

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

**Федеральное государственное автономное образовательное учреждение  
высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

**ИСТиД (филиал) в г.Пятигорске**

**Методические указания по выполнению лабораторных работ**

**По дисциплине «Безопасность информационных систем»**

Направление подготовки	09.03.02 Информационные системы и технологии
Профиль	<b>Информационные системы и технологии</b>
Квалификация выпускника	Бакалавр
Форма обучения	очный
Учебный план	2020
Изучается в 7 семестре	

**Пятигорск, 2020 г.**

Рассмотрено и утверждено на заседании кафедры систем управления и информационных технологий протокол № \_\_\_\_ от \_\_\_\_\_ 2020

Зав.кафедрой СУИТ \_\_\_\_\_ И.М. Першин

## ВВЕДЕНИЕ

В лабораторный практикум по дисциплине «Безопасность информационных систем» включены лабораторные работы по основным разделам этой дисциплины, читаемой на кафедре «Систем управления и информационных технологий». Лабораторные работы ориентированы на приобретение студентами навыков анализа сетевого трафика, фильтрации собранного трафика, нахождения и просмотра соединения, извлечения данных, передаваемых без шифрования, установки и настройки VPN-сервера, применения криптографии для безопасности данных, использования криптосистем PGP TrueCrypt, проверки безопасности хоста, выявления ошибок конфигурации.

Содержащиеся в данном пособии сведения теории, методические указания и рекомендации по выполнению лабораторных работ позволяют использовать его в качестве дополнительного пособия для закрепления курса лекций.

Целью данного лабораторного практикума является поэтапное формирование у студентов знаний, умений и навыков защиты информации в компьютерных сетях с использованием современного профессионального программного обеспечения.

Практикум предназначен для студентов Северо-Кавказского федерального университета и может быть полезным для всех желающих ознакомиться с основами защиты информации в компьютерных сетях.

Данный вид работы играет важную роль в формировании практических навыков защиты данных и способствует формированию следующих образовательных компетенций:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

## СОДЕРЖАНИЕ

Лабораторная работа №1. Межсетевые экраны. Изучение принципов работы межсетевых экранов.....	6
Лабораторная работа №2 . Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений. ....	19
Лабораторная работа №3. Базовое администрирование и разрешение сетевых проблем с использованием утилит командной строки Windows.....	23
Лабораторная работа №4. Анализ и изучение заголовков различных сетевых пакетов. ....	31
Лабораторная работа №5. Сканирование и исследования безопасности сети с помощью сканера Nmap.....	49
Лабораторная работа №6. Методы анализа сетевого трафика с использованием WireShark. ....	54
Лабораторная работа №7. Установка и настройка VPN сервера.....	65
Лабораторная работа №8. Применение криптографии для безопасности данных. Использование криптостем PGP TrueCrypt. ....	85
Лабораторная работа №9. Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft Baseline Security. ....	120
Лабораторная работа №10. Системы разграничения доступа. ....	128
Лабораторная работа №11. Управление доступом.....	136
Лабораторная работа №12. Аудит и журналы безопасности.....	146

## Лабораторная работа №1. Межсетевые экраны. Изучение принципов работы межсетевых экранов

**Цель:** изучение и конфигурирование межсетевого экрана Windows.

**Знать:** основные понятия межсетевых экранов.

**Уметь:** конфигурировать сетевой экран для защиты данных в сети.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть.

**Актуальность темы** объясняется особенностями подготовки магистров по инженерным направлениям. Технический характер изучаемых по данному направлению дисциплин требует от обучаемых наличие навыков работы с программными и аппаратными средствами защиты информации в компьютерных сетях.

#### **Теоретическая часть:**

Межсетевой экран, сетевой экран (так же употребляются названия файрвол и брандмауэр) — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

По своей сути межсетевой экран является **фильтром**, через который проходит сетевой трафик. Каждый сетевой пакет проходя через него проверяется на совпадение некоторых параметров пакета с характеристиками, описанными в **правиле** фильтрации. Такими характеристиками может быть направление пакета (входящий/исходящий/транзитный), порт приложения отправителя и/или получателя, тип протокола, IP-адреса, относится ли данный пакет к уже установленному соединению и ассоциирован ли он с каким-то приложением на компьютере. Если пакет соответствует правилу, к нему будет применено **действие**. Как правило пакет будет либо отброшен, либо пропущен. Но есть

и другие варианты, в частности на уровне сетевого экрана реализуется трансляция сетевых адресов (NAT).

Ход работы:

**1. Конфигурация сетевого экрана Windows**

- 1) Переведите сетевой адаптер виртуальной машины в режим сетевого моста и запустите машину (с Windows 7).
- 2) Запустите брандмауэр Windows. Для этого нажмите пуск и начните набирать “брандмауэр” в списке найденных приложений кликните на “Брандмауэр Windows в режиме повышенной безопасности”. Так же запустить приложение, можно через Пуск-Выполнить “fw.msc” (без кавычек).

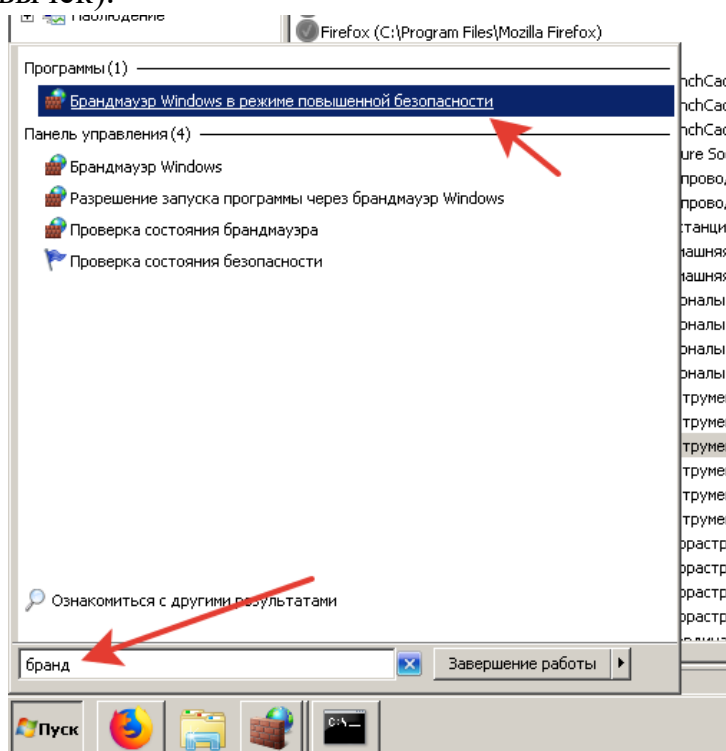


Рисунок 1 – Запуск брандмауэра

- 3) Откроется окно, показанное на рисунке 2.

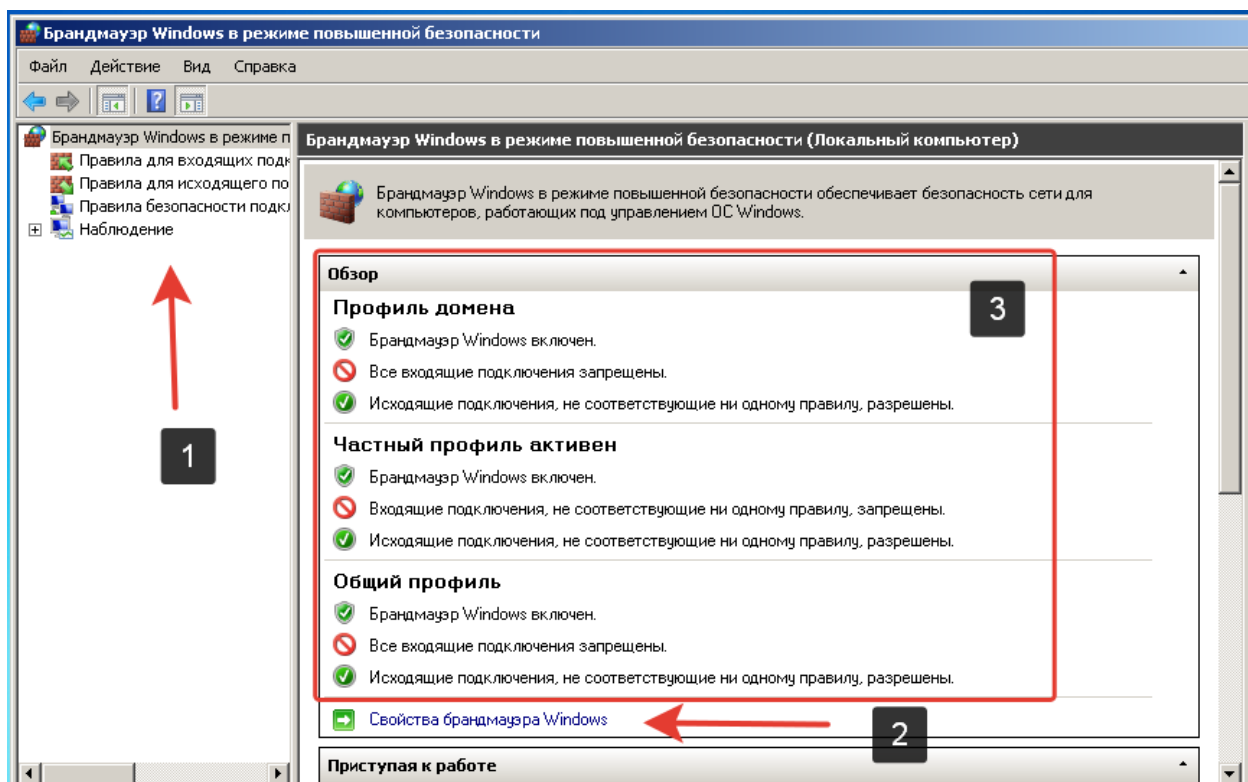


Рисунок 2 – главное окно оснастки Брандмауэра Windows

На рисунке 2 числом 1 отмечен список разделов:

- Брандмауэр Windows в режиме повышенной безопасности – раздел отображает основные текущие настройки всех профилей сети и позволяет их сконфигурировать. Если вам нужно отключить или включить брандмауэр – это здесь.
- Правила для входящих и исходящих подключений – разделы в которых задаются правила фильтрации трафика.
- Правила безопасности подключений – в данном разделе конфигурируются подключения с проверкой подлинности (тема выходит за рамки данной работы)
- Наблюдение – раздел в котором можно просмотреть какие профили активны сейчас для текущих сетевых подключений и активные правила фильтрации трафика.

Область (3) отмеченная на рисунке содержит информацию о текущих профилях брандмауэра. Профиль брандмауэра - это способ объединения настроек (например, правил брандмауэра и правил безопасности подключений), применяемых к компьютеру в зависимости от места подключения. На компьютерах, работающих под управлением этой версии



Windows, для брандмауэра Windows в режиме повышенной безопасности доступны три профиля:

<b>Профиль</b>	<b>Описание</b>
Домен	Применяется к сетевому адаптеру, подключенному к сети, в которой он может обнаружить контроллер домена, содержащего данный компьютер.
Частный	Применяется к сетевому адаптеру, если он подключен к сети, которая идентифицирована администратором как частная. Частная сеть - это сеть, которая подключена к Интернету не напрямую, но находится за каким-либо устройством безопасности, например маршрутизатором с преобразованием сетевых адресов (NAT) или аппаратным брандмауэром. Параметры частного профиля должны устанавливать большие ограничения, чем параметры профиля домена.
Общий	Применяется к сетевому адаптеру, если он подключен к публичной сети, например в аэропорту или кафе. Публичная сеть - это сеть, которая не имеет устройств безопасности между компьютером и Интернетом. Настройки общего профиля должны быть наиболее строгими, поскольку компьютер подключен к публичной сети, безопасность в которой нельзя контролировать.

4) Нажмите на ссылку (2) “Свойства брандмауэра Windows” откроется окно (Рисунок 3)

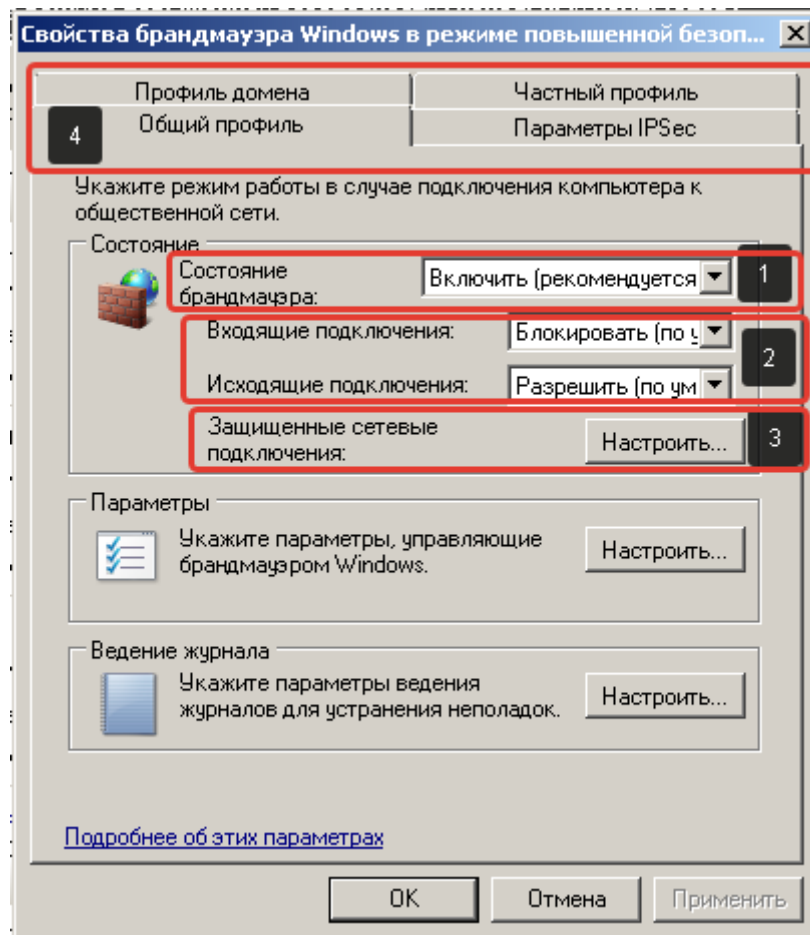


Рисунок 3 – Свойства брандмауэра Windows

- 1 Состояние брандмауэра – включает и отключает данный профиль брандмауэра.
  - 2 Входящие и исходящие подключения – задает правила поведения брандмауэра по-умолчанию. Есть два основных сценария поведения 1) все разрешено, кроме того, что явно запрещено правилами 2) все запрещено, кроме того, что явно правилами разрешено. Для входящих соединений так же есть третий вариант, “запрещено все”, в этом случае разрешающие правила игнорируются.
  - 3 Защищённые сетевые подключения – позволяет задать для каких сетевых адаптеров брандмауэр включен.
  - 4 Вкладки профилей.
- 4) Проверьте состояние всех профилей брандмауэра, если они выключены – включите их снова и закройте окно кнопкой ОК.
  - 5) Теперь попробуем заблокировать выход с нашего компьютера в интернет с помощью браузера. Запустите браузер и откройте сайт <https://ya.ru> убедитесь, что он открывается.
  - 6) Теперь перейдите в раздел “Правила для исходящего подключения” (Рисунок 4)

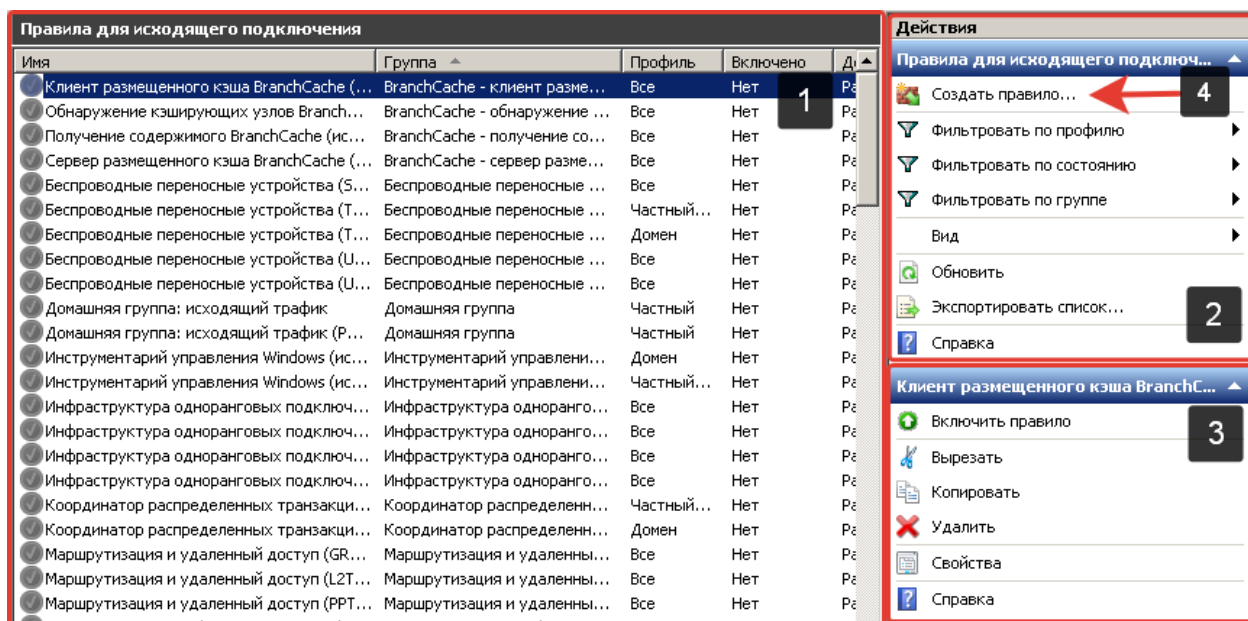


Рисунок 4 – Правила для исходящего соединения

Окно, приведенное на рисунке 4 состоит из нескольких областей.

Область 1 – список всех правил (в данном случае для исходящего соединения). Значок в левой части строки показывает тип правила (разрешить\запретить) и статус правила, включено оно или выключено (включенные правила – цветные, выключенные – серые).

