Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Направление подготовки: 09.04.03 «Прикладная информатика»

Магистерская программа «Информационные системы и технологии в управлении бизнес–процессами»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2024

Смоленск

Методические материалы составил:
канд. техн. наук, доцент кафедры
информационных технологий в экономике и управлении _____ Б.В. Окунев

«18» _____апреля____ 2024 г.

Заведующий кафедрой информационных технологий в экономике и управлении:

_____ __д-р техн. наук, профессор_М.И. Дли__
подпись ФИО

«02» мая 2024 г.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

Целью проведения лабораторных работ является развитие у студентов навыков использования современных средств защиты компьютерной информации.

В ходе изучения дисциплины «Методы и средства защиты компьютерной информации» предусмотрен цикл из 8 лабораторных работ.

Лабораторная работа 2.1. Организация комплексной защиты информационной инфраструктуры организации. Знакомство с основными возможностями и настройка лабораторного стенда по ИБ (Часть 1)

Цель работы: Изучить основные возможности специализированного виртуального лабораторного стенда по ИБ.

Задания на лабораторную работу:

1. Ознакомиться с основными элементами виртуального лабораторного стена по ИБ;
2. Изучить основные возможности настройки лабораторного стенда по ИБ.

Методические указания смотри в Приложении 1.

Лабораторная работа 2.2. Организация комплексной защиты информационной инфраструктуры организации. Дискреционное управление доступом к информационным ресурсам (Часть 2)

Цель работы: Изучить основные возможности дискреционного управления доступом к информационным ресурсам организации.

Задания на лабораторную работу:

1. Ознакомиться с основными особенностями дискреционного управления доступа к информационным ресурсам;
2. Разработать дискреционную (избирательную) политики безопасности для заданного преподавателем варианта предметной области.
3. Реализовать дискреционную (избирательную) политику безопасности для заданного преподавателем варианта предметной области, используя возможности виртуального лабораторного стенда по ИБ.

Методические указания смотри в приложении 1.

Лабораторная работа 2.3. Организация комплексной защиты информационной инфраструктуры организации. Полномочное управление доступом к информационным ресурсам (Часть3.)

Цель работы: Изучить основные возможности полномочного (мандатного) управления доступом к информационным ресурсам организации.

Задания на лабораторную работу:

1. Ознакомиться с основными особенностями полномочного (мандатного) управления доступа к информационным ресурсам;
2. Разработать полномочную (мандатную) политику безопасности для заданного преподавателем варианта предметной области.

3. Реализовать полномочную (мандатную) политику безопасности для заданного преподавателем варианта предметной области, используя возможности виртуального лабораторного стенда по ИБ.

Методические указания смотри в приложении 1.

Лабораторная работа 2.4. Организация комплексной защиты информационной инфраструктуры организации. Межсетевой экран (Часть 4).

Цель работы: Изучить основные возможности использования межсетевых экранов для обеспечения информационной безопасности в вычислительной сети.

Задания на лабораторную работу:

1. Ознакомиться с основными особенностями использования межсетевых экранов.

2. Изучить особенности разработки правил фильтрации межсетевых экранов.

3. Настроить межсетевые экраны на вычислительных ресурсах организации, используя возможности виртуального лабораторного стенда по ИБ.

Методические указания смотри в приложении 1.

Лабораторная работа 2.5. Организация комплексной защиты информационной инфраструктуры организации. Защита от вирусов и вредоносного ПО (Часть 5).

Цель работы: Изучить основные методы борьбы с вредоносными программами и вирусами.

Задания на лабораторную работу:

1. Ознакомиться с основными подходами при организации борьбы с вредоносными программами.

2. Ознакомиться с основными технологиями обнаружения вредоносных программ (сигнатурный анализ, эвристический анализ и т.д.)

3. Реализовать борьбу с вредоносными программами в вычислительной сети организации, используя возможности виртуальный лабораторного стенда по ИБ.

Методические указания смотри в приложении 1.

Лабораторная работа 2.6. Организация комплексной защиты информационной инфраструктуры организации. Обнаружение вторжений в информационную инфраструктуру организации (Часть 6)

Цель работы: Изучить основные подходы для обнаружения вторжений злоумышленников в информационные ресурсы организации.

Задания на лабораторную работу:

1. Ознакомиться с основными особенностями вторжений в информационную структуру организации;

2. Изучить возможности виртуального лабораторного стенда по ИБ по регистрации компьютерных инцидентов.

3. Реализовать регистрацию компьютерных инцидентов в вычислительной сети организации, используя возможности виртуального лабораторного стенда по ИБ.

Методические указания смотри в приложении 1.

Лабораторная работа 2.7. Организация комплексной защиты информационной инфраструктуры организации. Исследование и оценка эффективности защитных механизмов с помощью тестирования на проникновение (пентестинг) (Часть 7)

Цель работы: Изучить методы оценки эффективности защитных механизмов информационной инфраструктуры организации.

Задания на лабораторную работу:

1. Ознакомиться с основными особенностями пентестинга (тестирование на проникновение);

2. Изучить основные методы оценки эффективности защитных механизмов информационной инфраструктуры организации.

3. Реализовать тестирование на проникновение (пентестинг) и оценить эффективность механизмов защиты, используя возможности виртуального лабораторного стенда по ИБ.

Методические указания смотри в приложении 1.

Лабораторная работа 2.8. Применение электронной цифровой подписи.

Цель работы: Изучить методы использования ЭЦП.

Задания на лабораторную работу:

1. Ознакомиться с основными особенностями реализации ЭЦП.

2. Изучить основные возможности программы для реализации ЭЦП (на примере КриптоПро).

3. Осуществить использование ЭЦП в различных ситуациях (подписывание документа Word, файла PDF и т.д.).

Методические указания смотри в приложении 2.

Приложение 1.

Методические указания по использованию виртуального лабораторного стенда ИБ

Краткое описание стенда.

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

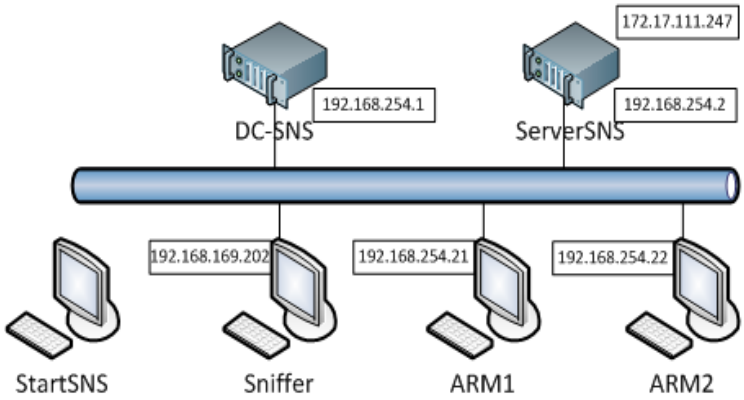


Рисунок 1 - Схема стенда Secret Net Studio

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.

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 (рисунок1):

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.

Рисунок 2 - Схема лицензирования Secret Net Studio

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 (рисунок 3):

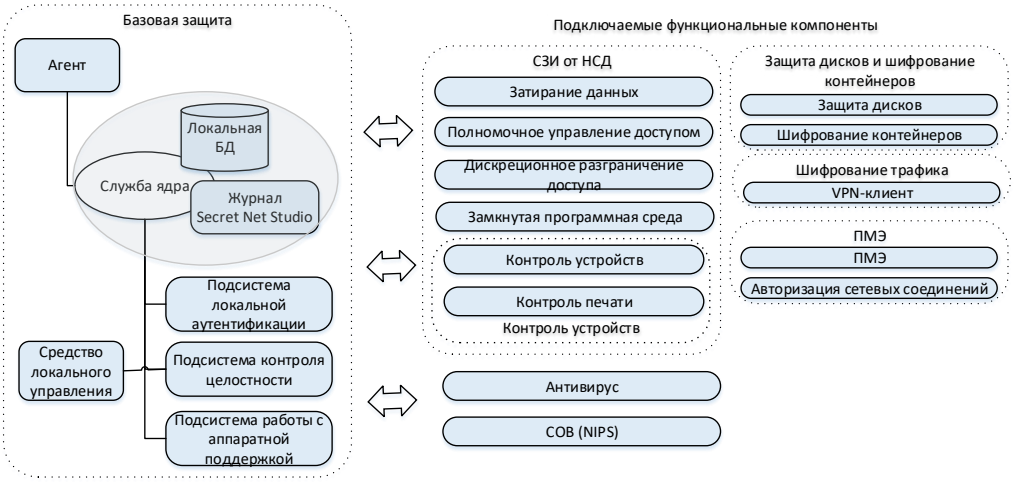


Рисунок 3 - Обобщенная структурная схема клиента

базовая защита – объединяет основные программные службы, модули и защитные подсистемы;

дополнительно подключаемые функциональные компоненты разделены согласно схеме лицензирования продукта (рисунок 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 (рисунок 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 рисунок 3).

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.

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 рисунок 4 представлен пример использования нескольких серверов безопасности СБ1 – СБ4 в структуре домена AD.

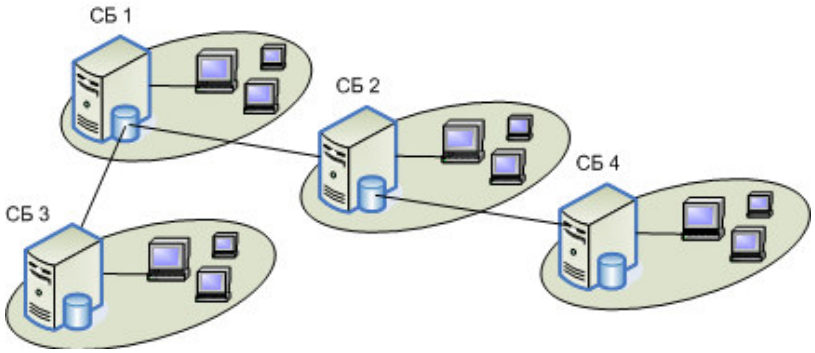


Рисунок 4 - Пример организации нескольких доменов безопасности

Следующий рисунок (рисунок 5) иллюстрирует расширенный пример организации леса доменов безопасности в структуре леса доменов Windows.

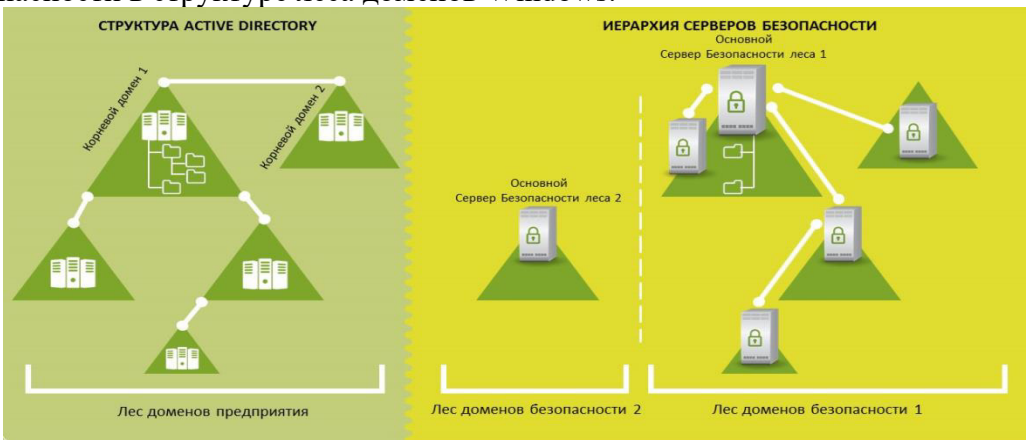


Рисунок 5- Лес доменов безопасности в лесу доменов AD

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 (рисунок3), 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 рисунок 6.

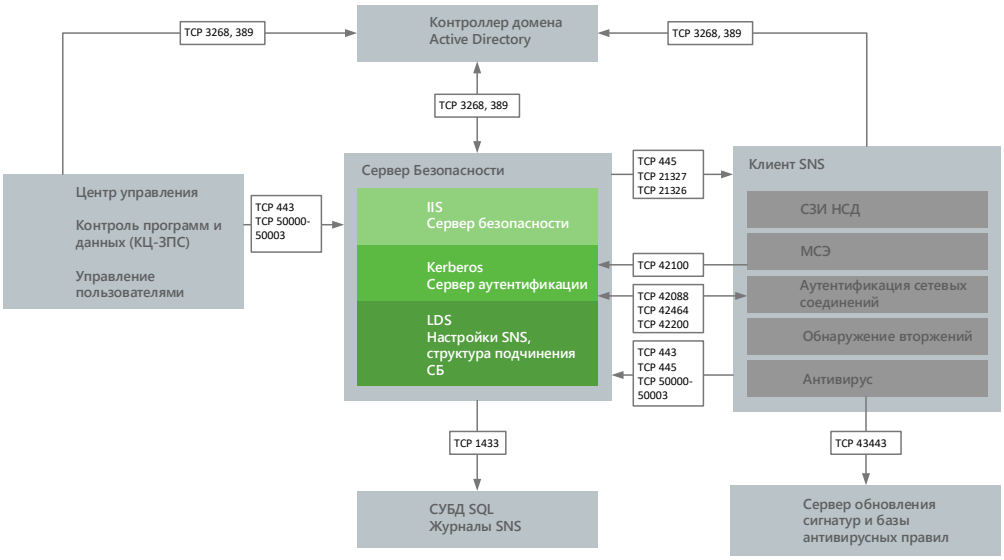


Рисунок 6 - Каналы взаимодействия компонентов системы Secret Net Studio

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.

Лабораторная работа «Сетевая установка компонентов Secret Net Studio на защищаемые компьютеры»

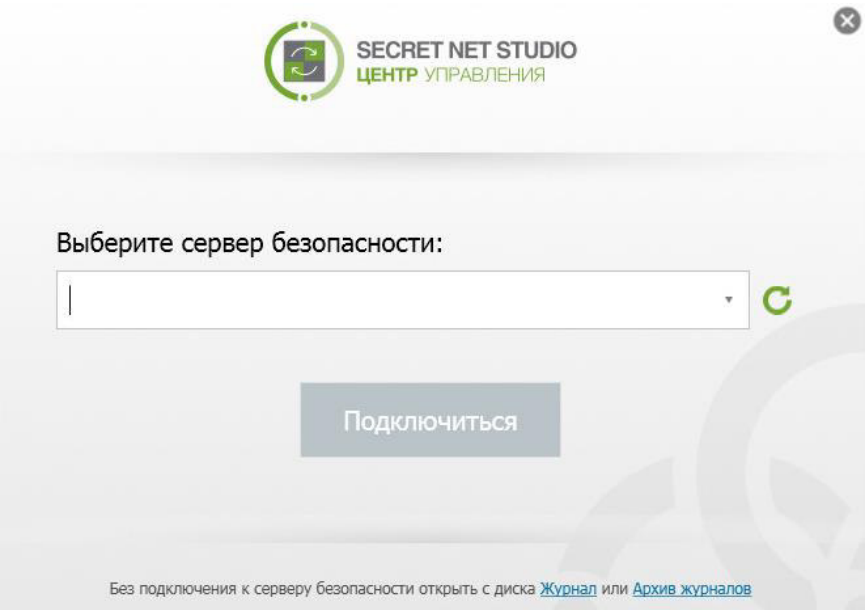
В рамках развертывания СЗИ Secret Net Studio в сетевом варианте на учебном стенде выполнены соответствующие подготовительные действия на компьютерах контроллера домена и сервера безопасности. После этого на ВМ ServerSNS установлено ПО сервера безопасности, а на ВМ ARM2 – программа "Центр управления"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

Примечание: Рекомендумаемая последовательность запуска виртуальных машин: DC-SNS, ServerSNS, ARM2, а далее в произвольном порядке.

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.

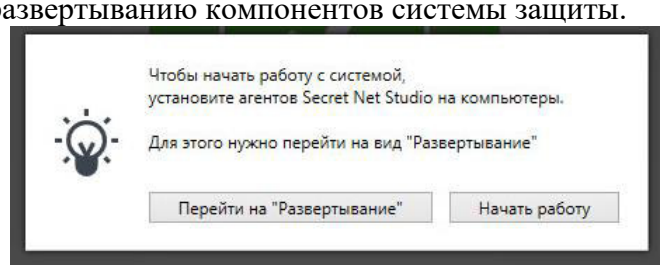
Примечание: Если подключение к серверу безопасности ServerSNS.SN7.local не происходит, то перейдите на виртуальную машину ServerSNS и проверьте запушена ли БД MSSQLExpress. Для этого запустите на рабочем столе виртуальной машины ServerSNS программу SQLManagmentStudio и в появившемся окне нажать кнопку Connect. В результате

успешного подключения появится дерево БД. Если этого не происходит, то далее выполнять лабораторные работы НЕ ИМЕЕТ СМЫСЛА!

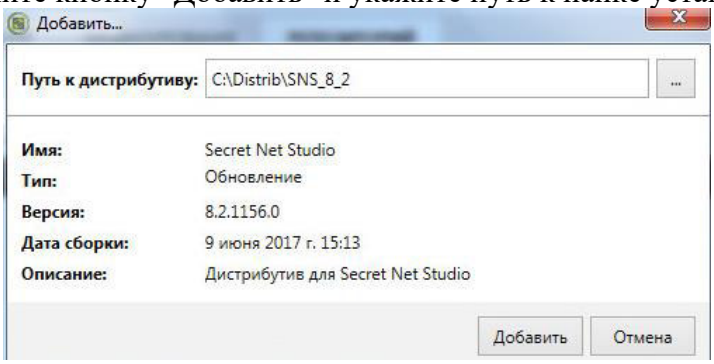
Если отсутсвует SQL Manager, то проверьте состояние MSSQLExpress можно с помощью средств Windows Server 2008 (SQL Server Configuration Manager).

Попробуйте перезагрузить виртуальную машину ServerSNS (используйте корректное завершение работы, например через кнопку Пуск-Завершить и т.д.).

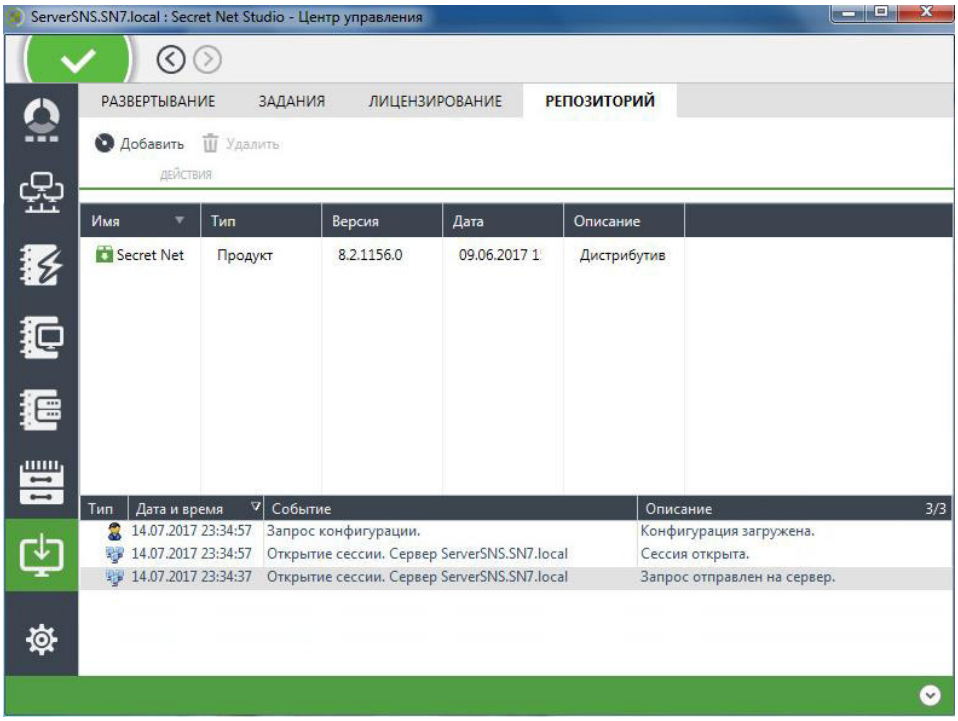
3. Нажмите кнопку "Подключиться" и дождитесь завершения процедуры подключения. В открывшемся окне программы управления появится окно подсказки с предложением перейти к развертыванию компонентов системы защиты.



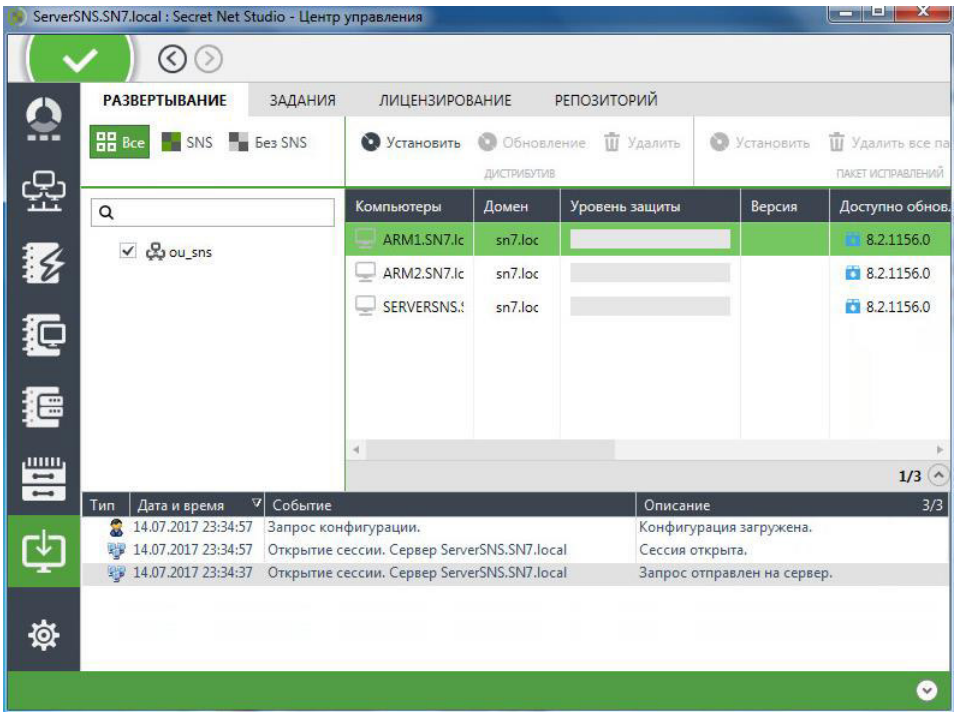
4. Нажмите кнопку "Перейти на "Развертывание". В панели "Развертывание" переключитесь на вкладку "Репозиторий", для добавления дистрибутива Secret Net Studio нажмите кнопку "Добавить" и укажите путь к папке установки: "C:\Distrib\SNS_8_2".



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.

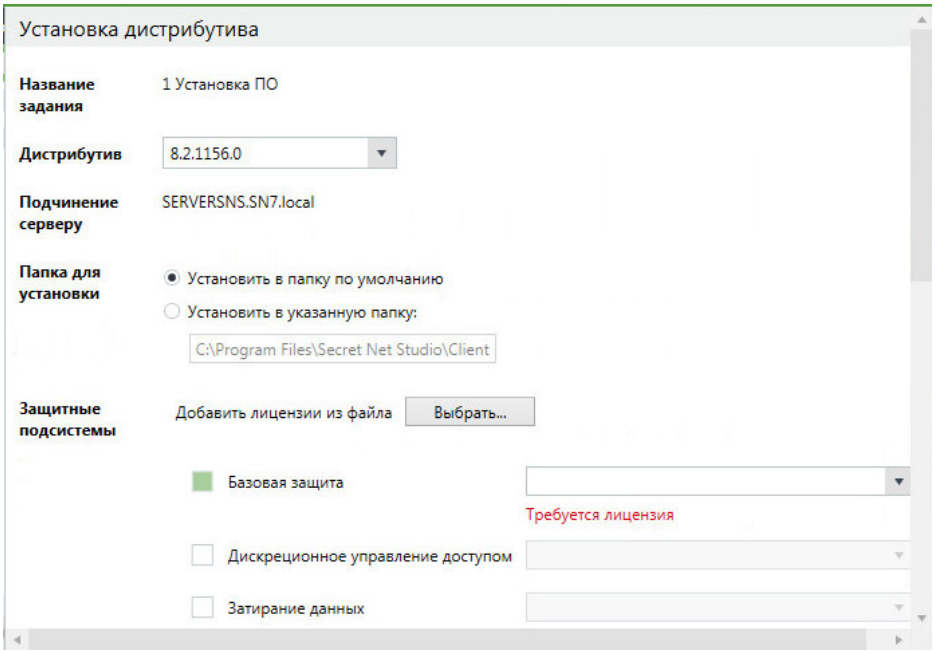


6. После формирования комплекта централизованно устанавливаемого ПО необходимо определить списки компьютеров, на которых в автоматическом режиме будет выполняться установка клиента SNS. В панели "Развертывание" перейдите на вкладку "Развертывание".



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: Рекомендуется устаналивать сетевые версии SNS последовательно по одному компьютеру: ARM2, далее ServerSNS и ARM1.

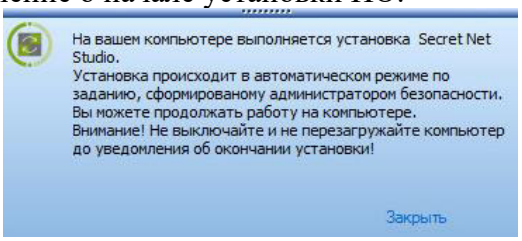


Примечание. Обратите внимание, что в список компьютеров для развертывания компонентов защиты не вошел контроллер домена. Это произошло потому, что ранее мы спроецировали домен безопасности не на весь домен "SN7.local", а только на входящее в его состав организационное подразделение "ou_sns". Для обеспечения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

8. Настройте параметры задания:

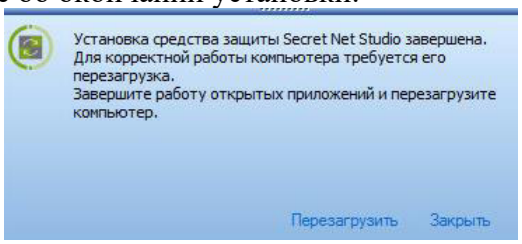
- "Дистрибутив" и "Папка для установки" – оставьте по умолчанию;
- "Защитные подсистемы" – нажмите кнопку "Выбрать" и выберите из папки "C:\Distrib\SNS_8_2\lic" файл с полным составом лицензий;
- прокрутите перечень лицензий вниз и для компонента "Антивирус" выберите "Антивирус (технология ESET)…";
-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



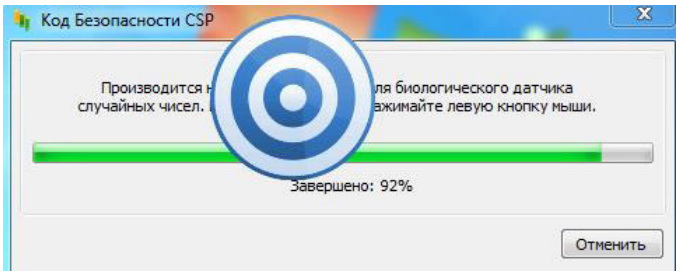
10. Ознакомьтесь с текстом уведомления, нажмите кнопку-ссылку "Закрыть" и перейдите на вкладку "Задания". Здесь вы можете видеть состояние процесса установки выбранного ПО на указанные компьютеры списка. До завершения процесса в области трея

будет мигать значок Secret Net Studio  . После завершения установки в области уведомлений окна ARM2 появится сообщение об окончании установки.



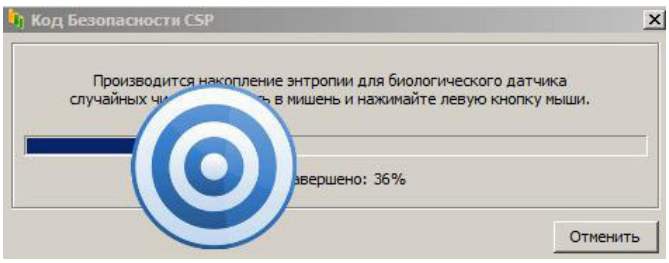
11. Ознакомьтесь с сообщением и перезагрузите ВМ ARM2. Обратите внимание, что загрузка ОС выполняется теперь под контролем защитных механизмов SNS.

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.

