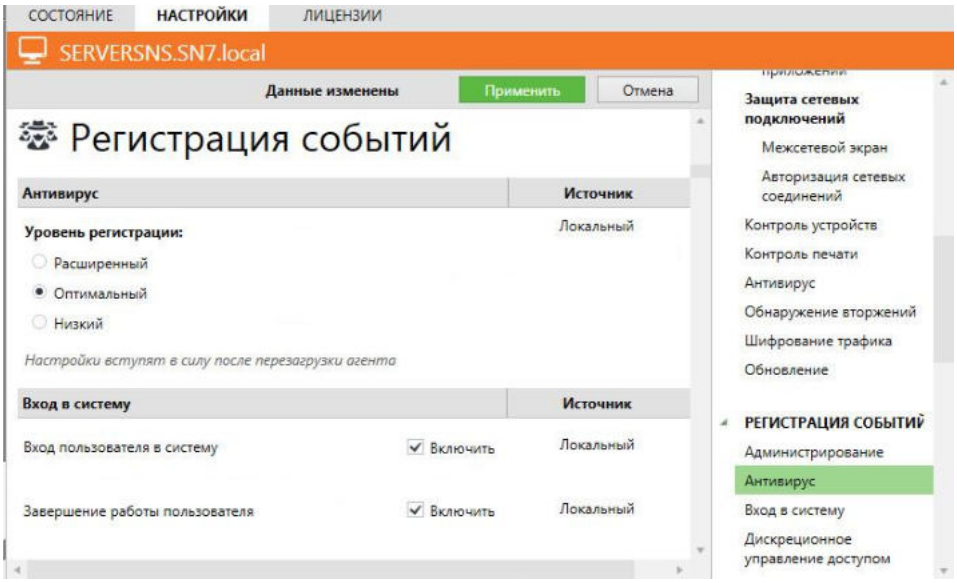
3. Проведите настройку политик СОВ на СБ. Для этого в программе управления в сетевом режиме выберите в панели "Компьютеры" объект ServerSNS, который НЕ помечен значком ⏻, и в панели его свойств на вкладке "Настройки" выберите раздел "Политики / Обнаружение вторжений".

Установите следующие параметры политик:



- "Включить детекторы атак" – установите флажок;
- "Блокировка атакующего хоста…" – оставьте отмеченным, "Время блокировки" – **1** минута;

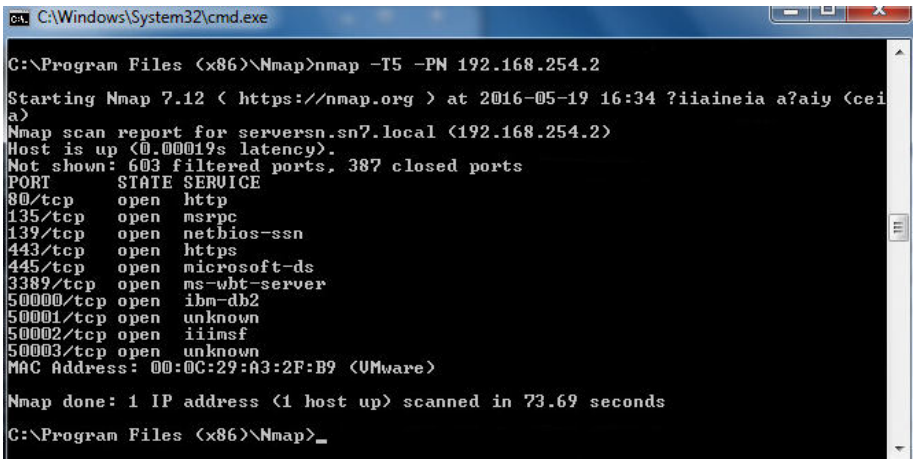
- ниже, в группе "Детекторы", установите отметку в поле "Сканирование портов". В параметрах "Период обнаружения" и "Максимальное количество обращений к портам" оставьте значения по умолчанию;
- выберите раздел политик "Регистрация событий / Антивирус" и убедитесь, что установлен уровень "Оптимальный", при котором регистрируются все важные и некоторые информационные события. Если выбрать опцию "Расширенный", то будут регистрироваться все происходящие события, и их количество может оказаться очень большим;



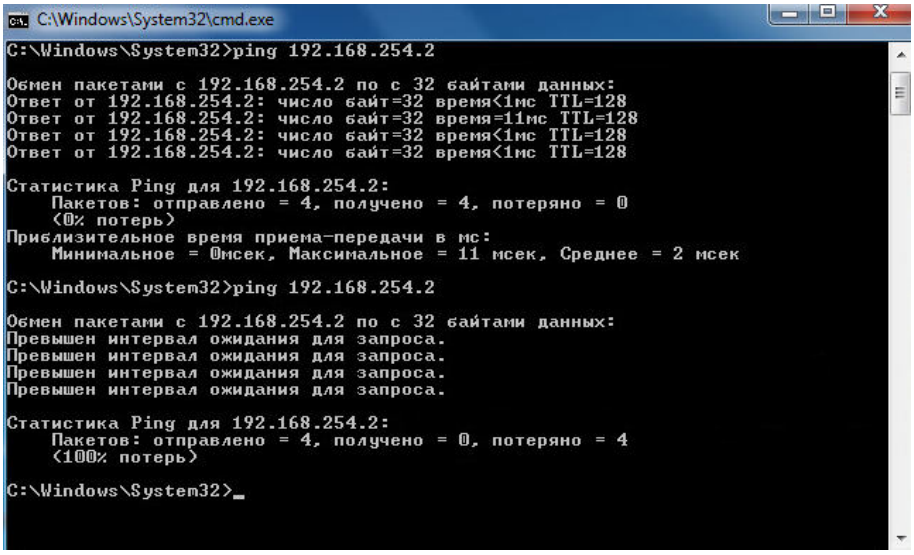
- нажмите кнопку "Применить"  и подождите около 4–6 минут, пока настройки применятся.

4. Перейдите в консоль ВМ ARM1 и сымитируйте атаку на компьютер ServerSNS. Для этого:

- откройте командную строку от имени администратора и с помощью утилиты **ping** убедитесь, что компьютер ServerSNS (192.168.254.2) доступен;
- откройте командную строку от имени администратора, перейдите в папку "C:\Progam files (x86)\nmap" и проведите сканирование портов защищаемого сервера с помощью команды: **nmap -T5 -PN 192.168.254.2**;



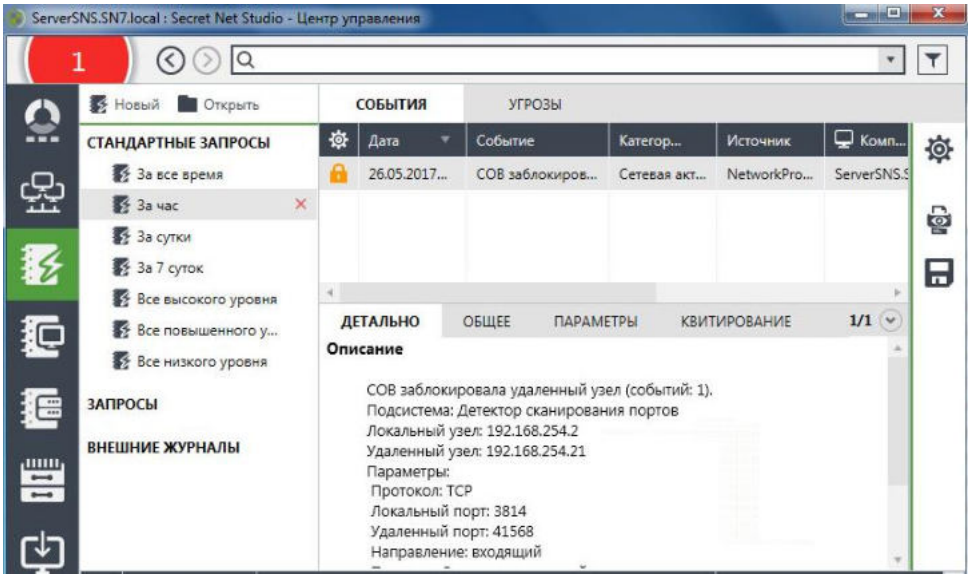
- с помощью утилиты **ping** повторно проверьте доступность компьютера ServerSNS (192.168.254.2) и убедитесь, что эхо-ответы не приходят.