Область 2 – Управление отображением списка правил, фильтрацией.

Область 3 – данная область появляется если выбрать правило из списка. Она позволяет включать и выключать правила, а так же конфигурировать их и удалять.

7) Нажмите на кнопку “Создать правило” (4 на рисунке 4). Откроется окно “Мастер создания правила для нового исходящего подключения”  
Рисунок 5

От выбора типа правила зависит количество шагов и настраиваемых параметров для правила. При выполнении самостоятельной работы рекомендуется поэкспериментировать с различными типами создания правил. Выберите “Настраиваемые” и нажмите “Далее”

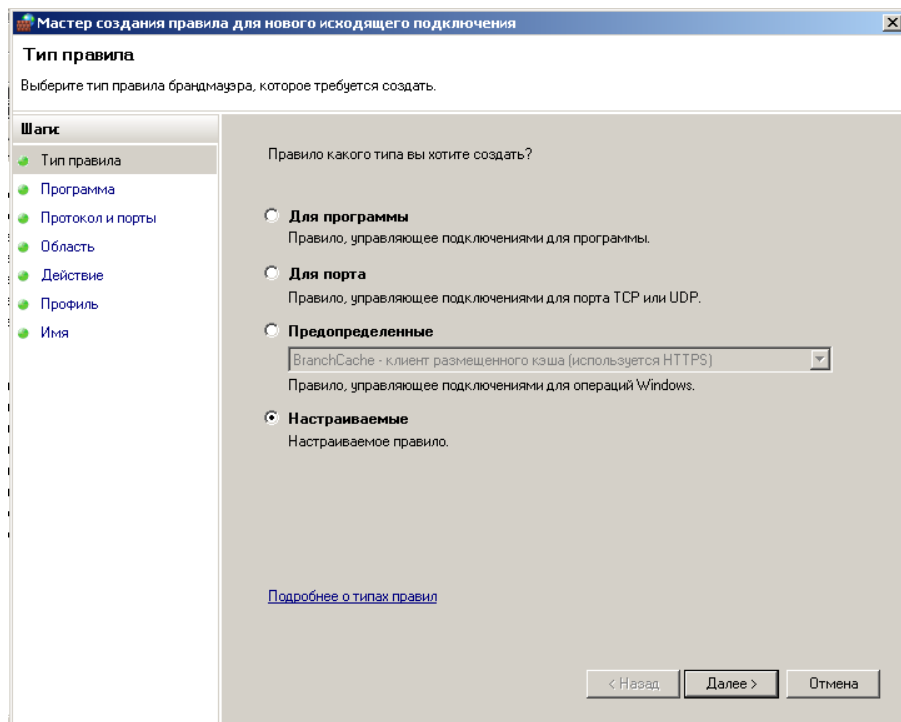


Рисунок 5 - Мастер создания правила для нового исходящего подключения

- 8) На этапе выбора программы (Рисунок 6), можно указать конкретное приложение которому нужно разрешить или запретить доступ к сети. В данном случае поставьте “Все программы” и нажмите далее

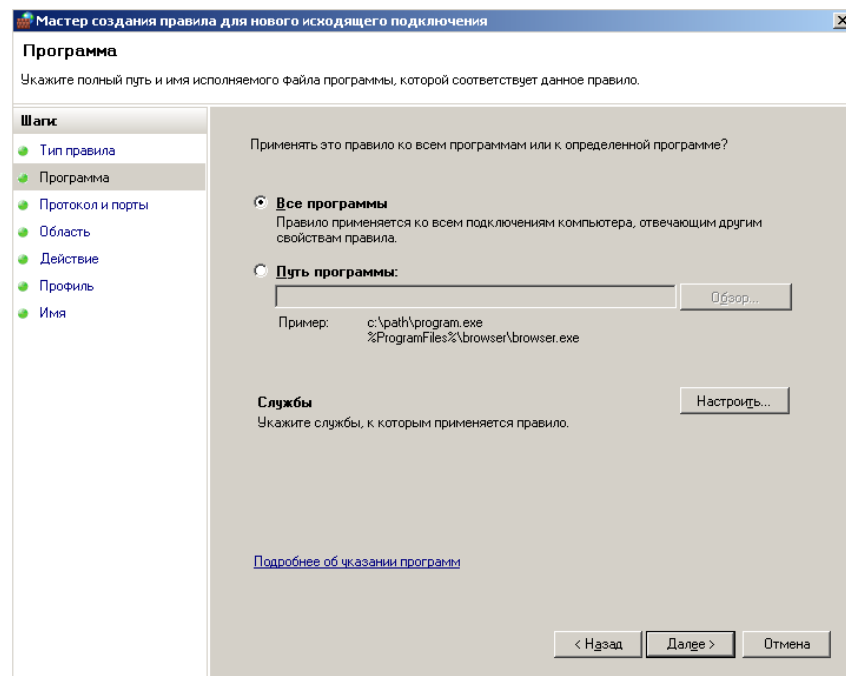


Рисунок 6 – Выбор программы

- 9) На шаге выбора протокола и портов указывается тип сетевого протокола и номера портов. Укажите протокол TCP и удаленные порты 80 и 443 (через запятую) (Рисунок 7)

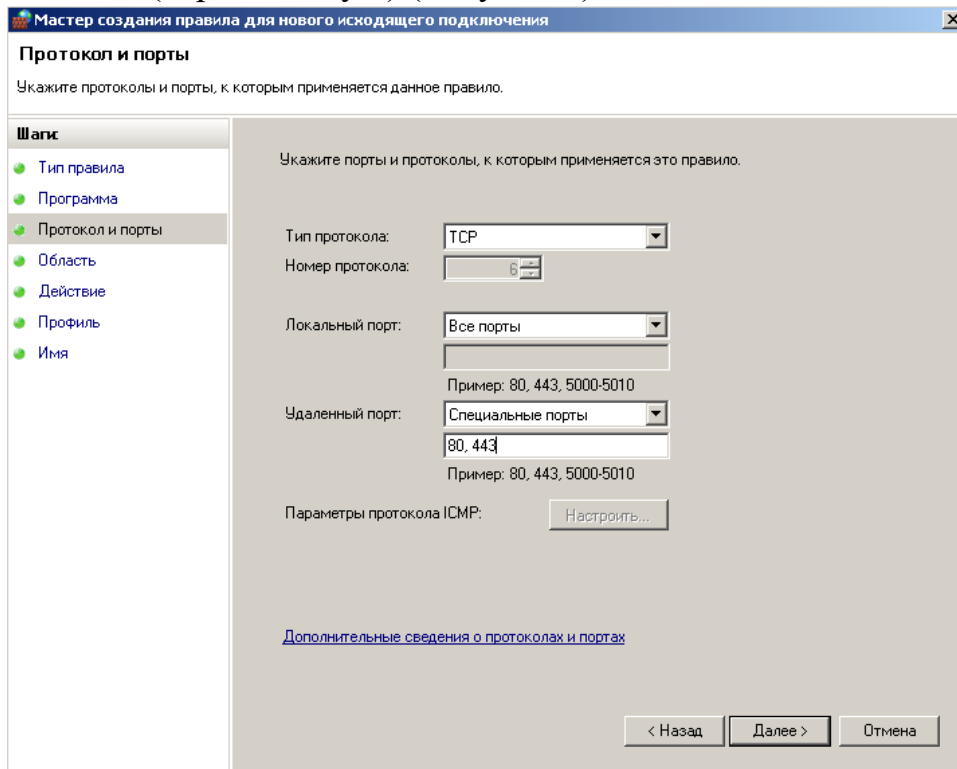


Рисунок 7 – Шаг выбора протокола и портов

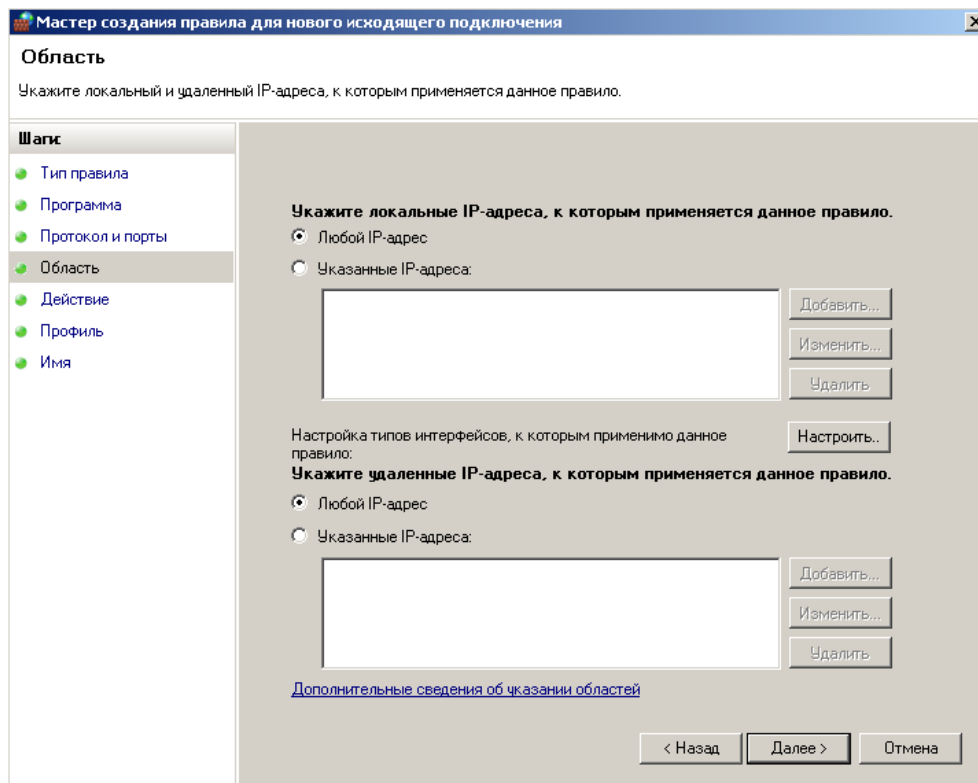


Рисунок 8 - Шаг Область

- 10) На шаге Область (Рисунок 8), можно задать IP-адреса на которые будет распространяться данное правило. Это удобно, если необходимо

разрешить доступ к приложению (например, веб-серверу) только для нескольких компьютеров в сети. Укажите, что для любых адресов и нажмите далее.

- 11) На шаге действие (Рисунок 9) определяются, что нужно сделать с соединением, пропустить его или отбросить. Выберите блокировать и нажмите Далее.

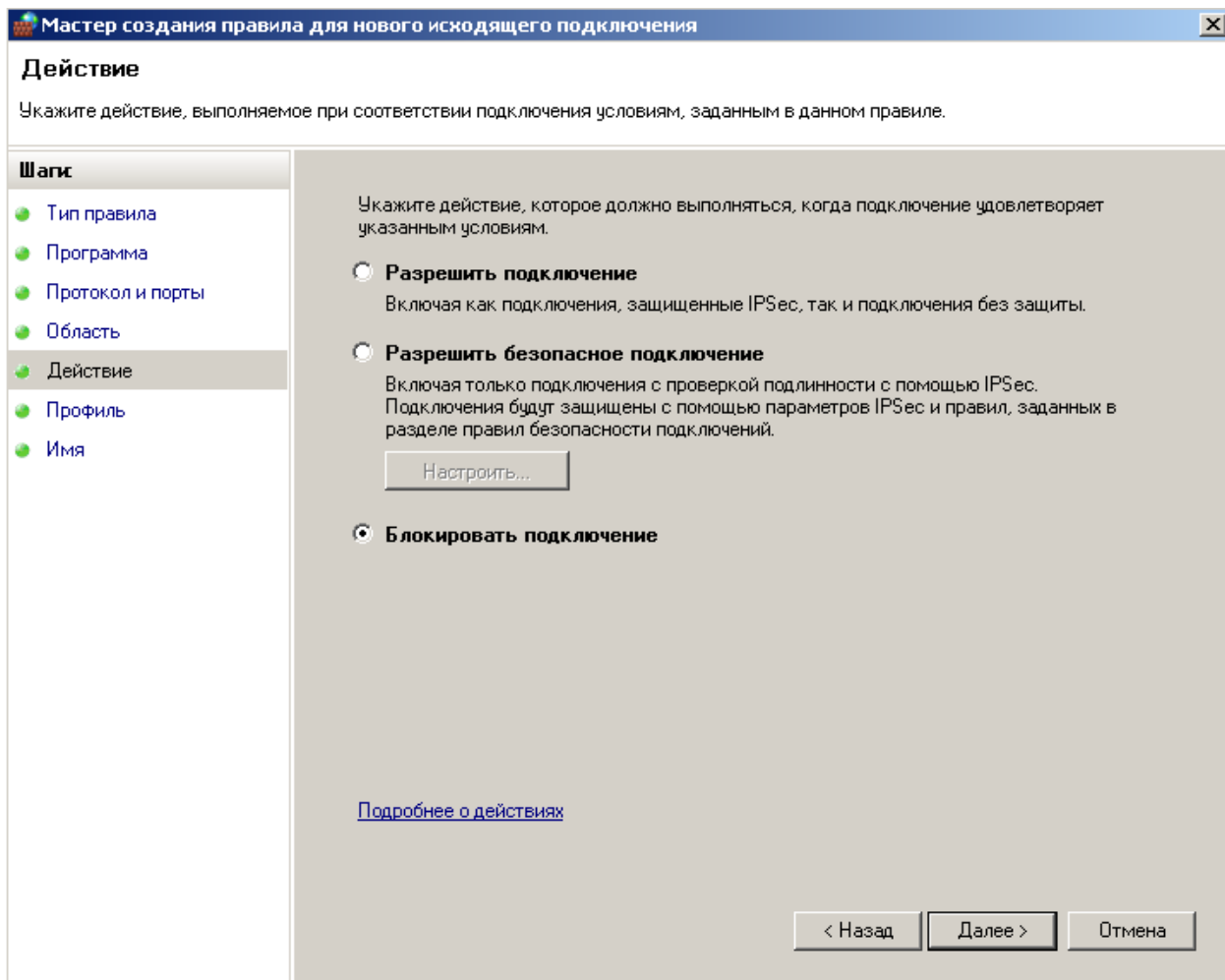


Рисунок 9 – Шаг Действие

- 12) На шаге Профиль (Рисунок 10), указывается для каких профилей брандмауэра применяется данное правило. Укажите все и нажмите Далее.

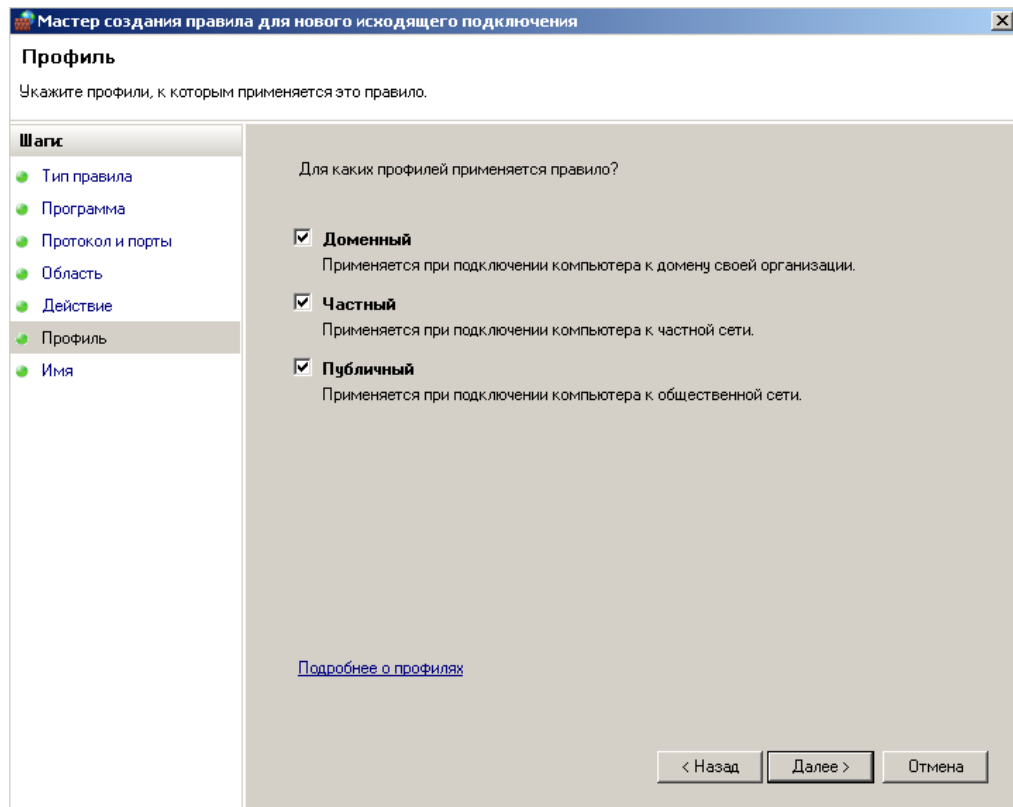


Рисунок 10 – Шаг Профиль

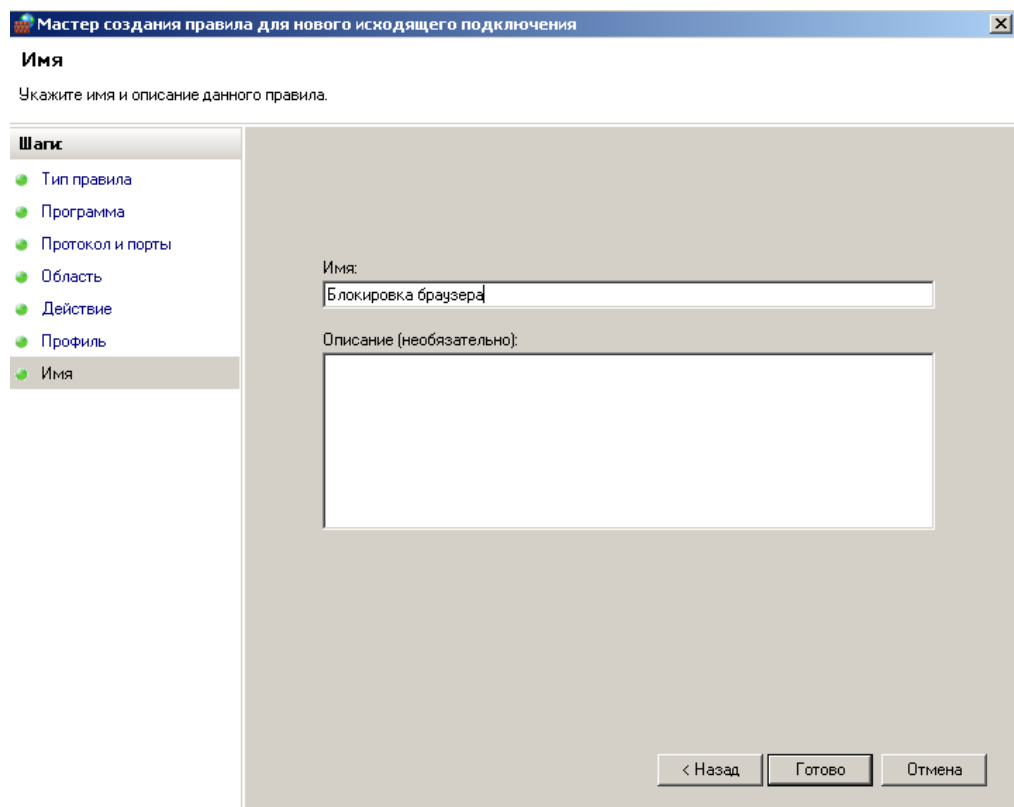


Рисунок 11 – Название правила

- 13) На последнем шаге (Рисунок 11) указывается название правила, под которым оно добавится с общий список правил. Хорошим тоном, считается указывать в имени правила его назначение и имя

программы/службы для которой оно создано. Укажите название “Блокировка браузера” и нажмите Готово.