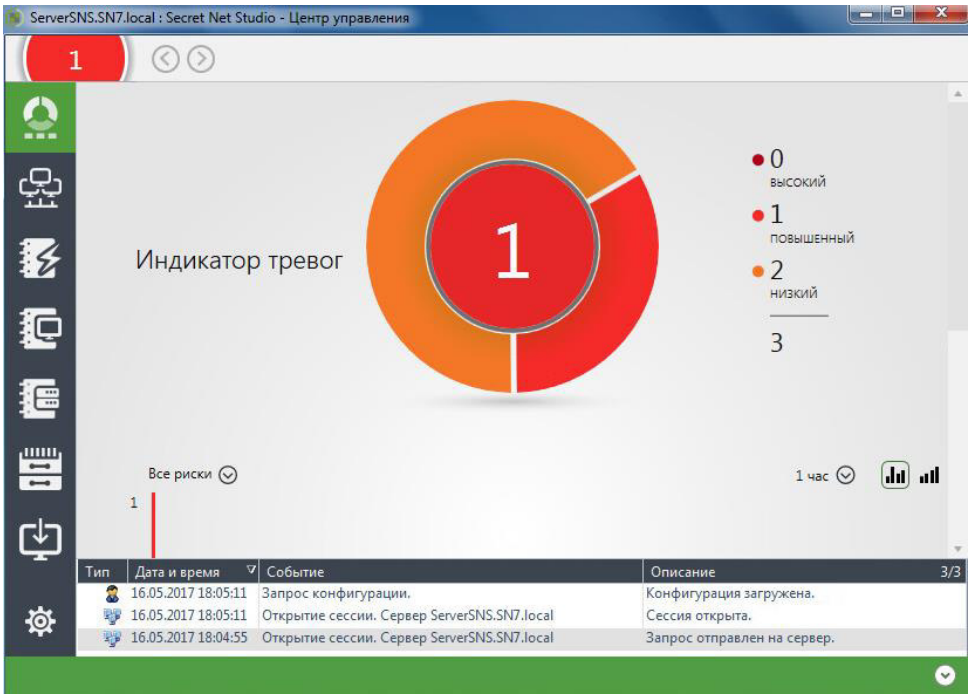


13. Обратите внимание, что в области уведомлений на панели задач в правом нижнем углу экрана появился значок системы Secret Net Studio  .

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.



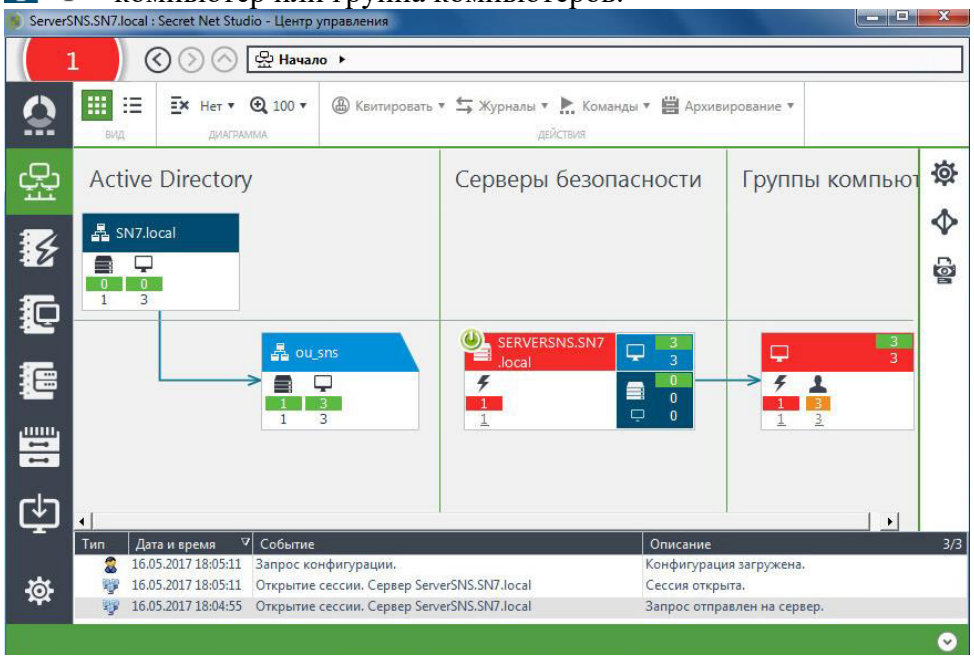
15. Проверьте работу установленных на ВМ ARM2, ServerSNS и ARM1 компонентов. Для этого в окне ВМ ARM2 запустите программу управления и подключитесь к серверу безопасности ServerSNS.


ServerSNS.SN7.local : Secret Net Studio - Центр управления
Индикатор тревог
1
0
ВЫСОКИЙ
1
ПОВЫШЕННЫЙ
2
НИЗКИЙ
3
Все риски
1 час
Тип
Дата и время
Событие
Описание
3/3
16.05.2017 18:05:11
Запрос конфигурации.
Конфигурация загружена.
16.05.2017 18:05:11
Открытие сессии. Сервер ServerSNS.SN7.local
Сессия открыта.
16.05.2017 18:04:55
Открытие сессии. Сервер ServerSNS.SN7.local
Запрос отправлен на сервер.

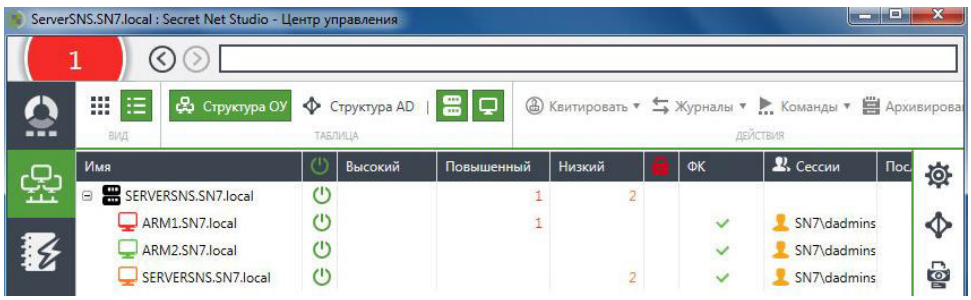
16. Обратите внимание, что в программе управления по умолчанию открылась панель "Начало" – кнопка на панели навигации в левой части окна окрашена в зеленый цвет. Эта панель содержит сведения о соотношении системных событий тревоги и о состоянии групп объектов управления.

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;

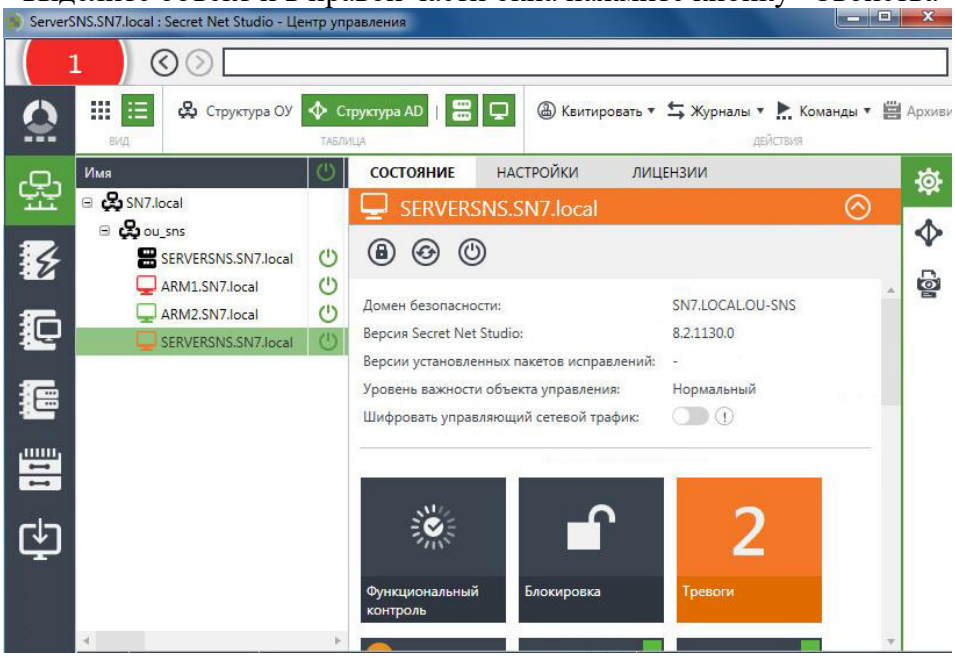
в колонке "ФК" обозначает, что пройден функциональный контроль;

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.

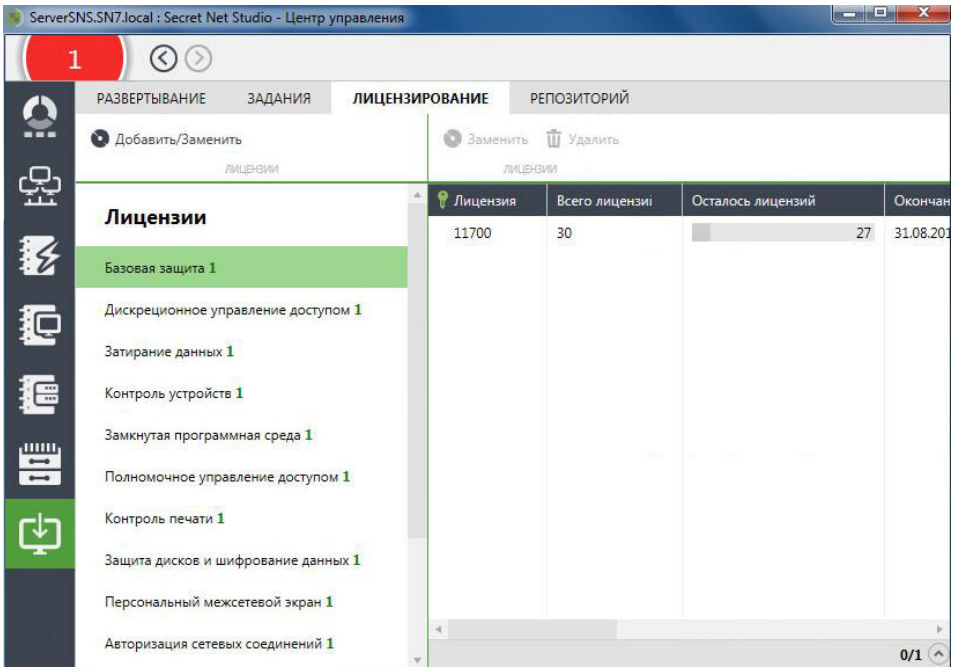
21. Для того чтобы просмотреть свойства любого объекта управляемой структуры, выполните одну из операций:

- 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 BM 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.

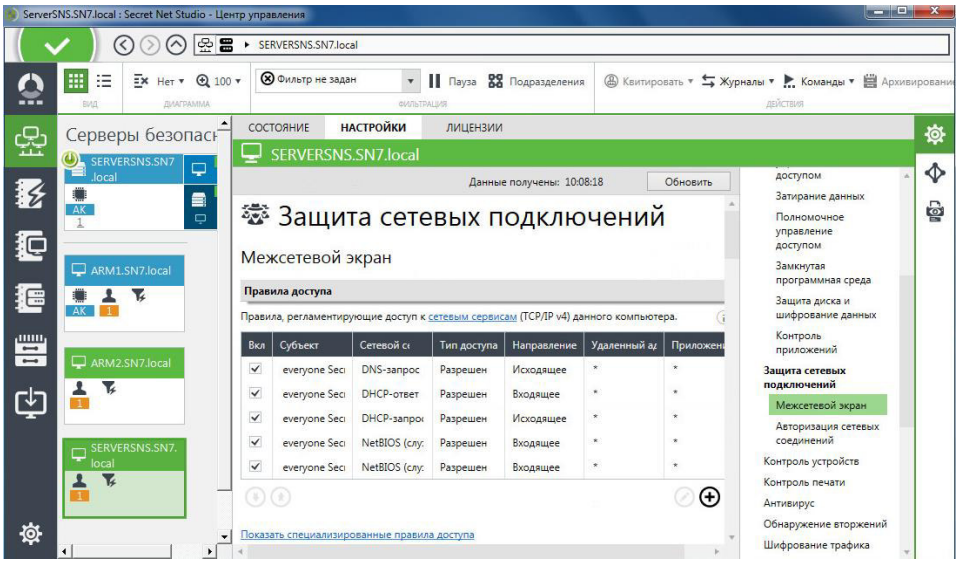
Лабораторная работа "Персональный межсетевой экран"

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.

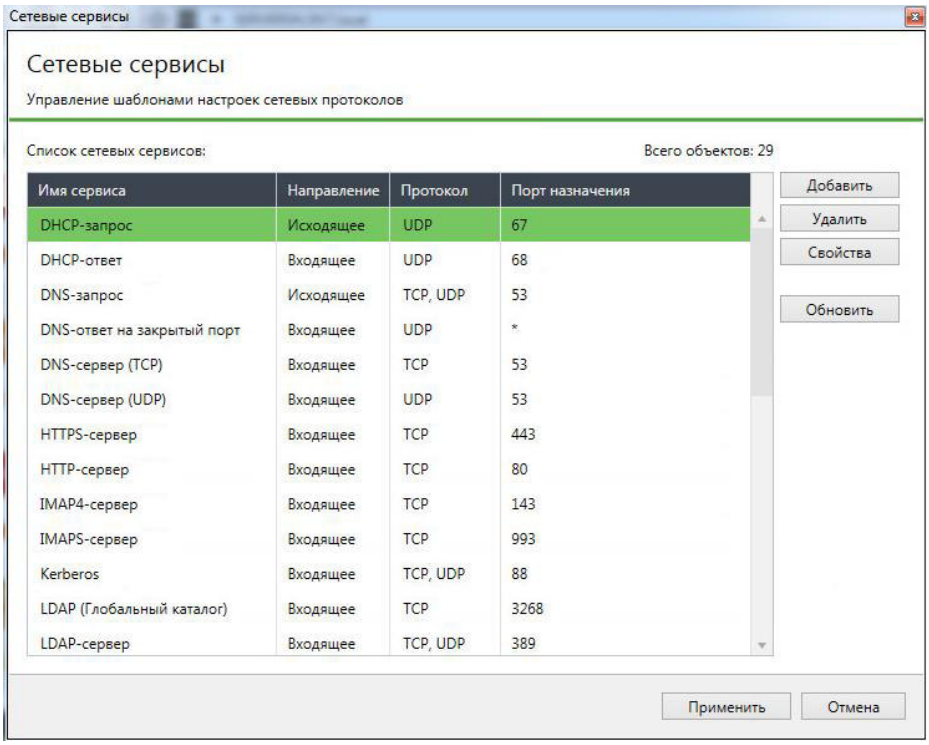
В соответствующем разделе главы 4 описаны группы правил, использующихся для управления доступом, а в данной лабораторной работе рассматриваются некоторые практические примеры их применения.

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.

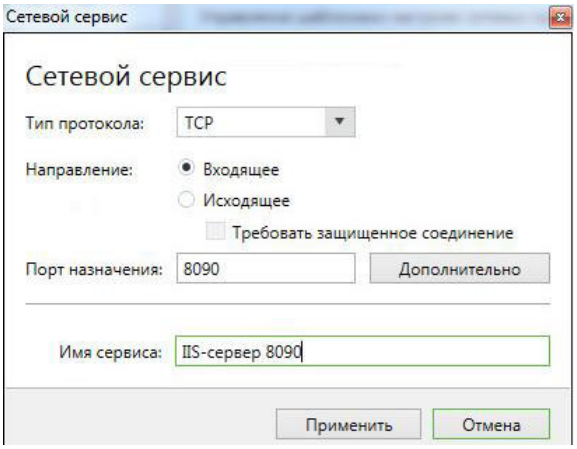


2. Обратите внимание, что первыми в перечне политик следуют правила доступа, которые, как уже отмечалось в главе 4, регулируют доступ пользователей к сетевым сервисам защищаемого компьютера. С помощью кнопки ознакомьтесь с описанием этой группы политик, а затем нажмите над таблицей правил ссылку сетевых 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".



Примечание: IIS (Internet Information Services) это проприетарный (то есть являющийся чей-то собственностью) набор серверов для нескольких служб Интернета от компании Microsoft. Похожие аналоги – Apache, NGINX.

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).

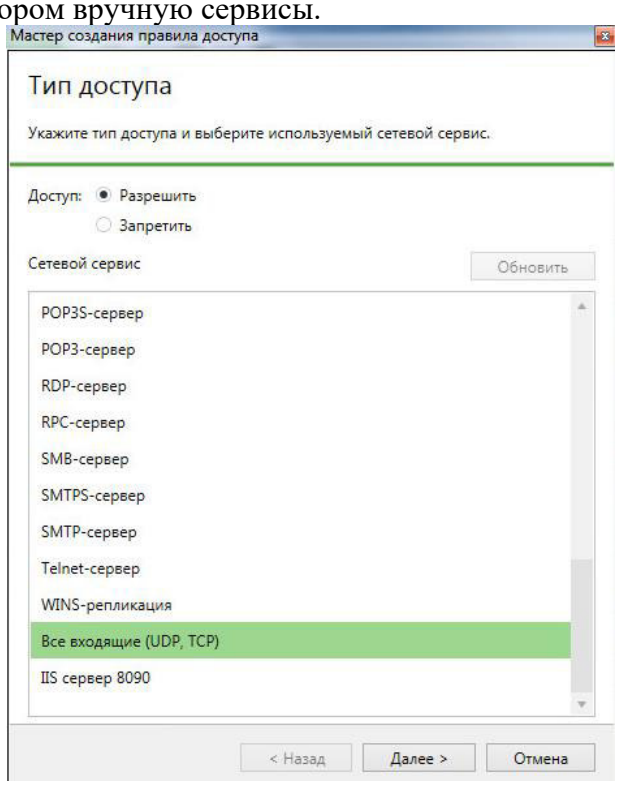
5. Закройте окно "Сетевые сервисы" и вернитесь к перечню политик межсетевого экрана. Добавим запрет RDP-подключения к серверу ServerSNS с компьютера ARM1 (192.168.254.21).

Примечание: RDP (Remote Desktop Protocol) - это проприетарный протокол прикладного уровня удаленного рабочего стола. Позволяет подключиться к серверу под управлением ОС Windows.

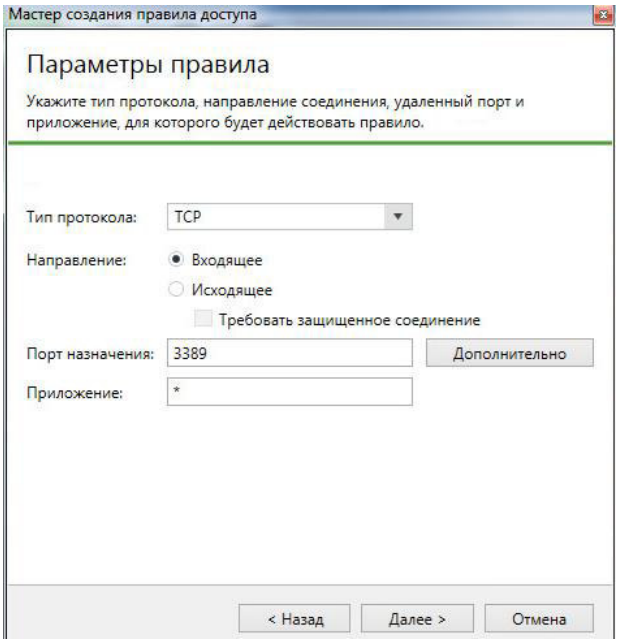
Для дальнейшего выполнения лабораторной работы убедитесь, что RDP-подключение к ServerSNS доступно для всех пользователей с ВМ ARM1 и ARM2. Если это не так, настройте удаленное подключение на сервере.

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.**



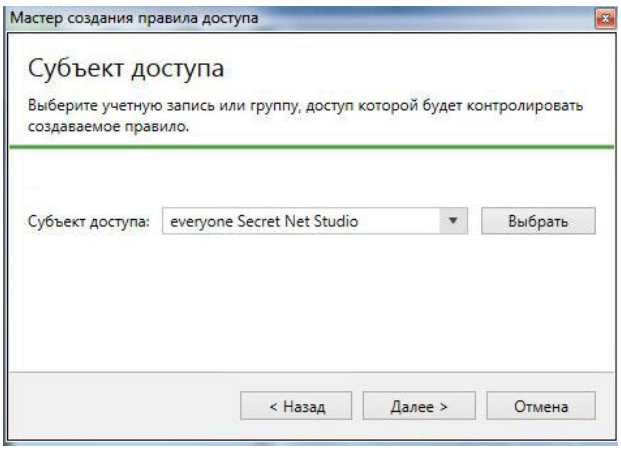
Если необходимо изменить порт, то можно указать нужный номер порта или задать диапазон номеров либо использовать символ "*" (см. п. 3).

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.

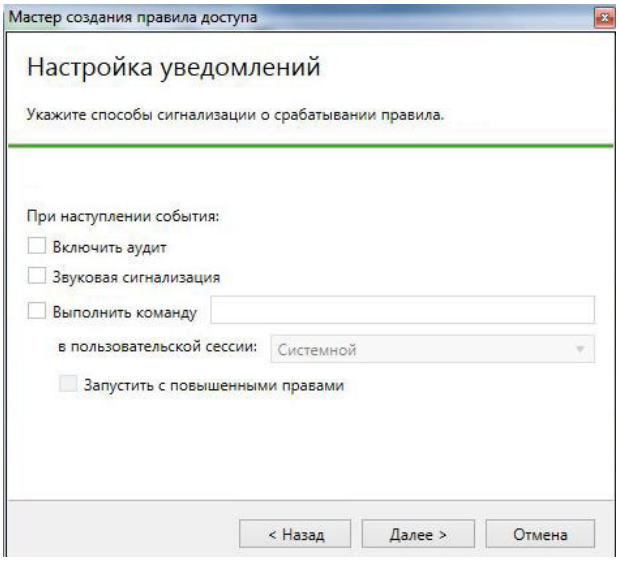
Данная возможность есть только при наличии отдельной лицензии на использование механизма авторизации сетевых соединений. Без такой лицензии в качестве пользователя будет задан “everyone”, т.е. фильтрация трафика будет в режиме обычного МЭ.



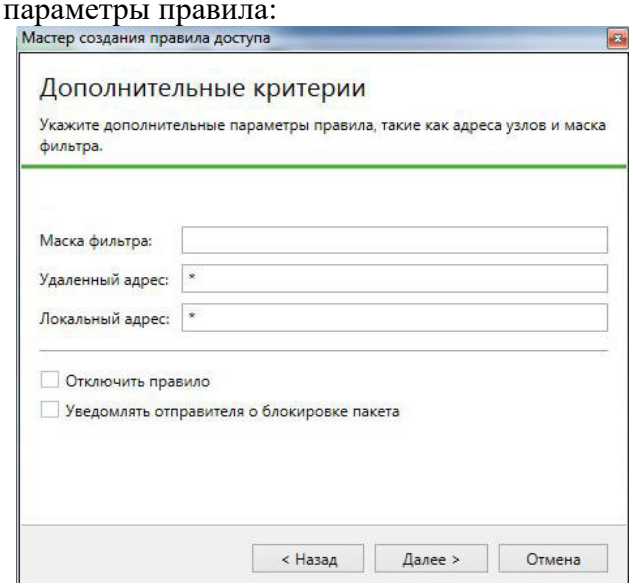
9. Нажмите кнопку "Далее". На этом шаге мастера можно настроить уведомления о срабатывании правила.

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.



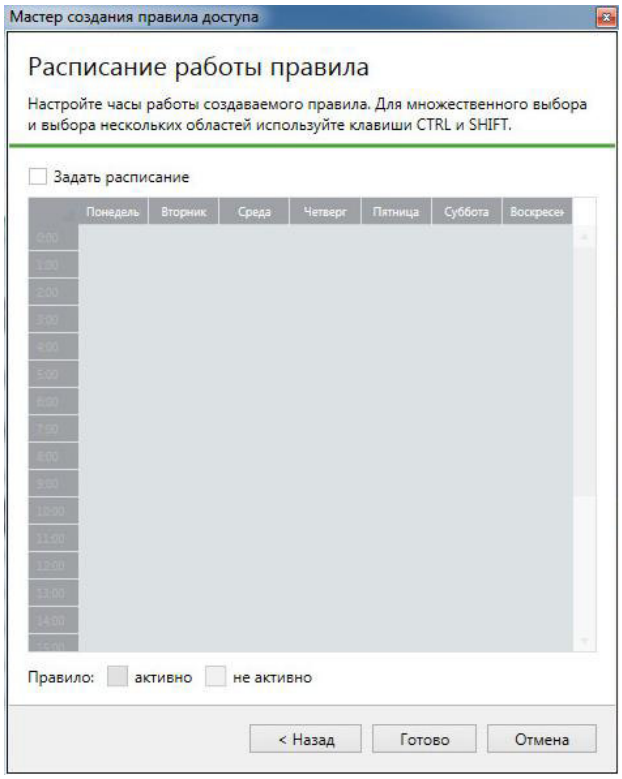
10. Чтобы фиксировать в журнале возникающее при срабатывании правила событие, установите отметку в поле "Включить аудит" и нажмите кнопку "Далее". На следующем шаге настройте дополнительные параметры правила:



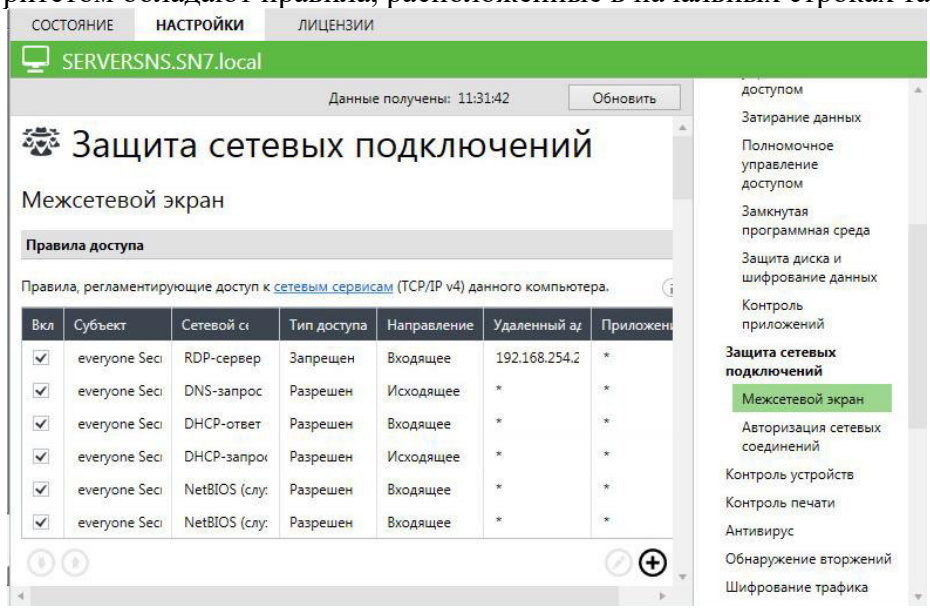
- "Маска фильтра" – оставьте пустым. При необходимости здесь указывается контекст для поиска IP-пакетов. Правилом будут обрабатываться только IP-пакеты, в теле которых содержится введенное значение;
- "Удаленный адрес" – введите IP-адрес компьютера ARM1 – 192.168.254.21. Символ "*" задает действие правила 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).

Примечание: RST-пакет – это заголовок, который сигнализирует о том, что необходимо переподключение.

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.



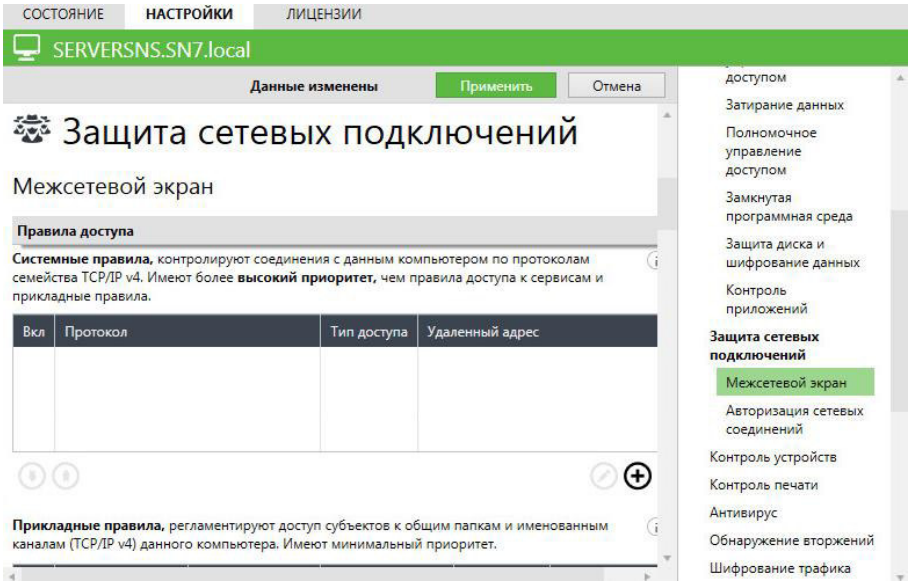
13. Используя описание пп. 6–12, добавьте следующие правила фильтрации доступа для созданного вами ранее сетевого сервиса "IIS-сервер 8090":

- 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.