5. Перейдите в консоль ARM2. Обратите внимание, что:

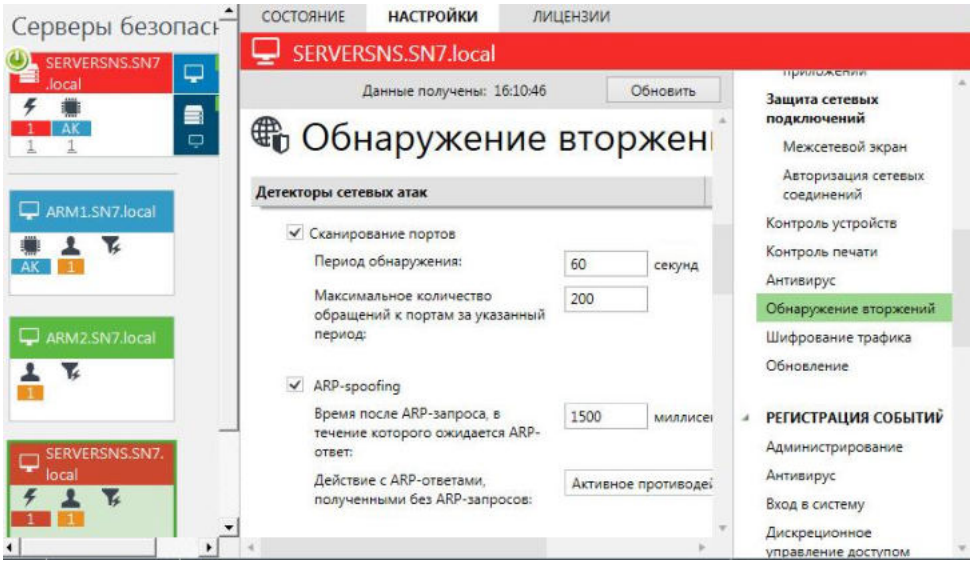
- в панели событий появились записи о событиях тревоги на СБ;

- в журнале тревог появились сообщения о блокировке атакующего узла (категория "Сетевая активность" тип "Аудит отказов").



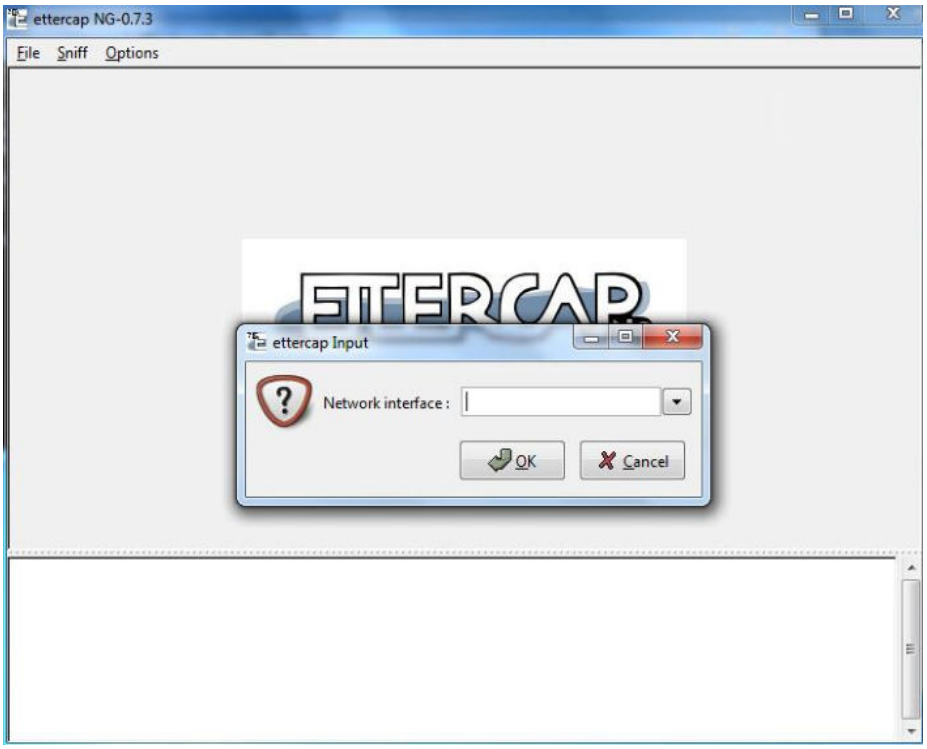
6. Выберите в панели "Компьютеры" объект ServerSNS, который НЕ помечен значком  , и в панели его свойств на вкладке "Настройки" выберите раздел "Политики / Обнаружение вторжений". Установите следующие параметры политик:

- в группе "Детекторы" установите отметку в поле "ARP-spoofing";
- параметры: "Время после ARP-запроса… " – 1500мс, "Действие с ARP-ответами…" – "Активное противодействие" (по умолчанию);
- нажмите кнопку "Применить"  и подождите около 4–6 минут, пока настройки применятся.

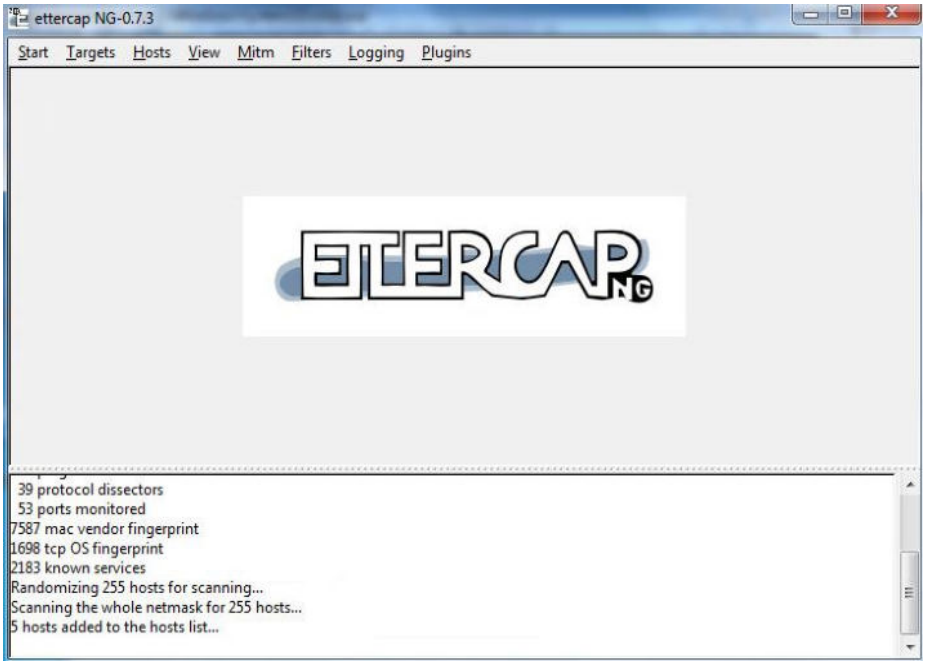


7. Сымитируйте атаку ARP-spoofing на компьютер ServerSNS. Для этого:

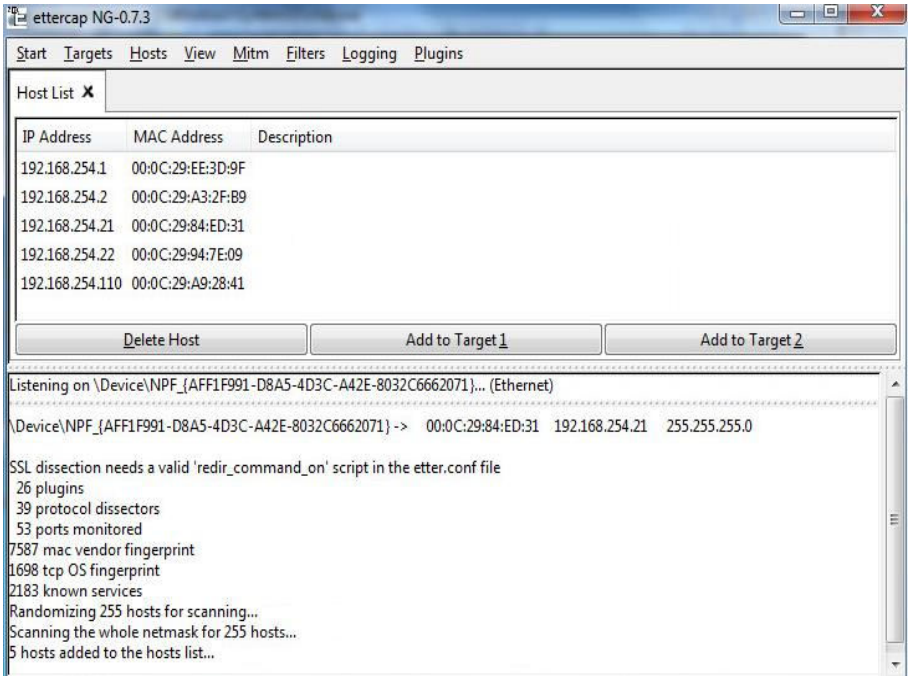
- в окне консоли ServerSNS с помощью утилиты **arp –a** определите и запишите MAC-адрес компьютера ARM2 (192.168.254.22): _____;
- в окне консоли ServerSNS запустите постоянную проверку доступности компьютера ARM2 командой **ping –t 192.168.254.22**;
- перейдите в консоль ВМ ARM1 и в командной строке выполните команду: **netsh interface ipv4 set interface LAN forwarding=enabled**;
- запустите Ettercap NG-0.7.3. В открывшемся окне программы в главном меню выберите опцию “Sniff / Unified sniffing…”;



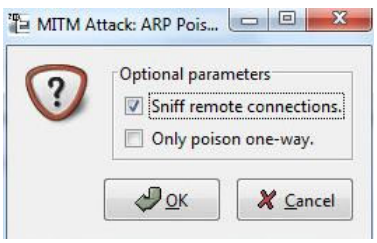
- в открывшемся диалоговом окне выберите из раскрывающегося списка сетевой интерфейс и нажмите кнопку "OK". Обратите внимание, что в нижней части окна "Ettercap NG-0.7.3" появилось описание параметров выбранного интерфейса компьютера ARM1;
- в окне "Ettercap NG-0.7.3" в главном меню выберите опцию “Hosts / Scan for hosts”. Дождитесь завершения сканирования доступных хостов в сети. В нижней части окна появятся сообщения об обнаруженных хостах и добавлении доступных хостов в список;



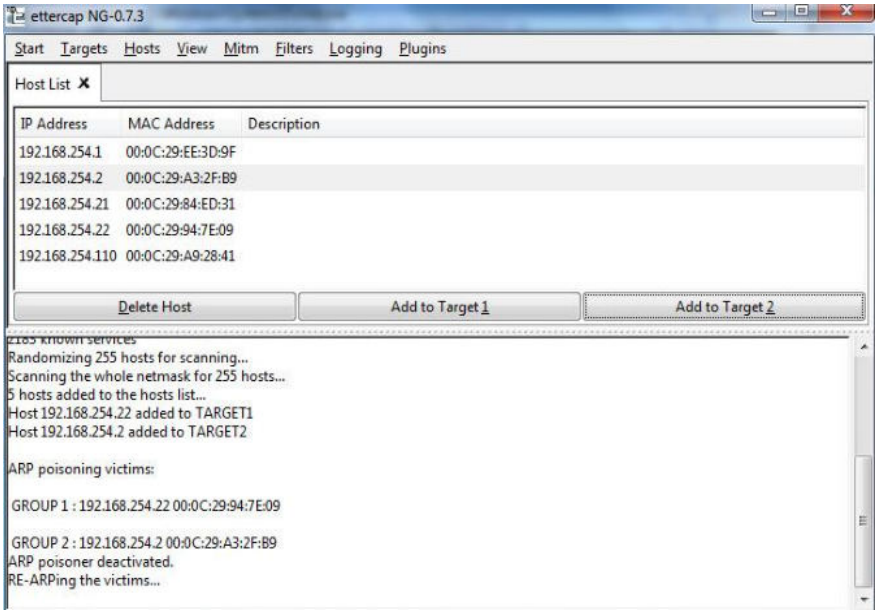
- в главном меню окна "Ettercap NG-0.7.3" выберите опцию “Hosts / Host list”. В верхней части окна вы увидите список доступных хостов в сети;



- выберите хост 192.168.254.22 (компьютер ARM2) и нажмите кнопку "Add to Target 1", а затем выберите атакуемый компьютер 192.168.254.2 (компьютер ServerSNS) и нажмите кнопку "Add to Target 2". В нижней части окна появятся записи по заданным целям;
- запустите атаку ARP-spoofing. Для этого из главного меню выберите опцию “Mitm / ARP poisoning…”, в открывшемся диалоговом окне отметьте опцию "Sniff remote connections" и нажмите кнопку "OK";



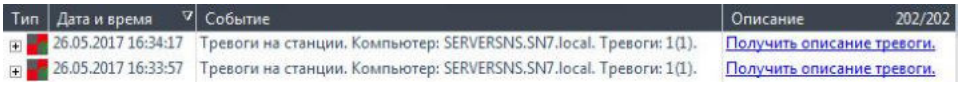
- перейдите в окно консоли ServerSNS и с помощью утилиты **arp –a** определите MAC-адрес компьютера ARM2 (192.168.254.22). Убедитесь, что он совпадает с тем, что вы записывали в начале теста. Атака была заблокирована системой защиты Secret Net Studio;
- в окне ARM1 и остановите атаку, выбрав опцию “Mitm / Stop mitm attack(s)”. В нижней части окна появится соответствующее сообщение.



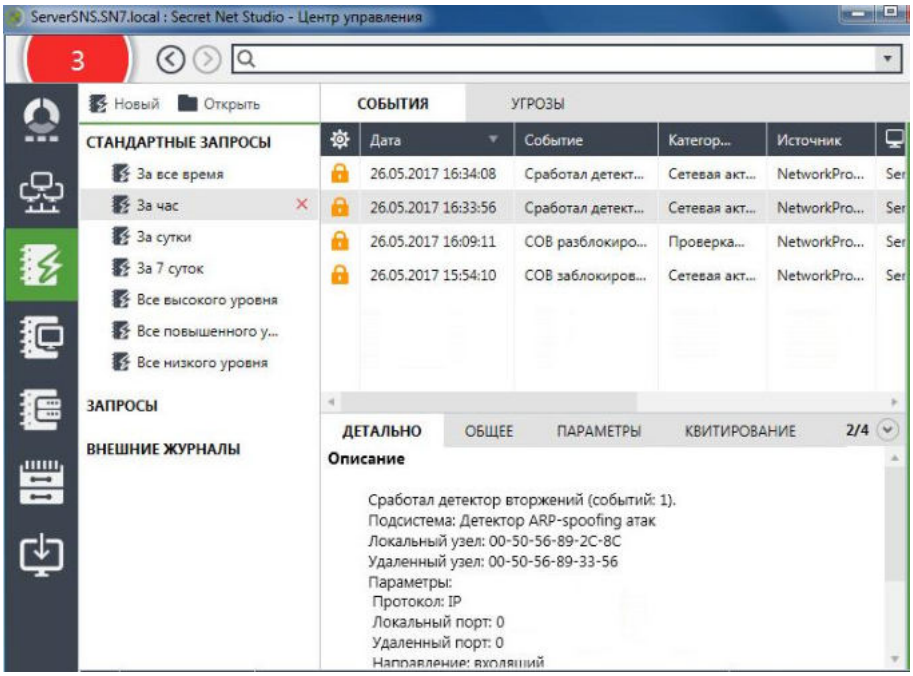
8. Переключитесь в окно консоли ServerSNS и остановите проверку доступности компьютера ARM2 командой **ping**;

9 Переключитесь в консоль ARM2 и вернитесь в окно программы управления. Обратите внимание, что:

- в панели событий появились записи о событиях тревоги на СБ;



- в журнале тревог появились сообщения детектора атак о вторжении (категория – "Сетевая активность", тип – "Аудит отказов").