- 14) Теперь перейдите в браузер и обновите страницу. Если все сделано правильно, то Браузер выведет сообщение об ошибке, т.к. не смог установить соединение. (Рисунок 12)

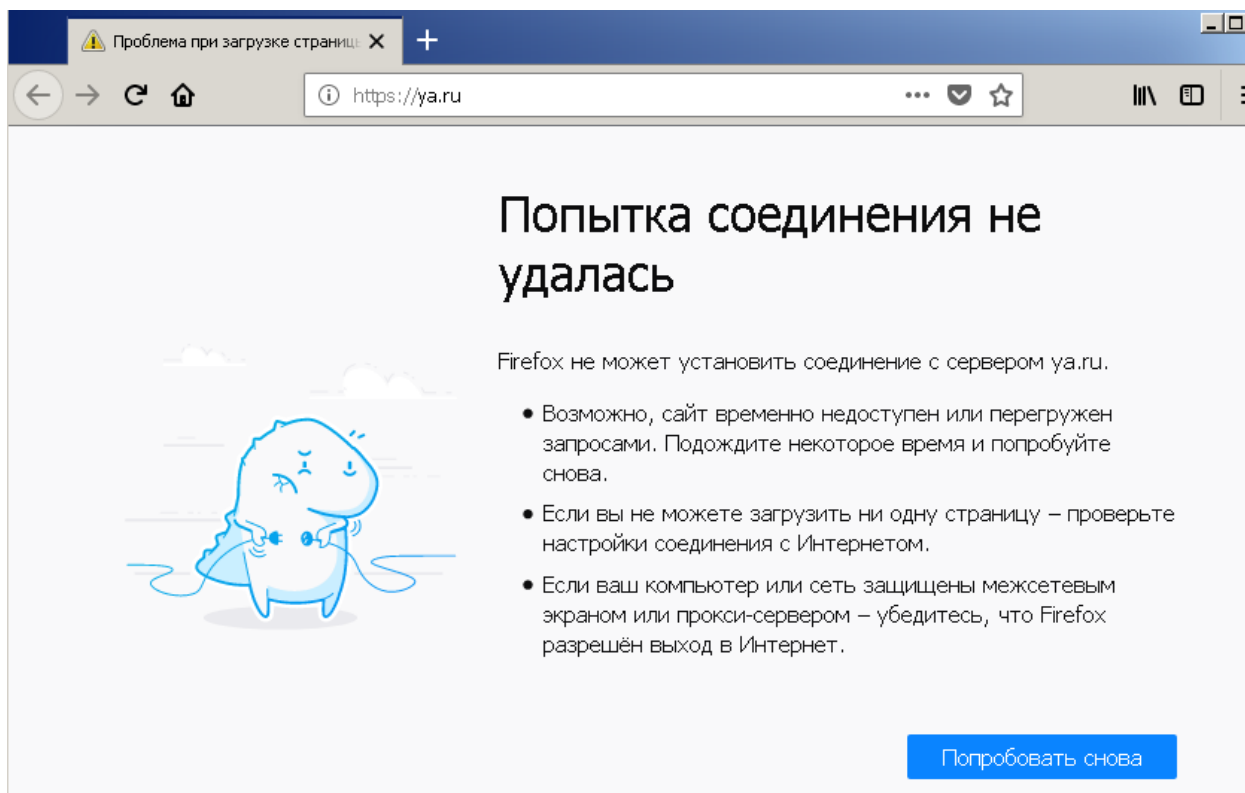


Рисунок 12 – Ошибка установления соединения.

- 15) Снова перейдите к конфигурации правил для исходящих соединений, выберите созданное правило и отключите его. Обновите страницу в браузере, соединение с Интернетом должно восстановиться.
- 16) Правила для исходящего трафика создаются аналогично.
- 17) На каждом шаге мастера создания правил, есть ссылка на справочную информацию, пользуйтесь ей при возникновении сложностей.

## 2. Самостоятельная работа

- 1) Создайте внутреннюю сеть между двумя виртуальными машинами с Windows 7 и запустите их.
- 2) Присвойте машинам ip-адреса 192.168.1.1 и 192.168.1.2.
- 3) Включите сетевой экран на узле 192.168.1.1, разрешите для всех профилей входящие соединения.



- 4) Просканируйте машину 192.168.1.1 с машины 192.168.1.2 с помощью Nmap, определите версию ОС и все открытые TCP и UDP порты. Порты должны быть открыты.
- 5) Проверьте доступность 192.168.1.1 с 192.168.1.2 утилитой ping. Ping должен проходить.
- 6) Создайте правило для входящего трафика для всех профилей запрещающее подключение на 130-140 TCP порты.
- 7) Повторите сканирование узла 192.168.1.1 Nmap, убедитесь, что порты фильтруются.
- 8) Создайте правило запрещающее входящие ICMPv4 пакеты. Проверьте доступность 192.168.1.1 с 192.168.1.2 утилитой ping. Ping не должен проходить.
- 9) Создайте правила, блокирующие все входящие TCP и UDP пакеты. Повторите сканирование узла 192.168.1.1 Nmap, убедитесь, что порты фильтруются. Отключите правила блокирующие все входящие TCP и UDP пакеты.
- 10) Отредактируйте правило запрещающее ICMPv4 запросы, так чтобы запретить запросы только с узла 192.168.1.2.
- 11) Проверьте доступность 192.168.1.1 с 192.168.1.2 утилитой ping. Измените IP-адрес с 192.168.1.2 на 192.168.1.3 и повторите проверку, ping должен проходить.
- 12) Запустите на узле 192.168.1.1 Wireshark и начните захват трафика. С узла 192.168.1.3 просканируйте Nmap порт TCP 445 на узле 192.168.1.1. Попробуйте syn-сканирование этого же порта. Создайте правило блокирующее порт 445. Повторите сканирование. Остановите захват трафика Wireshark. Найдите в перехваченных пакетах, попытки установления соединения. В чем разница между попыткой установления соединения с открытым и фильтруемым портом? Чем отличается сканирование с установлением соединения от syn-сканирования?

Контрольные вопросы:

1. Принципы работы межсетевых экранов.
2. Конфигурирование межсетевого экрана Windows.
3. Классификация.
4. Профиль брандмауэра – домен, частный, общий.
5. Состояние брандмауэра.
6. Правила для исходящих и входящих соединений.
7. Мастер создания правила для нового исходящего подключения.

Список литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## Лабораторная работа №2 . Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.

Цель работы: Получить сведения о том, как осуществляется защита с помощью систем обнаружения и предотвращения вторжений. Научиться использовать SNORT.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть.

Система обнаружения вторжений (IDS) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Сетевая система обнаружения вторжений (англ. network intrusion detection system, NIDS) — система обнаружения вторжений, которая отслеживает такие виды вредоносной деятельности, как DoS атаки, сканирование портов или даже попытки проникновения в сеть.

В пассивной IDS при обнаружении нарушения безопасности, информация о нарушении записывается в лог приложения, а также сигналы опасности отправляются на консоль и/или администратору системы по определенному каналу связи. В активной системе, также известной как Система Предотвращения Вторжений (IPS — Intrusion Prevention system (англ.)), IDS ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника. Ответные действия могут проводиться автоматически либо по команде оператора.

Обнаружение проникновения позволяет организациям защищать свои системы от угроз, которые связаны с возрастанием сетевой активности и важностью информационных систем. При понимании уровня и природы современных угроз сетевой безопасности, вопрос не в том, следует ли использовать системы обнаружения проникновений, а в том, какие

возможности и особенности систем обнаружения проникновений следует использовать.

Snort — свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом, способная выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP-сетях.

Выполняет протоколирование, анализ, поиск по содержимому, а также широко используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как попытки атак на переполнение буфера, скрытое сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения операционной системы. Программное обеспечение в основном используется для предотвращения проникновения, блокирования атак, если они имеют место.

Snort использует правила, написанные простым, но в то же время гибким и достаточно мощным языком. Существует ряд общих принципов написания, запомнить которые достаточно просто.

Большая часть правил Snort уместается в 1 строку. Это следствие того, что до версии 1.8 нельзя было использовать многострочные записи. В более поздних версиях правила можно растягивать на несколько строк, вставляя в конец строки символ “” (без кавычек).

Правила Snort состоят из двух частей: заголовка правила и параметров правила. Заголовок содержит описание действия, протокол передачи данных, IP-адреса, сетевые маски и порты источника и назначения. Параметры правила хранят предупреждающее сообщение, а также информацию о том, какую часть обнаруженного пакета нужно обработать в случае срабатывания правила.

#### Ход работы.

- Узнайте свой ip адрес командой ifconfig
- Установите SNORT <sudo apt-get install snort>
- При установке будет нужно указать защищаемую сеть. Введите \*.\*.0/24 (Где \*.\* - первые три числа вашего ip-адреса, например это будет 192.168.1.0/24, если вы используете VirtualBox и у вас в настройках сети стоит сетевой мост)
- Запустите SNORT <sudo service snort start>
- Настройка правил
- Перейдите в каталог /etc/snort/rules < cd /etc/snort/rules)
- Создайте файл с правилами <nano test.rules>  
alert tcp any any -> any any (content:»<https://www.google.ru/>» ; msg:»Someone open Google website» ; sid: 12312313;)
- Перейдите в каталог /etc/snort <cd /etc/snort)
- Теперь нужно изменить содержимое конфигурационного файла Snort < sudo nano snort.conf>
- Найдите строки с правилами (они начинаются с include \$RULE\_PATH, это в части Step 7) и добавьте файл с нашими правилами include \$RULE\_PATH/test.tules

- В файле snort.conf так же укажите домашнюю сеть. В Step 1 измените строчку «ipvar HOME\_NET any» , на ipvar HOME\_NET 192.168.1.0/24
- Запустите snort <sudo snort -A console -i eth0 -c snort.conf>
- Зайдите на <https://www.google.ru/> и проверьте в терминале, как работает правило.
- Теперь нам понадобится еще одна виртуальная машина, на ней должен быть установлен nmap.
- Со второй ВМ используйте ping, посмотрите, как реагирует SNORT
- Используйте различные методы сканирования nmap( используйте -sS, -sT, -sN, -sU, -sX, -sF и посмотрите, как реагирует SNORT;
- В файл test.rules добавьте правило обнаружения сканирования nmap -sN (NULL Scan)  
alert tcp any any -> any any (msg:»NULL Scan»; flags: 0; sid:322222;)
- Запустите snort <sudo snort -A console -i eth0 -c snort.conf>
- Со второй виртуальной машины произведите NULL сканирование <sudo nmap -sN>, проверьте, как работает правило.
- Можно загрузить обновленные правила SNORT, для этого:
- Зарегистрируйтесь на сайте <https://www.snort.org/> и скачайте последнюю версию правил
- Разархивируйте скачанный архив и скопируйте каталоги rules, so\_rules и preproc\_rules в /etc/snort :  
sudo cp -R ./rules/ /etc/snort/  
sudo cp -R ./so\_rules/ /etc/snort/  
sudo cp -R ./preproc\_rules/ /etc/snort/

### Контрольные вопросы:

1. Что такое IDS?
2. Что такое сетевая система обнаружения вторжений?
3. Чем отличаются пассивные и активные IDS?
4. Что такое SNORT?
5. Какие задачи выполняет SNORT?
6. Как работают правила SNORT?
7. Как писать правила для SNORT?
8. Зачем писать собственные правила SNORT?
9. Зачем загружать обновление правил SNORT?
10. Как в SNORT создавать логи?

### Список литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые

данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.

2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

### **Лабораторная работа №3. Базовое администрирование и разрешение сетевых проблем с использованием утилит командной строки Windows.**

**Цель:** В этой работе демонстрируется использование базовых команд командной строки windows применяемых для поиска проблем в сети.

**Знать:** базовые знания о поиске проблем в сетях требующихся для диагностики, мониторинга и восстановления сетевых подключений

**Уметь:** выполнять поиск и устранение сетевых проблем.

#### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

**Актуальность темы** объясняется особенностями подготовки магистров по инженерным направлениям. Технический характер изучаемых по данному направлению дисциплин требует от обучаемых наличие навыков работы с программными и аппаратными средствами защиты информации в компьютерных сетях.

#### ***Теоретическая часть:***

Поиск и устранение сетевых проблем является одним из важнейших навыков, который необходимо освоить администратору сети в крупных и средних организациях. Администраторам следует иметь базовые знания о поиске проблем в сетях требующихся для диагностики, мониторинга и восстановления сетевых подключений. Windows предлагает несколько мощных утилит командной строки которые помогают администраторам в поиске проблем в их сетевых соединениях.

Консольные утилиты Windows такие как ipconfig, ping, tracert, nslookup, netstat, arp и др, позволяют администрировать, диагностировать, наблюдать и восстанавливать сетевые соединения.

#### **Практическая часть.**

**Для выполнения работы потребуется:**

Виртуальная машина под управлением Windows 7. Установите в на виртуальной машине режим NAT для сетевого адаптера и запустите её.

### Задание 1- Проверка настроек IP

1. Запустите виртуальную машину и залогиньтесь в систему.
2. Запустите командную строку **cmd**
3. Напечатайте **ipconfig** в командной строке и нажмите Enter для проверки конфигурации IP на данной машине.
4. Детали IP конфигурации системы будут выведены на экран. Как сетевой администратор вы должны знать параметры конфигурации всех узлов в сети.

```

Администратор: C:\Windows\System32\cmd.exe
C:\Windows\system32>ipconfig
Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::b9df:2247:5145:f6e%11
    IPv4-адрес . . . . . : 10.0.2.15
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 10.0.2.2

Туннельный адаптер isatap.{3774DA73-2E49-4D96-A257-1D17BAC693B1}:

    Состояние среды . . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

C:\Windows\system32>
  
```

5. Вы можете использовать различные параметры ipconfig для разрешения различных сетевых проблем.

Параметры Ipconfig	
/all	Показать полные настройки TCP/IP конфигурации для всех адаптеров
/renew [адаптер]	Обновить конфигурацию DHCP для всех адаптеров (или конкретного указанного)
/release [адаптер]	Послать DHCPRELEASE сообщение DHCP серверу для освобождения текущей DHCP конфигурации и сброса конфигурации IP-адресов для каждого из адаптеров (если адаптер не указан) или для каждого конкретного адаптера.
/flushdns	Очистить и сбросить содержимое кэша локального DNS клиента
/displaydns	Отобразить содержимое локального кэша DNS-клиента, которые включает в себя загруженные записи из локального файла Hosts и все недавние ответы на запросы отправленные с данного компьютера.
/registerdns	Инициализирует ручную динамическую регистрацию событий для DNS имен и IP адресов которые сконфигурированы на компьютере
/showclassid Адаптер	Отобразить ID класса DHCP заданный для выбранного адаптера



/setclassid Адаптер [ClassID]	Сконфигурировать ID класса DHCP заданный для выбранного адаптера
/?	Показать справку в командной строке

6. Теперь, наберите ipconfig /all и нажмите Enter. Эта команда будет перечислять Системные настройки IP, имя хоста, каждый Ethernet адаптер установленный в системе и так далее, как показано на скриншоте

```
C:\Windows\system32>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : CL1
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет

Ethernet adapter Подключение по локальной сети:

DNS-суффикс подключения . . . . . :
Описание . . . . . : Адаптер рабочего стола Intel(R) PRO/1000
MT
Физический адрес . . . . . : 08-00-27-09-65-8A
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::b9df:2247:5145:f6e%11(Основной)
IPv4-адрес . . . . . : 10.0.2.15(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 15 сентября 2018 г. 20:19:14
Срок аренды истекает . . . . . : 17 сентября 2018 г. 11:13:42
Основной шлюз . . . . . : 10.0.2.2
DHCP-сервер . . . . . : 10.0.2.2
IAID DHCPv6 . . . . . : 235405351
DUID клиента DHCPv6 . . . . . : 00-01-00-01-23-07-0F-EA-08-00-27-09-65-8A

DNS-серверы . . . . . : 8.8.8.8
                        8.8.4.4
NetBios через TCP/IP . . . . . : Включен

Беспроводной адаптер isatap.{3774DA73-2E49-4D96-A257-1D17BAC693B1}:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : Адаптер Microsoft ISATAP
Физический адрес . . . . . : 00-00-00-00-00-00-E0
DHCP включен . . . . . : Нет
Автонастройка включена . . . . . : Да
```

7. Вы можете использовать полученную информацию из шага выше, для создания Инвентарного Списка всех компьютерных устройств в вашей сети.