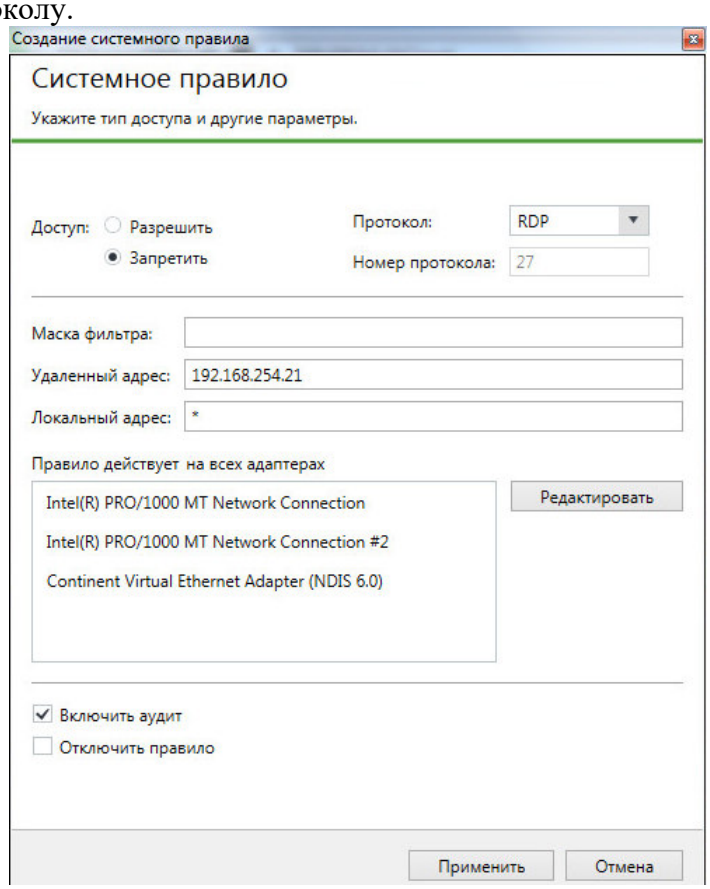
14. С помощью расположенных под таблицей кнопок "Вниз" и "Вверх" установите приоритет разрешающего правила выше, чем запрещающего.

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".

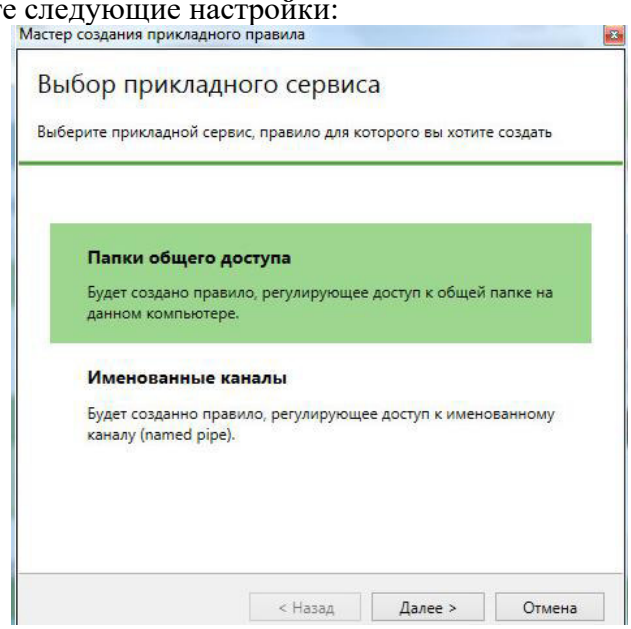


17. Системные правила являются более общими по сравнению с правилами доступа. Ниже на рисунке показан пример настройки рассмотренного выше запрета доступа к серверу ServerSNS по RDP-протоколу.

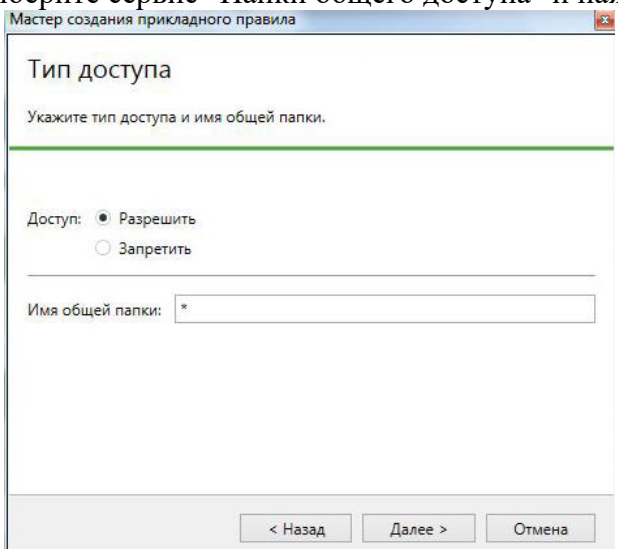


Самостоятельно опишите в качестве примера системных правил созданные вами в пп. 13–14 правила.

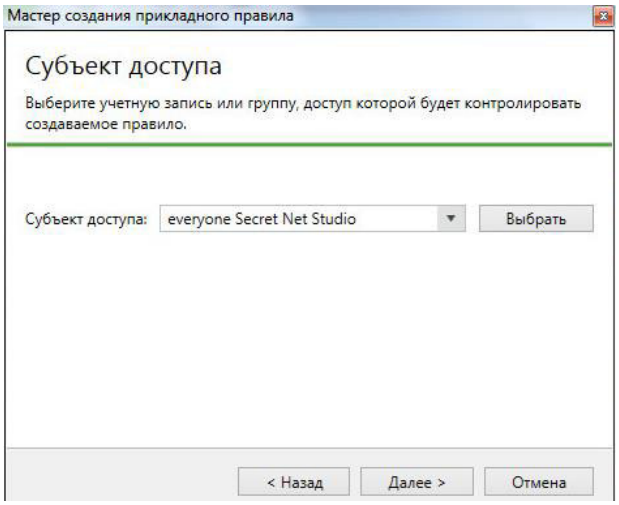
18. Создайте прикладное правило, запрещающее доступ с компьютера ARM1 (192.168.254.21) к общедоступной папке "user_files", расположенной на сервере ServerSNS. Для этого под таблицей "Прикладные правила" нажмите кнопку "Добавить" ⊕ и в окне мастера создания правила выполните следующие настройки:



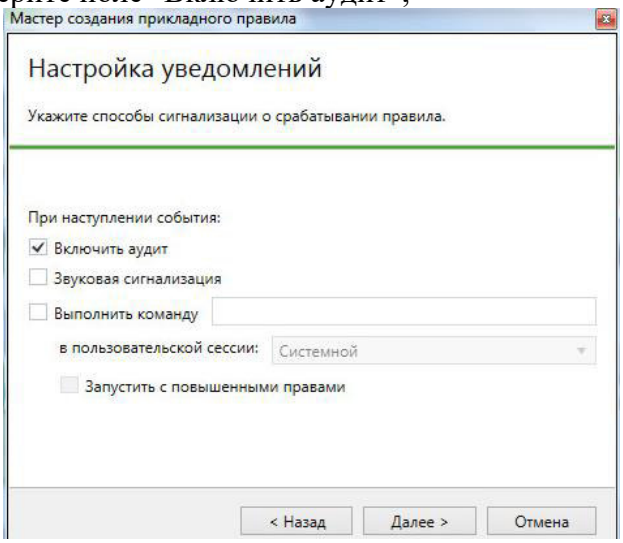
- на начальном шаге выберите сервис "Папки общего доступа" и нажмите кнопку "Далее";



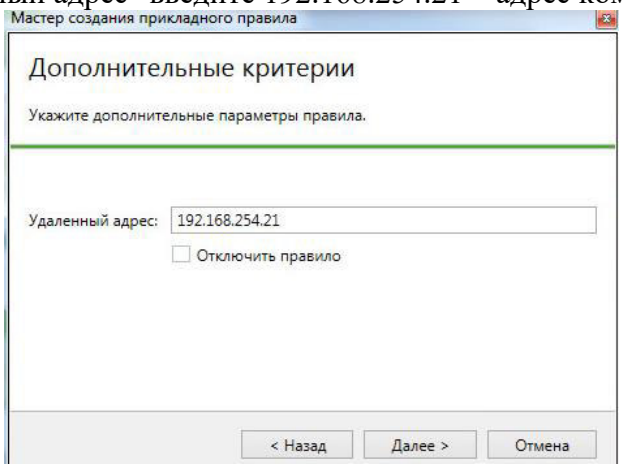
- на следующем шаге установите: "Тип доступа" – "Запретить", "Имя общей папки" – введите user_files;
- нажмите кнопку "Далее". На следующем шаге мастера можно выбрать учетные записи, для которых действует правило;



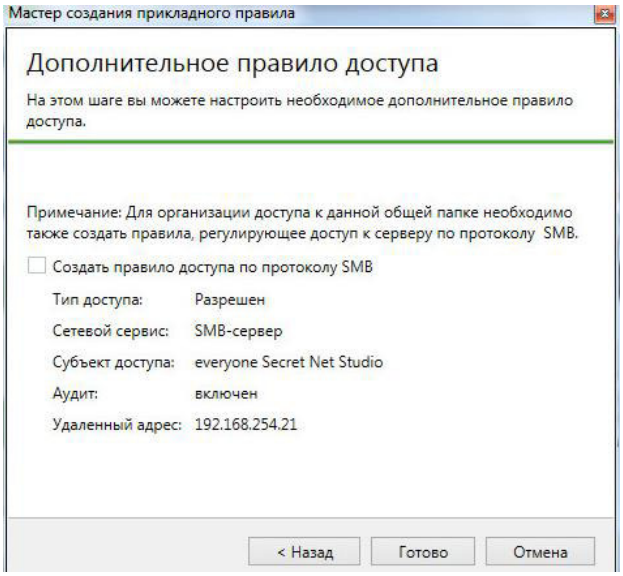
- нажмите кнопку "Далее". На следующем шаге нужно настроить уведомления о срабатывании правила. Выберите поле "Включить аудит";



- нажмите кнопку "Далее". На следующем шаге настраиваются дополнительные параметры. В поле "Удаленный адрес" введите 192.168.254.21 – адрес компьютера ARM1;



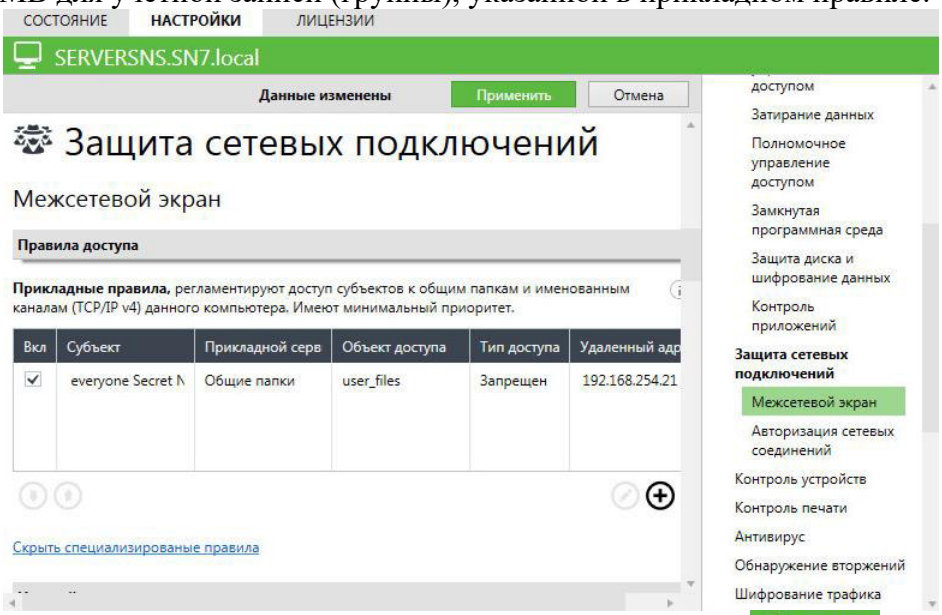
- нажмите кнопку "Далее". На предпоследнем шаге можно настроить расписание. Еще раз нажмите кнопку "Далее" – откроется завершающее окно для создания дополнительного правила доступа;



• 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;

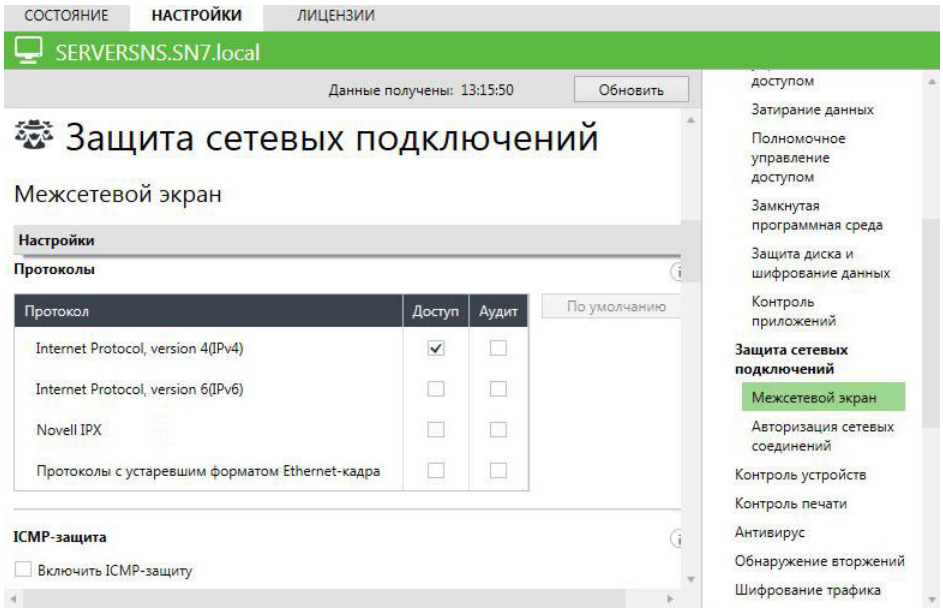
Внимание! Если прохождение пакетов по протоколу SMB запрещается системными правилами или правилами доступа, то прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.

• 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.

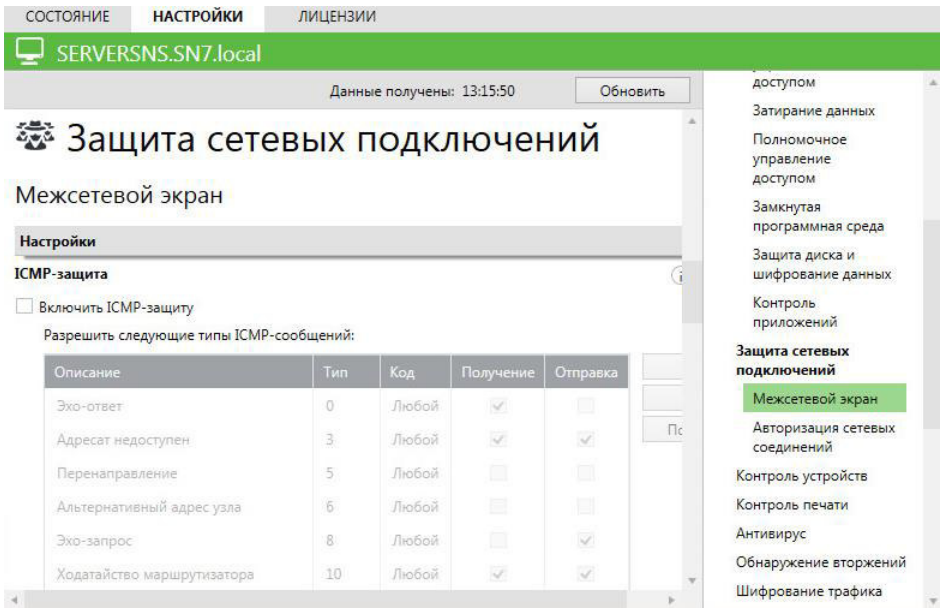


19. На вкладке "Настройки" нажмите кнопку "Применить" Применить. Под таблицей "Прикладные правила" нажмите кнопку-ссылку "Скрыть специализированные правила".

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.



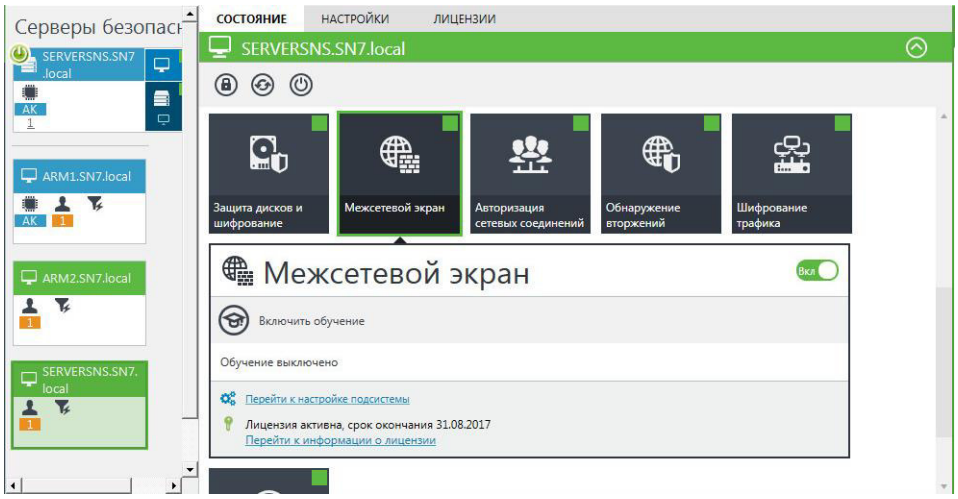
21. Ознакомьтесь с группой настроек "ICMP-защита", которая используется для организации обмена сообщениями по данному протоколу. По умолчанию режим управления пакетами протокола ICMP выключен.



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.

Лабораторная работа "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 ВМ Sniffer и убедитесь, что ее сетевой интерфейс подключен к виртуальному коммутатору в режиме Promiscouos mode и на ней установлена программа Wireshark.

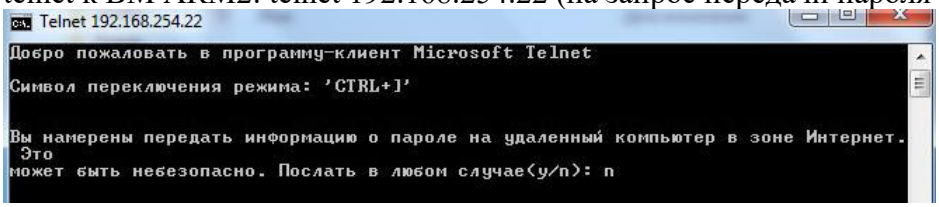
Примечание: Если ВМ Sniffer своим сетевым иртерфейсом подключен неверно (не к виртуальному коммутатору в режиме Promiscouos mode), то АНАЛИЗ ТРАФИКА НЕВОЗМОЖЕН!

При возникновении проблем с нормальной работой ВМ Snifer следует проверить, к какому виртуальному коммутатору он подключен (в нашем случае он назван SNS_snifer), далее проверить свойства этого коммутатора (это долно быть - Promiscouos mode).

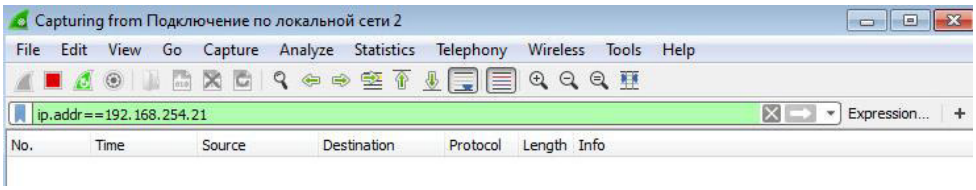
Если все вышеуказанное параметры установлено правильно, а ВМ Snifer все равно работает не корректно (не прослушивает сеть), то попробуете переподключить один из сетевых интерфейсов (их всего два) ВМ Server_SNS к виртуальному коммутатору SNS_snifer. Таким образом, один сетевой интерфейс так и сотанется подключенным к виртуальному коммутатору SNS_test, а второй сетевой интерфейс вместо коммутатора с именем 172.17.108.0/22 следует включить в виртуальный коммутотор с именем SNS_snif.

1. На ВМ 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 ВМ ARM1 откройте от имени администратора командную строку и начните подключение по telnet к ВМ ARM2: telnet 192.168.254.22 (на запрос передачи пароля введите n);

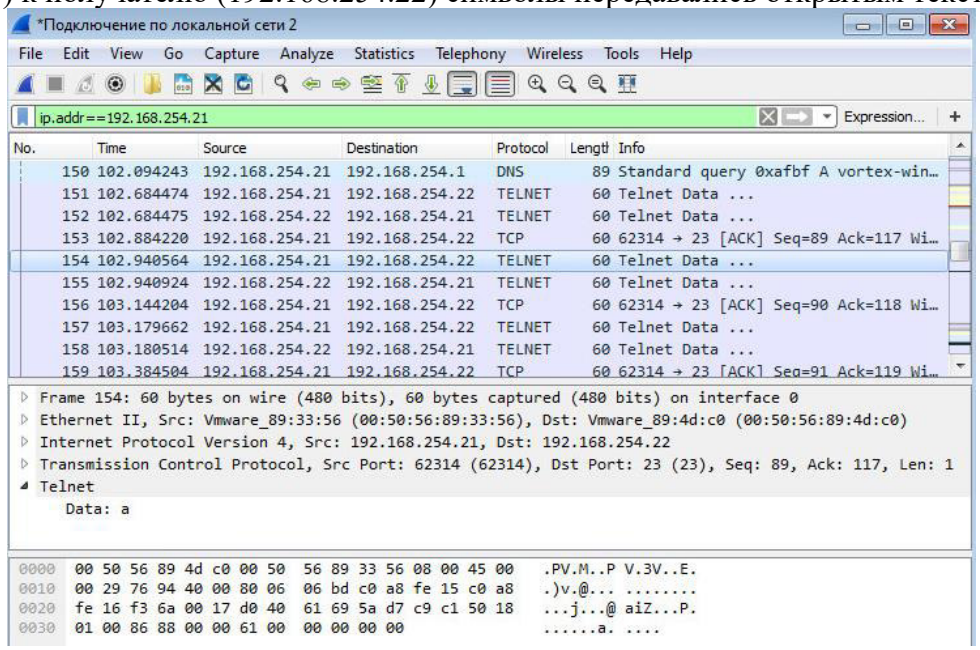


- переключитесь в окно ВМ Sniffer, запустите утилиту Wireshark и начните перехват трафика, указав в поле "Apply a display filter" строку фильтра ip.addr==192.168.254.21;



- переключитесь на ВМ 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 ВМ 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.

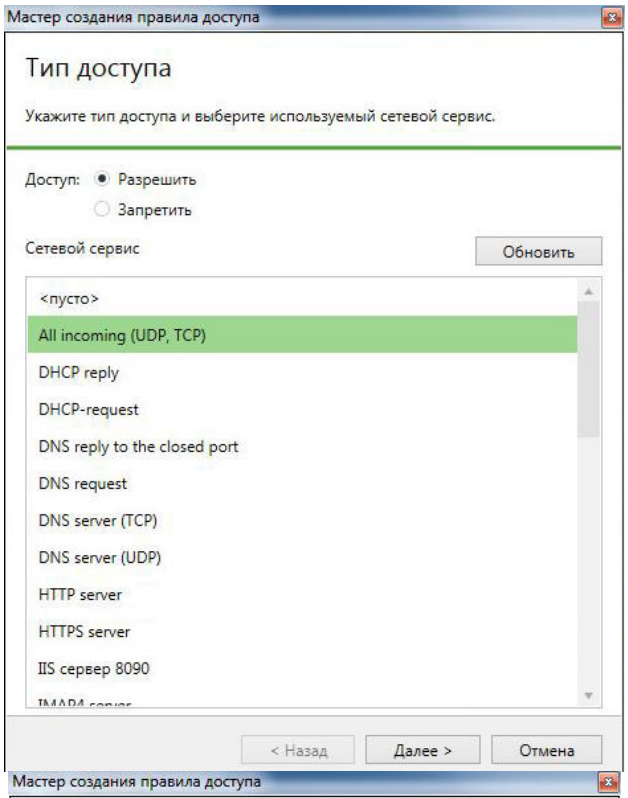


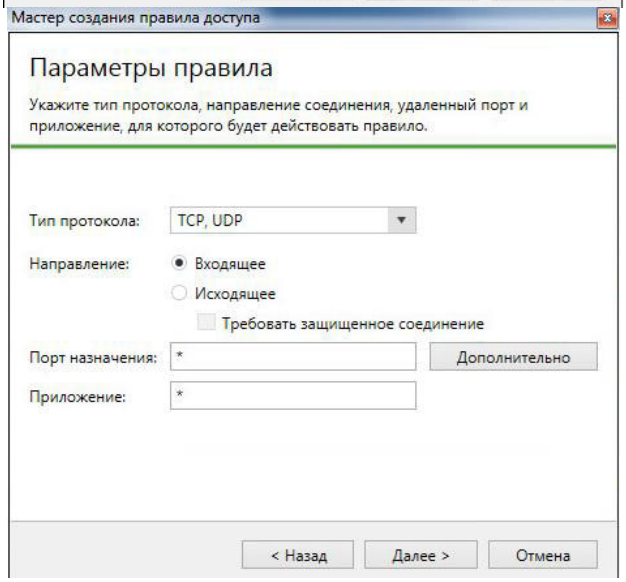
Таким образом, можно констатировать, что при отключенном механизме авторизации сетевых соединений между клиентами Secret Net Studio передается не защищенный трафик.

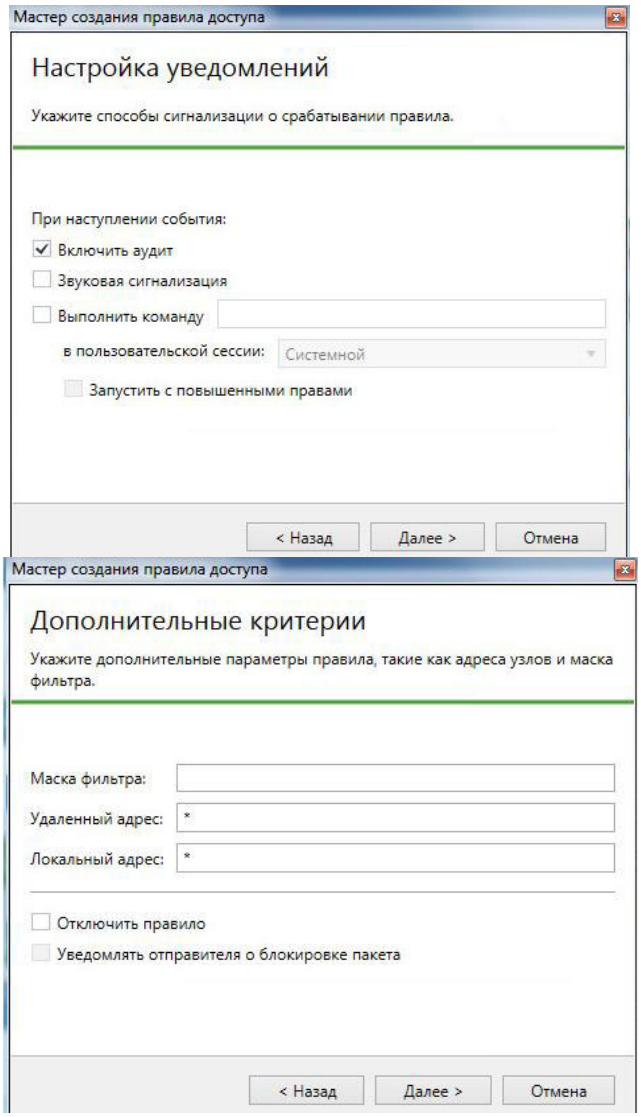
3. Перед установкой защищенного соединения для взаимодействия между компьютерами отправителя и получателя на ВМ ARM2 в программе управления в сетевом режиме настройте правила доступа. Для этого:

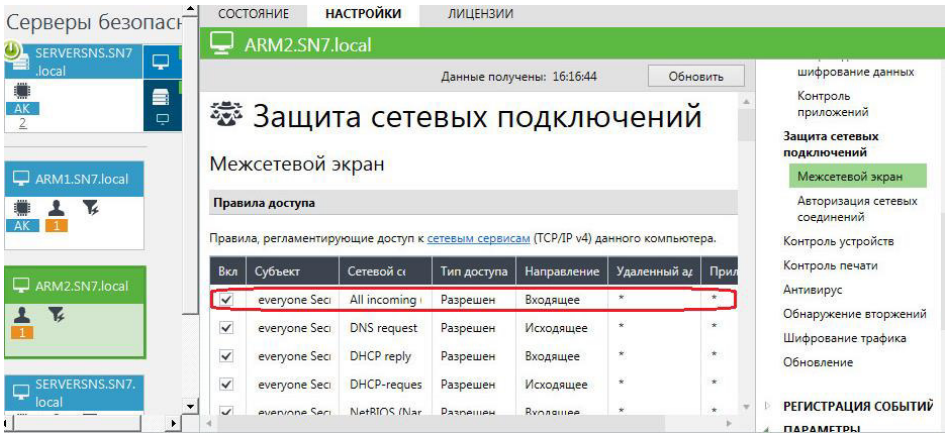
- в панели "Компьютеры" раскройте панель объекта ARM2;
- на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Межсетевой экран" и, используя описание пп. 6–12 предыдущей лабораторной работы, создайте для клиентов группы Everyone разрешающее правило для TCP /UDP – трафика на 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
Тип доступа
Укажите тип доступа и выберите используемый сетевой сервис.
Доступ:
Разрешить
Запретить
Сетевой сервис
Обновить
<пусто>
All incoming (UDP, TCP)
DHCP reply
DHCP-request
DNS reply to the closed port
DNS request
DNS server (TCP)
DNS server (UDP)
HTTP server
HTTPS server
IIS сервер 8090
< Назад
Далее >
Отмена


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

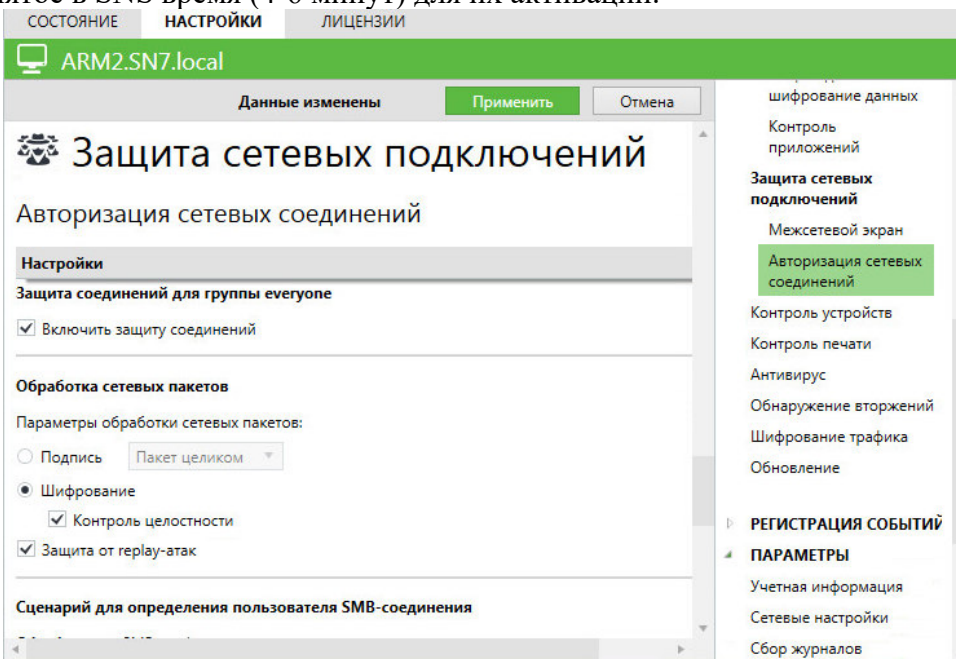


Примечание. Группа Everyone включает в себя пользователей и компьютеры, которые:

- 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:

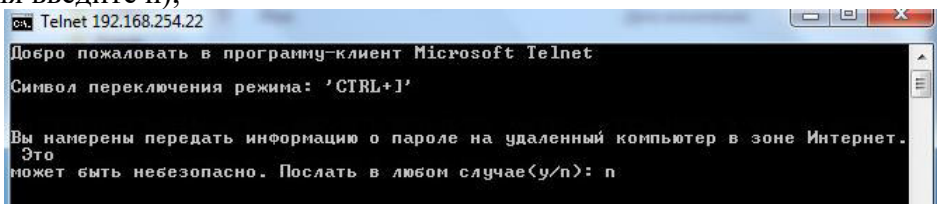
- для объекта ARM2 на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Авторизация сетевых соединений";
- в группе настроек "Защита для группы everyone" установите отметку в поле "Включить защиту соединений";
- в группе настроек "Обработка сетевых пакетов" установите отметку 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.