Выполнение лабораторной работы завершено.

Контрольные вопросы

1. Какими программными средствами Secret Net Studio выполняется настройка компонентов "Антивирус" и "СОВ"?
2. Какие функции защиты реализуются компонентом "Антивирус" в Secret Net Studio?
3. Какие функции защиты реализуются компонентом "СОВ" в Secret Net Studio?
4. Какое программное средство в Secret Net Studio используется для централизованного обновления антивирусных баз на защищаемых компьютерах?

Приложение 1. Организация защиты средствами Secret Net Studio

Данное приложение содержит лабораторную работу для самостоятельного выполнения слушателями в качестве дополнительного задания. В ней приводятся примеры настройки механизмов защиты Secret Net Studio для реализации практических задач организации доступа к конфиденциальной информации и разделяемым ресурсам при построении сетевых решений.

Лабораторная работа №1 "Построение закрытого контура"

В данной лабораторной работе приводится пример реализации задачи построения на учебном стенде системы обеспечения информационной безопасности (закрытого контура) на базе ВМ ARM2, см. рис. 7, с соблюдением ряда заданных защитных мер и требований безопасности (см. ниже). При этом предлагается использовать **только механизмы защиты SNS**.

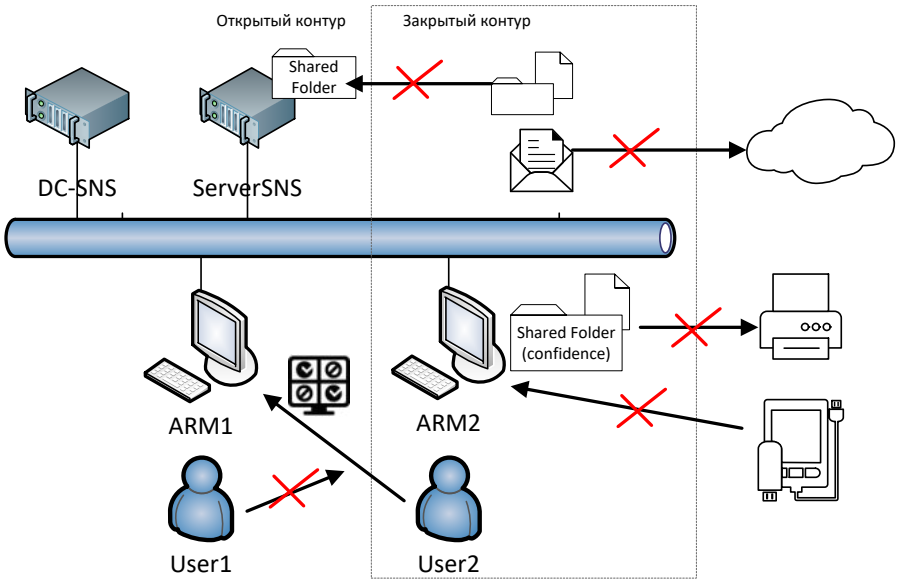


Рис. 7. Схема построения закрытого контура

Предлагается следующий порядок выполнения лабораторной работы:

1. Ознакомьтесь с формулировкой задачи, составом защитных мер и требований к организации закрытого контура (см. ниже). По каждому из перечисленных требований указывается инструмент Secret Net Studio для его реализации, а также пункты лабораторной работы с соответствующим описанием настроек.
2. Попробуйте **самостоятельно**, без обращения к указанным пунктам с описанием, настроить предлагаемые механизмы защиты в соответствии с приведенными требованиями.
3. Если самостоятельно настроить не удалось, перейдите к п. 6.
4. Протестируйте полученный в результате сделанных вами настроек результат на соответствие требованиям защиты.
5. Если в результате сделанных вами настроек все требования защиты соблюдены, ознакомьтесь с описанием лабораторной работы и сравните ваши настройки с предлагаемыми в тексте. Сделайте соответствующие выводы. Выполнение лабораторной работы завершено.
6. Если самостоятельно настроить механизмы защиты SNS в соответствии с заданными требованиями не удалось, выполните лабораторную работу от начала до конца и протестируйте результат.

Задача: обеспечить обработку конфиденциальной информации (например, персональных данных) на одном АРМ (ВМ ARM2) в сети организации при условии

неизменности сетевой инфраструктуры. Для этого необходимо изолировать указанную ВМ от основной сети с соблюдением ряда защитных мер и требований безопасности.

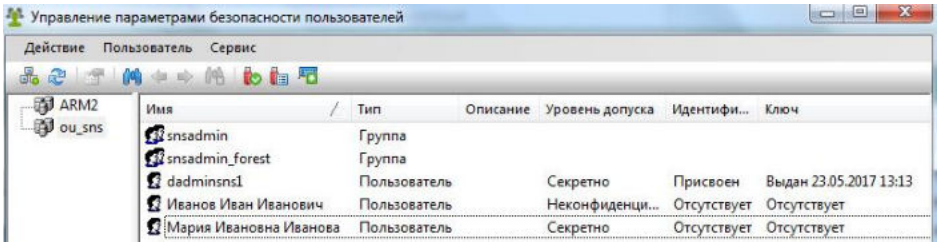
Состав **мер по обеспечению безопасности** с указанием **требований** для реализации поставленной задачи:

1. Контроль и управление доступом к защищаемым данным. Требования:
   - обеспечить обработку конфиденциальной информации только на ВМ ARM2 для пользователя закрытого контура user2 – в SNS механизм полномочного управления доступом, см. в лабораторной работе пп. 1–3;
   - запретить возможность авторизации на ВМ ARM2 всем, кроме пользователя закрытого контура, – в SNS механизм замкнутой программной среды, см. в лабораторной работе п. 14.
2. Контроль вывода информации за пределы контролируемой зоны (закрытого контура, который в нашем случае ограничивается ВМ ARM2). Требования:
   - обеспечить невозможность вывода из ARM2 конфиденциальной информации через внешние носители (USB-флеш-накопители) – в SNS механизм контроля устройств с включенным режимом контроля потоков в конфиденциальных сессиях, см. пп. 4–6 и 15–17;
   - обеспечить невозможность печати на ВМ ARM2 конфиденциальной информации – в SNS механизм контроля печати с включенным режимом контроля потоков в конфиденциальных сессиях, см. пп. 7–8 и 15–17.
3. Контроль запуска программ. Требование:
   - предоставить пользователю закрытого контура возможность запуска на ARM1 ограниченного набора приложений, например, Проводник, MS Wordpad, MS Word, MS Excel, Корзина – в SNS механизм замкнутой программной среды, см. в лабораторной работе пп. 9–13;
4. Ограничение межсетевого взаимодействия защищаемого АРМ и остальной сети. Требования:
   - изолировать ВМ ARM2 без возможности доступа к ней по TCP и RDP-протоколам, за исключением каналов взаимодействия с контроллером домена и сервером безопасности SNS, – в SNS механизм "Межсетевой экран" с настроенными системными правилами, см. в лабораторной работе пп. 18–21;
   - обеспечить невозможность передачи конфиденциальной информации из ARM2 в общедоступные сетевые ресурсы открытого контура – механизм "Межсетевой экран" с настроенным прикладным правилом на протокол SMB, см. в лабораторной работе пп. 20–21.