№	Имя компьютера	MAC Адрес	NDSCP Статус	IP Адрес	Маска подсети	Шлюз

## Задание 2 – проверка соединения на уровне протокола IP с использованием команды Ping

8. Теперь мы исследуем использование команды **ping**. Сетевые администраторы часто сталкиваются с ошибками IP соединений такими как **Превышен интервал ожидания запроса** и **Заданный узел недоступен**. С помощью команды ping они могут проверить доступность (связность) от одного хоста до других узлов сети.
9. Выполните в командной строке команду **ping 10.10.10.10**. (где 10.10.10.10 – адрес некоего удаленного узла)
10. Вы можете видеть ошибку “Превышен интервал ожидания запроса”. Это означает, что удаленная система не ответила в предусмотренный отрезок времени. Причина этого в том, что-либо удаленная машина выключена или отключен сетевой адаптер

на удаленной машине. (Так же возможно, что на удаленной машине запущен межсетевой экран).

Параметр	Применение
-n Количество	Определяет количество отправляемых эхо-запросов. По умолчанию 4.
-w Таймаут	Позволяет регулировать таймаут (в миллисекундах). По умолчанию 1000 (1 секунда)
-l Размер	Позволяет регулировать размер пинг-пакета. По умолчанию 32 байта
-f	Устанавливает флаг “Не фрагментировать (Do not fragment)” в заголовке ICMP пакета. По умолчанию выключен.

```
C:\Users\User>ping 10.10.10.10

Обмен пакетами с 10.10.10.10 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 10.10.10.10:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)
```

11. Проверьте доступность шлюза указанного в настройках IP и сервера **ya.ru**.

### Задание 3 – Определение маршрута (трассировка) пакетов с использованием команды **tracert**

12. Теперь мы увидим как использовать команду **tracert** для определения числа хопов (hops, прыжков) между узлом отправителя и получателя в сети. Tracert полезен для поиска проблем в больших сетях, где несколько путей могут вести к одной точке или где используется много промежуточных компонентов (мостов и маршрутизаторов).

Про **tracert**:

Диагностическая утилита **tracert** определяет маршрут до узла назначения путем отправки Internet Control Message Protocol (Протокол контрольных сообщений Internet) (ICMP) эхо-пакетов на удаленный адрес. В этих пакетах, **tracert** использует различные значения IP Time-To-Live (TTL, Время жизни). Поскольку каждый роутер на протяжении пути требует уменьшить TTL пакета на единицу перед пересылкой пакета, TTL может служить эффективным счетчиком прыжков. Когда TTL в пакете достигает нуля (0), маршрутизатор отправляет ICMP сообщение “Time Exceeded” (Превышено время) назад компьютеру отправителю.

**Tracert** отправляет первый эхо-пакет с TTL равным 1 и увеличивает TTL на 1 для каждой следующей передаче, пока не ответит узел назначения, или не будет достигнут максимальный TTL. ICMP сообщения “Time Exceeded” которые отправляют назад промежуточные маршрутизаторы показывают маршрут. Однако заметим, что некоторые маршрутизаторы молча отбрасывают пакеты у которых истек TTL и эти пакеты невидимы для **tracert**.

Tracert печатает упорядоченный список промежуточных маршрутизаторов которые возвращают ICMP сообщение “Time Exceeded”. Используйте опцию -d команды tracert чтобы отключить разрешение IP адресов в доменные имена для промежуточных узлов.

13. Определите путь до pf.ncfu.ru. Для этого наберите tracert pf.ncfu.ru в командной строке и нажмите Enter. Пример результата приведен на скриншоте ниже.

```
C:\Users\User>tracert pf.ncfu.ru

Трассировка маршрута к pf.ncfu.ru [81.177.166.88]
с максимальным числом прыжков 30:

  1  <1 ms     1 ms     2 ms     10.0.2.1
  2   35 ms    160 ms    26 ms    192.168.1.1
  3  1047 ms   904 ms   430 ms   stvr-bras1.ug.ip.rostelecom.ru [178.34.128.11]
  4   *         *         *         Превышен интервал ожидания для запроса.
  5   *         *         *         Превышен интервал ожидания для запроса.
  6   *         *         *         Превышен интервал ожидания для запроса.
  7   *         309 ms   330 ms   msk-bgw1-xe-2-0-0-0.rt-comm.ru [195.161.4.137]
  8   *         371 ms   355 ms   msk-dsr10-tg3-4.rt-comm.ru [217.106.7.150]
  9  301 ms    346 ms   292 ms   msk-dsr10-tg3-4.rt-comm.ru [217.106.7.150]
 10  333 ms    358 ms   357 ms   81.177.166.88

Трассировка завершена.
```

#### Задание 4 – Разрешение доменных имен с использованием команды nslookup

14. Теперь рассмотрим демонстрацию использования команды nslookup. Nslookup поиск по серверу имен (Name server lookup). Он использует запросы к DNS серверу для получения доменных имен и ассоциированных с ними IP адресов. Это может использоваться с доменным именем в качестве аргумента или независимо от него.
15. В командной строке наберите nslookup и доменное имя которое вы хотите разрешить (например pf.ncfu.ru) и нажмите Enter.

```
C:\Users\User>nslookup pf.ncfu.ru
Получены данные: google-public-dns-a.google.com
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Цель: pf.ncfu.ru
Address: 81.177.166.88
```

16. На скриншоте выше можно увидеть, что доменное имя (pf.ncfu.ru) разрешилось в соответствующий ему IP адрес (81.177.166.88)
17. Вы можете также использовать команду nslookup с параметрами для получения ответа от неавторизованного сервера имен, как показано на скриншоте ниже.

```
C:\Users\User>nslookup -type=A pf.ncfu.ru
Получены данные: google-public-dns-a.google.com
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Цель: pf.ncfu.ru
Address: 81.177.166.88
```

18. Для получения авторизованной информации вы можете использовать параметр -type=soa для nslookup.

```
C:\Users\User>nslookup -type=soa pf.ncfu.ru
Server: google public dns [google.com]
Address: 8.8.8.8

ncfu.ru
primary name server = ns1.ncfu.ru
responsible mail addr = noc.ncfu.ru
serial = 2018091100
refresh = 1800 (30 mins)
retry = 300 (5 mins)
expire = 1209600 (14 days)
default TTL = 300 (5 mins)
```

19. В данном случае главным авторизованным сервером имен, обслуживающим данную доменную зону является ns1.ncfu.ru.

**Задание 5 – Проверка вашей сетевой конфигурации и сетевой статистики командой netstat.**

20. Теперь рассмотрим использование команды netstat. Netstat обозначает сетевая статистика (network statistics). Показывает активные сетевые подключения, порты которые компьютер прослушивает, Ethernet статистику, таблицу маршрутизации, статистику IPv4/IPv6 протоколов. Запущенная без параметров, netstat выведет активные TCP соединения.

21. Наберите netstat в командной строке для проверки вашей сетевой статистики как показано на скриншоте

```
C:\Users\User>netstat

Активные подключения

Имя      Локальный адрес      Внешний адрес      Состояние
TCP      10.0.2.10:1036      a2-23-167-41:http  ESTABLISHED
TCP      10.0.2.10:1037      ec2-52-44-173-95:http  ESTABLISHED
TCP      10.0.2.10:1039      ec2-52-17-59-31:https  ESTABLISHED
TCP      127.0.0.1:1032      CL1:1033           ESTABLISHED
TCP      127.0.0.1:1033      CL1:1032           ESTABLISHED
TCP      127.0.0.1:1034      CL1:1035           ESTABLISHED
TCP      127.0.0.1:1035      CL1:activesync     ESTABLISHED
```

22. Вы можете использовать netstat с различными параметрами для получения важной информации о подключениях.

Параметр	Применение
-a	Отобразить все активные TCP соединения и TCP и UDP порты которые прослушивает компьютер
-e	Отобразить Ethernet статистику, количество байт полученных и переданных. Этот параметр может сочетаться с -s
-n	Отобразить активные TCP соединения, адреса и номера портов выраженный числами в не определенными именами (например порт 80, а не http)
-o	Отобразить активные TCP соединения включая PID идентификатор процесса для каждого процесса. Вы можете найти приложение по его PID на вкладке процессы Диспетчера Задач Windows. Этот параметр совместим с -a, -n и -p
-p протокол	Показать соединения по указанному протоколу. В этом случае протокол может быть tcp, udp, tcpv6 или udpv6. Если этот параметр используется с -s то отображается статистика по

	конкретному протоколу, Протокол может быть tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6 или ipv6.
-s	Отображает статистику по протоколу. По умолчанию, статистика показывается для TCP, UDP, ICMP и IP протоколам. Этот параметр может использоваться с параметром -p
-r	Показывает содержание таблицы маршрутизации IP. Это аналог команды route print.
<i>Интервал</i>	Обновляет выбранную информацию каждые Интервал секунд. Нажмите Ctrl+C для остановки этого процесса. Если этот параметр не указан, информация будет выведена один раз.
/?	Показать справку в командной строке

Задание 6 – Отображение Address Resolution Protocol (ARP) кэша с использование команды arp.

23. Команда arp -a выводит ARP кэш. Кэш это отображение IP адреса с соответствующим ему MAC адресом. Команда arp имеет много опций, если запустить ее без опций, то она выведет справку с перечислением доступных опций.
24. Наберите команду arp -a и нажмите Enter для отображения записей в ARP кэше.

```
C:\Users\User>arp -a
Интерфейс: 10.0.2.10 --- 0xb
адрес в Интернете          Физический адрес          Тип
10.0.2.1                   52-54-00-12-35-00        динамический
10.0.2.3                   08-00-27-59-1c-67        динамический
10.0.2.255                 ff-ff-ff-ff-ff-ff        статический
224.0.0.22                 01-00-5e-00-00-16        статический
224.0.0.252               01-00-5e-00-00-fc        статический
239.255.255.250           01-00-5e-7f-ff-fa        статический
255.255.255.255           ff-ff-ff-ff-ff-ff        статический
```

25. Найдите дополнительную информацию об описанных выше утилитах в Интернете.

Контрольные вопросы:

1. Использование базовых команд командной строки Windows, применяемых для поиска проблем в сети.
2. Проверка настроек IP. проверка соединения на уровне протокола IP с использованием команды Ping.
3. Определение маршрута (трассировка) пакетов с использованием команды tracert.
4. Разрешение доменных имен с использованием команды nslookup.
5. Проверка вашей сетевой конфигурации и сетевой статистики командой netstat.

Список литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.

2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## Лабораторная работа №4. Анализ и изучение заголовков различных сетевых пакетов.

### Цель работы:

научиться осуществлять анализ различных пакетов такие как TCP, HTTP, ICMP, DNS с использованием Wireshark. Установку Wireshark. Файл с захваченным трафиком. Исследование заголовка ARP. Исследование заголовка TCP. Исследование заголовка HTTP. Исследование заголовка ICMP. Исследование заголовка DNS. Исследование заголовка UDP.

**Знать:** основные сетевые протоколы, структуру их пакетов.

**Уметь:** осуществлять анализ различных пакетов такие как TCP, HTTP, ICMP, DNS с использованием Wireshark. Установку Wireshark. Файл с захваченным трафиком. Исследование заголовка ARP. Исследование заголовка TCP. Исследование заголовка HTTP. Исследование заголовка ICMP. Исследование заголовка DNS. Исследование заголовка UDP.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

**Актуальность темы** объясняется особенностями подготовки магистров по инженерным направлениям. Технический характер изучаемых по данному направлению дисциплин требует от обучаемых наличие навыков работы с программными и аппаратными средствами защиты информации в компьютерных сетях.

### **Теоретическая часть:**

Каждый пакет в сети содержит управляющую информацию и пользовательские данные известные как полезная нагрузка (payload). Управляющая информация содержит данные необходимые для доставки данных пользователя, включая IP-адреса отправителя и получателя, MAC-адреса, информацию о последовательности сборки и др. Заголовок – часть пакета содержащую управляющую информацию. Для работы сетевым администратором Вам необходимо знать, как исследовать заголовки пакетов в процессе анализа сетевого трафика.

Захват пакетов (packet capture) - это перехват пакетов данных, перемещающихся по сети с помощью инструментов перехвата, каких как

Wireshark. Захваченные пакеты анализируются, чтобы определить, соблюдаются ли установленные политики сетевой безопасности.

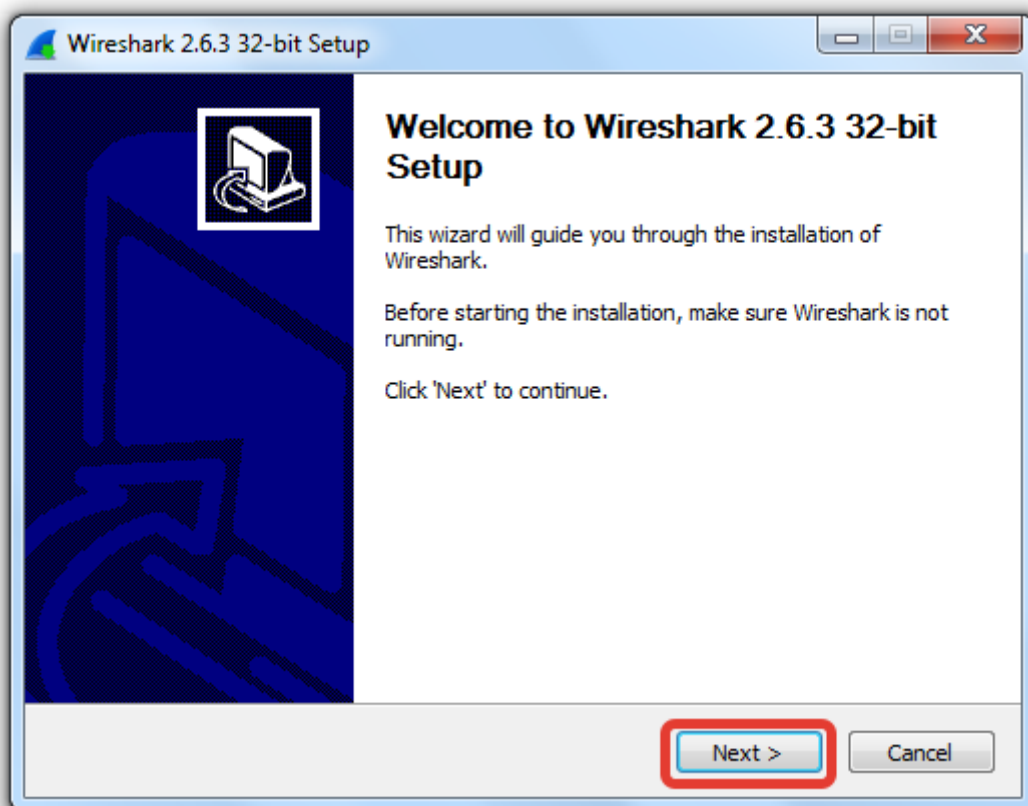
### Практическая часть.

Для выполнения работы потребуется

- Виртуальная машина с ОС Windows 7 или новее
- Сниффер пакетов Wireshark

#### **Задание 1 – установка Wireshark**

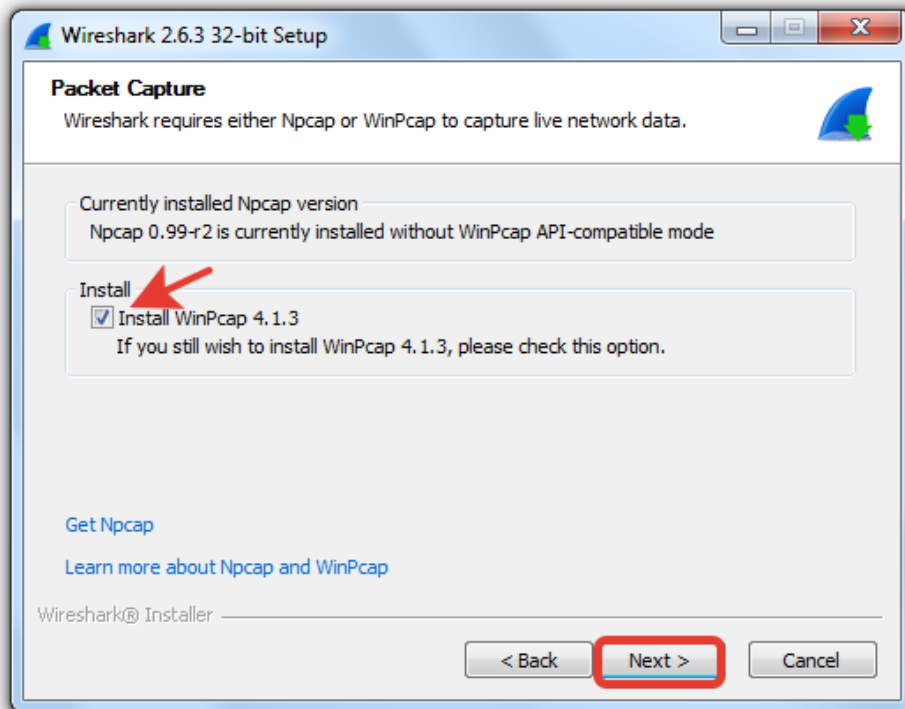
1. Запустите виртуальную машину и залогиньтесь в систему.
2. Скопируйте файл Packet Capture.pcapng из папки лабораторной работы на рабочий стол гостевой машины.
3. Проверьте установлен ли на вашей машине Wireshark. Для этого проверьте наличие ярлыка Wireshark на рабочем столе или в меню “Пуск -> Все программы -> Wireshark”. Если программа установлена, запускайте ее и переходите к Заданию 2.
4. Если программа не установлена, скопируйте установочный файл Wireshark-win32-2.6.3.exe из папки с лабораторной работой в виртуальную машину и запустите его.
5. Если появится окно с предупреждением безопасности(Контроль учетных записей), нажмите ДА.
6. Следуйте указаниям мастера установки для установки Wireshark