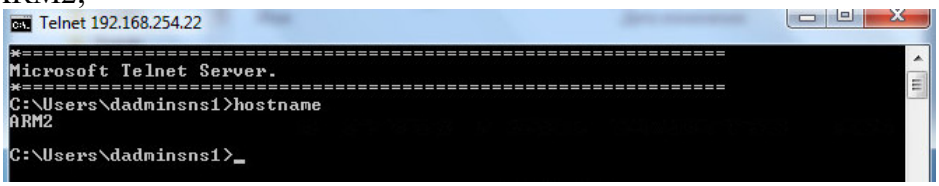
5. Убедитесь, что после включения механизма авторизации сетевых соединений между клиентами SNS передается защищенный трафик. Для этого:

- на ВМ ARM1 закройте открытое ранее подключение по telnet к ВМ ARM2, используя комбинацию клавиш [Ctrl+]] и команду quit:

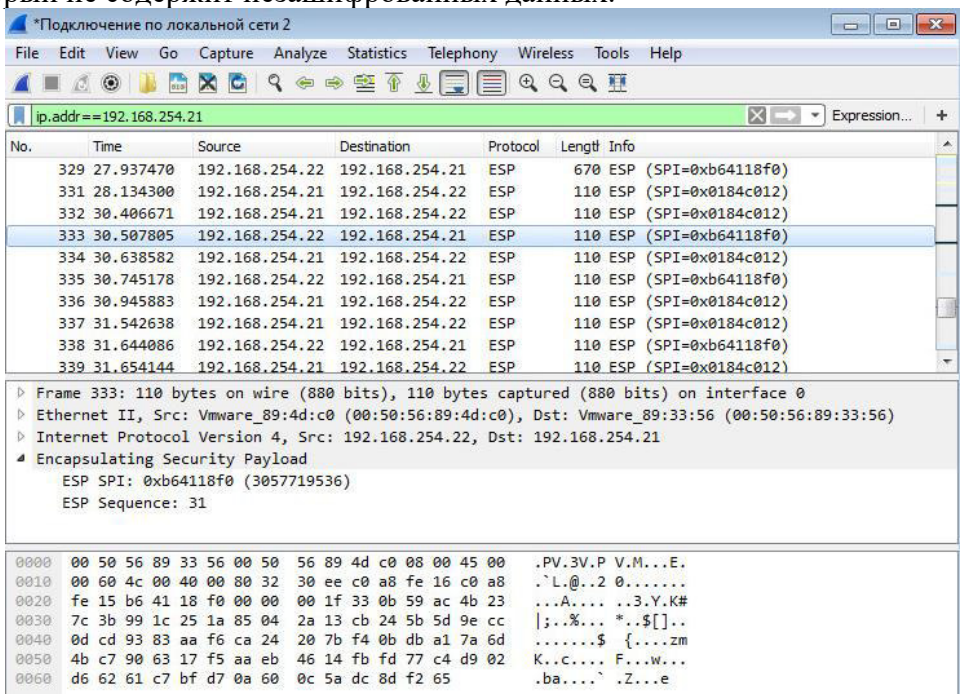
- начните новое telnet-подключение к ВМ ARM2: telnet 192.168.254.22 (на запрос передачи пароля введите n);



- переключитесь в окно ВМ 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 ВМ 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 ВМ 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 ВМ ARM1 и закройте открытое ранее подключение по telnet к ВМ ARM2, используя комбинацию клавиш [Ctrl+]] и команду quit.

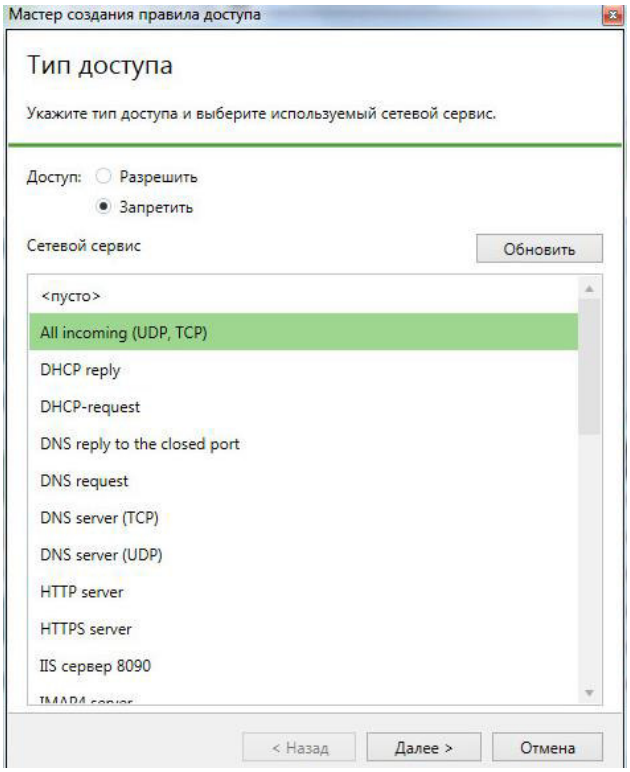
Аналогичный подход может применяться для обеспечения безопасности не только telnet-подключений, но и других сетевых сервисов, которые используются и передают информацию в открытом виде, например, http (обеспечение безопасного подключения клиентов к развернутому в организации веб-серверу).

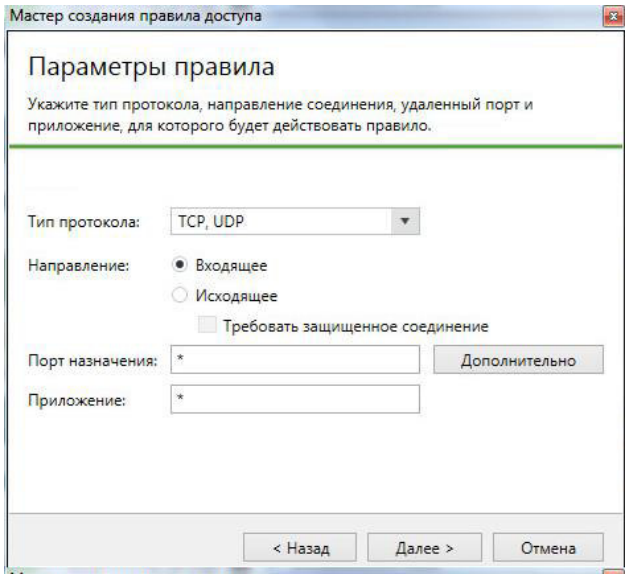
7. Как уже отмечалось выше, механизм авторизации сетевых соединений обеспечивает защиту взаимодействия только между авторизованными на СБ клиентами Secret Net Studio. Если на компьютере пользователя не установлен Secret Net Studio или пользователь по каким-либо причинам не прошел аутентификацию на СБ SNS (anonymous), то трафик между ним и авторизованным клиентом SNS не будет защищаться.

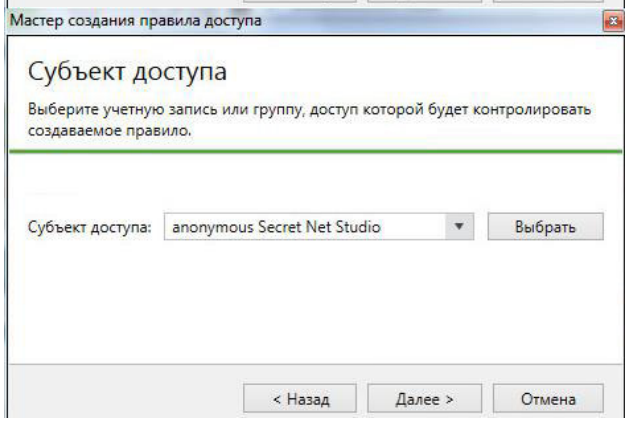
Однако с помощью соответствующих правил межсетевого экранирования администратор может настроить блокировку соединений для неавторизованных на СБ пользователей (anonymous). Для этого:

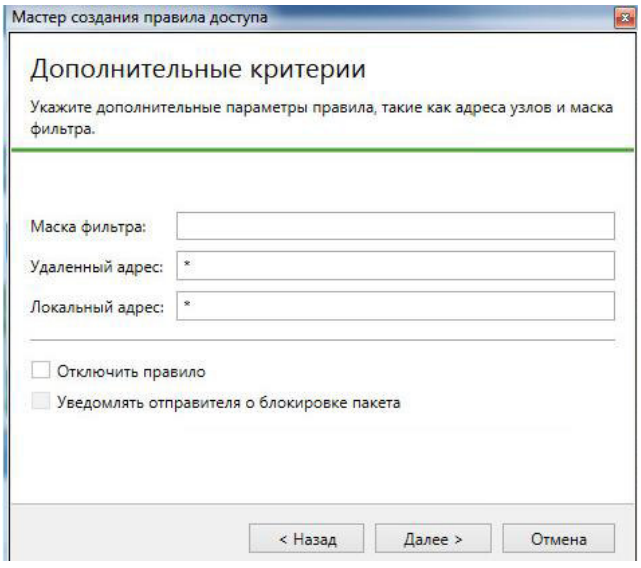
- переключитесь в окно программы управления на ВМ ARM2, в панели "Компьютеры" выберите объект ARM2 и раскройте панель его свойств;
- на вкладке "Настройки" выберите раздел "Политики / Защита сетевых подключений / Межсетевой экран" и, используя описание пп. 6–12 предыдущей лабораторной работы, создайте для клиентов группы anonymous запрещающее правило для TCP /UDP–трафика на любой порт с любого удаленного порта.

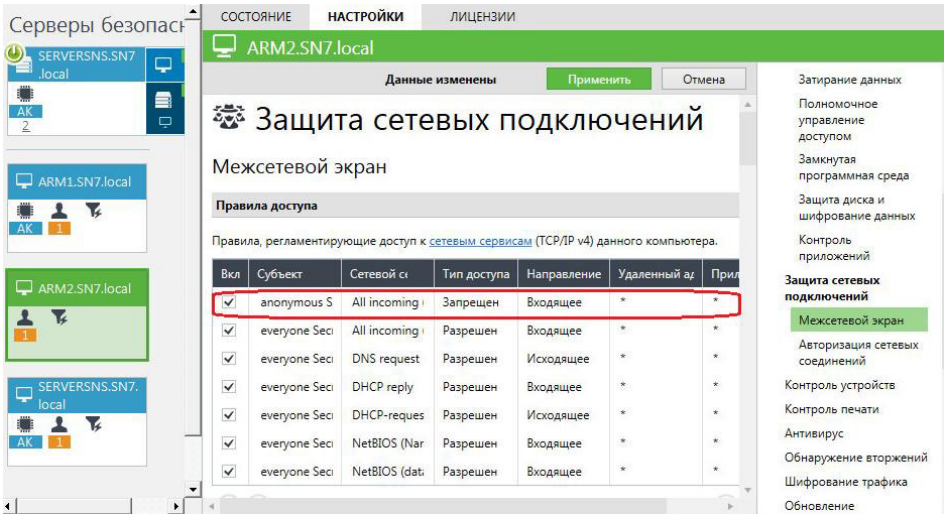
Пользователь	Источник	Протокол/порт	Получатель	Протокол/порт	Действие
anonymous	*	TCP, UDP / any	*	any / any	deny




Мастер создания правила доступа
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
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
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.

Лабораторная работа "Настройка антивируса и СОВ"

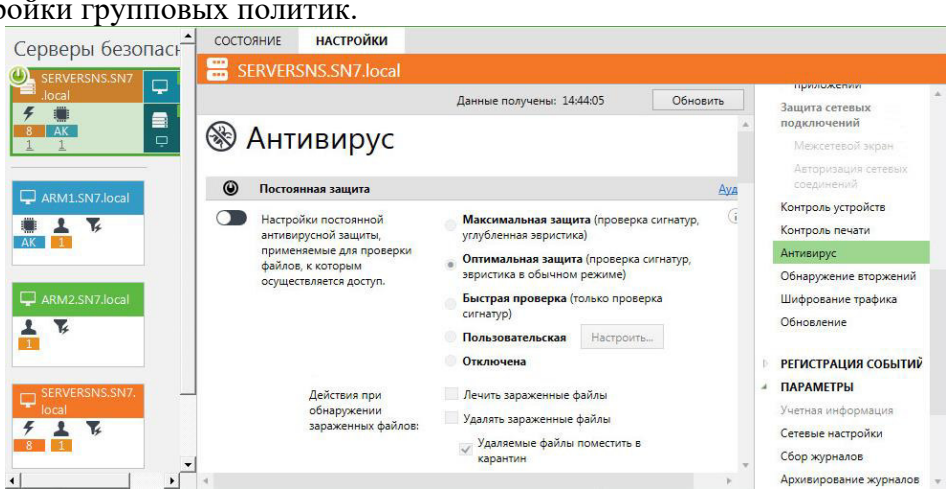
Настройка параметров антивируса и СОВ осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления Secret Net Studio.

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.

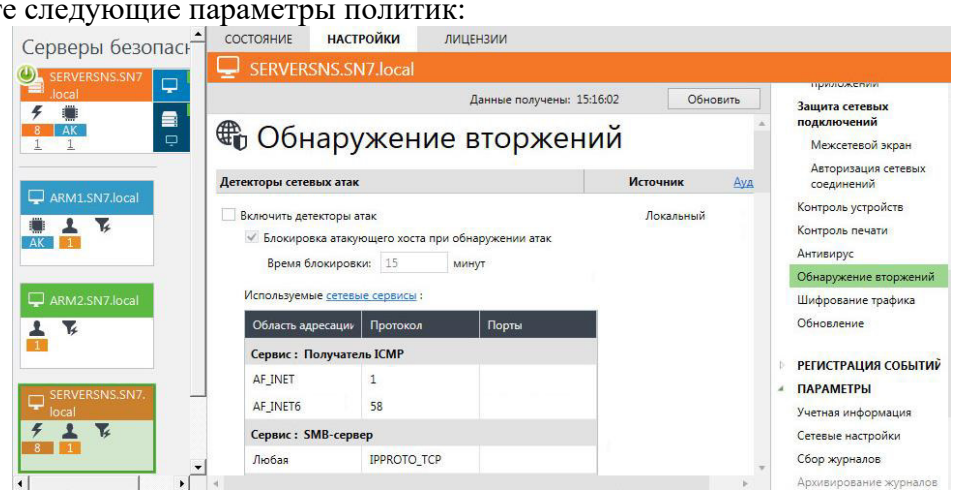
С помощью кнопки ⓘ ознакомьтесь с описанием профиля "Постоянная защита". Обратите внимание, что если одновременно отмечены пункты "Лечить зараженные файлы" и "Удалять зараженные файлы", то при обнаружении зараженных объектов сначала будет выполнена попытка их лечения, а затем, при неудаче, файлы будут 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.

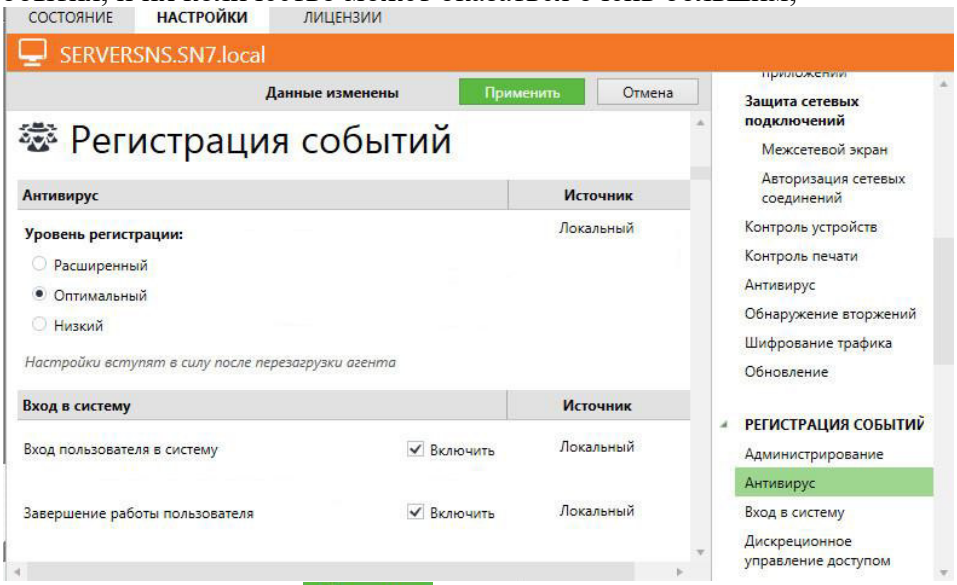
3. Проведите настройку политик СОВ (Системы Обнаружения Вторжений) на СБ. Для этого в программе управления в сетевом режиме выберите в панели "Компьютеры" объект

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" 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;

Примечание. В Windows для проверки соединений в сетях на основе TCP/IP рекомендуется использовать команду ping.

- откройте командную строку от имени администратора, перейдите в папку "C:\Progam files (x86)\nmap" и проведите сканирование портов защищаемого сервера с помощью команды nmap («Network Mapper»):

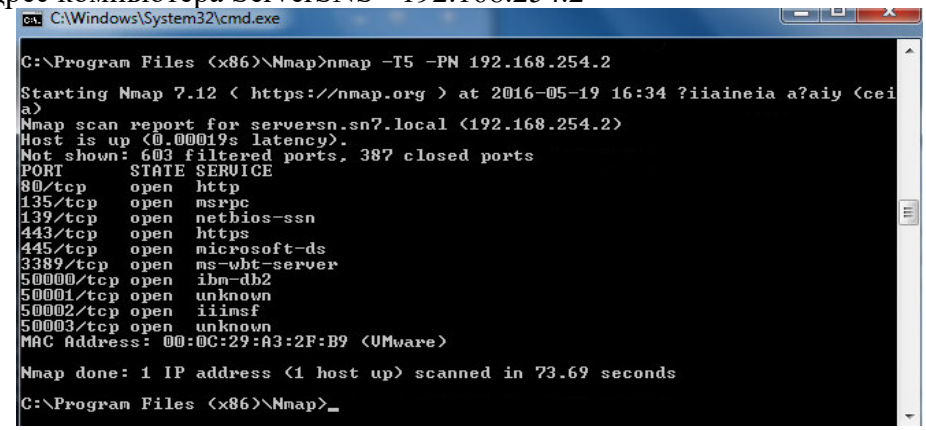
nmap -T5 -PN 192.168.254.2;

Примечание. Формат команды: nmap <ключи> цель

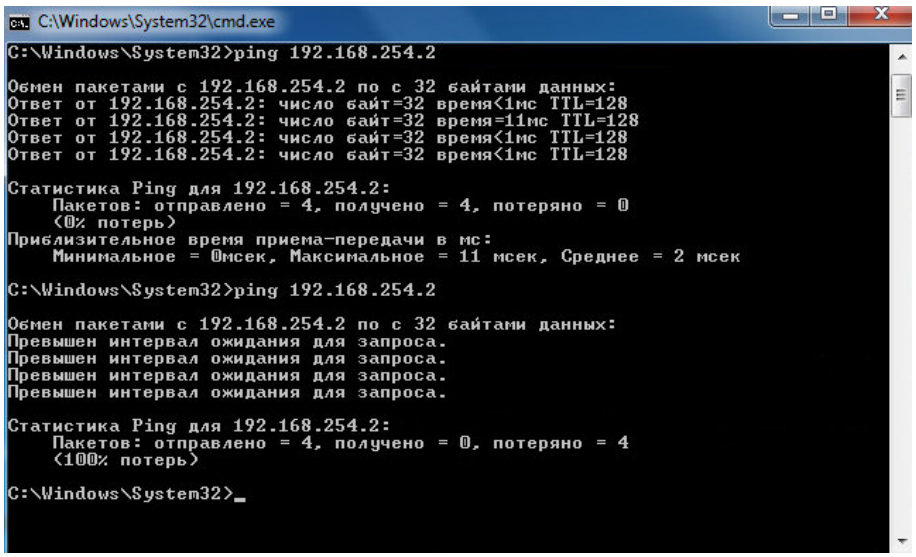
Ключ: -T5 устанавливает большую скорость, маленькие тайминги.

Ключ: -PN Не пинговать (No ping) хосты перед сканированием.

Цель: IP адрес компьютера ServerSNS - 192.168.254.2



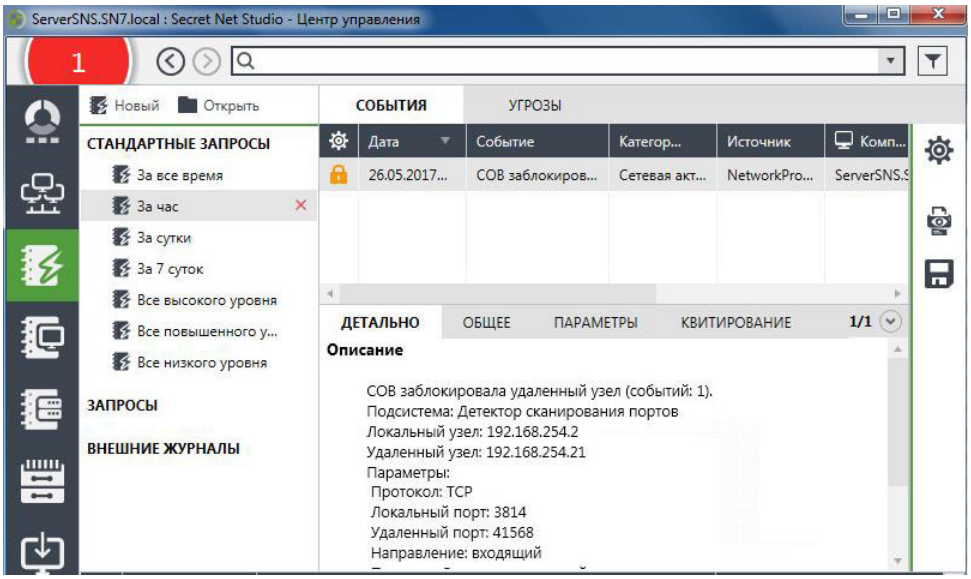
- с помощью утилиты ping повторно проверьте доступность компьютера ServerSNS (192.168.254.2) и убедитесь, что эхо-ответы не приходят (то есть сработала защита SNS-Secret Net Studio).



5. Перейдите в консоль ARM2. Обратите внимание, что:

- в панели событий появились записи о событиях тревоги на СБ;

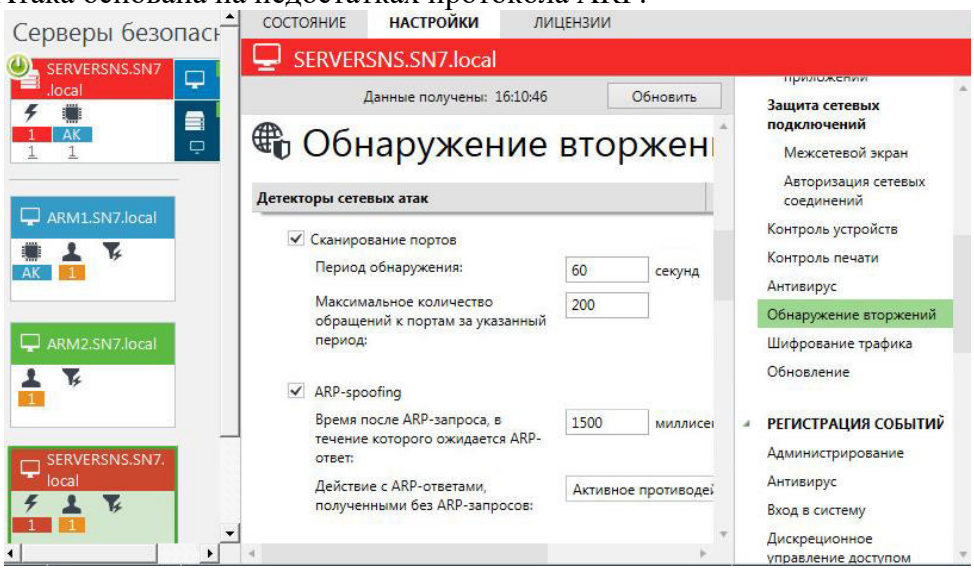
- в журнале тревог появились сообщения о блокировке атакующего узла (категория "Сетевая активность" тип "Аудит отказов").



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" Применить и подождите около 4–6 минут, пока настройки применятся.

Примечание. Атака ARP-spoofing разновидность сетевых атак типа MITM (Man in the middle – «человек посередине»), применяемая в сетях с использованием протокола ARP (Address Resolution Protocol - протокол разрешения адреса). В основном применяется в сетях Ethernet. Атака основана на недостатках протокола ARP.



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): ;

Примечание. Рекомендуется перепроверить полученный MAC-адрес компьютера ARM2 в соотвествующих свойствах сетевого адаптера (network adapter) для ВМ ARM2-SNS1.

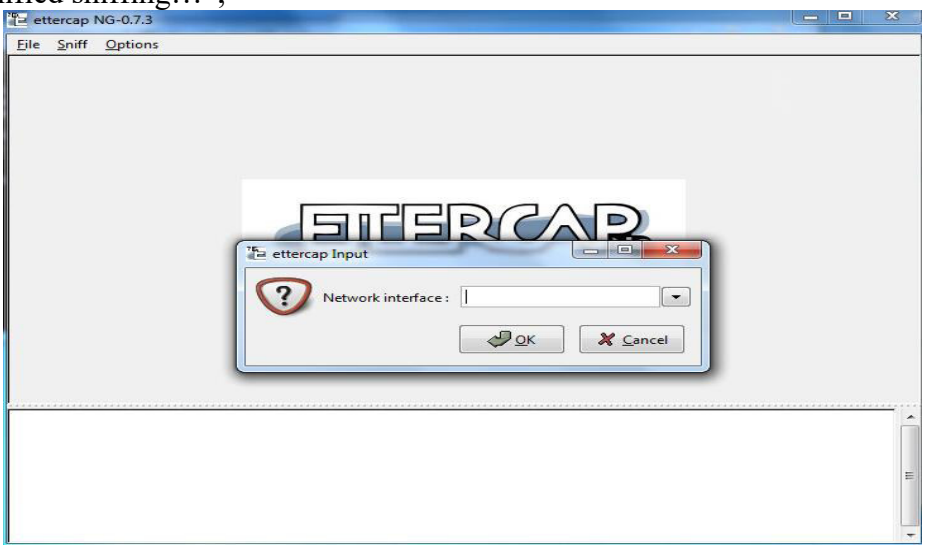
- в окне консоли ServerSNS запустите постоянную проверку доступности компьютера ARM2 командой ping –t 192.168.254.22;

Примечание. Параметр –t задает для команды ping отправку сообщений с эхо-запросом к точке назначения до тех пор, пока команда НЕ будет прервана. Для прерывания команды и вывода статистики нажмите комбинацию клавиш CTRL-BREAK. Для прерывания команды ping и выйхода из нее нажмите клавиши CTRL-C.