Описание последовательности выполнения поставленной задачи

1. Для разграничения доступа к конфиденциальной информации в закрытом контуре запустите на ВМ ARM2 программу "Управление пользователями" и измените настройки уровней доступа и привилегий в соответствии с представленной ниже таблицей (доступ к конфиденциальной информации только для пользователя user2).

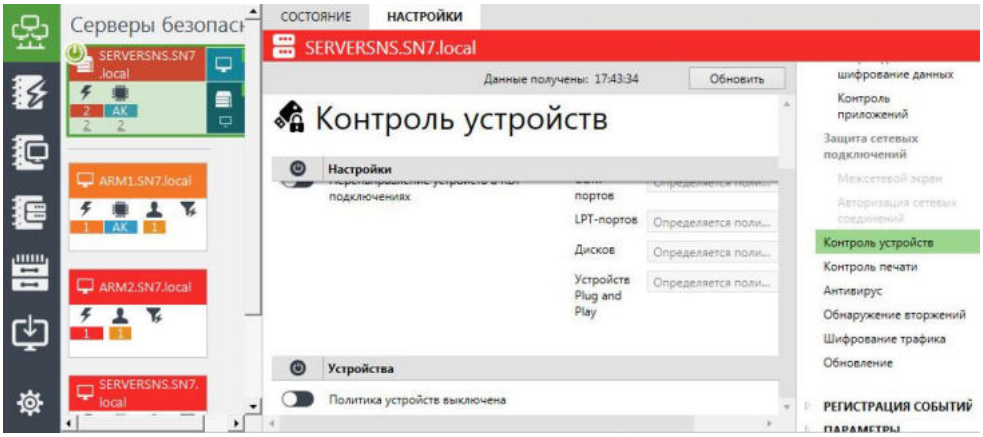
Пользователь	Полное имя	Уровень допуска	Привилегии
User1	Иван Иванович Иванов	Неконфиденциально	Нет
User2	Мария Ивановна Иванова	Секретно	Снять привилегии: "Печать конфиденциальных документов" и "Вывод конфиденциальной информации". Установить привилегию "Управление категориями конфиденциальности"



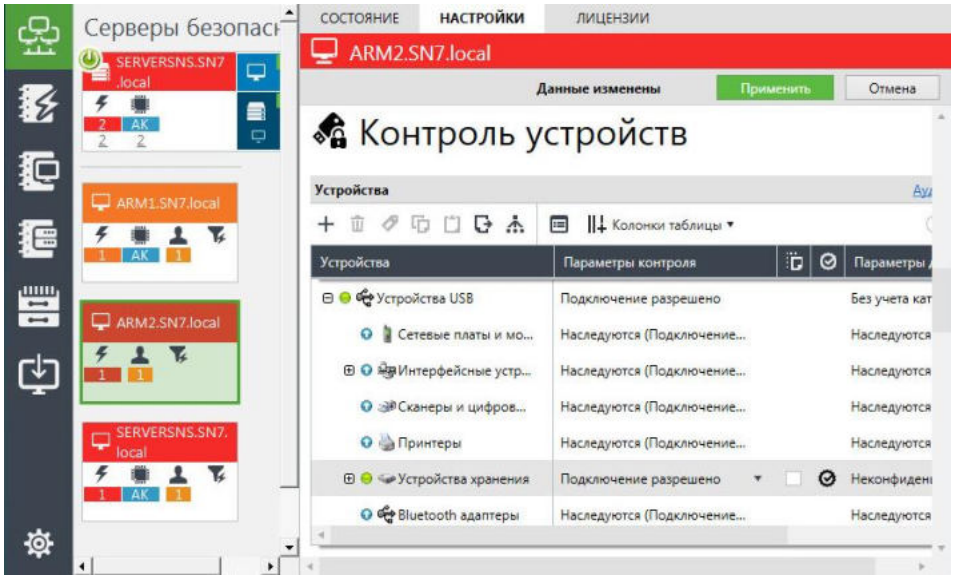
2. Для хранения на ВМ ARM2 конфиденциальной информации создайте папки:
   - общедоступную папку "C:\user_files" с максимальными разрешениями (permissions) на уровне ОС Windows;
   - в папке "user_files" создайте подпапку "Секретно" и установите для нее уровень допуска "секретно". В этой папке создайте файл любого формата, например, Microsoft Word, с произвольным содержанием.
3. Убедитесь, что к созданному на ВМ ARM2 секретному файлу:
   - возможен доступ по сети с ВМ ARM1 для пользователя user2;
   - невозможен ни локальный, ни сетевой доступ для пользователя user1.

   На ВМ ARM2 под УЗ dadminsns1 запустите программу "Центр управления".
4. Для последующей локальной установки запрета вывода конфиденциальной информации с ARM2 на USB-флеш-накопители убедитесь, что соответствующие групповые политики сервера безопасности отключены. В программе управления выберите объект СБ, откройте раздел настроек "Контроль устройств" и проверьте, что в таблице "Устройства" отключены групповые политики: "Устройства USB / Устройства хранения" и "Политика устройств включена". В данный момент подключение USB-флеш-накопителей на подчиненных серверу безопасности компьютерах разрешено.

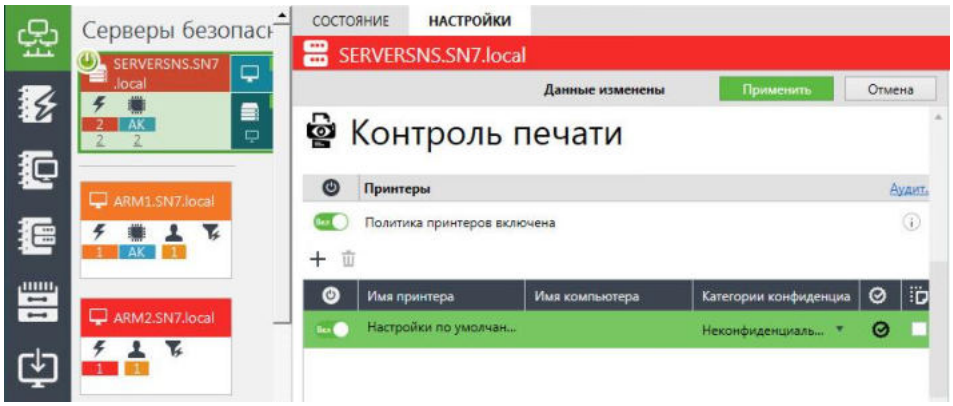
   Если в групповых политиках были сделаны изменения, примените их для объектов ARM1 и ARM2.



5. Для ARM2 задайте для всех подключаемых USB-флеш-накопителей категорию "Неконфиденциально". В таблице "Устройства" для политики "Устройства USB / Устройства хранения" установите:
   - в графе "Параметры контроля" удалите отметку из поля "Наследовать настройки контроля от родительского объекта" и установите флажок "Подключение устройства разрешено";
   - в графе "Параметры доступа" удалите отметку из поля "Для новых устройств использовать настройки категории с родительского объекта" и установите опцию "Неконфиденциально".