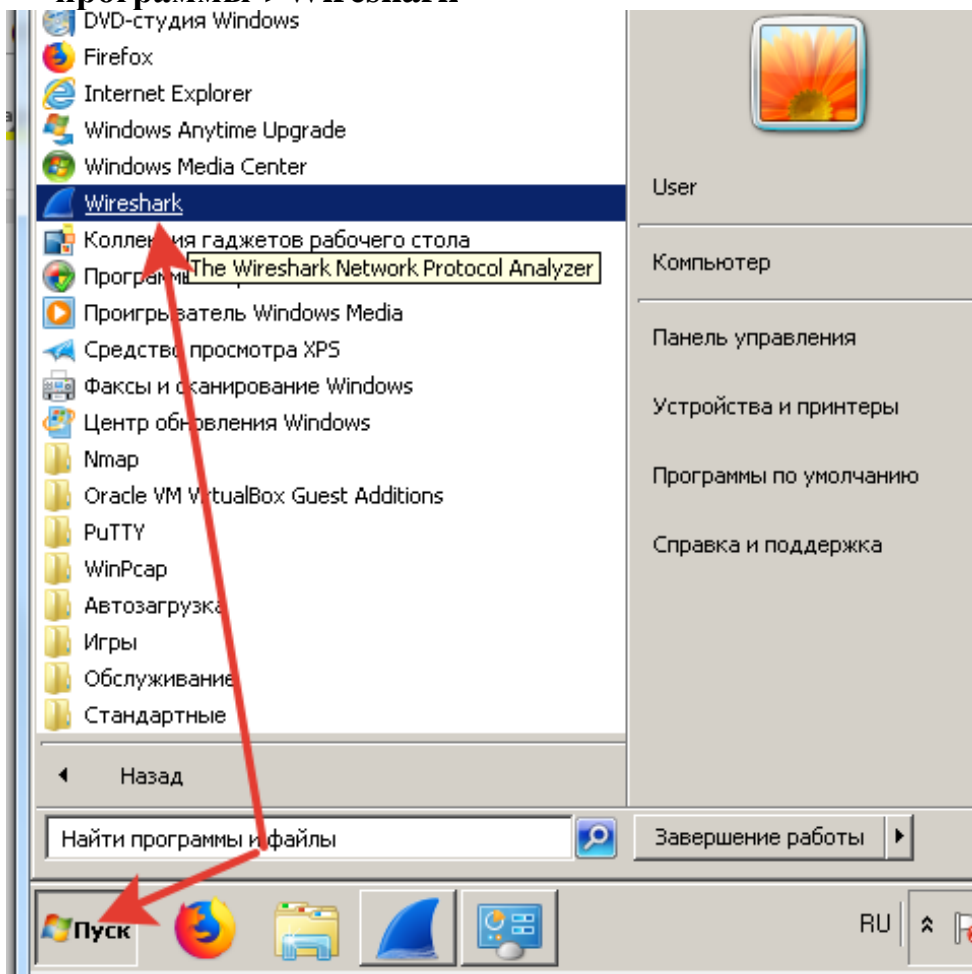
7. В ходе установки повится окно спрашивающеее вас установить ли WinPcap. Если вы уже устанавливали приложение, снимите галочку



Install WinPcap, в противном случае галочку поставьте. Нажмите **Next**.

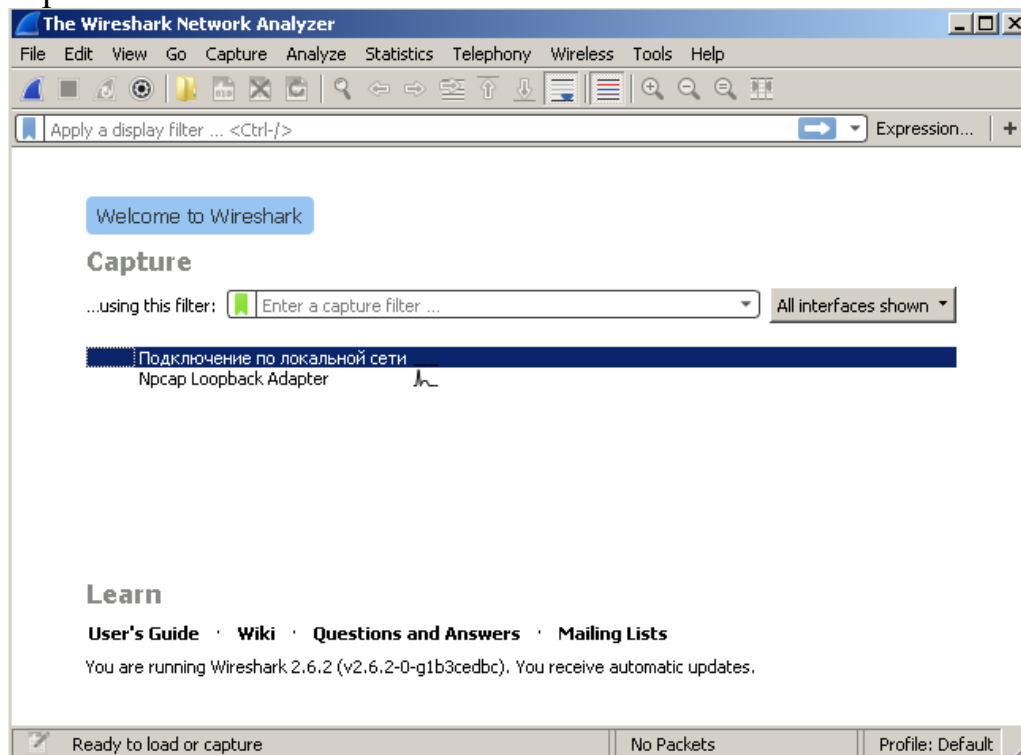


8. После окончания установки запустите Wireshark из меню **Пуск->Все программы->Wireshark**

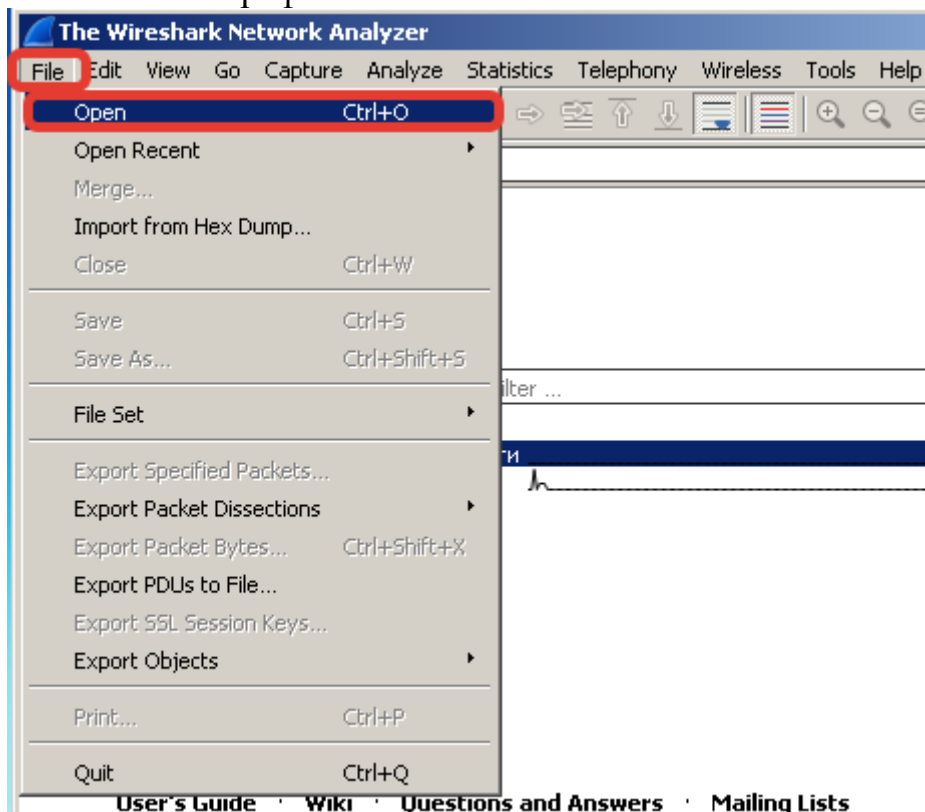


## Задание 2 – Открыть файл с захваченным трафиком.

9. Главное окно Wireshark показано на следующем скриншоте



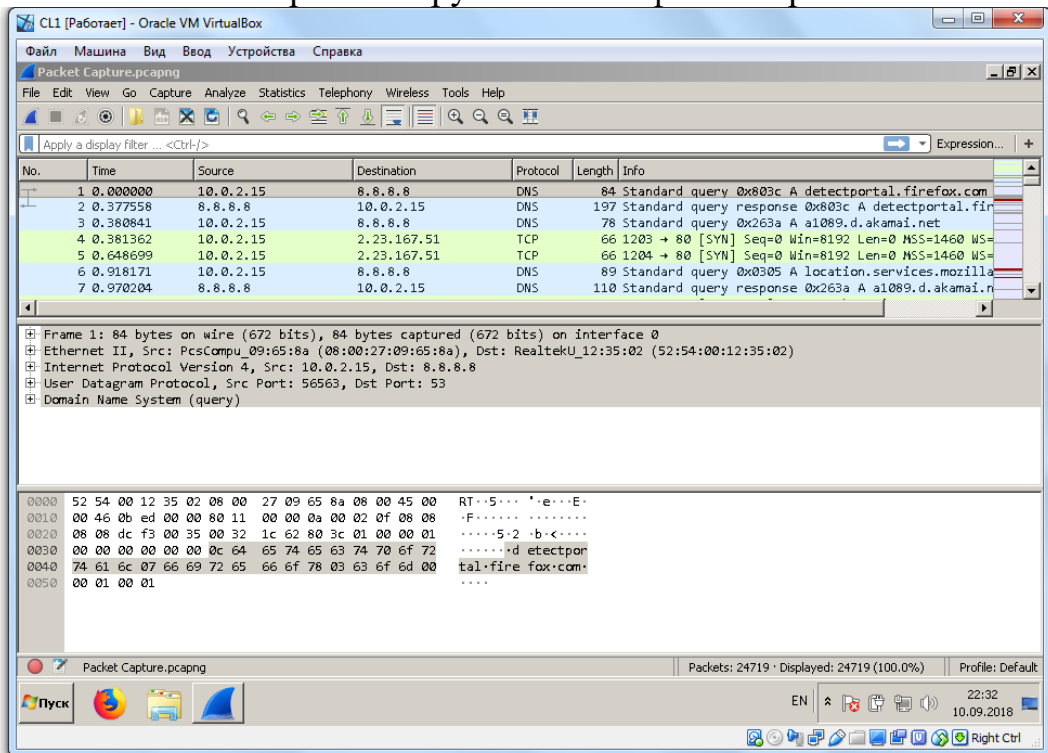
10. Перейдите в меню **File** и нажмите на **Open** для открытия файла с захваченным трафиком.



11. В открывшемся диалоге перейдите на рабочий стол виртуальной машины и выберите файл Packet Capture.pcapng

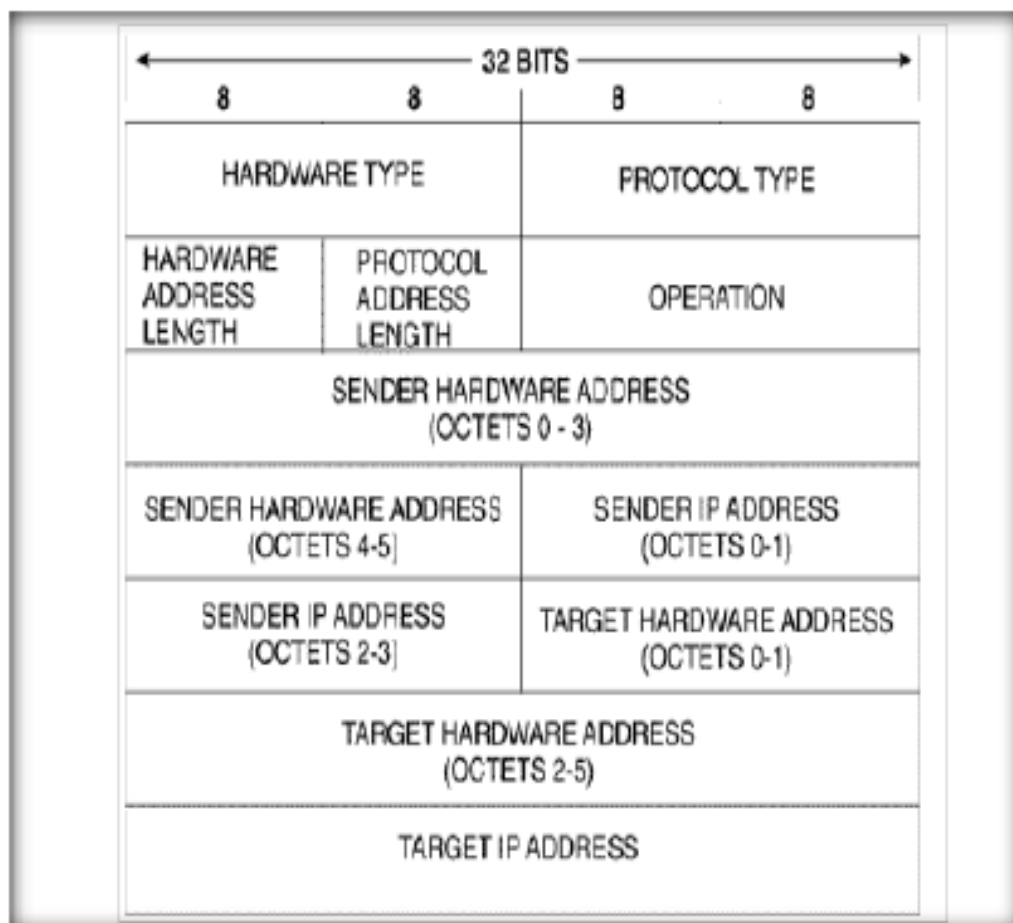


## 12. Wireshark отобразит загруженные из файла перехваченные пакеты



### Задание 3 – Исследование заголовка ARP

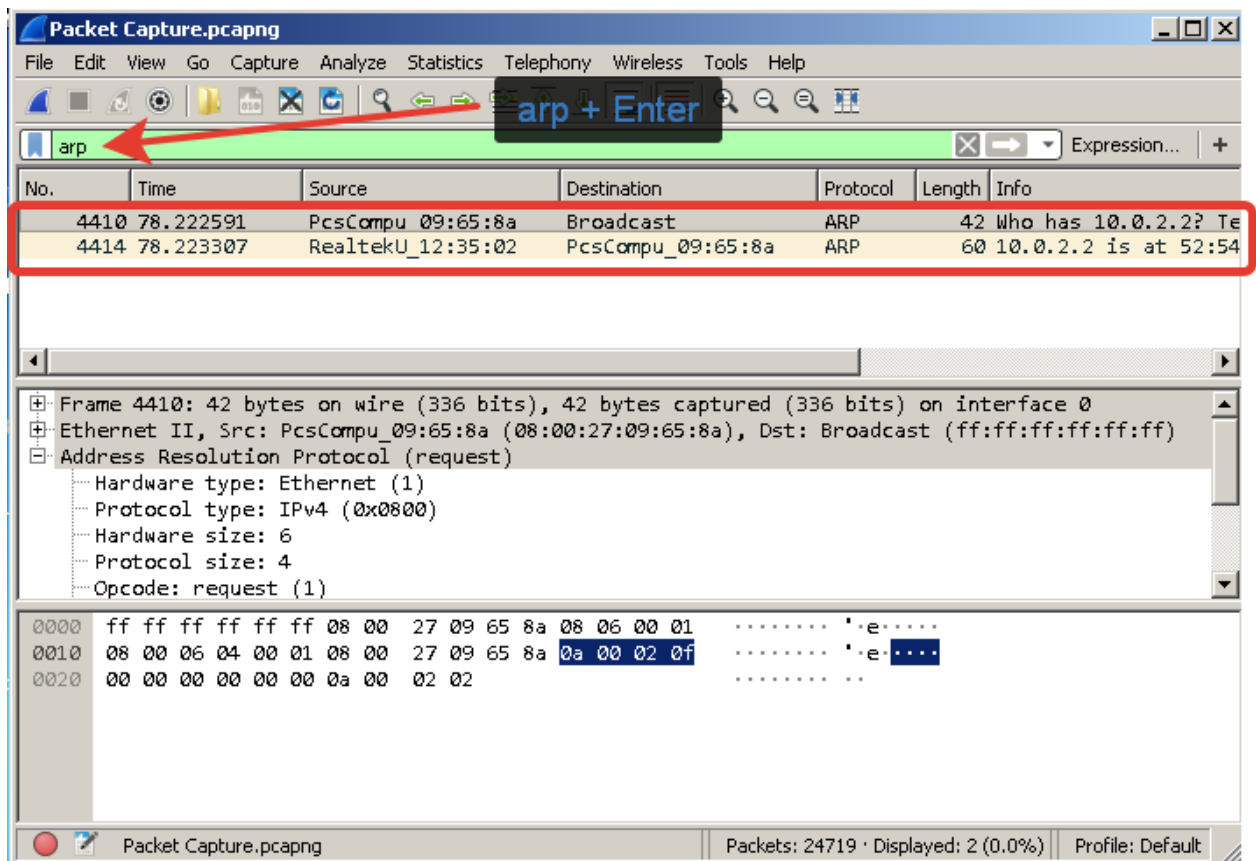
## 13. Формат заголовка ARP-пакета показан на следующем рисунке



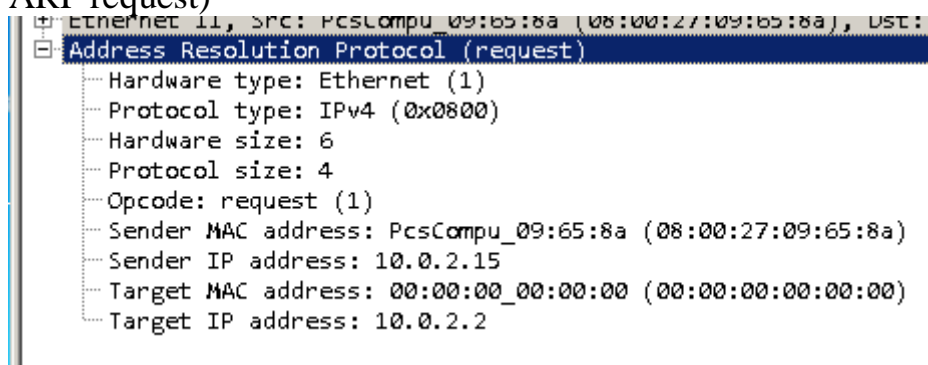
Значения полей приводятся ниже:

- I. Hardware Type (HTYPE) – Каждый канальный протокол передачи данных имеет свой номер, который хранится в этом поле. Например, Ethernet имеет номер 0x0001
- II. Protocol Type (PTYPE) - Код сетевого протокола. Например, для IPv4 будет записано 0x0800
- III. Hardware size (HLEN) - Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт.
- IV. Protocol size (PSIZE) - Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта.
- V. Opcode - Код операции отправителя: 1 в случае запроса и 2 в случае ответа.
- VI. Sender MAC address - Физический адрес отправителя.
- VII. Sender IP Address - Логический адрес отправителя.
- VIII. Target MAC address - Физический адрес получателя. Поле пусто при запросе.
- IX. Target IP address - Логический адрес получателя.