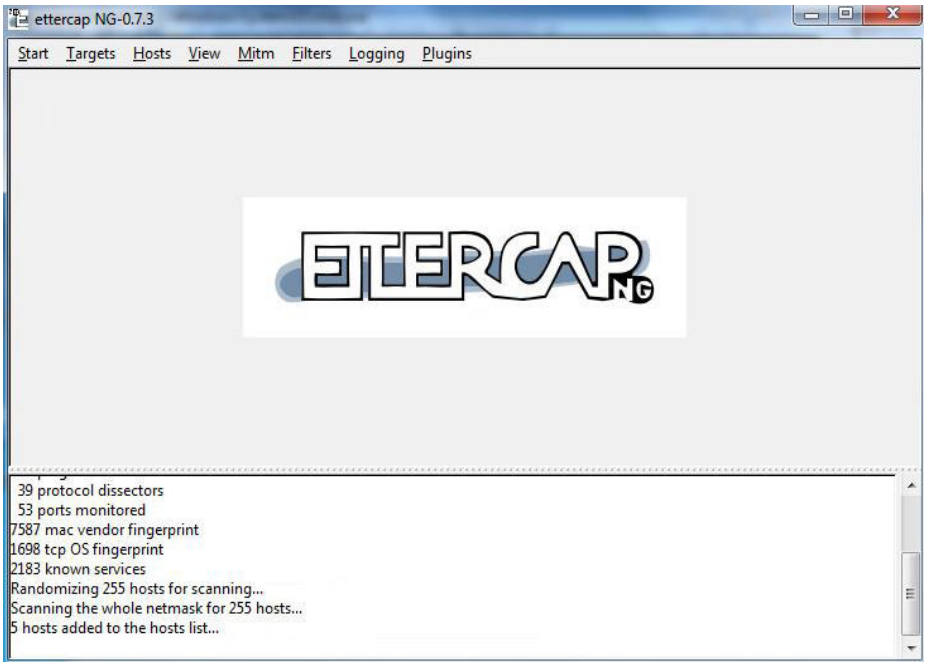
- перейдите в консоль ВМ ARM1 и в командной строке выполните команду: netsh interface ipv4 set interface LAN forwarding=enabled;

Примечание. Netsh — это служебная программа для работы со сценариями командной строки, которая позволяет отображать или изменять конфигурацию сети компьютера, работающего в данный момент (разберитесь, что реализовано в данном случае с помощью команды Netsh).

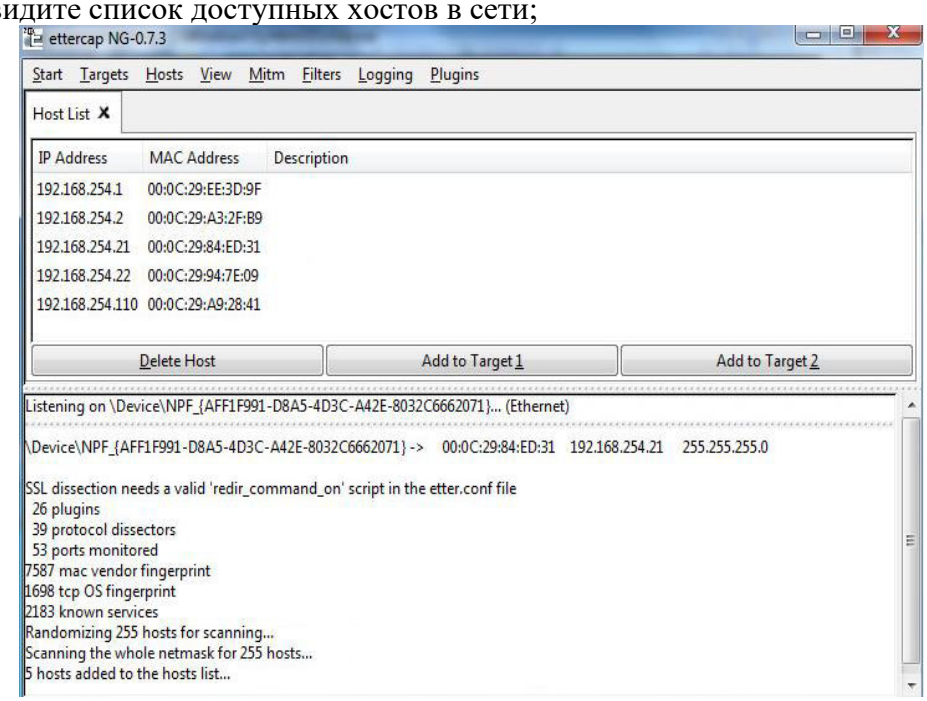
- запустите Ettercap NG-0.7.3. В открывшемся окне программы в главном меню выберите опцию “Sniff / Unified sniffing…”;



- в открывшемся диалоговом окне выберите из раскрывающегося списка сетевой интерфейс и нажмите кнопку "ОК". 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;



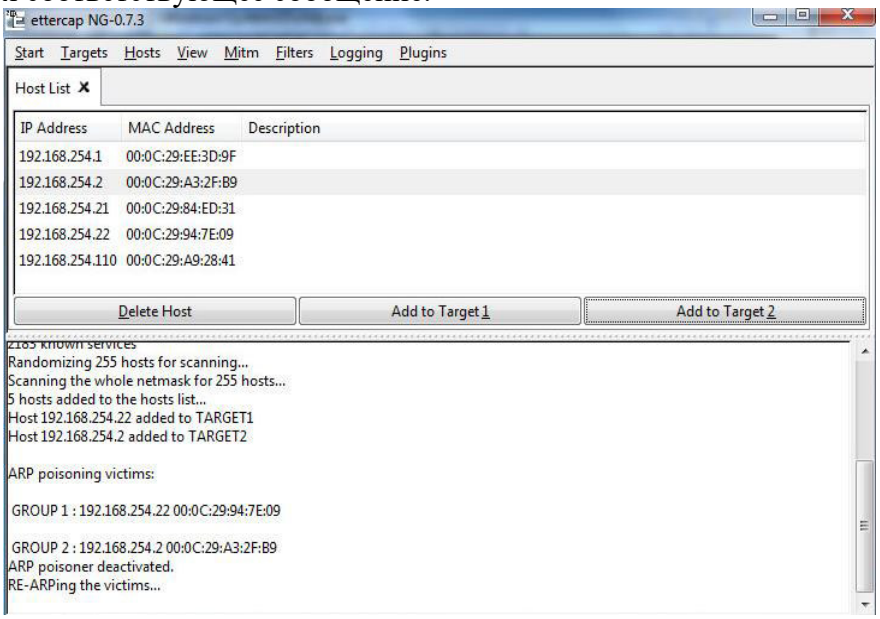
- выберите хост 192.168.254.22 (компьютер ARM2) и нажмите кнопку "Add to Target 1", а затем выберите атакуемый компьютер 192.168.254.2 (компьютер ServerSNS) и нажмите кнопку "Add to Target 2". В нижней части окна появятся записи по заданным целям;

Примечание. Именно между хостом 192.168.254.22 (компьютер ARM2) и хостом 192.168.254.2 (компьютер ServerSNS) будет располагаться так называемый Mitm - «Человек посередине».

- 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 "ОК"

Примечание. Sniff – «вынюхивать», «почуять».

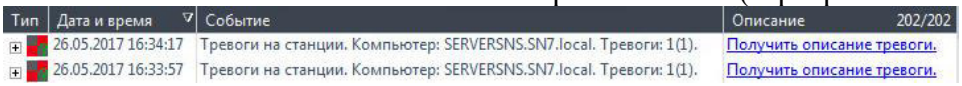
- перейдите в окно консоли ServerSNS и с помощью утилиты arp –a определите MAC-адрес компьютера ARM2 (192.168.254.22). Убедитесь, что он полностью совпадает с тем, что вы записывали в начале теста (смотри ранее). То есть так называемому «Человеку посредине» НЕ удалось подменить MAC-адрес. Следовательно, 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.



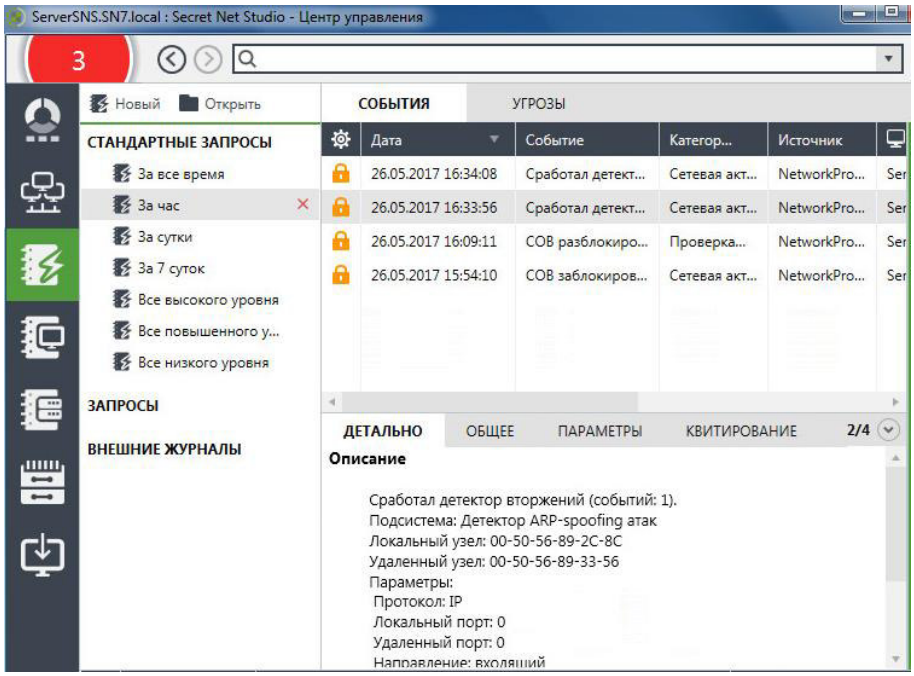
8. Переключитесь в окно консоли ServerSNS и остановите проверку доступности компьютера ARM2 командой ping;

9 Переключитесь в консоль ARM2 и вернитесь в окно программы управления. Обратите внимание, что:

- в панели событий появились записи о событиях тревоги на СБ (сервере безопасности);



- в журнале тревог появились сообщения детектора атак о вторжении (категория – "Сетевая активность", тип – "Аудит отказов").


ServerSNS.SN7.local : Secret Net Studio - Центр управления
Новый
Открыть
СТАНДАРТНЫЕ ЗАПРОСЫ
За все время
За час
За сутки
За 7 суток
Все высокого уровня
Все повышенного у...
Все низкого уровня
ЗАПРОСЫ
ВНЕШНИЕ ЖУРНАЛЫ
СОБЫТИЯ
УГРОЗЫ
Дата
Событие
Категор...
Источник
26.05.2017 16:34:08
Сработал детект...
Сетевая акт...
NetworkPro...
26.05.2017 16:33:56
Сработал детект...
Сетевая акт...
NetworkPro...
26.05.2017 16:09:11
СОВ разблокиро...
Проверка...
NetworkPro...
26.05.2017 15:54:10
СОВ заблокиров...
Сетевая акт...
NetworkPro...
ДЕТАЛЬНО
ОБЩЕЕ
ПАРАМЕТРЫ
КВИТИРОВАНИЕ
2/4
Описание
Сработал детектор вторжений (событий: 1).
Подсистема: Детектор ARP-spoofing атак
Локальный узел: 00-50-56-89-2C-8C
Удаленный узел: 00-50-56-89-33-56
Параметры:
Протокол: IP
Локальный порт: 0
Удаленный порт: 0
Направление: входящий

Приложение 2.

Методические указания по использованию программной среды «КриптоПРО».

Крипто-ПРО предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной цифровой подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах с выполнением функций:

- авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки (с использованием сертификатов стандарта X.509 Удостоверяющего центра) электронной подписи в соответствии с отечественными стандартами: ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования".
- обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с отечественным стандартом ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая";
- контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом;
- обеспечение аутентификации связывающихся сторон, конфиденциальности и целостности пересылаемой информации с использованием сертификатов стандарта X.509;
- установление аутентичного защищенного соединения с использованием протокола КриптоПро TLS;
- защита IP-соединений с использованием протоколов КриптоПро IKE, КриптоПро ESP;
- обеспечение конфиденциальности и контроля целостности и авторизация файлов и информационных сообщений;
- аутентификация в домене Windows с использованием КриптоПро Winlogon;

Исполнение 1 класса защиты КС1 выполнено в составе: криптопровайдер; криптодрайвер; модуль сетевой аутентификации (TLS); модуль аутентификации пользователя в домене Windows (в ОС Windows); модуль протоколов КриптоПро IKE, КриптоПро ESP (в ОС Windows, Linux); модуль шифрующей файловой системы КриптоПро EFS (ОС Windows); модуль поддержки интерфейса Microsoft CNG; модуль поддержки интерфейса Mozilla NSS; сервисные модули (cpverify, wipefile, stunnel).

К основным характеристикам можно отнести:

1. Размеры ключей

Размеры ключей электронной подписи:

- ключ электронной подписи – 256 бит;
- ключ проверки электронной подписи - 512 бит.

Размеры ключей, используемых при шифровании:

- закрытый ключ – 256 бит;
- открытый ключ - 512 бит;
- симметричный ключ – 256 бит.

2. Типы ключевых носителей

В качестве ключевых носителей используются:

- ГМД 3,5’’;
- USB диски;

- электронный ключ с интерфейсом USB (e-Token, Jacarta);
- Смарткарты РИК, Оскар, Магистра, УЭК;
- Смарткарта MS_KEY K;
- идентификаторы Touch-Memory DS1995 – DS1996 ПАК защиты от НСД (Аккорд-АМДЗ, электронный замок "Соболь);
- Rutoken, Rutoken SD;
- Смарткарты Athena IDProtect, INPASPOT, MorphoKST, Cha cardOS, Cha JCOP, MPCOSGemalto;
- Раздел HDD ПЭВМ (в ОС Windows – реестр).

Общая структура КриптоПРО представлена на рисунке. Список сокращений, используемых на рисунке 7.6 представлен в таблице

Таблица 7.1 – Список сокращений

Сокращение	Расшифровка
ДСЧ	Датчик случайных чисел
НСД	Несанкционированный доступ
ОС	Операционная система
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации

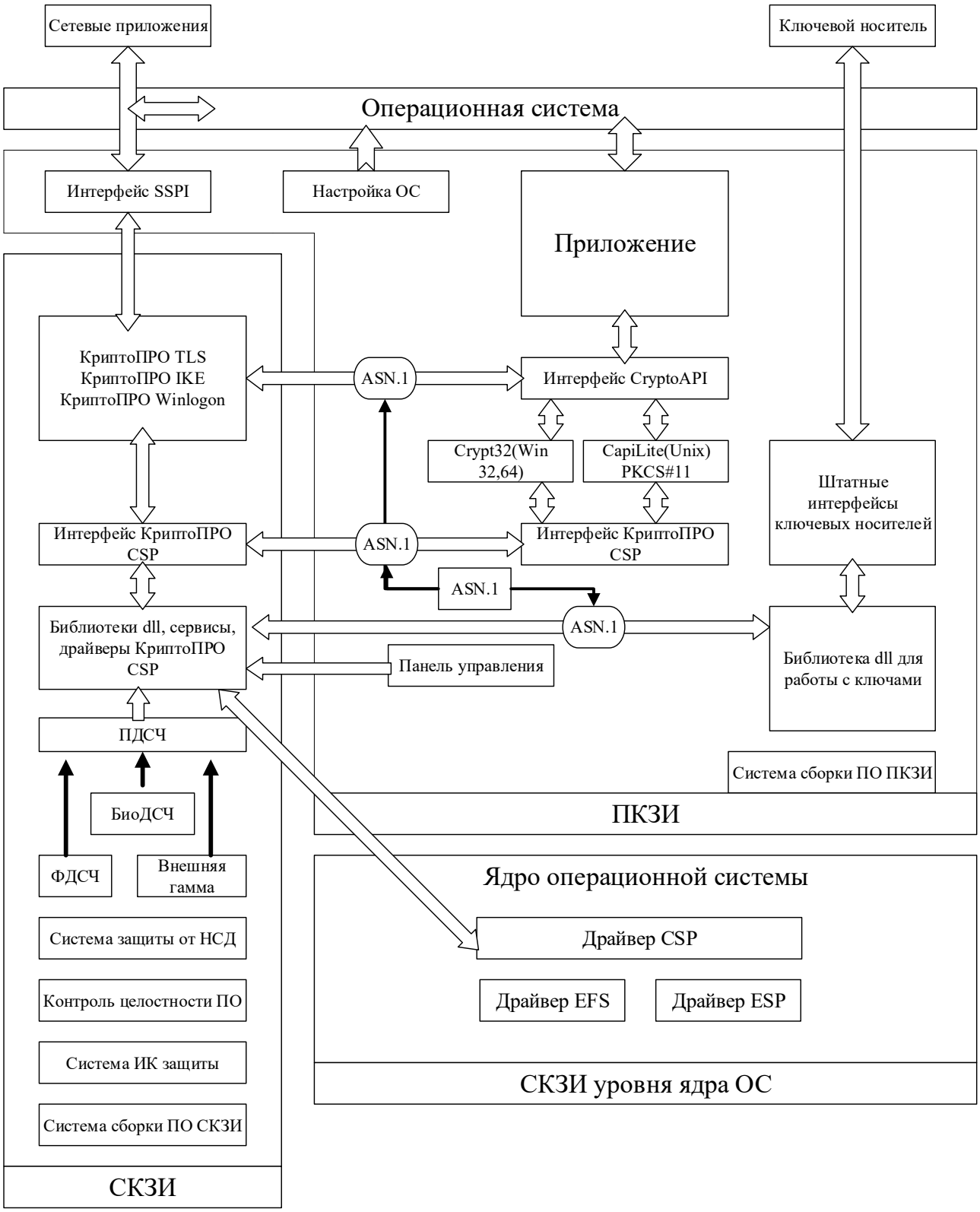


Рисунок – Структура СКЗИ КриптоПРО CSP

СКЗИ «КриптоПро CSP» является системой с открытым распределением ключей на основе асимметричной криптографии с использованием закрытого ключа на одной стороне и соответствующего ему открытого ключа информационного взаимодействия.

Пользователь, обладающий правом подписи и/или шифрования данных, вырабатывает на своем рабочем месте или получает у администратора безопасности (в зависимости от принятой политики безопасности) личные закрытый ключ (ключ ЭП) и открытый ключ (ключ проверки ЭП). На основе каждого открытого ключа (ключа проверки ЭП) Удостоверяющим Центром формируется сертификат открытого ключа (сертификат ключа проверки ЭП).

При зашифровании сообщения пользователем А для пользователя Б, пользователь А формирует симметричный ключ связи (сеансовый ключ информационного обмена) на основе своего закрытого ключа обмена и открытого ключа обмена пользователя Б. Соответственно, для расшифрования этого сообщения пользователем Б формируется тот же симметричный ключ на основе своего закрытого ключа обмена и открытого ключа обмена пользователя А.

Таким образом, для обмена данными каждому пользователю необходимо иметь:

1. личный закрытый ключ обмена;

2. открытые ключи обмена других пользователей.

Сеансовый ключ информационного обмена вырабатывается на основе алгоритма ДиффиХеллмана. Алгоритм Диффи-Хеллмана обеспечивает формирование сеансовых ключей, но не обеспечивает аутентификацию связывающихся сторон. Поэтому данный алгоритм должен использоваться совместно с протоколами аутентификации, например, с протоколом КриптоПро IKE.

Для формирования электронной подписи используется ключ электронной подписи, для проверки подписи – соответствующий ключ проверки электронной. При проверке подписи проверяющий должен располагать ключом проверки (сертификатом ключа проверки ЭП) пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности ключа проверки ЭП, а именно в том, что имеющийся у него ключ проверки ЭП соответствует ключу проверки ЭП конкретного пользователя. Для этой цели используется сертификат ключа проверки ЭП, подписанный Удостоверяющим Центром.

Каждому пользователю, обладающему правом подписи, необходимо иметь:

1. ключ электронной подписи;

2. ключи проверки электронной подписи (сертификаты ключей проверки электронной подписи) других пользователей.

Ключ электронной подписи может быть использован только для формирования ЭП.

Закрытый ключ обмена может быть использован как для формирования ключа связи с другим пользователем, так и для формирования ЭП.

Закрытые ключи СКЗИ «КриптоПро CSP» записываются в ключевом контейнере.

Ключевой контейнер может содержать:

- только ключ подписи;
- только ключ обмена;
- ключ подписи и ключ обмена одновременно.

Единственный ключ ключевого контейнера (ключ подписи или ключ обмена) называется главным ключом. Если в контейнере два ключа, то первый ключ - ключ подписи - называется главным, второй ключ – ключ обмена - вторичным.

Ключевой контейнер содержит кроме ключей служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п.

Каждый ключевой контейнер (независимо от типа носителя), является самодостаточным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми (и соответствующими им открытыми) ключами.

На ключевом носителе ключи хранятся в формате ключевого контейнера.

Ключевой контейнер содержит следующую информацию: главный ключ, маски главного ключа, контрольную информацию главного ключа, вторичный ключ (опциональный), резервную копию ключевого контейнера.

Каждый закрытый ключ и ключ ЭП хранится в формате, дополнительно содержащем все константы, необходимые для формирования и экспорта открытого ключа и ключа проверки ЭП.

Формат ключевого контейнера обеспечивает чтение ключей и соответствующих масок отдельными операциями в раздельные (разнесенные по адресам) области памяти, для чего он содержит шесть зон (реализация зон зависит от типа ключевого носителя).

Ключевой контейнер содержит также дополнительную информацию, необходимую для обеспечения его восстановления при возникновении различных программно-аппаратных сбоев (дополнительная информация включается в тех случаях, когда размер ключевого контейнера не ограничен размерами памяти физического носителя).

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

Запрещается оставлять без контроля вычислительные средства с установленным СКЗИ после ввода ключевой информации.

При наличии в организации, эксплуатирующей СКЗИ, администратора безопасности и централизованном хранении ключевых носителей, администратор безопасности несет персональную ответственность за хранение личных ключевых носителей пользователей.

При хранении ключей в реестре Windows и на HDD ПЭВМ требования по хранению личных ключевых носителей распространяются на ПЭВМ (HDD ПЭВМ) (в том числе и после удаления ключей из реестра, из HDD).

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ПЭВМ организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ПЭВМ с ключами.

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

СКЗИ может функционировать и хранить ключевую информацию в двух режимах:

- в памяти приложения для исполнения 1.

- в "Службе хранения ключей", реализованной в виде системного сервиса для исполнения 2.

Ключи находятся в кэше до завершения приложения или до выключения компьютера (остановки службы), что позволяет использовать закрытый ключ даже после закрытия криптографического контекста.

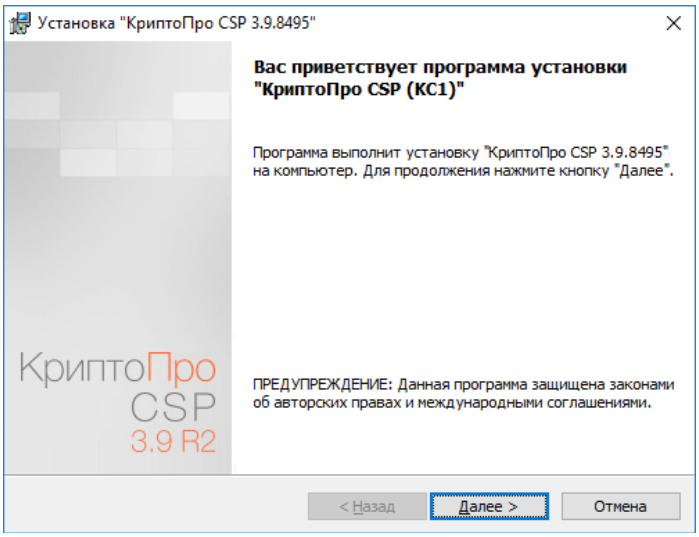
Функционирование и хранение ключей СКЗИ КриптоПро CSP в "Службе хранения ключей" обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на ПЭВМ, но может незначительно замедлить производительность системы.

В случае необходимости проведения ремонтных и регламентных работ аппаратной части СКЗИ/СФК необходимо обеспечить невозможность доступа нарушителя к ключевой информации, содержащейся в аппаратной части СКЗИ/СФК. Конкретный перечень мер должен быть определен исходя из условий эксплуатации СКЗИ.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

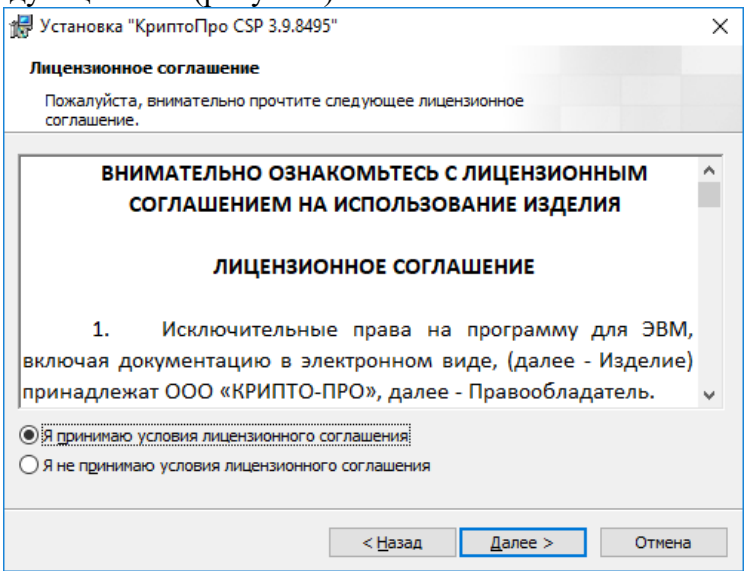
Установить систему Крипто-ПРО CSP в тестовом режиме. Установить тестовый сертификат.

Сначала необходимо установить Крипто-ПРО CSP версии 3.9. Для этого необходимо запустить инсталляционный файл csp-win32-kc1-rus.msi или csp-x64-kc1-rus.msi в зависимости от разрядности вашей операционной системы. После чего запустится установка программы (рисунок).



Начало установки Крипто-ПРО CSP

После нажатия на кнопку «Далее», в появившемся окне, читает лицензионное соглашение, выставляем флажок в позицию «Я принимаю условия лицензионного соглашения» и переходим «Далее» не следующий шаг (рисунок).



Установка Крипто-ПРО CSP

В новом окне необходимо ввести лицензионный ключ для использования программы (рисунок). Если у вас нет лицензионного ключа, то данное поле оставляем пустым. Программа установится бесплатно на 90 дней. Также, после установки программы, будет возможность ввести и активировать лицензионный ключ, для дальнейшего использования программы.

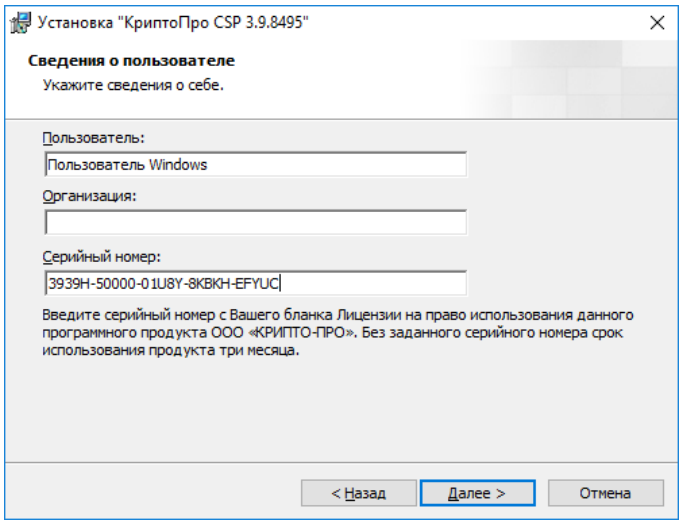


Рисунок – Ввод лицензионного ключа

На следующем шаге установки программы необходимо выбрать вид установки. Выбираем обычную установку программы (рисунок).