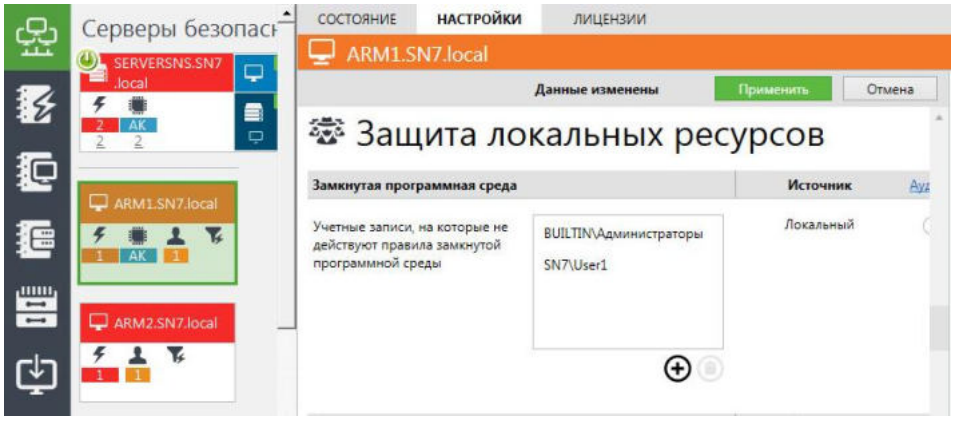


6. Примените сделанные изменения. Теперь, после включения режима контроля потоков, подключение USB-флеш-накопителей будет возможно только в неконфиденциальных сессиях.
7. Для запрета вывода на печать конфиденциальных документов выберите объект СБ и в разделе настроек "Политики / Контроль печати" измените настройки групповой политики "Настройка по умолчанию":
   - в графе "Категория конфиденциальности" оставьте отметку только для категории "Неконфиденциально";
   - в графе "Теневое копирование" снимите отметку.

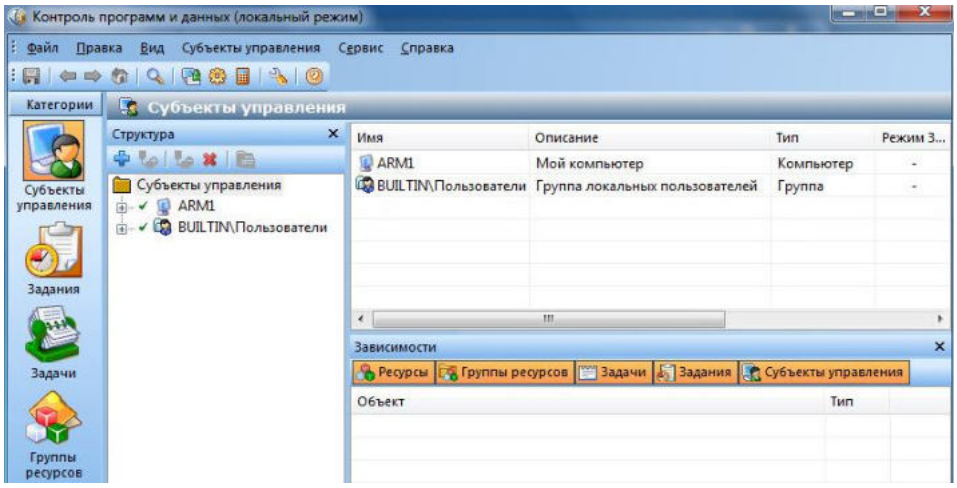


8. Примените сделанные изменения. Теперь, после включения режима контроля потоков, на подключаемых принтерах будет возможно печатать документы только в неконфиденциальных сессиях.
9. Чтобы установить для пользователя user2 авторизацию на ARM1 с возможностью запуска ограниченного набора приложений (Проводник, MS Wordpad, MS Word, MS Excel, Корзина), проведите на данной ВМ настройку для этого пользователя механизма ЗПС (см. описание лабораторной работы №4 главы 3).

   В окне программы "Центр управления" выберите объект ARM1 и на вкладке его настроек раскройте раздел "Политики / Защита локальных ресурсов / Замкнутая программная среда". Чтобы действие ЗПС не распространялось на доменного пользователя user1, добавьте его с помощью кнопки "Добавить" ⊕ в группу привилегированных пользователей, а затем сохраните внесенные в политики изменения, используя кнопку "Применить" Применить.



10. На ARM1 проведите локальную настройку ЗПС. Для этого запустите программу "Контроль программ и данных" в локальном режиме и, используя описание пп. 3–5 лабораторной работы №4 главы 3, сформируйте новую модель данных. В окне программы управления КЦ-ЗПС появится новая структура объектов, содержащая сформированное по умолчанию задание контроля ресурсов самой SNS и ОС Windows.



11. В категории "Субъекты управления" появилась вновь созданная структура "BUILTIN\Пользователи". Используя описание пп. 6 – 9 лабораторной работы №4 главы 3, создайте для нее новое задание с произвольным именем, а затем для субъекта управления "ARM1" включите мягкий режим работы ЗПС. Перезагрузите ВМ и авторизуйтесь под УЗ dadminsns1.

12. Используя описание пп. 10–15 лабораторной работы №4 главы 3, выполните следующие операции:

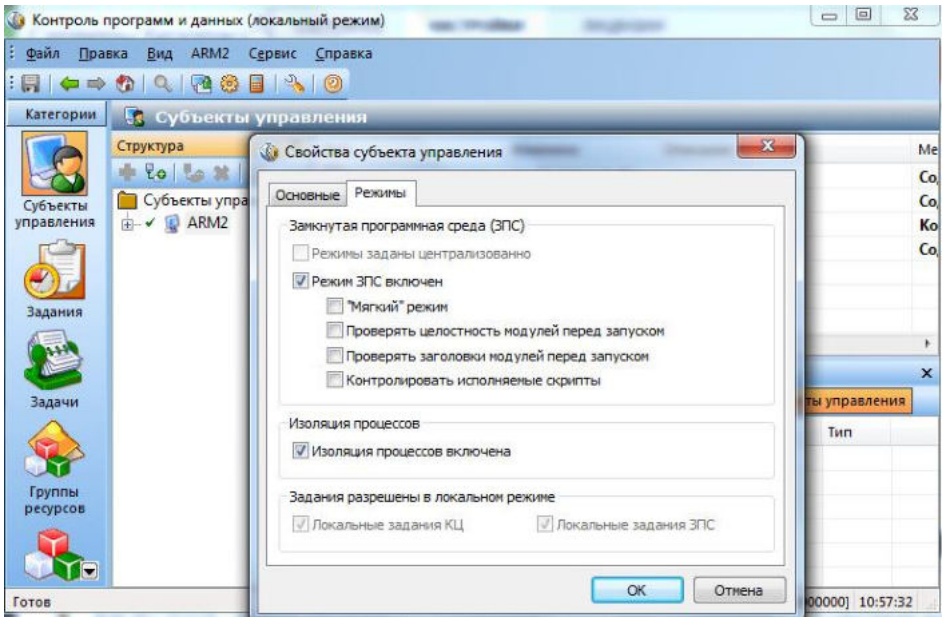
- экспортируйте (в локальном центре управления) журнал Secret Net Studio во внешний файл;
- перезагрузите ОС и авторизуйтесь под УЗ user2;
- последовательно запустите все разрешенные в дальнейшем программы: Проводник, WordPad, MS Word, MS Excel, Корзина;
- переавторизуйтесь на ВМ ARM1 под учетной записью dadminsns1;
- к созданному ранее заданию ЗПС добавьте задачи на основании данных из журнала Secret Net Studio.

13. Используя описание пп. 16–17 лабораторной работы №4 главы 3, выполните следующие действия:

- установите режим изоляции процессов для приложений WordPad и MS Word;
- включите жесткий режим работы ЗПС.