14. Кликните на ARP-пакет для анализа различных полей заголовка (можно использовать поле фильтра для поиска пакетов заданного типа)



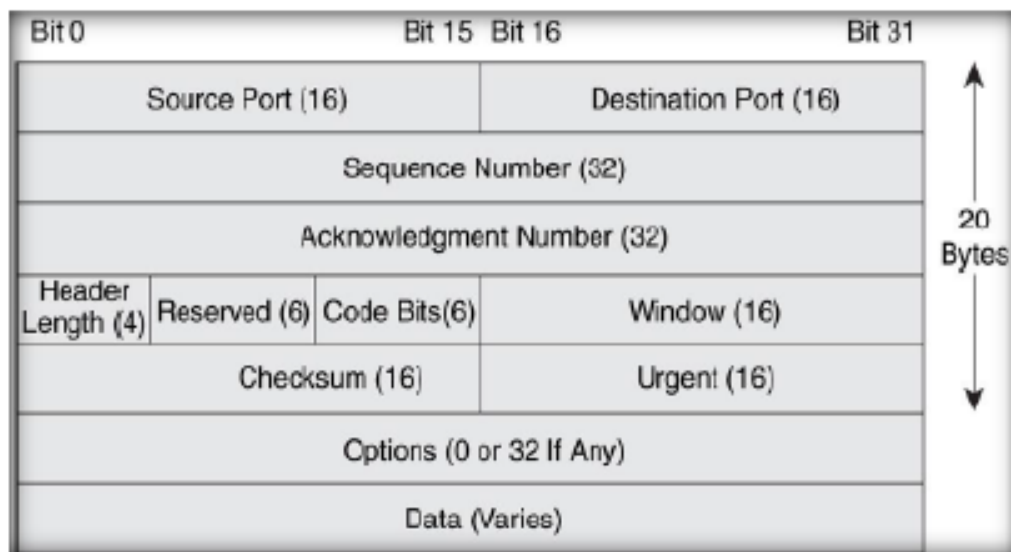
15. Разверните раздел **Address Resolution Protocol** (здесь приведен ARP request)



16. Сравните и проанализируйте различные поля захваченного ARP-пакета с форматом заголовка ARP-пакета из пункта 13.

#### Задание 4 – Исследование заголовка TCP

17. Формат заголовка TCP-пакета показан на следующем рисунке



Значения полей приводятся ниже:

I. Source port – Порт отправителя

II. Destination port – Порт получателя

III. Sequence number – Порядковый номер сегмента

IV. Acknowledgement number - Номер подтверждения сегмента

V. Header length – Указывает длину заголовка. Смещение начала полезных данных относительно начала сегмента

VI. Reserved - Зарезервированно

VII. Code bits (flags) – Флаги пакета

VIII. Window size – Размер окна

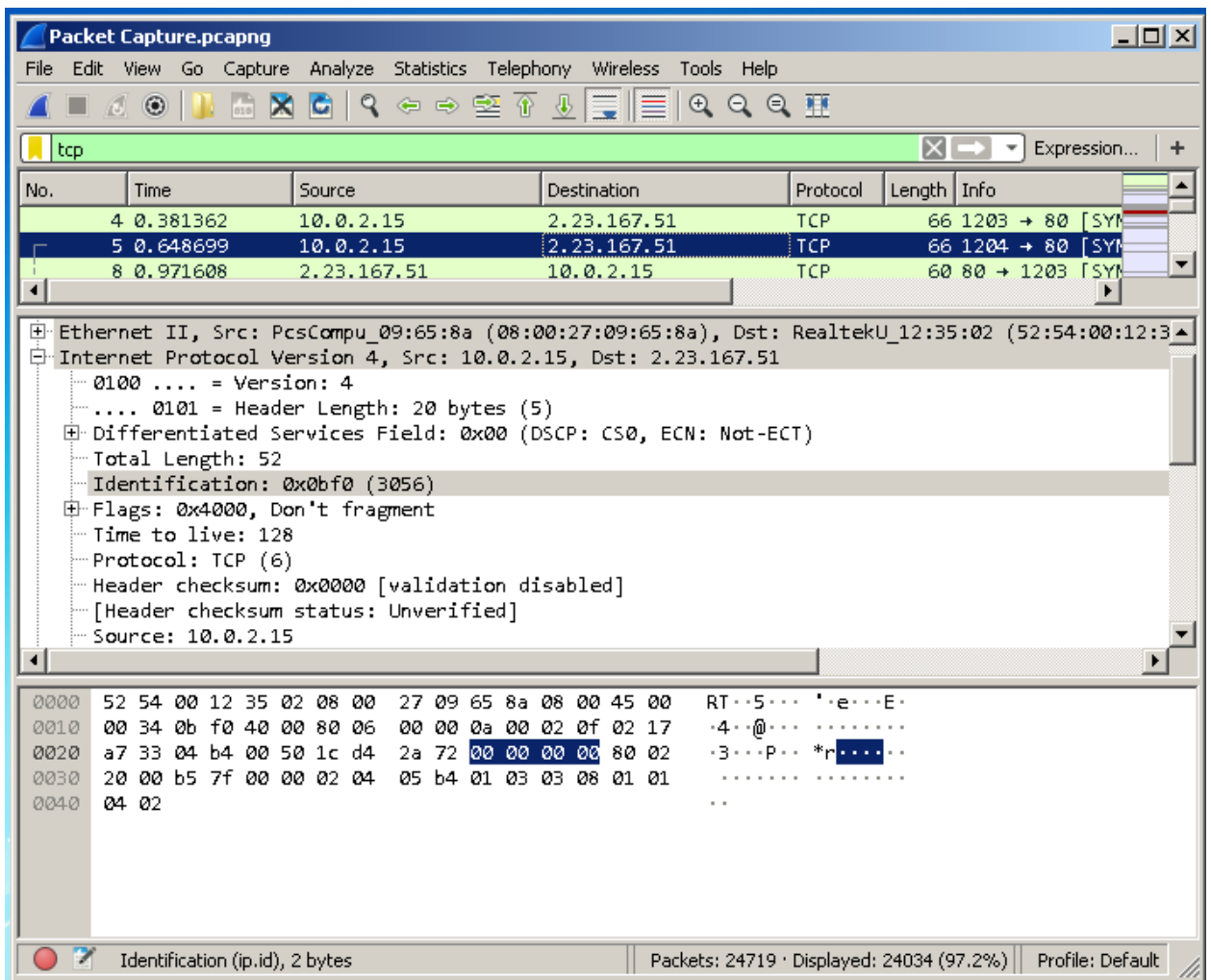
IX. Checksum – Контрольная сумма

X. Urgent – Указатель важности

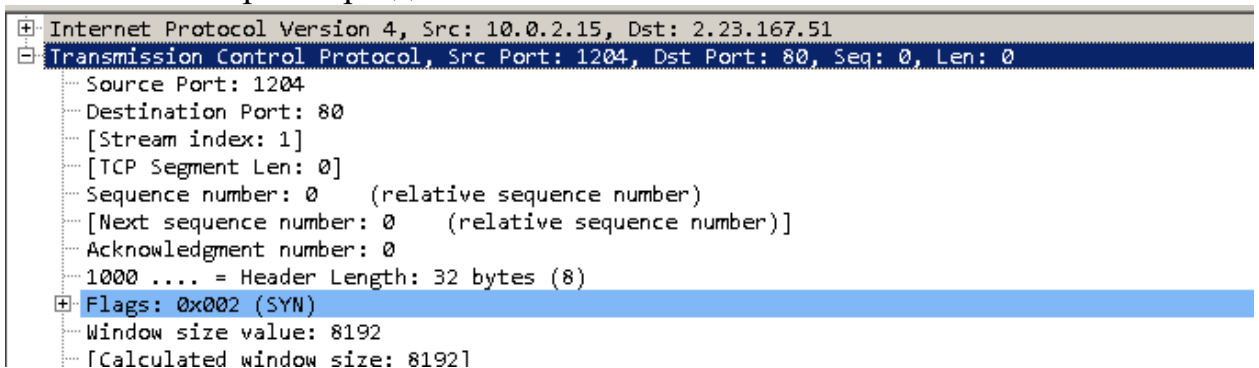
XI. Options - Опции

XII. Segment data – Сегмент данных.

18. Кликните на TCP-пакет для анализа различных полей заголовка (можно использовать поле фильтра для поиска пакетов заданного типа)



## 19. Разверните раздел Transmission Control Protocol



20. Сравните и проанализируйте различные поля захваченного TCP-пакета с форматом заголовка TCP-пакета из пункта 17

## Задание 5 – Исследование заголовка HTTP

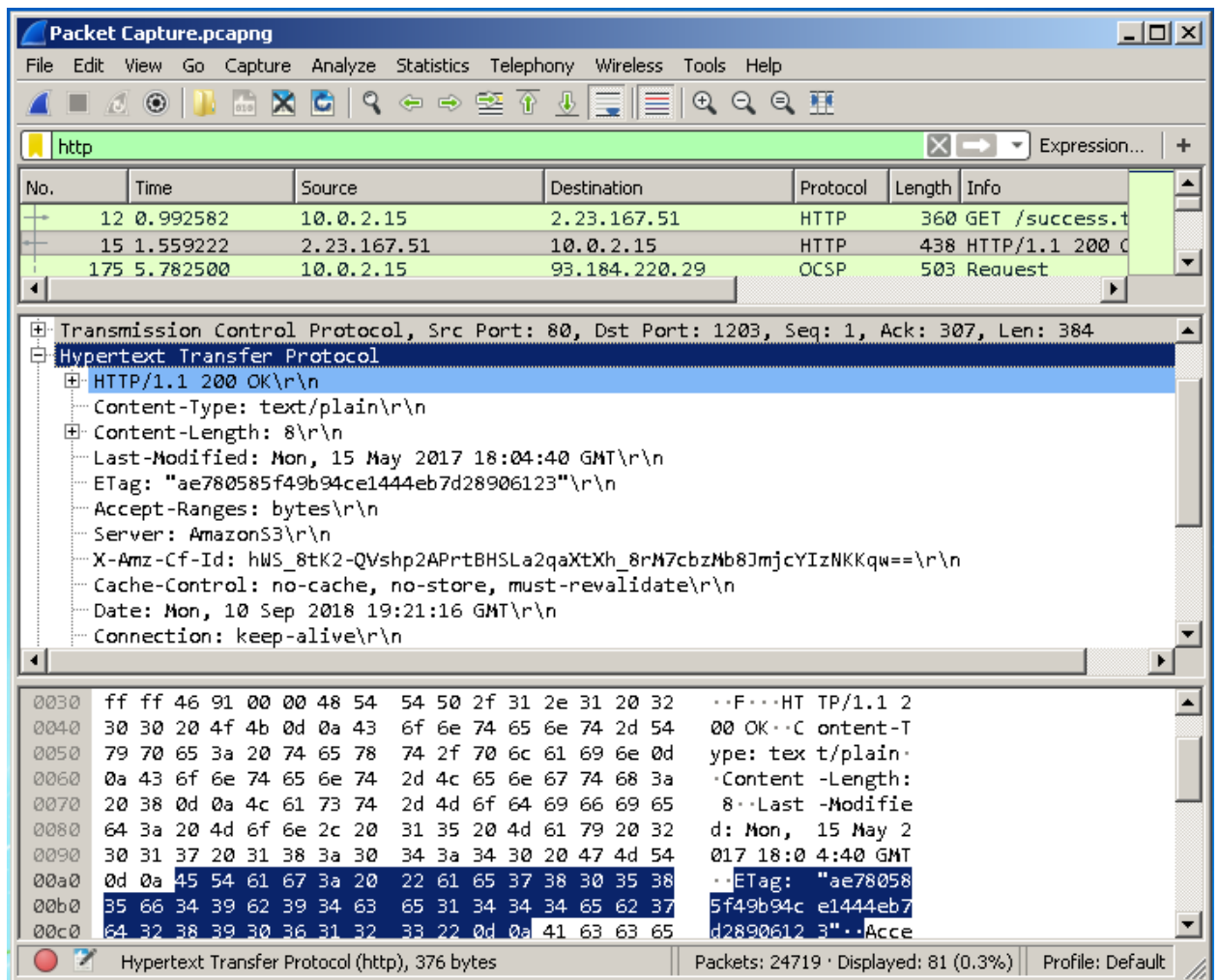
21. Формат заголовка HTTP запроса показан на следующем рисунке

Key	Value
Request	GET /Protocols/rfc2616/rfc2616-sec14.html HTTP/1.1
Accept	text/html, application/xhtml+xml, */*
Referer	http://www.google.com/url?sa=t&source=web&cd=3&ved=0CC4QFJAC8
Accept-Language	en-US
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5
Accept-Encoding	gzip, deflate
Host	www.w3.org
If-Modified-Since	Wed, 01 Sep 2004 13:24:52 GMT
If-None-Match	"1edec-3e3073913b100"
Connection	Keep-Alive

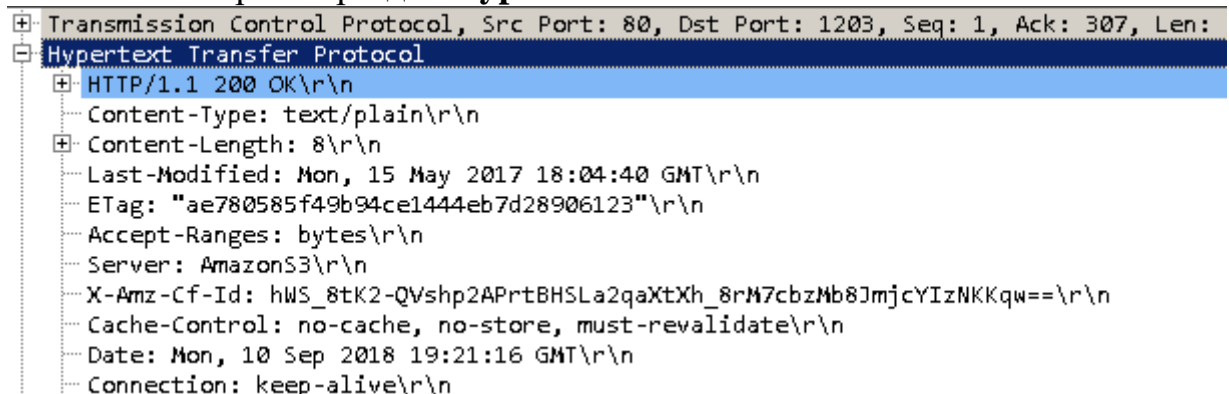
Значения полей приводятся ниже:

- I.HTTP type – Существует два типа HTTP сообщений. Запрос и ответ (Request и Response). Все HTTP пакеты относятся к одному из этих форматов
  - II.Request Type – Тип запроса. GET, POST, HEAD или др.
  - III.Accept – Список MIME типов, которые ожидает клиент.
  - IV.Referer - Заголовок запроса Referer содержит URL исходной страницы, с которой был осуществлен переход на текущую страницу
  - V.Accept language – Предпочитаемый язык (обычно список в порядке убывания)
  - VI.User agent – Версия клиентского браузера.
  - VII.Accept encoding - Список форматов сжатия данных, которые поддерживает клиент.
  - VIII.Host – Определяет доменное имя сервера (и опционально TCP порт) к которому адресован запрос.
  - IX.If-modified-since – Используется для наложения условия. Если запрошенный ресурс не изменился с момента указанного в запросе, то ресурс не отправляется. Отправляется статус 304- not modified.
  - X.If-none-match – Используется для наложения условия. Для методов GET и HEAD сервер вернет запрошенный документ только если у него нет заголовка ETag совпадающего с указанным.
  - XI.Connection – Определяет тип установленного соединения.
22. Кликните на HTTP пакет для анализа различных полей заголовка (можно использовать поле фильтра для поиска пакетов заданного типа)