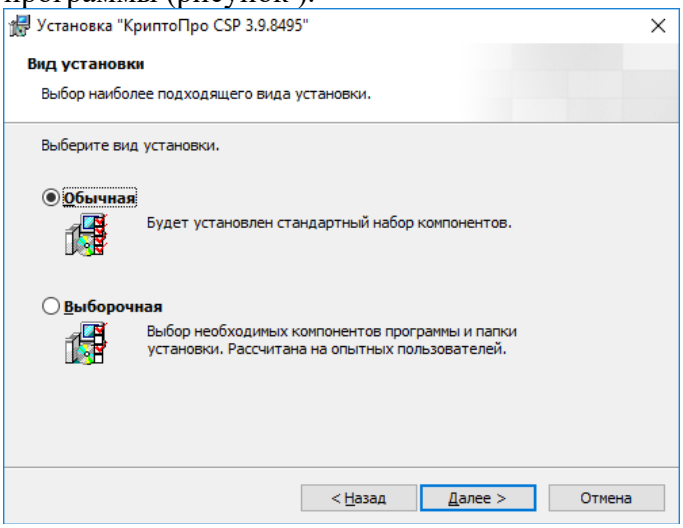


Рисунок 7.10 – Выбор вида установки

В новом открывшемся окне выбираем «Установить» (рисунок). После установки программы будет выведено окно об успешной установке Крипто-ПРО CSP (рисунок).

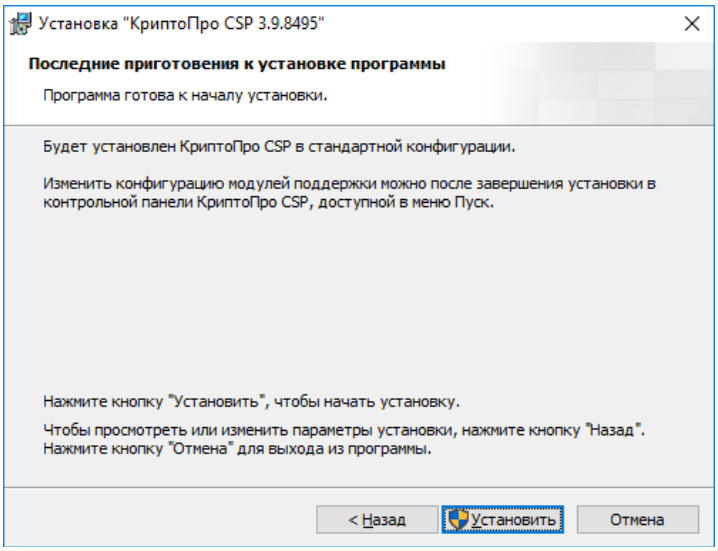


Рисунок 7.11 – Последний этап установки

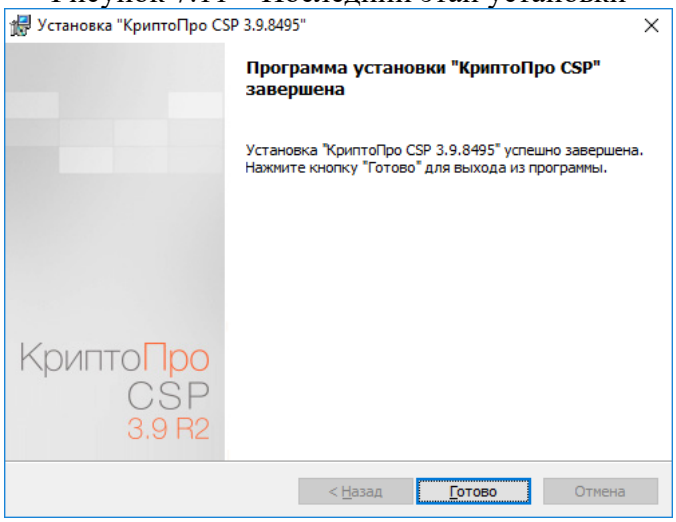


Рисунок – Успешное завершение установки программы

После чего, выполните проверку на установку программы. Нажмите Пуск -> Все программы, и найдите папку Крипто-ПРО (рисунок).

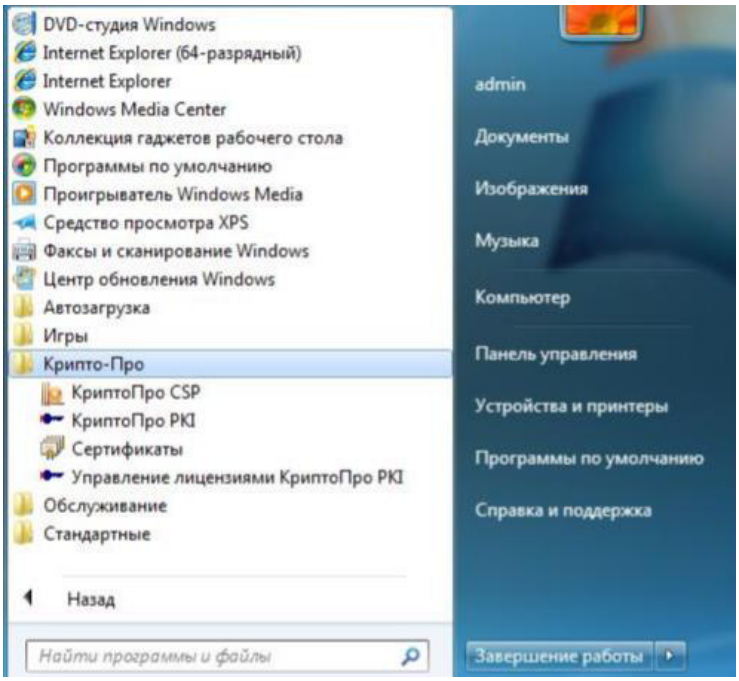


Рисунок – Доступ к Крипто-ПРО

Далее необходимо получить и установить тестовый сертификат. Для этого сначала нужно установить «КриптоПро Эцп Browser plug-in». Запустите инсталляционный файл cadesplugin.exe и произведите установку. После в Вашем браузере необходимо включить данное дополнение в настройках браузера.

Внимание! Если дополнение «КриптоПро Эцп Browser plug-in» в Ваш браузер включить не удалось, то выполнять действия далее не имеет смысла!

После чего переходим на сайт тестового удостоверяющего центра ООО "КРИПТО-ПРО" по ссылке: https://www.cryptopro.ru/certsrv/

Для того, чтобы тестовый личный сертификат был действителен и установлен, сначала требуется установка сертификата цепочки сертификатов (ЦС). Для этого на сайте выбираем «Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов» (рисунок).

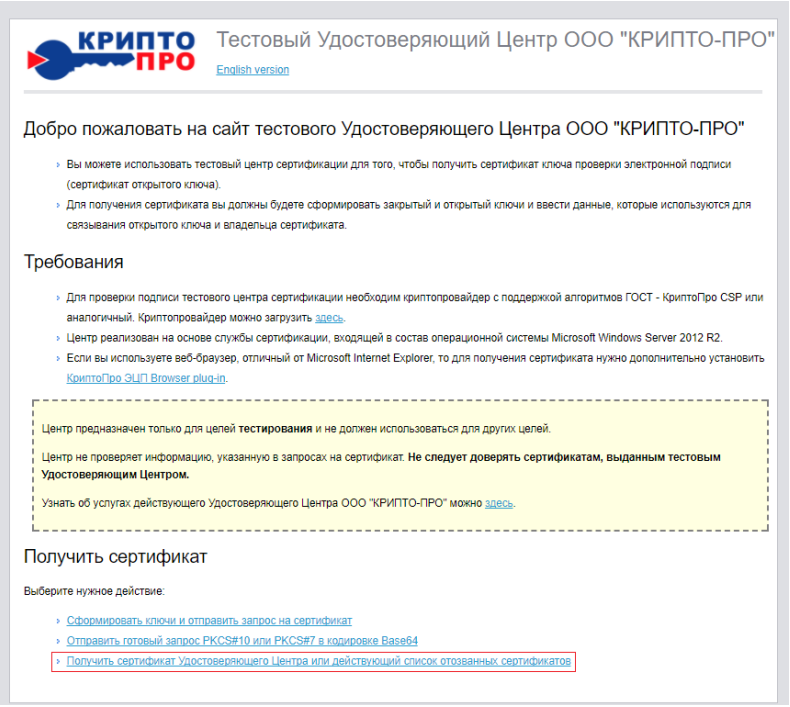


Рисунок – Сайт тестового Удостоверяющего Центра Крипто-ПРО

На открывшейся странице необходимо выбрать «Загрузка сертификата ЦС» (рисунок), после чего будет скачен файл certnew.cer, который необходимо установить. Откройте данный файл (рисунок).

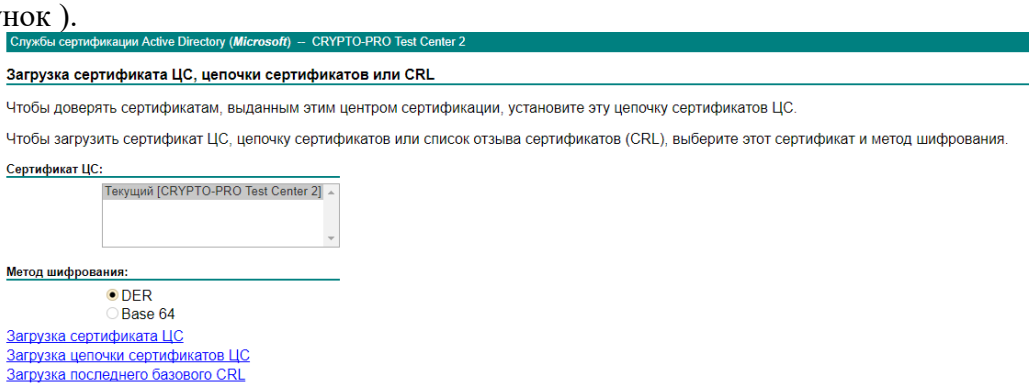


Рисунок 7.15 – Загрузка сертификата ЦС

После открытия файла сертификата ЦС, в появившемся окне требуется выбрать «Установить сертификат» (рисунок). После чего необходимо выбрать хранилище сертификата (рисунок).

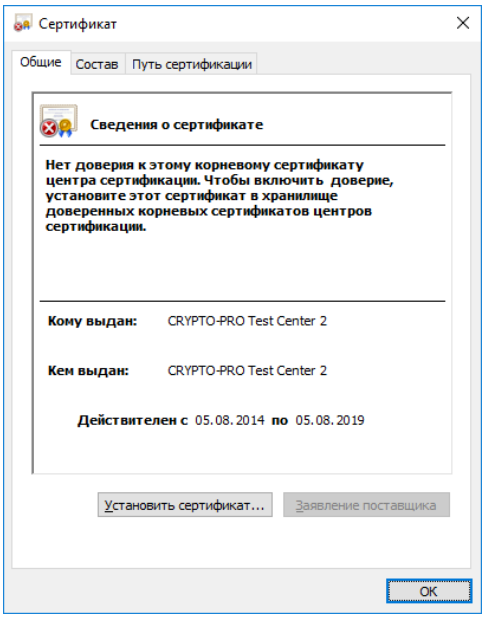


Рисунок – Установка сертификата ЦС

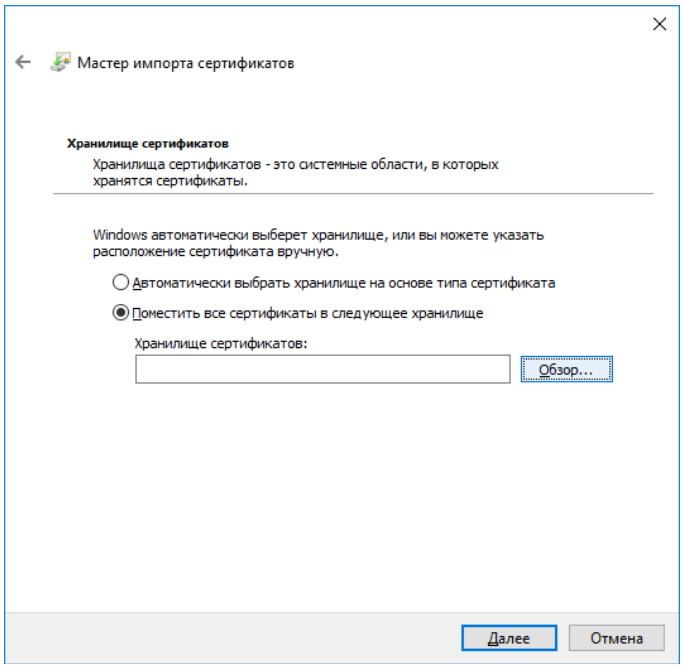


Рисунок – Выбор хранилища сертификата

Сертификаты Удостоверяющего центра должны храниться в специальном хранилище. Поэтому нажав «Обзор», выберите «Доверенные корневые центры сертификации» (рисунок).

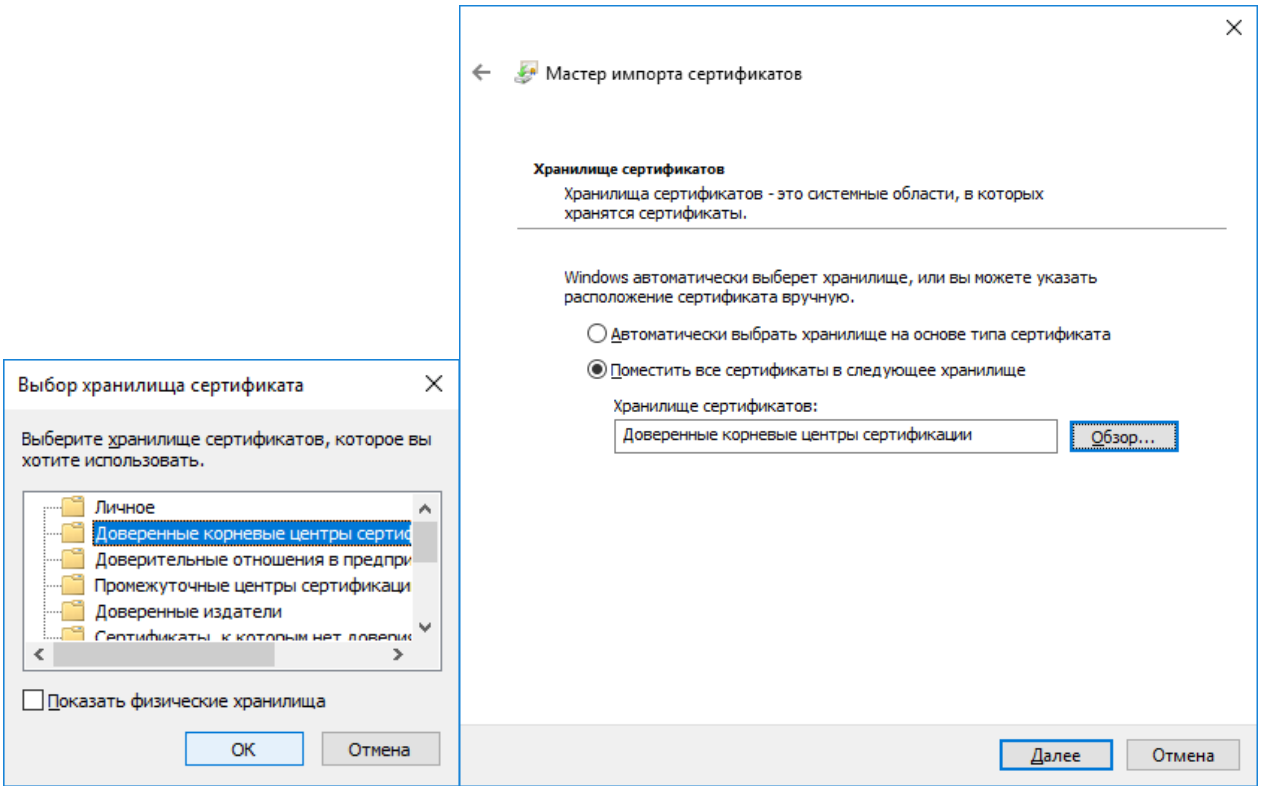


Рисунок – Выбор места хранилища

После чего необходимо начать установку, нажав «Готово». В появившемся окне сообщения необходимо согласиться (нажать «Да») для установки сертификата (рисунок).

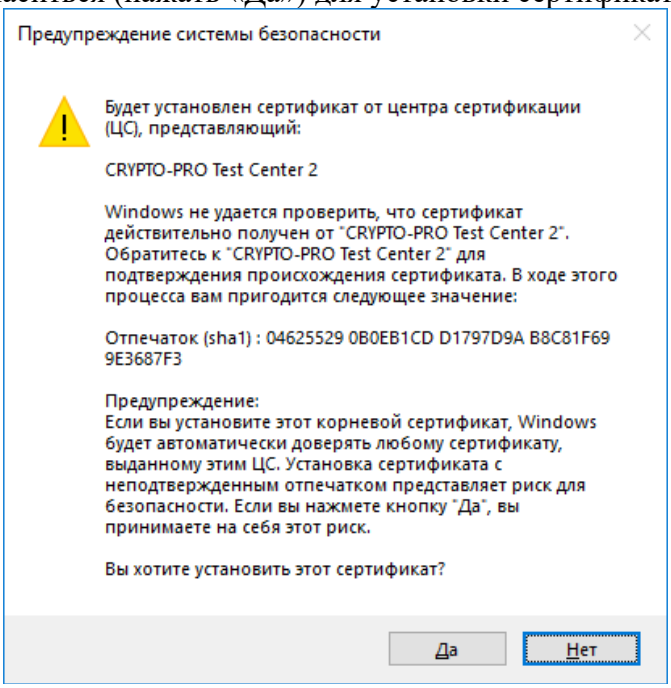


Рисунок – Окончание установки сертификата

После установки необходимо проверить, правильно ли установлен сертификат ЦС и является ли он действительным. Для этого переходим Пуск -> Все программы -> Крипто-ПРО -> Сертификаты. В открывшемся окне программы выбираем директорию Сертификаты-текущий

пользователь -> Доверенные корневые центры сертификации -> Реест -> Сертификаты (рисунок), где в правой части окна должен быть сертификат CRYPTO-PRO Test Center 2.

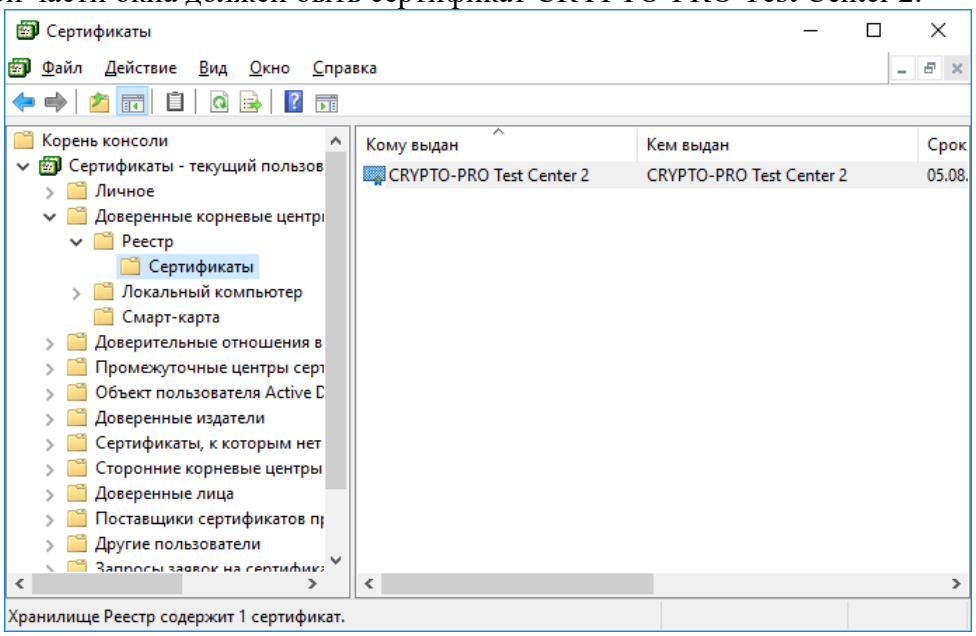


Рисунок – Установленный сертификат ЦС

Открываем данный сертификат, переходим на вкладку Путь сертификации, где в поле Состояние сертификата должна быть надпись: «Этот сертификат действителен» (рисунок 7.21), что будет означать успешную установку сертификата ЦС.

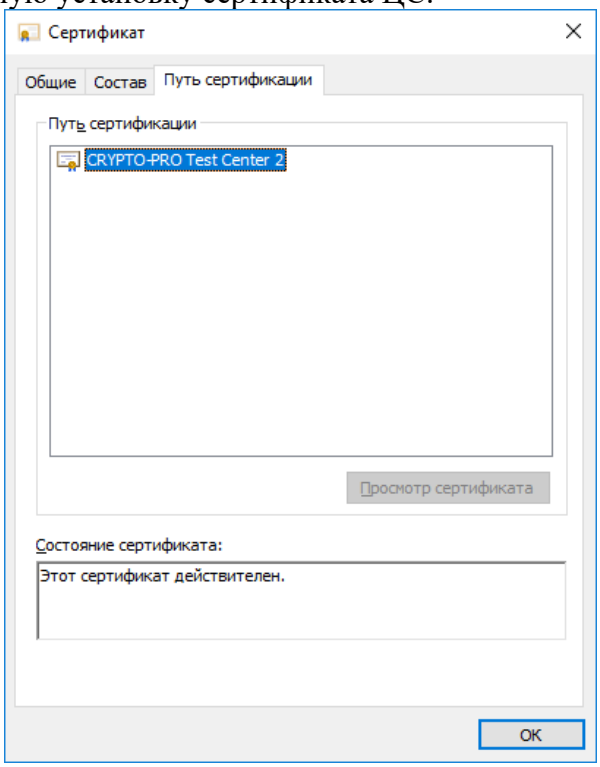


Рисунок – Сертификат ЦС

Далее в браузере возвращаемся на сайт тестового удостоверяющего центра ООО "КРИПТО-ПРО" по ссылке: https://www.cryptopro.ru/certsrv/ и выбираем «Сформировать ключи и отправить запрос на сертификат» (рисунок).

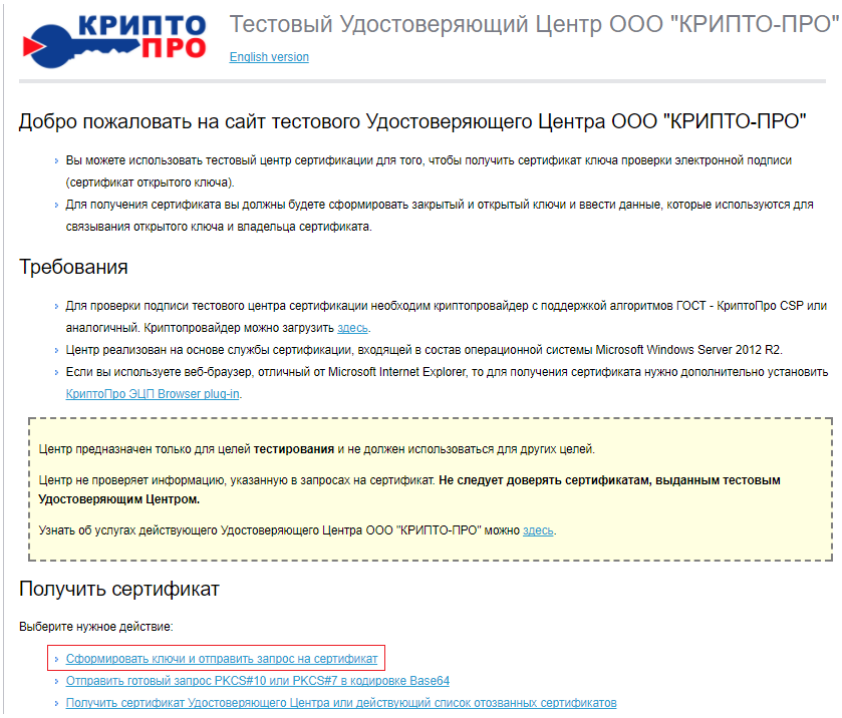


Рисунок - Сайт тестового Удостоверяющего Центра Крипто-ПРО

В открывшемся окне заполняем тестовые идентифицирующие сведения, выбираем для ключа параметр «Пометить ключ как экспортируемый» и нажимаем «Выдать» (рисунок)

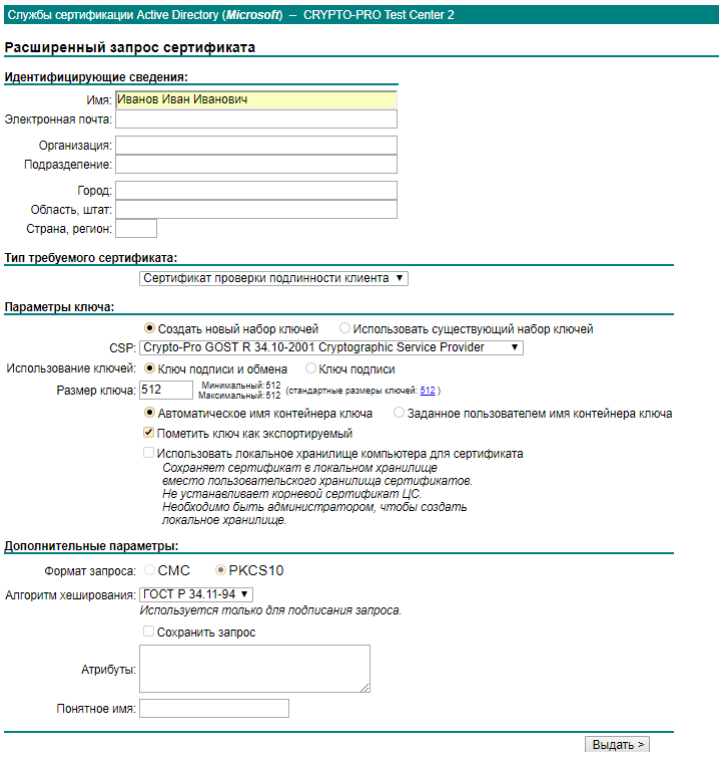


Рисунок – Расширенный запрос сертификата

После появится окно выбора носителя для хранения контейнера закрытого ключа. Выбираем требуемое устройство и нажимаем «ОК». Если выбрать «Реестр» (рисунок 7.24), то сертификат будет помещен в контейнер, расположенный в директории личных ключей на компьютере. Если выбрать другой носитель (например, USB-флеш-накопитель), то контейнер сертифика-

та будет помещен на данный носитель и подпись документа может быть осуществлена только при его наличии.

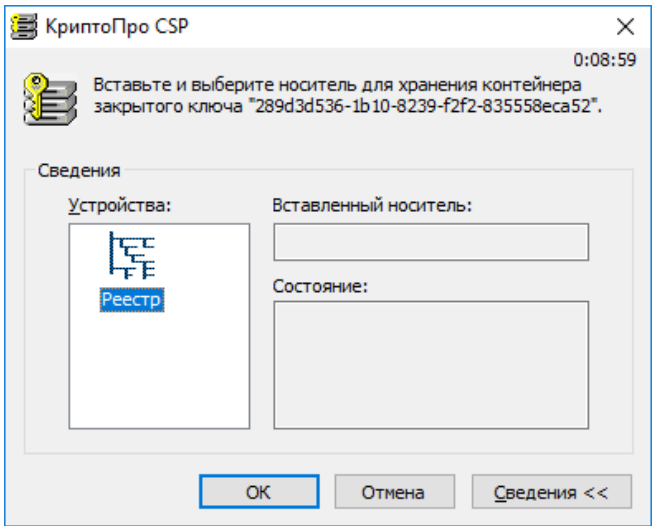


Рисунок – Выбор носителя

Далее следуйте указаниям в появившемся окне (рисунок).

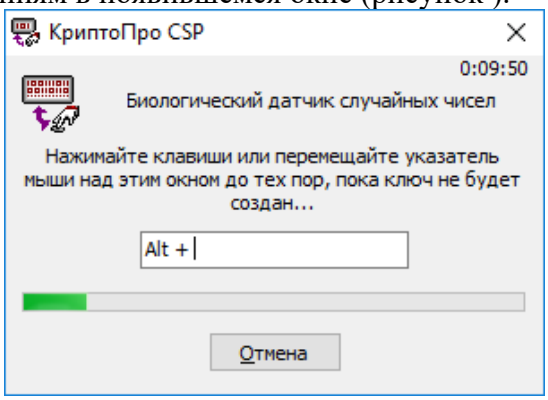


Рисунок 7.25 – Биологический датчик случайных чисел

В появившемся окне необходимо установить пароль доступа к создаваемому контейнеру (рисунок), например, admin.

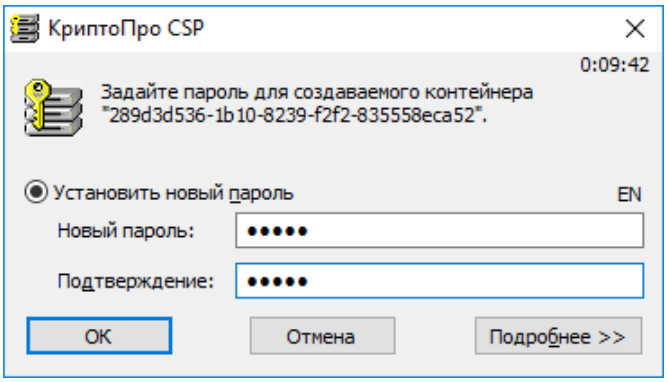


Рисунок – Установка пароля доступа к сертификату

Если все действия выполнены правильно, откроется страница в браузере, позволяющая установить личный сертификат (рисунок). Наживаем «Установить этот сертификат», после чего появится окно, запрашивающее пароль контейнера (рисунок 8.28). Вводим пароль, установлен-

ный вами на предыдущем этапе. Если все прошло успешно, откроется страница в браузере, подтверждающая успешную установку сертификата.