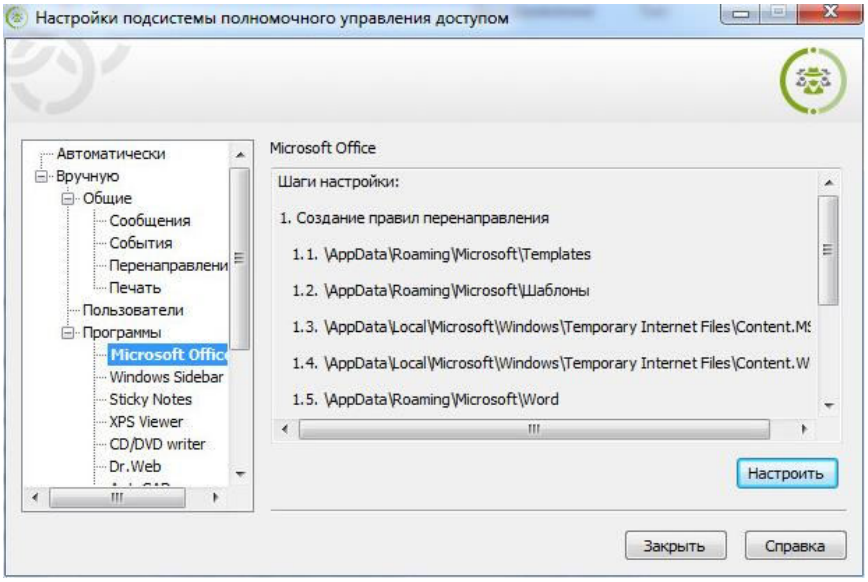
14. Чтобы запретить доменному пользователю user1 авторизацию на ВМ ARM2, проведите на этой ВМ настройку механизма ЗПС следующим образом:

- доменного пользователя user2 добавьте в группу привилегированных, для которых не действует механизм ЗПС (см. выше, п. 10);
- на ВМ ARM2 запустите программу "Контроль программ и данных" в локальном режиме и, не создавая никакой модели данных, отключите для объекта ARM2 "мягкий" режим работы ЗПС.

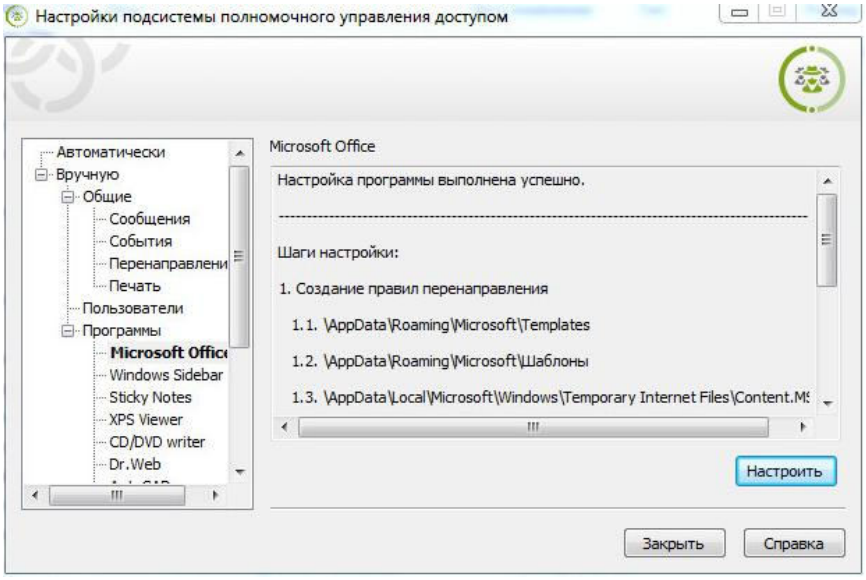


15. Для того чтобы ограничить пользователю user2 возможность вывода из ARM2 конфиденциальной информации на внешние носители или на печать, следует использовать настроенные ранее механизмы полномочного управления доступом, контроля устройств и печати при включенном режиме контроля потоков. Запустите программу "Пуск / Все программы / Код безопасности / Secret Net Studio / Настройка подсистемы полномочного управления доступом" и проведите дополнительный настройки:

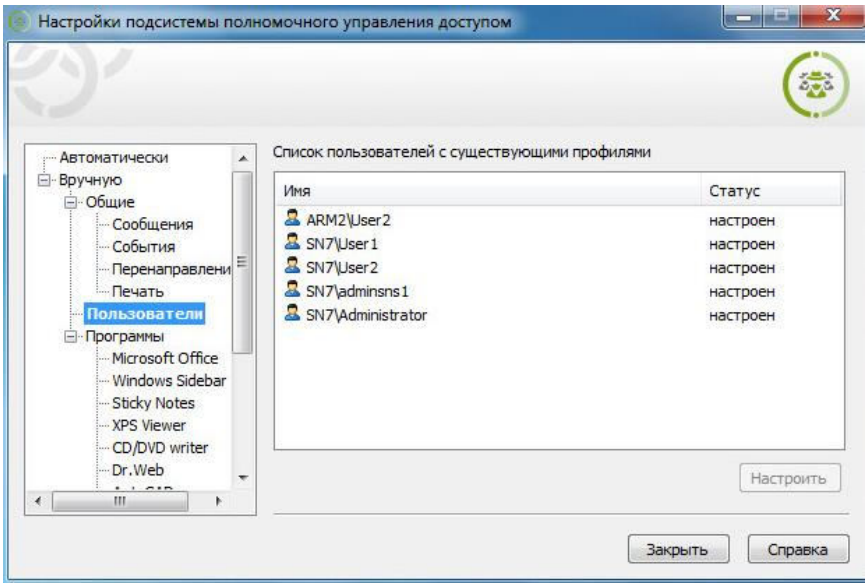
- запустите настройку для программ Microsoft Office. Для этого в разделе настроек выберите "Вручную / Программы / Microsoft Office" и нажмите кнопку "Настроить";



- будет выполнена настройка перенаправления файлов. Дождитесь завершения этого процесса. После создания правил перенаправления появится окно с информацией об успешном проведении настройки;



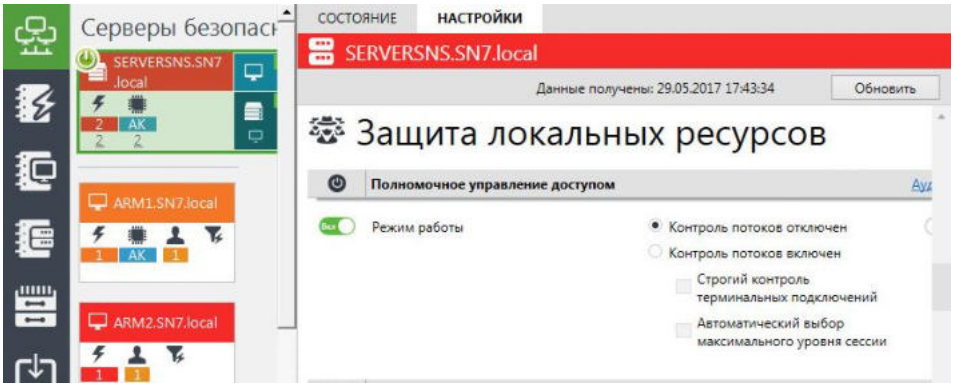
- проведите аналогичную настройку для пользователей в разделе "Вручную / Пользователи".