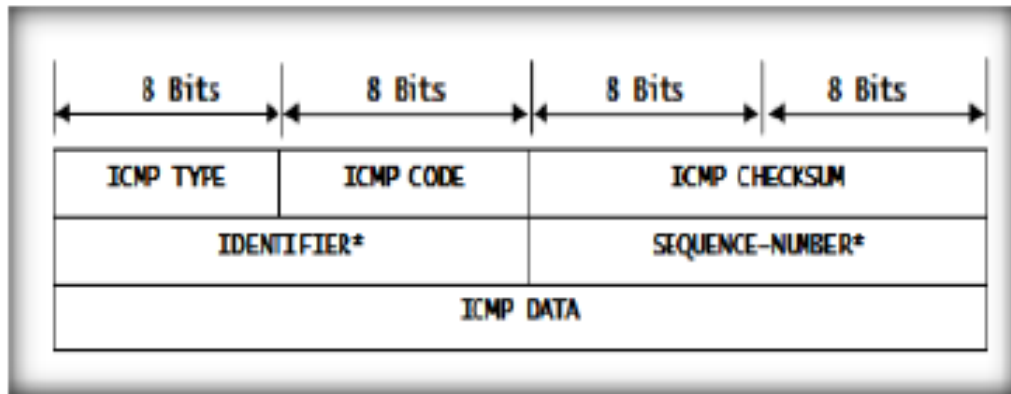
### 23. Разверните раздел Hypertext Transfer Protocol



24. Сравните и проанализируйте различные поля захваченного HTTP пакета с форматом заголовка HTTP пакета из пункта 21

### Задание 6 – Исследование заголовка ICMP

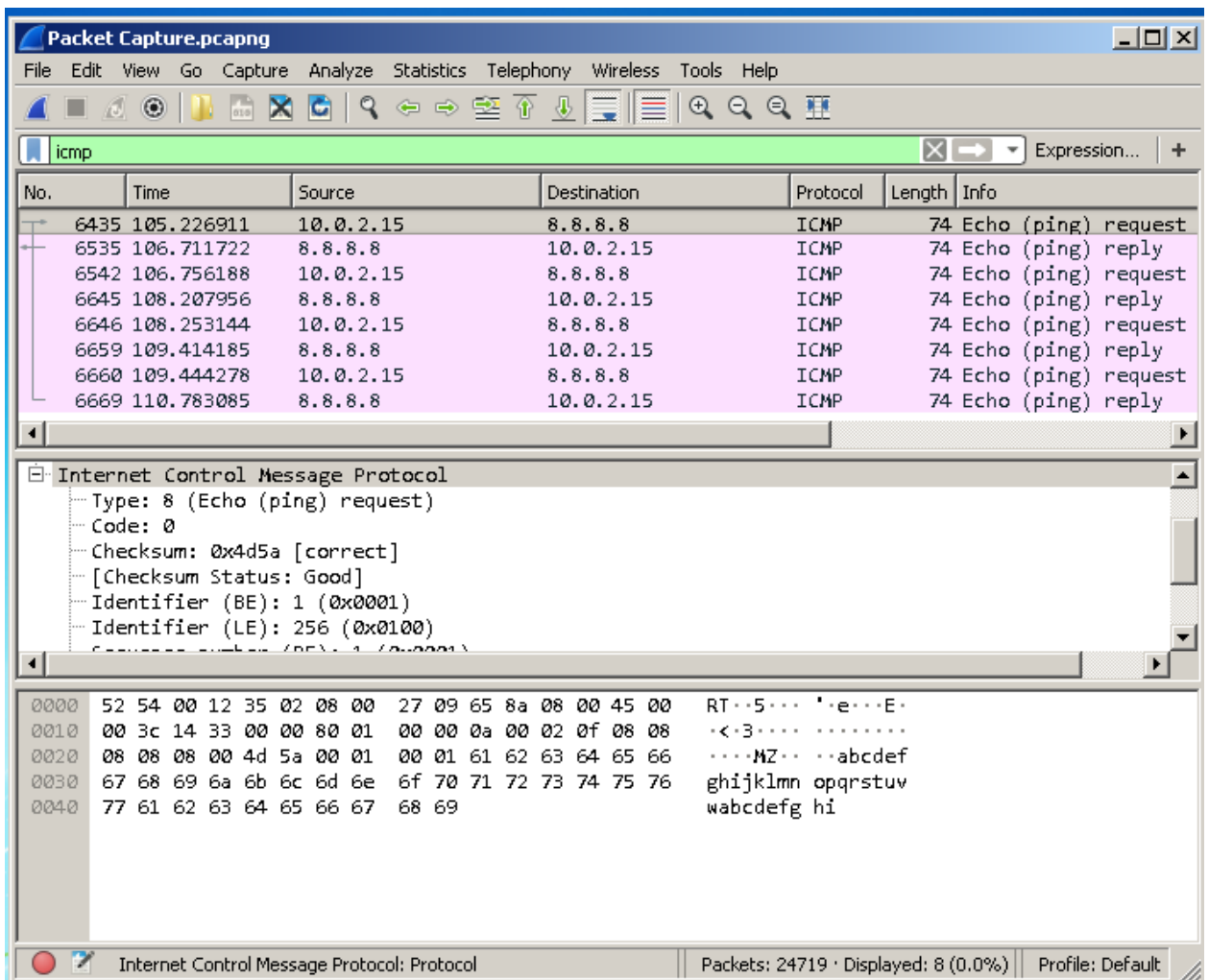
25. Формат заголовка ICMP-пакета показан на следующем рисунке



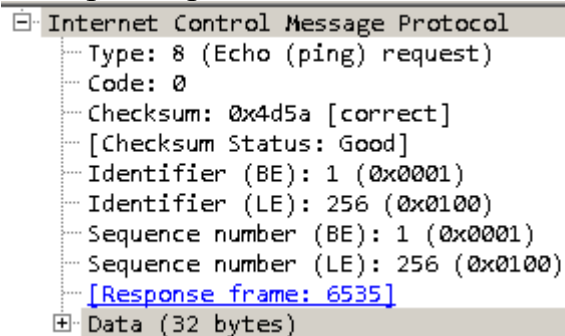
Значения полей приводятся ниже:

- I. Type - идентификатор типа сообщения. 0 или 8 – ICMP Reply (ответ), 8 – ICMP request (запрос)
- II. Code – числовой идентификатор, указывающий более точный код ошибки
- III. Checksum - контрольная сумма, используется для обнаружения ошибок
- IV. Identifier – Это устанавливает идентификатор процесса отправителя
- V. Sequence Number – порядковый номер
- VI. Data (Payload) – Содержит ICMP данные. Например, TimeStamp.

26. Кликните на ICMP пакет для анализа различных полей заголовка (можно использовать поле фильтра для поиска пакетов заданного типа)



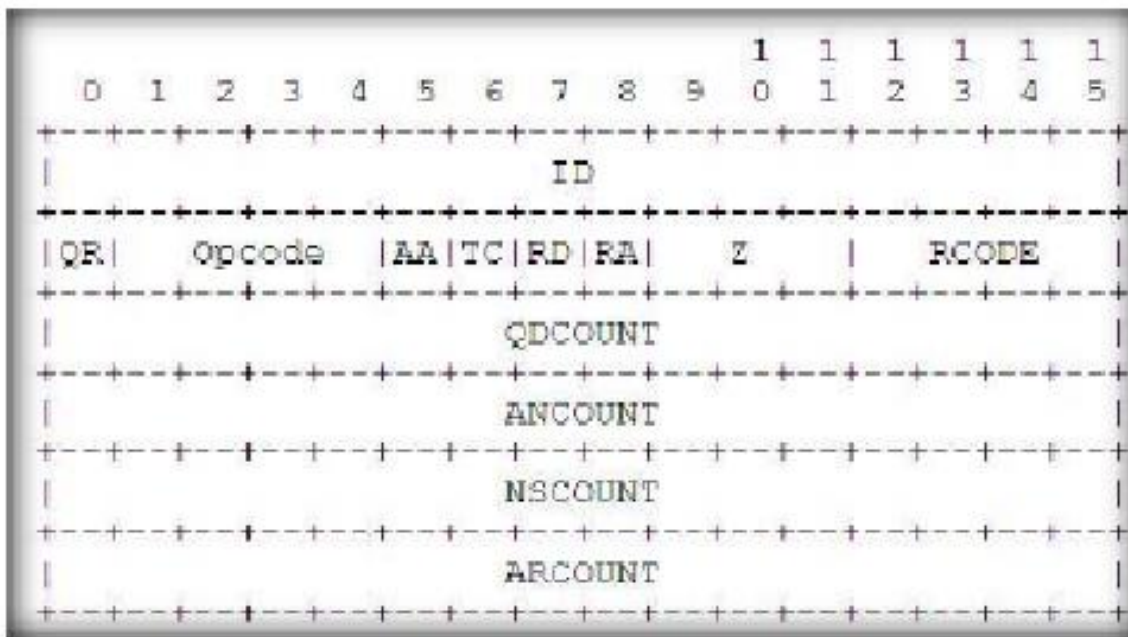
## 27. Разверните раздел **Internet Control Message Protocol**



28. Сравните и проанализируйте различные поля захваченного ICMP пакета с форматом заголовка ICMP пакета из пункта 25

## Задание 7 – Исследование заголовка DNS

29. Формат заголовка DNS пакета показан на следующем рисунке



Значения полей приводятся ниже:

- I. Identifier – Двухбайтовый идентификатор транзакции. Создается при создании DNS-запроса.
- II. Query/response flag – Флаг определяющий тип DNS-пакета (Запрос или ответ). 0 – запрос, 1 – ответ.
- III. Operational code - с помощью данного кода клиент может указать тип запроса, где обычное значение 0 — стандартный запрос, другие значения — это 1, то есть инверсный запрос, и 2 — запрос статуса сервера.
- IV. Authoritative answer flag (AA) - данное поле имеет смысл только в DNS-ответах от сервера и сообщает о том, является ли ответ авторитетным либо нет (Authority Answer).
- V. Truncation flag (TC) - данный флаг устанавливается в ответе от DNS-сервера, если он не смог поместить всю информацию в UDP-дейтаграмму (Transaction).
- VI. Recursion Desired (RD) - этот однобитовый флаг устанавливается в запросе и копируется в ответ. Если он флаг устанавливается в запросе — это значит, что клиент просит сервер не сообщать ему промежуточных ответов, а вернуть только IP-адрес.
- VII. Recursion available (RA) - отправляется только в ответах, и сообщает о том, что сервер поддерживает рекурсию (RA = 1).
- VIII. Zero (Z) - являются зарезервированными и всегда равны нулю.
- IX. Response code (Rcode) - это поле служит для уведомления клиентов о том, успешно ли выполнен запрос или с ошибкой.
- X. Question count (QD count) – определяет количество запросов в сегменте запросов
- XI. Answer record count (AN count) – определяет количество записей ресурсов в секции ответа
- XII. Authority record count (NS count) – определяет количество записей в секции authority ответа

XIII. Additional record count (AR count) – Определяет количество записей ресурсов в дополнительной секции

30. Кликните на DNS пакет для анализа различных полей заголовка (можно использовать поле фильтра для поиска пакетов заданного типа)

The screenshot shows the Wireshark interface with a packet capture named 'Packet Capture.pcapng'. The filter is set to 'dns'. The packet list pane shows several DNS packets. Packet 6415 is selected, showing a 'Standard query' from 10.0.2.15 to 8.8.8.8. The packet details pane shows the following structure:

- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 64683, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0xa88c
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - [Response In: 6519]

The packet bytes pane shows the raw data of the DNS query, including the transaction ID and the query name 'rt.5.e.E.?.+.5+.[.c.r14.digi.cert.com'.

31. Разверните раздел **Domain Name System**

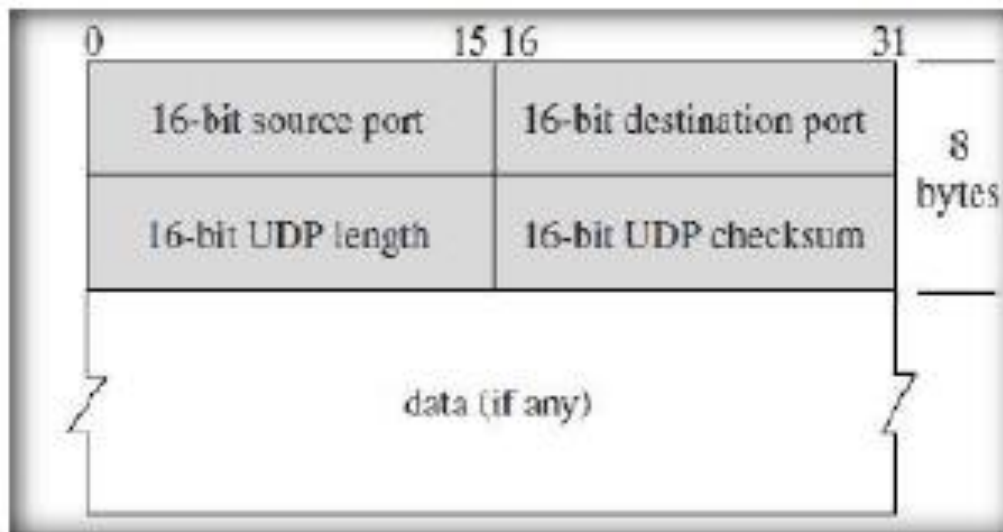
This screenshot shows the expanded 'Domain Name System (query)' section from the previous image. The details are as follows:

- Transaction ID: 0xa88c
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
  - [Response In: 6519]

32. Сравните и проанализируйте различные поля захваченного DNS пакета с форматом заголовка DNS пакета из пункта 29

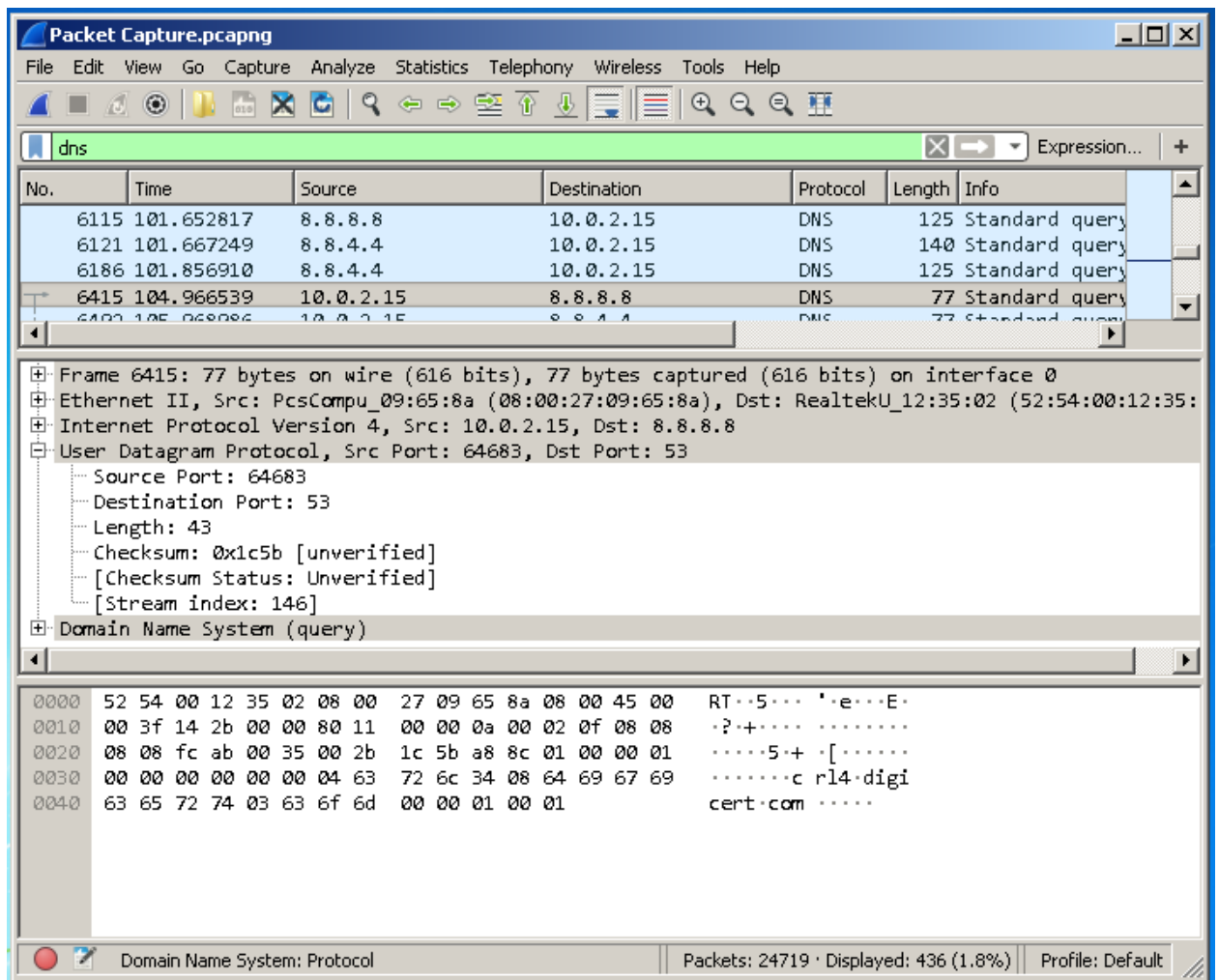
### Задание 8 – Исследование заголовка UDP

33. Формат заголовка UDP пакета показан на следующем рисунке

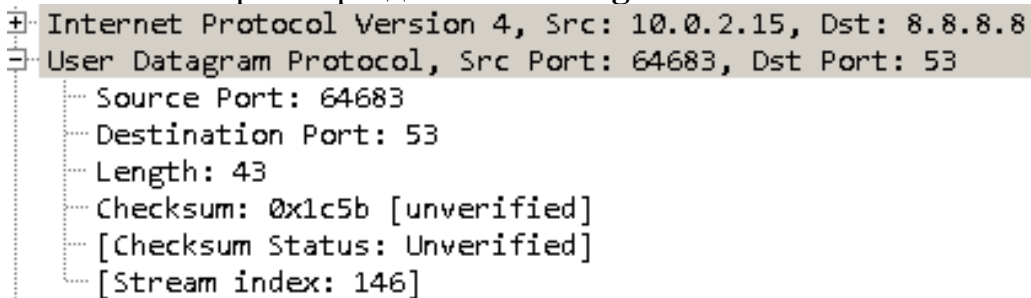


Значения полей приводятся ниже:

- I. Source port – UDP порт отправителя
  - II. Destination port – UDP порт получателя
  - III. UDP length – Длина дейтаграммы, включая заголовок и сегмент данных
  - IV. UDP Checksum – Контрольная сумма пакета
  - V. Data – Данные (payload)
34. Снова кликните на DNS пакет для анализа различных полей заголовка (можно использовать поле фильтра для поиска пакетов заданного типа)



### 35. Разверните раздел User Datagram Protocol



36. Сравните и проанализируйте различные поля захваченного UDP пакета с форматом заголовка UDP пакета из пункта 33

#### Контрольные вопросы:

1. Анализ различных пакетов такие как TCP, HTTP, ICMP, DNS с использованием Wireshark.
2. Установка Wireshark.
3. Файл с захваченным трафиком.
4. Исследование заголовка ARP.
5. Исследование заголовка TCP.
6. Исследование заголовка HTTP.
7. Исследование заголовка ICMP.
8. Исследование заголовка DNS.