Примечание: Если проверка действительности сертификата не оказалась успешной, то попробуйте установить системное время компьютера на 1 час вперед. После этого снова проверьте действительность сертификата.

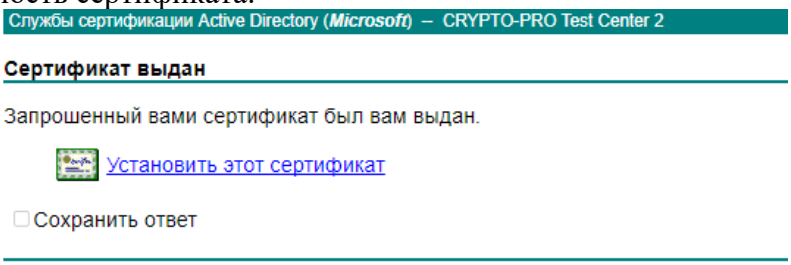


Рисунок 8.27 – Установка личного сертификата

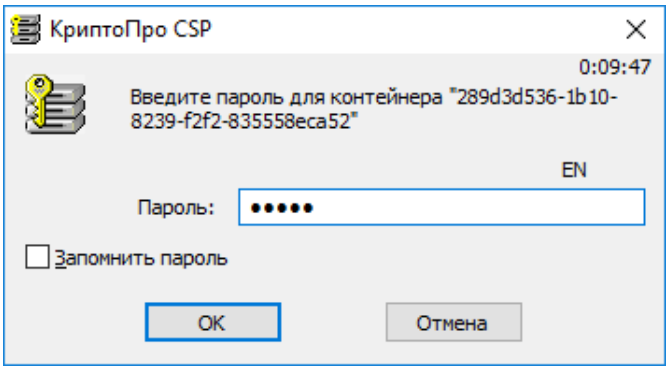


Рисунок – Ввод пароля

Далее обязательно проверяем успешно ли установлен сертификат. Для этого переходим Пуск -> Все программы -> Крипто-ПРО -> Сертификаты. В открывшемся окне программы выбираем директорию Сертификаты-текущий пользователь -> Личное -> Сертификаты (рисунок), где в правой части окна должен быть сертификат имеющий заполненное вами в форме браузера имя (в примере это Иванов Иван Иванович).

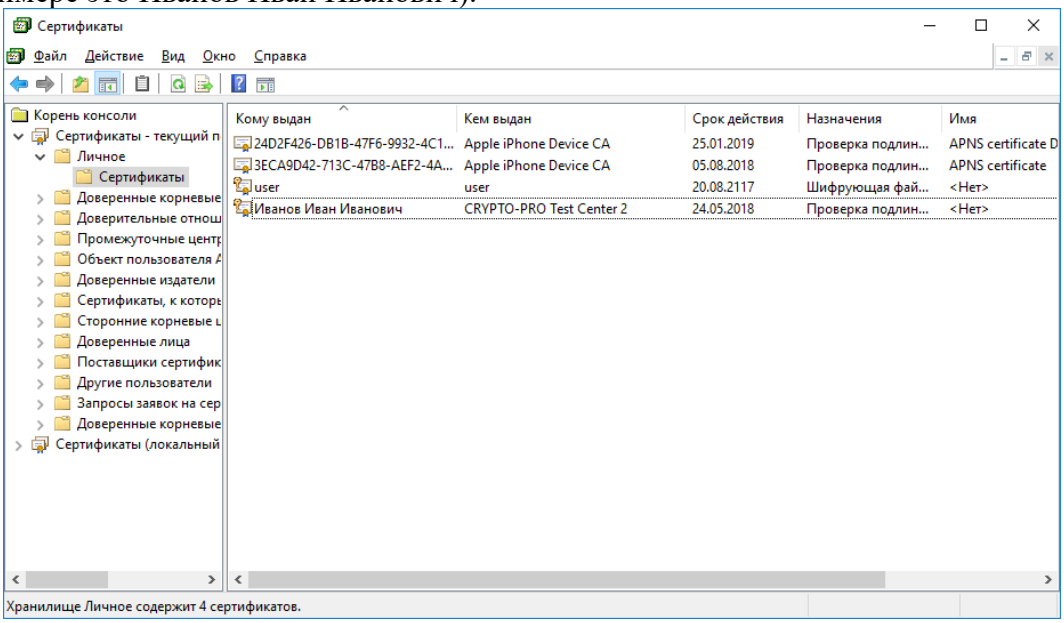


Рисунок – Установленный личный сертификат

Открываем данный сертификат, переходим на вкладку Путь сертификации, где в поле Состояние сертификата должна быть надпись: «Этот сертификат действителен» (рисунок), что будет означать успешную установку личного сертификата.

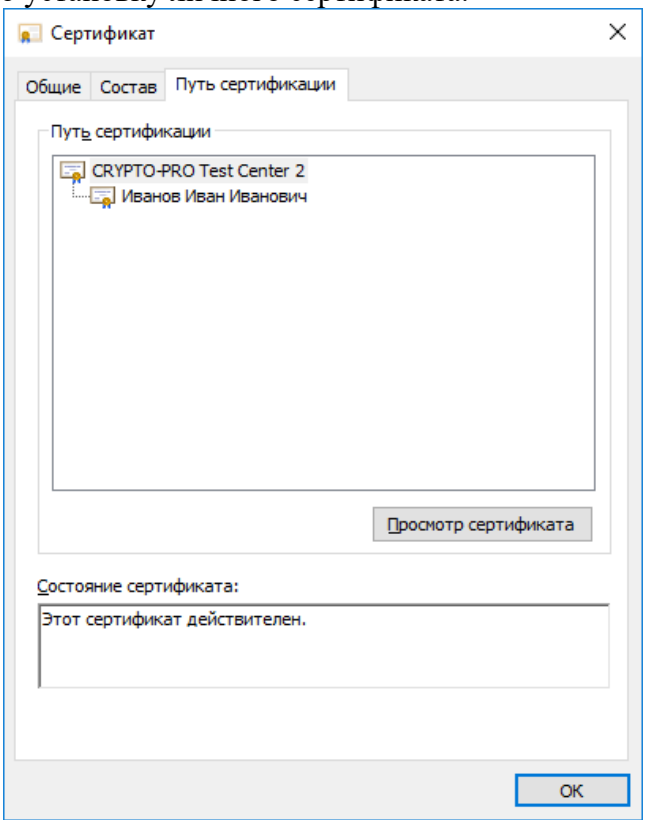


Рисунок – Проверка действительности личного сертификата

Использование ЭЦП Крипто-ПРО для подписания документов Microsoft Office

Для работы Крипто-ПРО с документами MSOfficeнеобходимо установить плагин Крипто-ПРО OfficeSignature. Для этого необходимо запустить инсталляционный файл XMLDSigAddIn-win32.msi или XMLDSigAddIn-x64.msi в зависимости от разрядности вашей операционной системы. После чего запустится установка программы (рисунок).

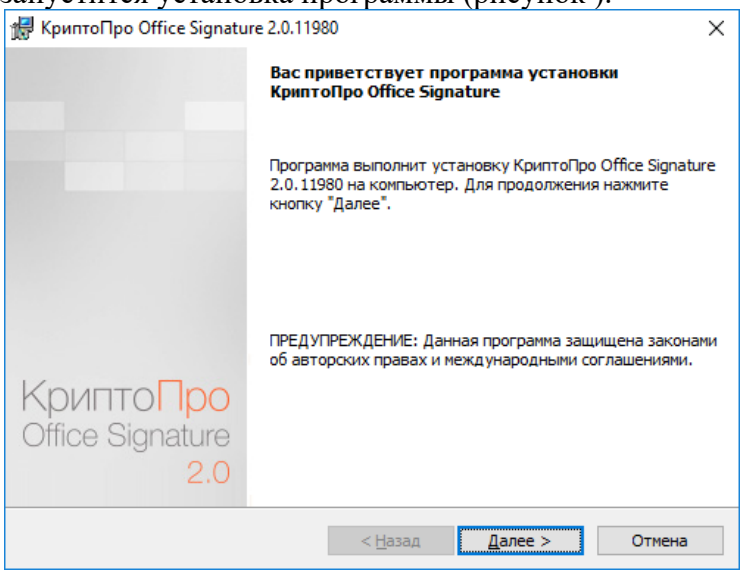


Рисунок – Начало установки Крипто-ПРО OfficeSignature

После нажатия на кнопку «Далее», в появившемся окне, читаем лицензионное соглашение, выставляем флажок в позицию «Я принимаю условия лицензионного соглашения» и нажимаем «Далее» (рисунок).

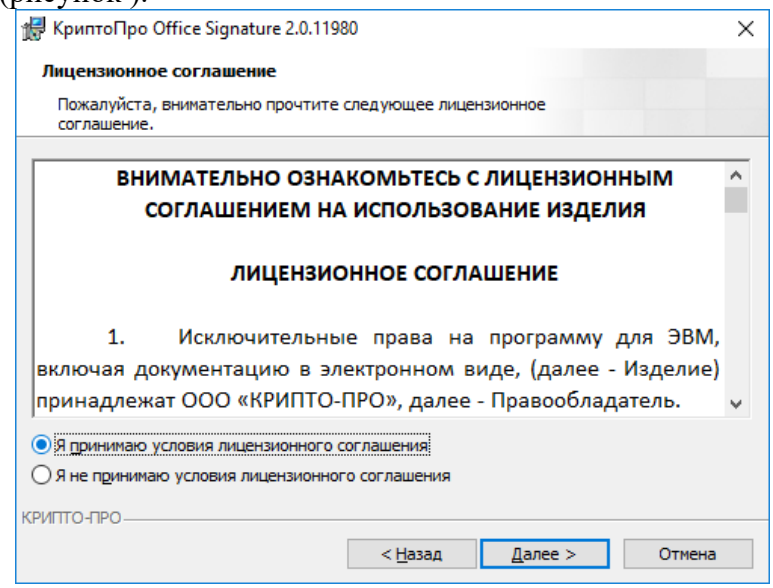


Рисунок – Установка Крипто-ПРО OfficeSignature

В новом окне необходимо ввести лицензионный ключ для использования программы (рисунок). Если у вас нет лицензионного ключа, то данное поле оставляем пустым. Программа установится бесплатно на 90 дней. Также, после установки программы, будет возможность ввести и активировать лицензионный ключ, для дальнейшего использования программы.

Примечание: Программный комплекс КриптоПро контролирует дату первой установки. Рекомендуется перед установкой новых версий использовать специальную программу cspclean для очистки следов предыдущих компонентов системы.

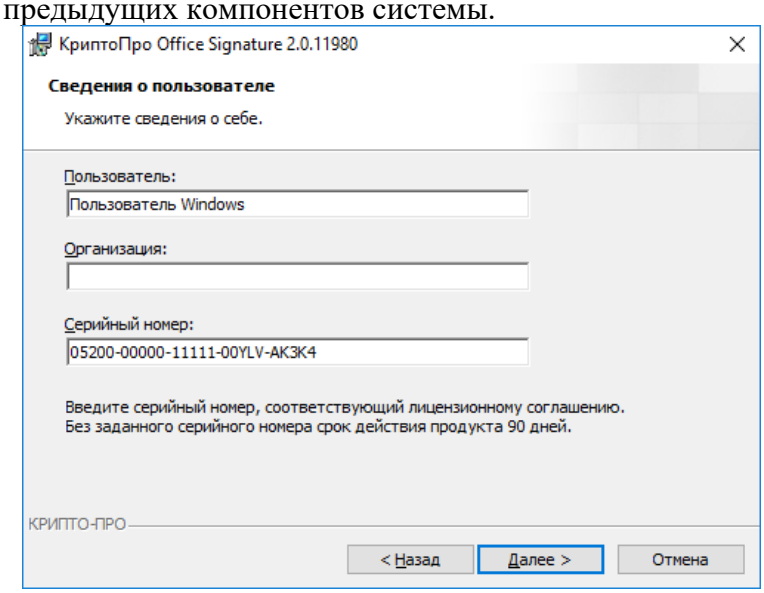


Рисунок – Ввод лицензионного ключа

На следующем шаге установки программы необходимо выбрать вид установки. Выбираем обычную установку программы (рисунок).

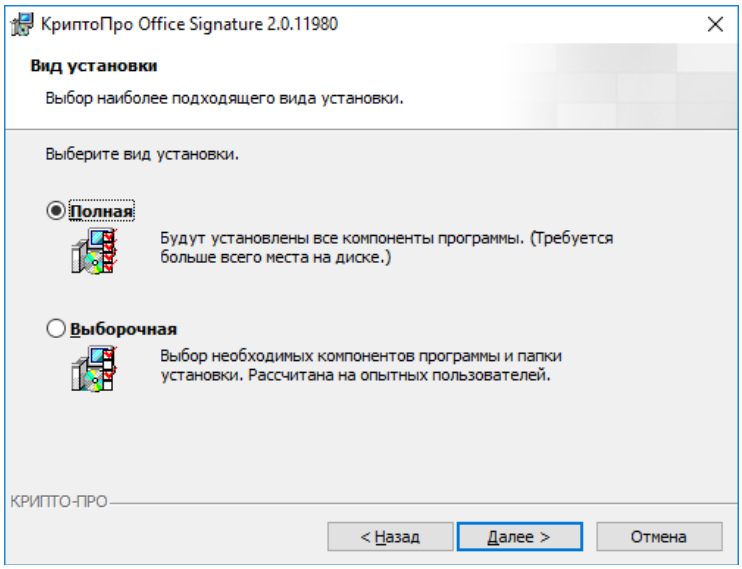


Рисунок – Выбор вида установки

В новом открывшемся окне выбираем «Установить» (рисунок) . После установки программы будет выведено окно об успешной установке Крипто-ПРО OfficeSignature (рисунок). Перезагрузите ПК.

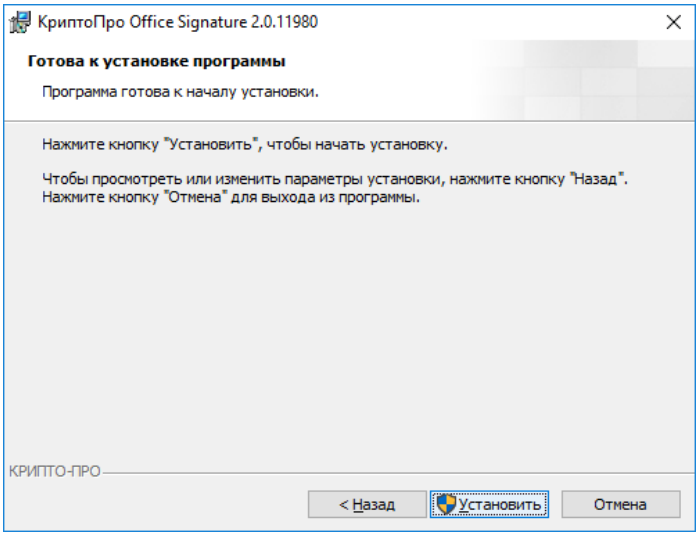


Рисунок – Последний этап установки

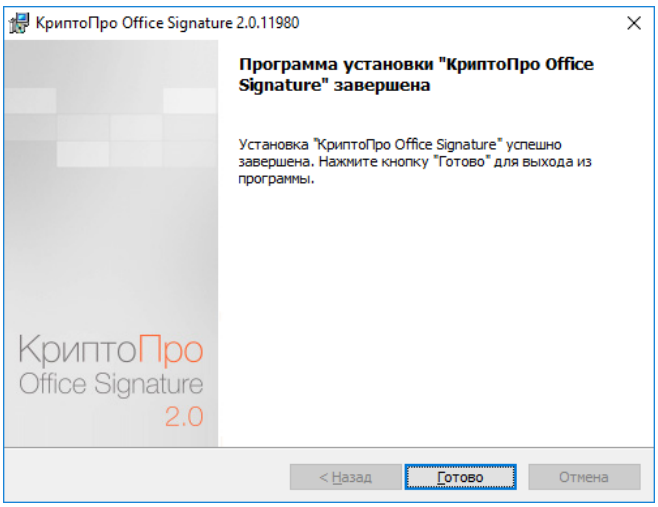


Рисунок – Успешное завершение установки программы

После перезагрузки ПК, создайте тестовый документ и откройте его. Крипто-ПРО OfficeSignature позволяет сделать два вида подписей: неотображаемую и отображаемую электронную подпись. Подписанный документ будет доступен только для чтения. Если в подписанный документ нужно внести изменения, то все созданные ЭП следует удалить из документа, поскольку они станут недействительными.

Рассмотрим создание неотображаемой ЭП в Microsoft Office Word 2007 или Excel 2007 для этого в главном меню выберите пункт «Подготовить», затем «Добавить электронную подпись (КРИПТО-ПРО)» (рисунок). Для создания неотображаемой электронной подписи в Microsoft Office Word 2010/2013 или Excel 2010/2013 на вкладке «Файл» в разделе «Сведения» нажмите кнопку «Добавить электронную подпись (КРИПТО-ПРО)» (рисунок 7.38). После этого появится диалог подписи документа, в котором нажатием кнопки «Изменить» можно выбрать личный сертификат подписи. После выбора сертификата нажмите «Подписать» (рисунок).Если для доступа к ключевому контейнеру требуется задать пароль - появится окно ввода пароля.

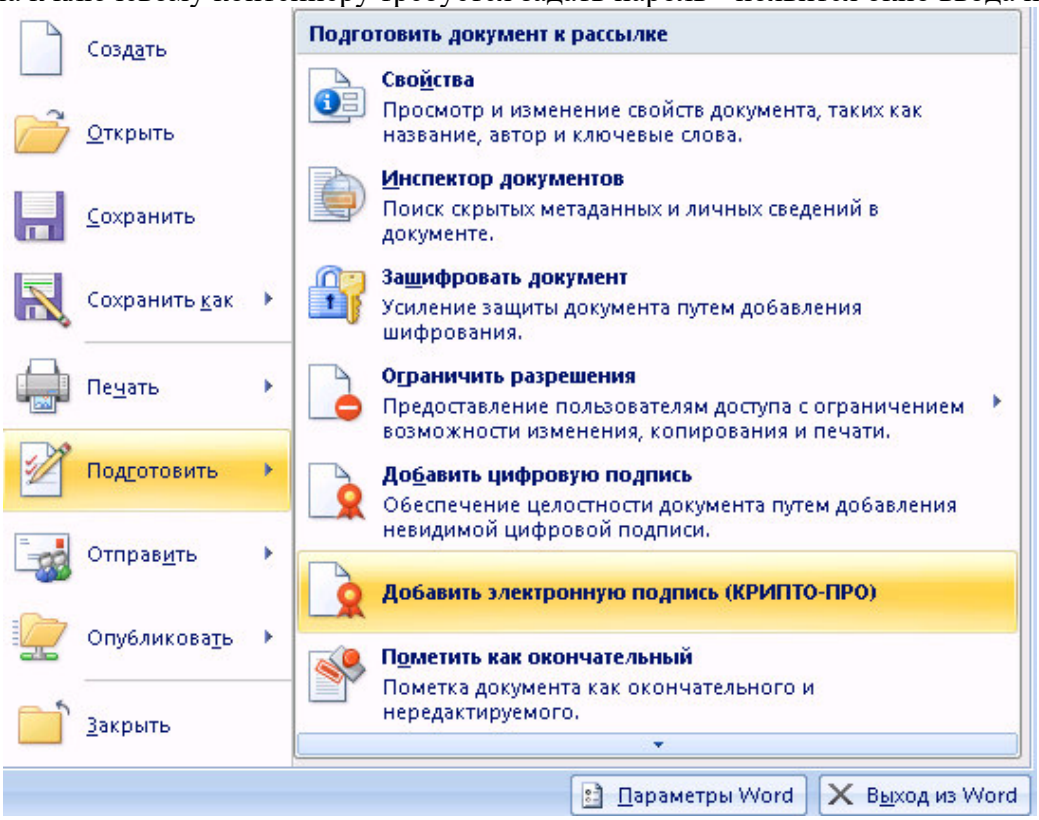


Рисунок –Добавление электронной подписи в Microsoft Word 2007

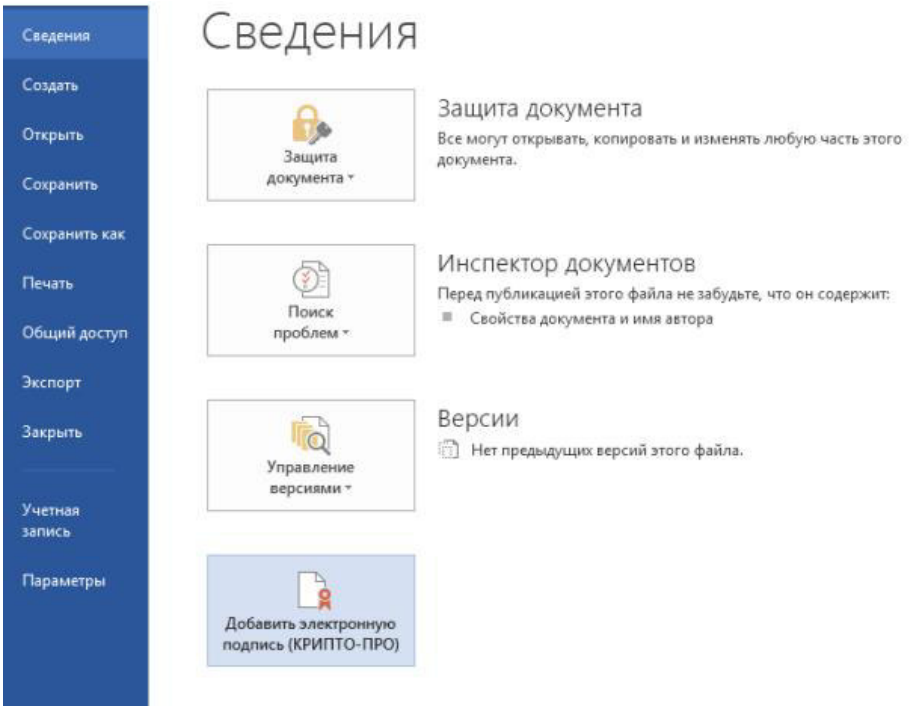


Рисунок –Добавление электронной подписи в Microsoft Office 2010/2013

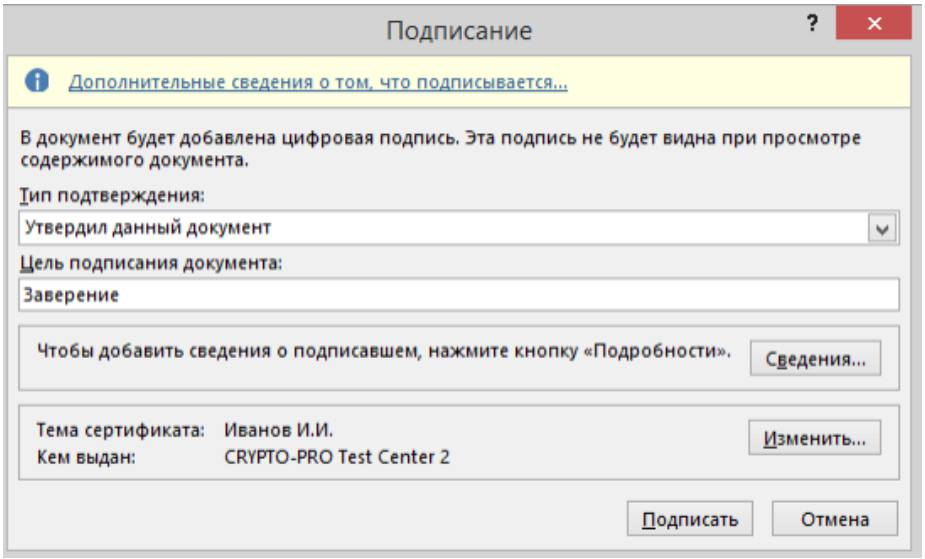


Рисунок – Подписание документа

Изучение свойств подписанного документа MS Office на предмет его подлинности и фальсификации.

После подписи документа в меню «Файл», разделе «Сведения» выводится информация о том, что документ подписан и редактирование запрещено (рисунок). В строке состояния окна документа появится значок, свидетельствующий о том, что данный документ имеет электронную подпись (рисунок). Для проверки статуса подписи, нажмите на этот значок, и справа появится вкладка Подписи, в которой указан статус подписи (Рисунок). Для просмотра состава подписи, щелкните правой кнопкой мыши на строке подписи и выберите пункт «Состав подписи». Появится детальное сообщение о составе подписи.

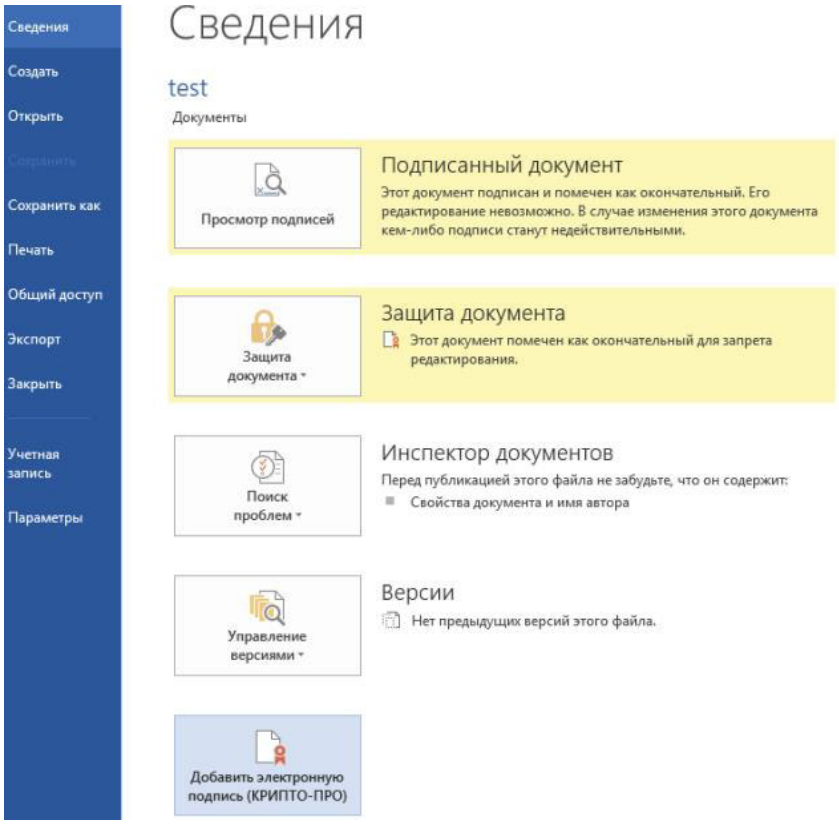


Рисунок – Сведения о подписанном документе

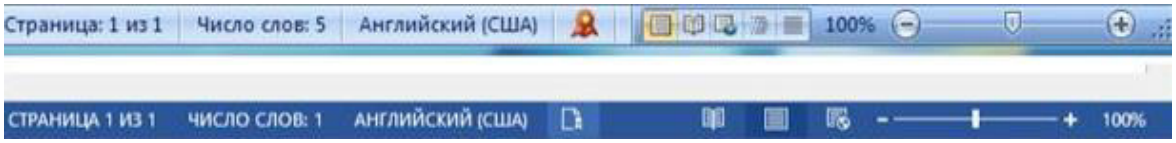


Рисунок – Строка состояния Microsoft Word 2007 и 2013

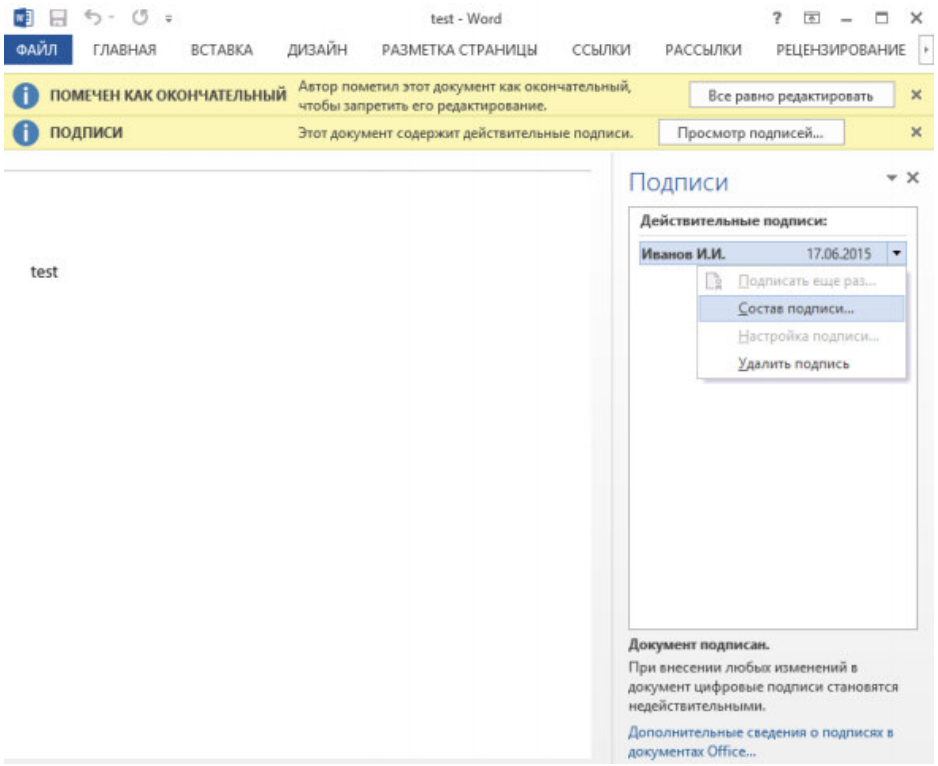


Рисунок – Статус подписи

Если открыть документ для редактирования, все подписи удаляются, об этом выводится предупреждение. Документ можно подписать еще несколькими подписями без удаления изначальной, для этого повторите все действия для осуществления подписи документа (рисунок).