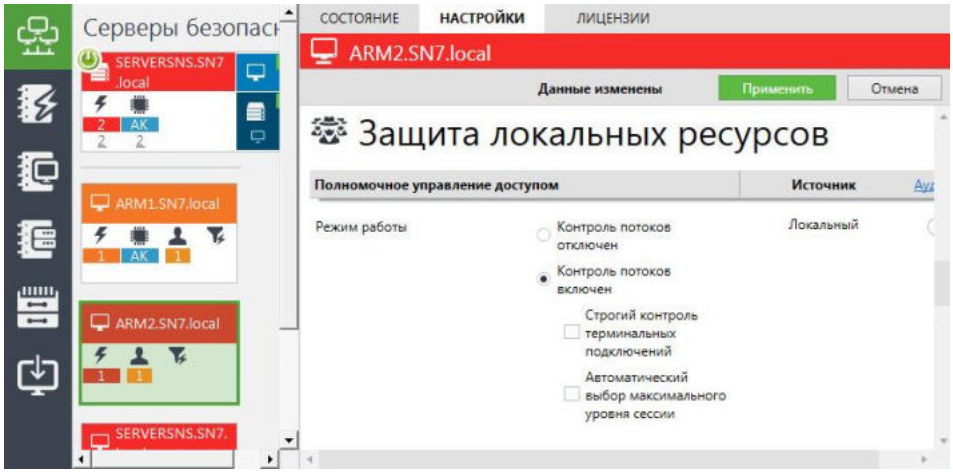
16. Закройте окно "Настройка подсистемы полномочного управления доступом" и перезагрузите ОС на ВМ ARM2.

17. Включите режим контроля потоков на ВМ ARM2. Для этого:

- в окне программы "Центр управления" выберите объект сервера безопасности и на вкладке его настроек раскройте раздел "Политики / Защита локальных ресурсов / Полномочное управление доступом";



- убедитесь, что в поле "Режим работы" выбран переключатель "Контроль потоков отключен". Выключите данную групповую политику и примените настройки;
- выберите объект ARM2, примените для него групповые политики, а затем в разделе его настроек "Политики / Защита локальных ресурсов / Полномочное управление доступом" в политике "Режим работы" установите переключатель "Контроль потоков включен";



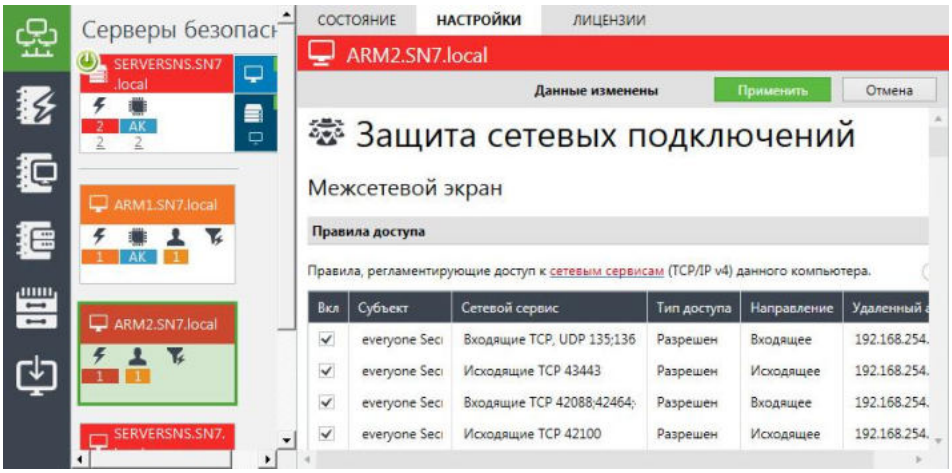
- примените сделанные настройки. Теперь возможность доступа к конфиденциальным файлам, использования устройств и печати на ВМ ARM2 будет определяться уровнем конфиденциальности сессии, который выберет пользователь при входе в систему.

18. Для того чтобы изолировать ВМ ARM2, но разрешить обращение к СБ и контроллеру домена, следует настроить политики межсетевого экрана на этой ВМ. В программе "Центр управления" выберите объект ARM2, раскройте панель его свойств и на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Межсетевой экран".

19. Для взаимодействия программы управления и клиента SNS на ВМ ARM2 с сервером безопасности и контроллером домена (см. рис. 5 и таблицу в разделе "Способы развертывания компонентов Secret Net Studio" главы 1) добавьте разрешающие правила доступа (см. описание пп. 6–12 лабораторной работы №1 главы 4). При этом, если необходимо, добавьте соответствующие сетевые сервисы (см. пп. 2–5 лабораторной работы №1 главы №4):

Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
everyone	192.168.254.22	TCP/3268, 389	192.168.254.1	any	allow
everyone	192.168.254.22	TCP,UDP/135 – 139	192.168.254.1	any	allow
everyone	192.168.254.22	TCP/443	192.168.254.2	any	allow
everyone	192.168.254.2	any	192.168.254.22	TCP/443	allow
everyone	192.168.254.22	TCP/50000 – 50003	192.168.254.2	any	allow
everyone	192.168.254.22	TCP/445	192.168.254.2	any	allow
everyone	192.168.254.2	any	192.168.254.22	TCP/445	allow
everyone	192.168.254.22	TCP/21326, 21327	192.168.254.2	any	allow
everyone	192.168.254.2	any	192.168.254.22	TCP/21326, 21327	allow
everyone	192.168.254.22	TCP/42100	192.168.254.2	any	allow
everyone	192.168.254.22	TCP/42088, 42464, 42200	192.168.254.2	any	allow
everyone	192.168.254.2	any	192.168.254.22	TCP/42088, 42464, 42200	allow
everyone	192.168.254.22	TCP/43443	192.168.254.2	any	allow
everyone	192.168.254.2	any	192.168.254.22	TCP,UDP/135 – 139	allow

- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и портам 3268 и 389 для всех пользователей на удаленный IP-адрес 192.168.254.1 (DC);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколам TCP, UDP и портам 135 – 139 для всех пользователей на удаленный IP-адрес 192.168.254.1 (DC);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и порту 443 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить входящие на 192.168.254.22 (ARM2) по протоколу TCP и порту 443 для всех пользователей с удаленного IP-адреса 192.168.254.2 (ServerSNS);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и портам 50000 – 50003 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и порту 445 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить входящие на 192.168.254.22 (ARM2) по протоколу TCP и порту 445 для всех пользователей с удаленного IP-адреса 192.168.254.2 (ServerSNS);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и портам 21326, 21327 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить входящие на 192.168.254.22 (ARM2) по протоколу TCP и портам 21326, 21327 для всех пользователей с удаленного IP-адреса 192.168.254.2 (ServerSNS);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и порту 42100 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и портам 42088, 42464, 42200 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить входящие на 192.168.254.22 (ARM2) по протоколу TCP и портам 42088, 42464, 42200 для всех пользователей с удаленного IP-адреса 192.168.254.2 (ServerSNS);
- разрешить исходящие с 192.168.254.22 (ARM2) по протоколу TCP и порту 43443 для всех пользователей на удаленный IP-адрес 192.168.254.2 (ServerSNS);
- разрешить входящие на 192.168.254.22 (ARM2) по протоколам TCP, UDP и портам 135 – 139 для всех пользователей с удаленного IP-адреса 192.168.254.2 (ServerSNS).



20. Добавьте запрещающие правила доступа (если необходимо, опишите соответствующие сетевые сервисы):

- запретить входящие на 192.168.254.22 (ARM2) по протоколу TCP и всем портам для всех пользователей и IP-адресов;

Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
everyone	any	any/any	192.168.254.22	TCP/any	deny

- системное правило, запрещающее доступ к ARM2 (192.168.254.22) по протоколу RDP (используйте описание пп. 16–17 лабораторной работы №1 главы 4);
- прикладное правило, запрещающее доступ к общедоступной папке "user_files" на ВМ ARM2 (192.168.254.22) с любого компьютера (используйте описание пп. 18–19 лабораторной работы №1 главы 4).

Пользователь	Источник	Протокол/Порт	Получатель	Протокол/Порт	Действие
everyone	any	any/any	192.168.254.22	SMB/any	deny

21. С помощью расположенных под таблицей "Правила доступа" кнопок "Вниз" и "Вверх" установите приоритет всех добавленных разрешающих правил выше, чем всех запрещающих (переместите запрещающие правила в нижнюю часть таблицы, после разрешающих). На вкладке "Настройки" нажмите кнопку "Применить" Применить.

22. Протестируйте полученный результат. Выполнение лабораторной работы завершено.