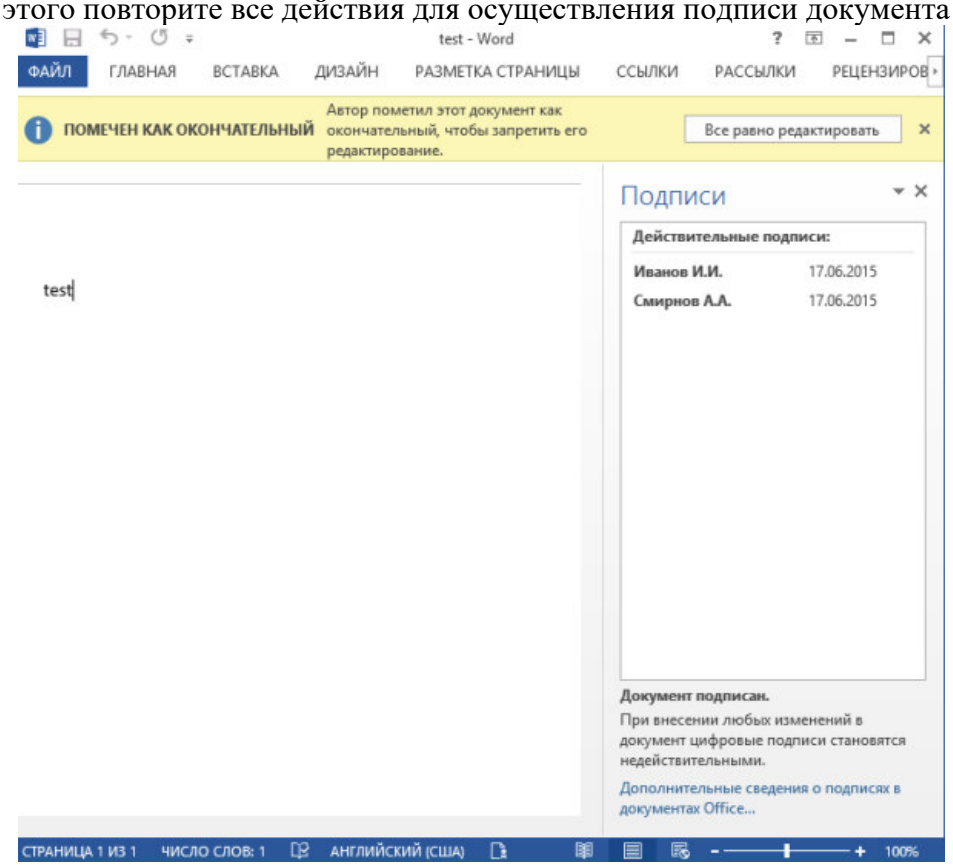


Рисунок – Несколько подписей в документе

При открытии измененного документа, содержащего недействительную ЭП, появится сообщение (рисунок). Для более детального просмотра статуса, нажмите на значок ЭП в строке состояния. В результате справа появится окно, содержащее недействительный статус подписи. Состав подписи можно посмотреть нажатием правой кнопки мыши и выбором пункта «Состав подписи» в выпадающем меню (рисунок).

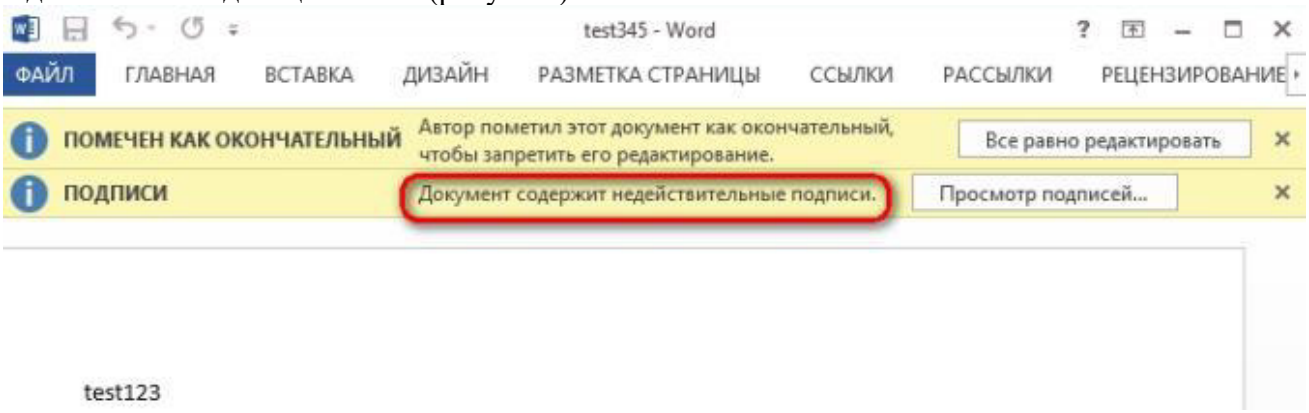


Рисунок – Документ с недействительной подписью

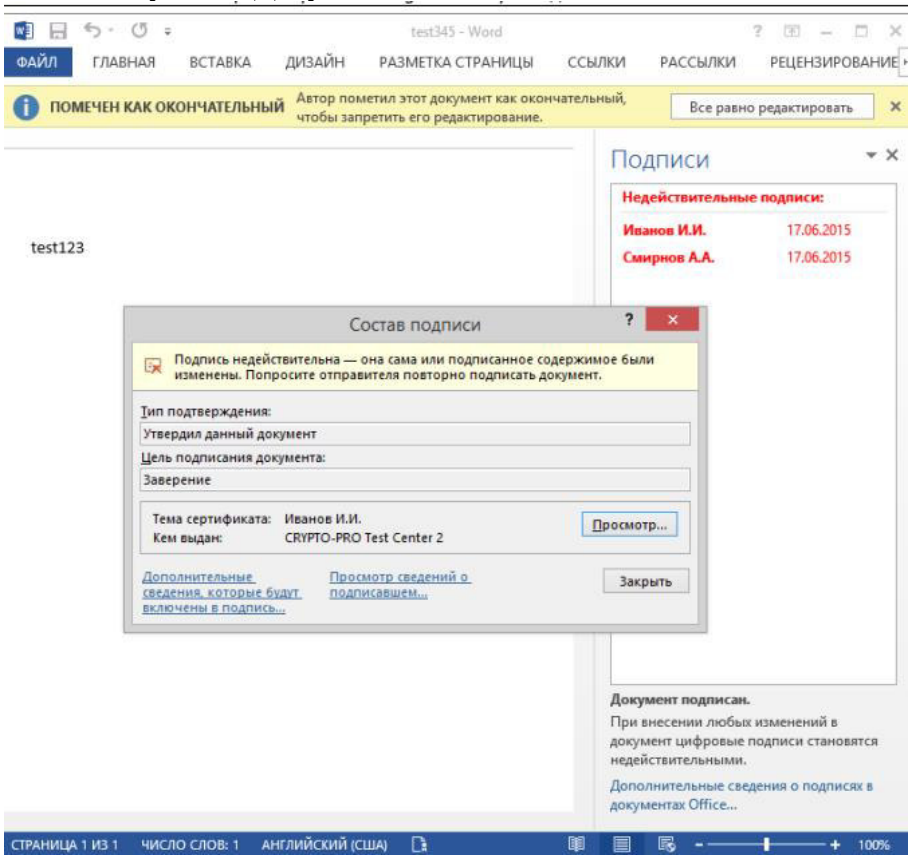


Рисунок – Состав недействительной подписи

Примечание. Если работа с подписанным документом происходит на компьютере, где нет сертификата пользователя, то документ доступен только для просмотра (без прав редактирования).

Если необходимо защитить не только редактирование, но и просмотр документа, то кроме ЭП необходимо организовать шифрование содержимого документа.

Использование ЭЦП Крипто-ПРО для подписания PDF-документов

Для работы Крипто-ПРО с PDF-документами необходимо установить плагин Крипто-ПРО PDF. Для этого необходимо запустить инсталляционный файл cppdf-win32.msi или cppdf-x64.msi в зависимости от разрядности вашей операционной системы. После чего запустится установка программы (рисунок).

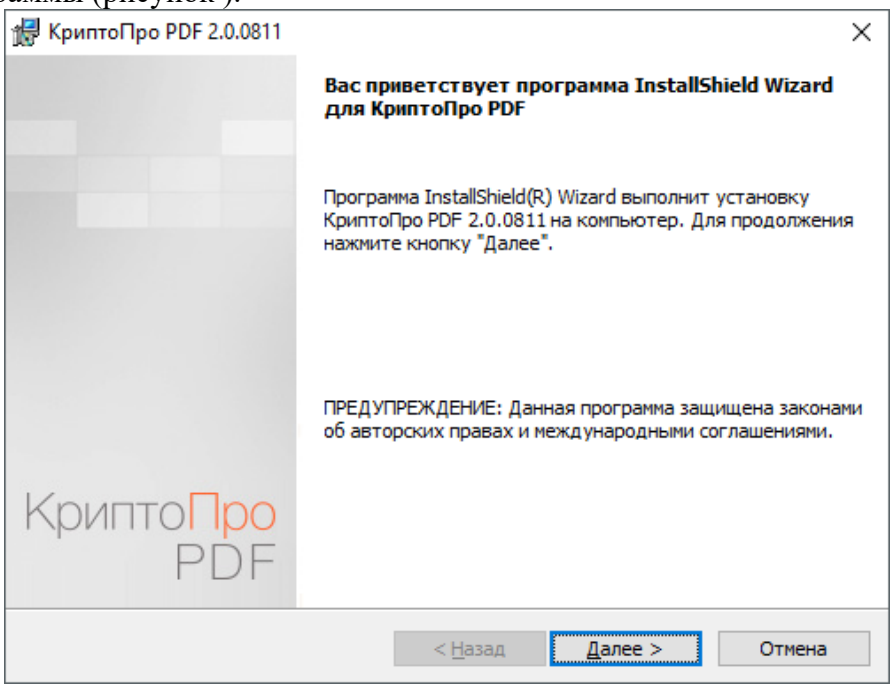


Рисунок – Начало установки Крипто-ПРО PDF

После нажатия на кнопку «Далее», в появившемся окне, читаем лицензионное соглашение, выставляем флажок в позицию «Я принимаю условия лицензионного соглашения» и нажимаем «Далее» (рисунок).

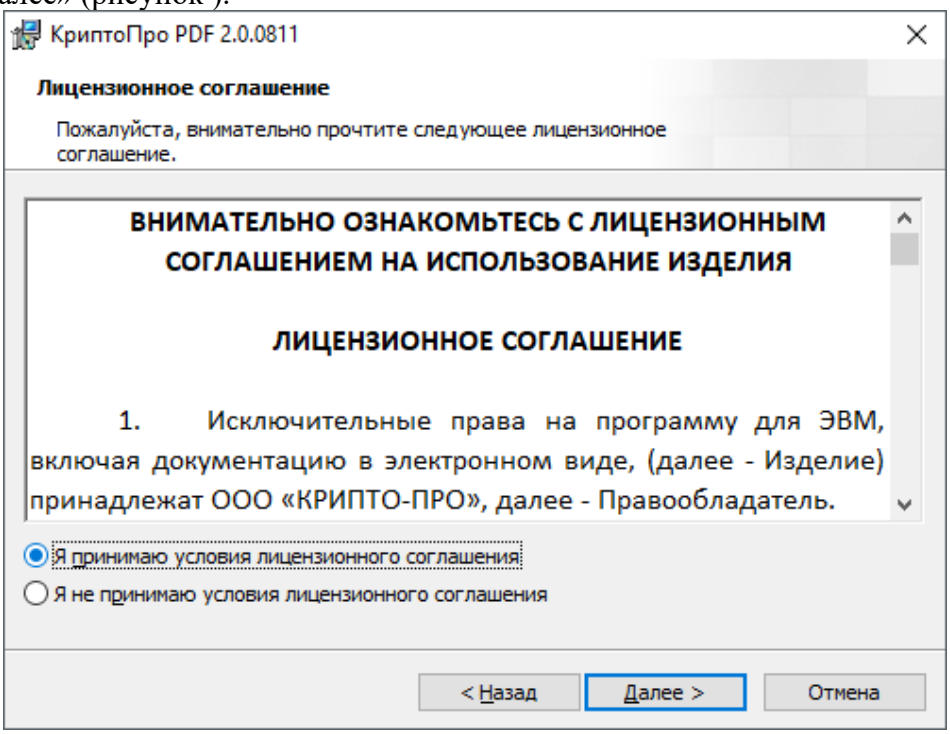


Рисунок – Установка Крипто-ПРО PDF

В новом окне необходимо ввести лицензионный ключ для использования программы, (рисунок). Для использования Крипто-ПРО PDFспродуктами AdobeReaderлицензионный ключ не требуется, тогда данное поле оставляем пустым. Но если для работы с другими программами, работающими с PDF-документами, тогда требуется лицензионный ключ, но если у Вас его нету, то программа установится бесплатно на 90 дней. Также, после установки программы, будет возможность ввести и активировать лицензионный ключ, для дальнейшего использования Крипто-ПРО PDFс другими программами, работающими с PDF-документами.

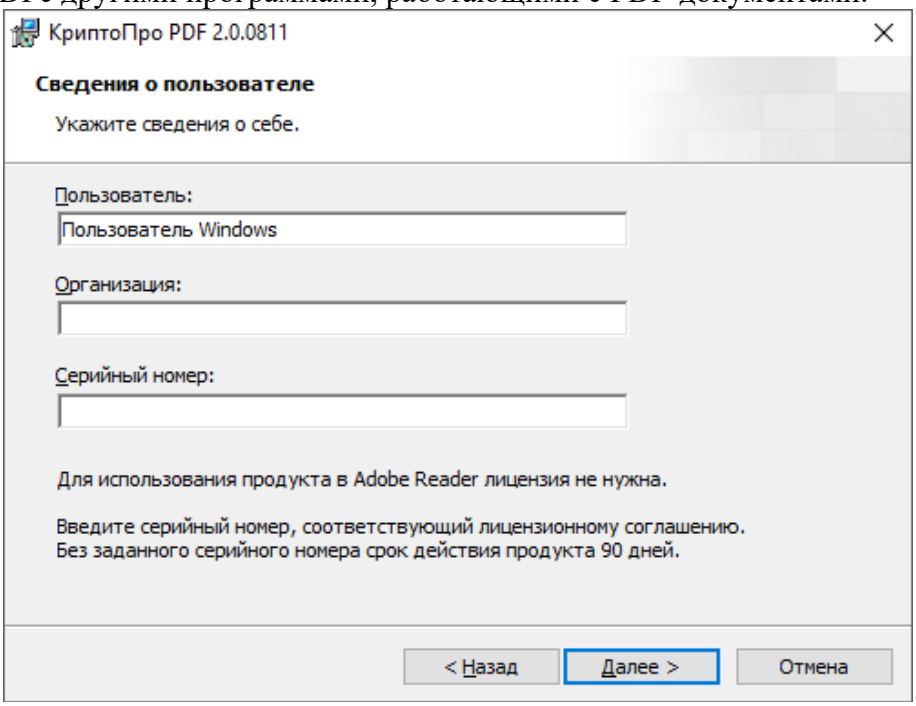


Рисунок – Ввод лицензионного ключа

На следующем шаге установки программы необходимо выбрать вид установки. Выбираем обычную установку программы (рисунок).

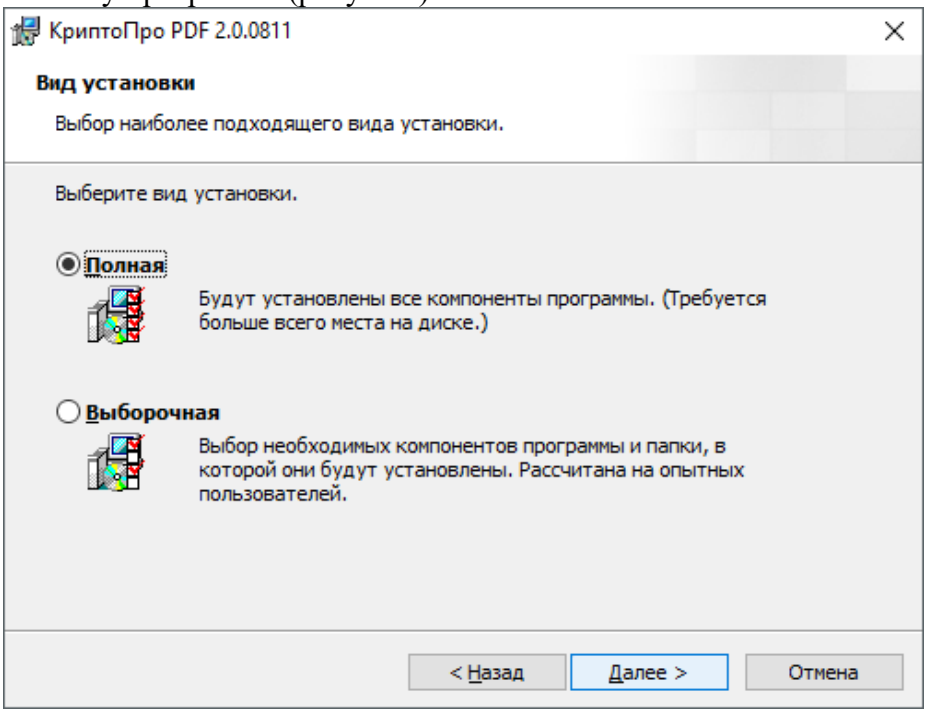


Рисунок – Выбор вида установки

В новом открывшемся окне ставим галочку напротив «Настроить КриптоПРО PDFкак метод подписи по умолчанию» и выбираем «Установить» (рисунок). После установки программы будет выведено окно об успешной установке Крипто-ПРО PDF (рисунок). Перезагрузите ПК.

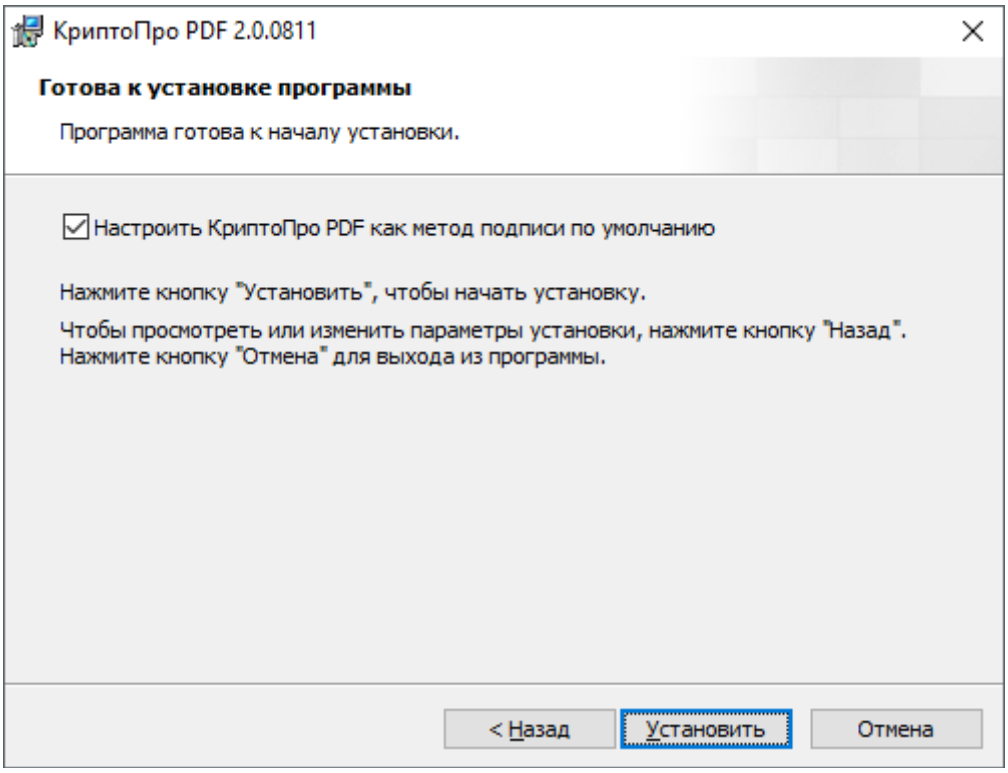


Рисунок – Последний этап установки

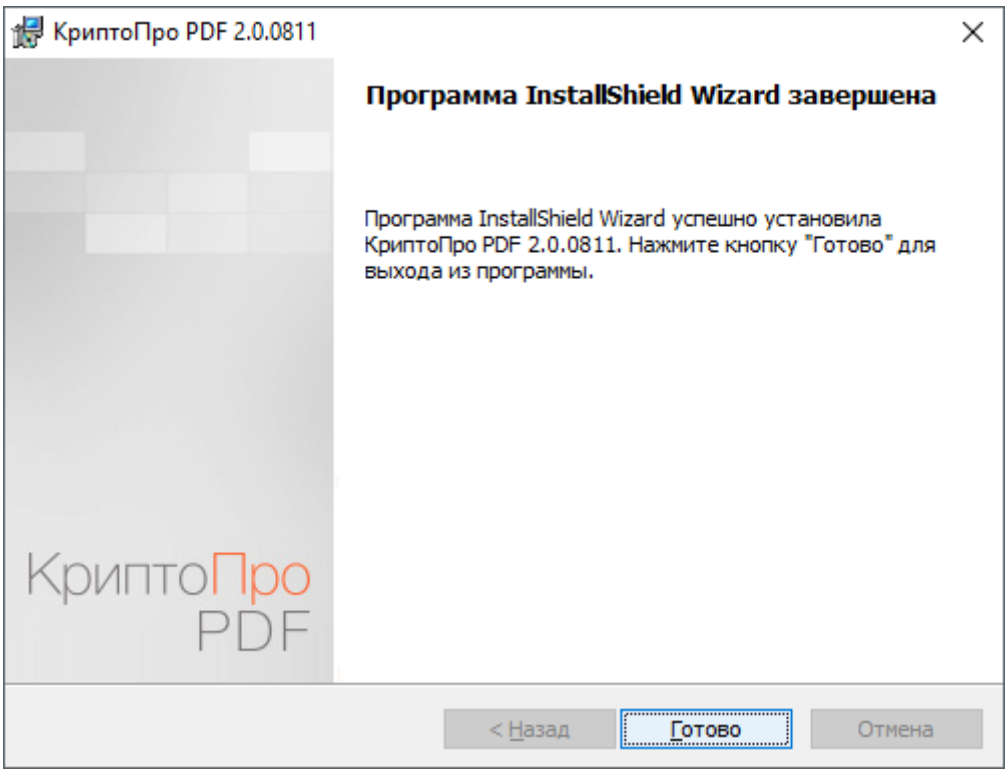


Рисунок – Успешное завершение установки программы

Все рисунки интерфейса ЭП будут представлены для Adobe Acrobat версии DC. Для других версий возможно незначительное отличие в интерфейсе. Откройте PDF-документ с помощью одного из программных продуктовAdobe Acrobat.Выберите пункт меню Инструменты ⇒ Сертификаты. На следующем шаге в документе следует выделить область для отображения ЭП. После чего в появившемся окне выберите требуемый сертификат из списка сертификатов, имеющихся в стандартном хранилище сертификатов Windows и нажмите «ОК» (рисунок). Для удобства работы список сертификатов можно отсортировать по каждой графе, нажав на соответствующее название «Субъект», «Издатель», «Действителен с» или «Действителен по».

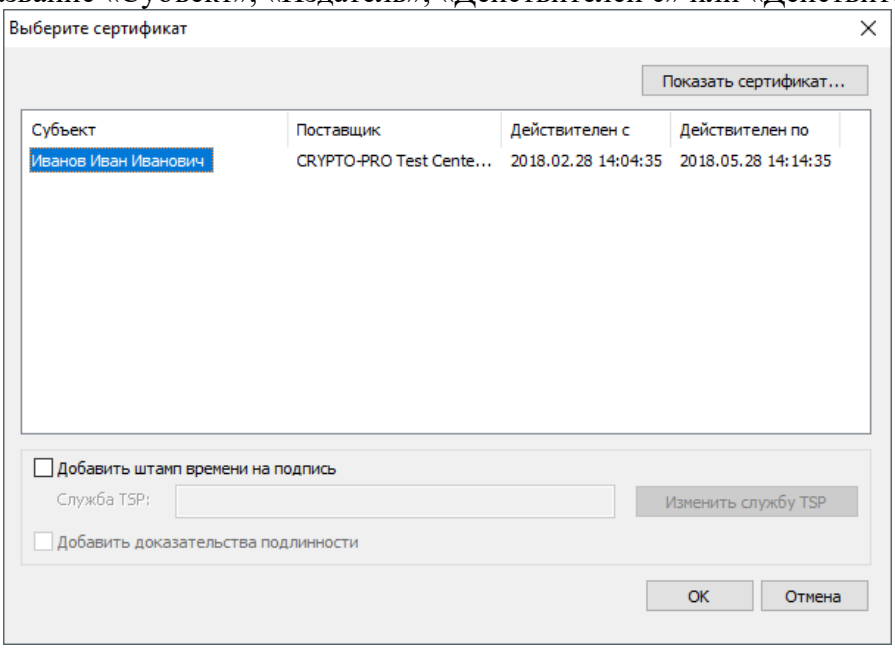


Рисунок –Выбор сертификата для формирования ЭП

Далее в окне «Подписать документ» будет предоставлена возможность заполнить дополнительные поля, отображаемые в свойствах ЭП (рисунок). Для формирования ЭП следует нажать кнопку «Подписать».

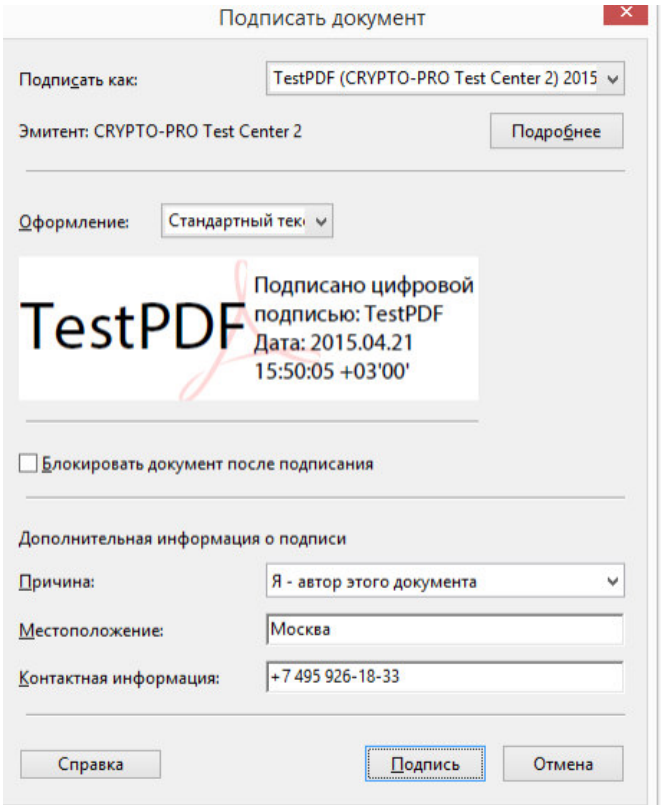


Рисунок –Окно создания подписи

Последним шагом следует указать файл в окне «Сохранить как», в который будет сохранена подписанная копия документа. Пример созданной в документе ЭП приведен на рисунке.

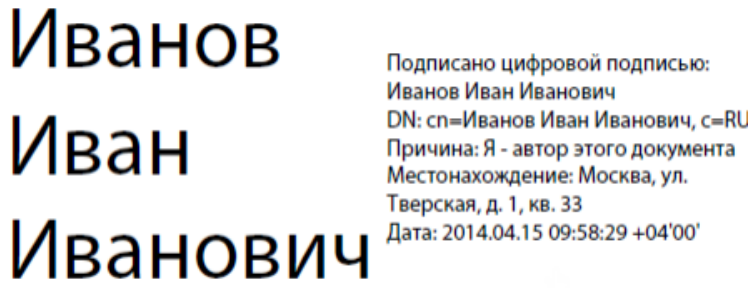


Рисунок – Пример ЭП в PDF-документе