## 9. Исследование заголовка UDP.

### *Список литературы:*

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.



## Лабораторная работа №5. Сканирование и исследования безопасности сети с помощью сканера Nmap.

### Цель работы:

Изучение и практическое применение утилиты для сканирования и исследования безопасности сети Nmap и графической оболочки Zenmap. Получение списка открытых портов. Определение операционной системы. Определение адресов активных хостов без сканирования портов. Сканирование хостов разными методами. Определение наличия сетевого экрана. Выбор оптимальных методов сканирования портов с целью избежать обнаружения.

**Знать:** основные способы практического применения утилиты для сканирования и исследования безопасности сети Nmap и графической оболочки Zenmap

**Уметь:** выполнять получение списка открытых портов. Определение операционной системы. Определение адресов активных хостов без сканирования портов. Сканирование хостов разными методами. Определение наличия сетевого экрана. Выбор оптимальных методов сканирования портов с целью избежать обнаружения.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть.

**Актуальность темы** объясняется особенностями подготовки магистров по инженерным направлениям. Технический характер изучаемых по данному направлению дисциплин требует от обучаемых наличие навыков работы с программными и аппаратными средствами защиты информации в компьютерных сетях.

### **Теоретическая часть:**

**Nmap** («Network Mapper») это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с

единичными целями. Nmap использует сырые IP пакеты оригинальными способами, чтобы определить какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще дюжины других характеристик. В тот время как Nmap обычно используется для проверки безопасности, многие сетевые и системные администраторы находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.

Выходные данные Nmap это список просканированных целей с дополнительной информацией по каждой в зависимости от заданных опций. Ключевой информацией является «таблица важных портов». Эта таблица содержит номер порта, протокол, имя службы и состояние. Состояние может иметь значение open (открыт), filtered (фильтруется), closed (закрыт) или unfiltered (не фильтруется). Открыт означает, что приложение на целевой машине готово для установки соединения/принятия пакетов на этот порт. Фильтруется означает, что брандмауэр, сетевой фильтр или какая-то другая помеха в сети блокирует порт, и Nmap не может установить открыт этот порт или закрыт. Закрытые порты не связаны ни с каким приложением, так что они могут быть открыты в любой момент. Порты расцениваются как не фильтрованные, когда они отвечают на запросы Nmap, но Nmap не может определить открыты они или закрыты. Nmap выдает комбинации открыт|фильтруется и закрыт|фильтруется, когда не может определить, какое из этих двух состояний описывает порт. Эта таблица также может предоставлять детали о версии программного обеспечения, если это было запрошено. Когда осуществляется сканирование по IP протоколу (-sO), Nmap предоставляет информацию о поддерживаемых IP протоколах, а не об открытых портах.

В дополнение к таблице важных портов Nmap может предоставлять дальнейшую информацию о целях: преобразованные DNS имена, предположение о используемой операционной системе, типы устройств и MAC адреса.

Zenmap – графический интерфейс для Nmap.

Типичное сканирование с использованием Nmap показано на Рисунке 1. Единственные аргументы, использованные в этом примере это -A, для определения версии ОС, сканирования с использованием скриптов и трассировки; -T4 для более быстрого выполнения; затем два целевых хоста.

Поскольку сканнер Nmap активно развивается и его поведение, и функционал немного изменяется от версии к версии, внимательно изучите следующие главы последней версии официального руководства:

- 1) <https://nmap.org/man/ru/man-briefoptions.html>
- 2) <https://nmap.org/man/ru/man-target-specification.html>
- 3) <https://nmap.org/man/ru/man-host-discovery.html>
- 4) <https://nmap.org/man/ru/man-port-scanning-basics.html>
- 5) <https://nmap.org/man/ru/man-port-scanning-techniques.html>

- 6) <https://nmap.org/man/ru/man-port-specification.html>
- 7) <https://nmap.org/man/ru/man-version-detection.html>
- 8) <https://nmap.org/man/ru/man-os-detection.html>
- 9) <https://nmap.org/man/ru/man-bypass-firewalls-ids.html>
- 10) <https://nmap.org/man/ru/man-output.html>

```
# nmap -A -T4 scanme.nmap.org playground

Starting Nmap ( https://nmap.org )
Interesting ports on scanme.nmap.org (64.134.52):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11

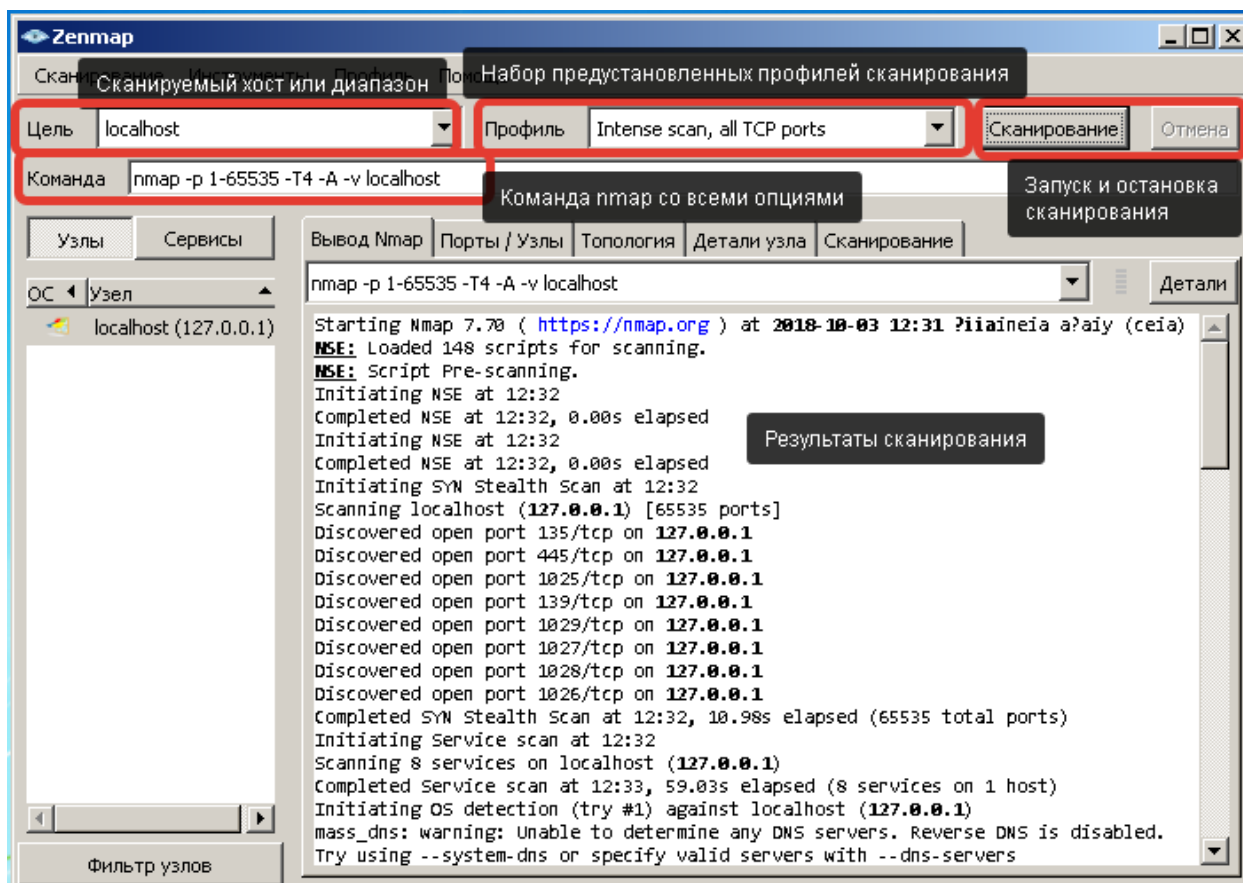
Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1002/tcp  open  windows-icfw?
1025/tcp  open  msrpc    Microsoft Windows RPC
1720/tcp  open  H.323/Q.931 CompTek AquaGateKeeper
5800/tcp  open  vnc-http RealVNC 4.0 (Resolution 400x250; VNC port: 5900)
5900/tcp  open  vnc      VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

**Рисунок 1 – Пример сканирования Nmap**

### Практическая часть.

- 1) Настройте режим сетевого моста для адаптера виртуальной машины.
- 2) Запустите виртуальную машину.
- 3) Установите nmap (Zenmap) на виртуальную машину. (Если он не установлен). Актуальную версию можно получить <https://nmap.org/download.html> (Ссылка Latest stable release self-installer: nmap-7.70-setup.exe)
- 4) Запустите Zenmap (Ярлык “Nmap - Zenmap GUI” на рабочем столе или в Пуск-Программы)



**Рисунок 2 – Главное окно Zenmap**

Адреса сети лаборатории и целевых хостов будут предоставлены преподавателем.

1) Получите список открытых портов (TCP и UDP) виртуальной машины, на которой выполняется лабораторная работа (localhost). Воспользуйтесь несколькими методами сканирования. Сравните результаты.

2) Определите операционную систему этой же машины.

3) Узнайте адреса активных хостов в сети лаборатории (без сканирования портов).

4) Просканируйте хост №1, разными методами. Сравните результаты.

5) Для хостов(1-2), заданных преподавателем, выполните следующие действия:

a. Определите, защищен ли хост межсетевым экраном.

b. Определите поддерживаемые протоколы.

c. Выберите оптимальный метод сканирования портов, чтобы избежать обнаружения. Определите открытые и фильтрованные порты и по возможности версии служб.

d. Определите операционную систему.

б) С помощью Wireshark посмотрите, как Nmap сканирует порты в различных режимах (для этого удобнее ограничивать сканирование несколькими портами).

Контрольные вопросы:

1. Какими способами можно задать диапазон сканируемых хостов? Как задать несколько адресов?
2. Какие существуют способы поиска активных (включённых) хостов в сети?
3. Какие способы сканирования портов существуют в Nmap? Какими ключами они задаются?
4. Как задать диапазон портов? Как просканировать все порты? Как просканировать UDP порты? Как просканировать порты 21,80,8080?
5. Как с помощью nmap определить операционную систему, установленную на удаленном хосте?
6. Для чего используются ключи `-v -O -sV -sT -sU -sS -A`?

Список литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## Лабораторная работа №6. Методы анализа сетевого трафика с использованием Wireshark.

### Цель работы:

Научиться собирать сетевой трафик с помощью программы Wireshark. Научиться фильтровать собранный трафик, находить и просматривать соединения. Извлекать пароли и передаваемые без шифрования файлы.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть.

Захват пакетов (packet capture) - это перехват пакетов данных, перемещающихся по сети с помощью инструментов перехвата, таких как Wireshark.

Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс. Функциональность, которую предоставляет Wireshark, очень схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (англ. promiscuous mode).

Promiscuous mode или promisc mode — так называемый «неразборчивый» режим, в котором сетевая плата позволяет принимать все пакеты независимо от того, кому они адресованы.

В нормальном состоянии на Ethernet-интерфейсе используется фильтрация пакетов канального уровня и если MAC-адрес в заголовке назначения принятого пакета не совпадает с MAC-адресом текущего сетевого интерфейса и не является широковещательным, то пакет отбрасывается. В «неразборчивом» режиме фильтрация на сетевом интерфейсе отключается и все пакеты, включая непредназначенные текущему узлу, пропускаются в систему.

Большинство операционных систем требуют прав администратора для включения «неразборчивого» режима. Данный режим позволяет мониторить трафик только в данном коллизийном домене (для Ethernet или беспроводных сетей) или кольце (для сетей Token ring или FDDI), потому что использование сетевых концентраторов является менее безопасным решением, чем использование коммутаторов, так как последние в нормальном режиме работы не передают трафик всем вне зависимости от адреса назначения.

Однако, есть случай, при котором коммутаторы всё равно срабатывают в отношении не широковещательных фреймов так же, как концентраторы. Например, при отсутствии MAC-адреса получателя в таблице коммутации. В таком случае, производится отправка на все порты коммутатора сразу, порт с которого придёт ответ на этот фрейм (с соответствующим адресом отправителя) вносится в таблицу коммутации, после чего, коммутатор отправляет фреймы уже в соответствии с записью в таблице — конкретно на порт с приписанным MAC-адресом для этого получателя.

### **Оборудование и материалы.**

- Виртуальная машина с ОС Windows 7 или новее
- Wireshark
- Образцы перехваченного трафика (Папка Lab7)

### **Указания по технике безопасности:**

Соответствуют технике безопасности по работе с компьютерной техникой.

### **Задания**

#### **1. Захват трафика**

- 1) Переведите сетевой адаптер виртуальной машины в режим сетевого моста и запустите виртуальную машину
- 2) Запустите Wireshark. Откроется окно выбора интерфейса захвата или загрузки данных из файла. (Рисунок 1)

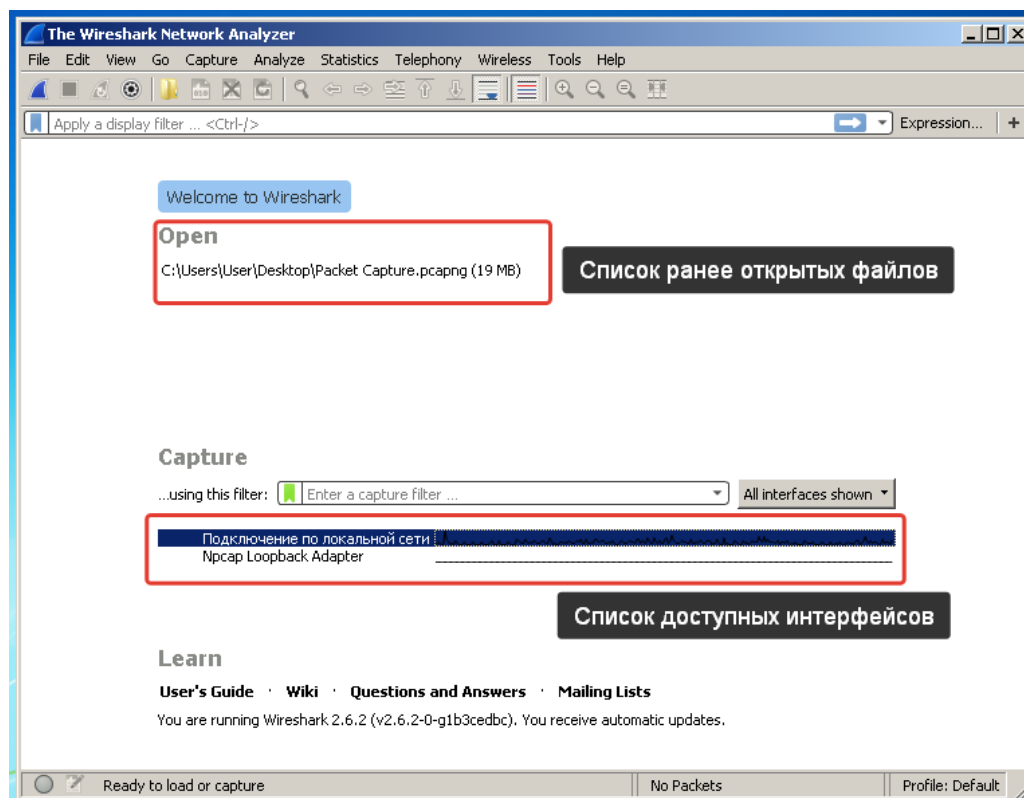


Рисунок 1 – Стартовое окно WireShark

3) Для запуска захвата трафика дважды нажмите на тот интерфейс (сетевой адаптер) который хотите прослушать (в данном примере “Подключение по локальной сети”). Определить ведется ли передача данных через интерфейс можно по небольшому графику рядом с его названием. По Рисунку 1 видно, что по интерфейсу “Подключение по локальной сети” передача ведется, а по интерфейсу Nrcap LoopBack Adapter – нет, т.к. график передачи данных – прямая линия.

Дважды кликните на “Подключение по локальной сети” для начала перехвата трафика.

4) Откроется окно (Рисунок 2). Это главное окно программы. Оно состоит из шести блоков. Рассмотрим их подробнее.

1 – Главное меню.

2 – Панель инструментов

3 – Поле условия фильтрации. С его помощью, можно вывести только те пакеты/соединения, которые удовлетворяют указанному условию. Выбранные пакеты отобразятся в поле 4

4 – список захваченных пакетов. По умолчанию тут отображаются перехваченные пакеты, но если в поле 3 указано условие, то отображаться будут только те пакеты, что удовлетворяют условию. В столбцах таблицы приводится информация о номере пакета, моменте получения (от начала захвата), отправителе и получателе, протоколе, размере, а так же дополнительная информация, которую добавляет Wireshark на основе анализа пакета.

5 – Развернутая информация о выделенном пакете. Если в поле 4 кликнуть на пакет, то в данном поле отобразится информация о его



заголовках и содержанием. Для удобства информация разбита по уровням модели OSI

6 – “Сырое” представление пакета, по умолчанию в шестнадцатеричном виде. Правая колонка показывает представление данных значений в ASCII символах.

7 – строка состояния. Показывает текущий режим работы (в данном случае захват пакетов). Если захват завершен, то имя файла, в котором сохранен трафик. В правой части строки, содержится статистика о количестве захваченных пакетов и то какой процент из них отображен в списке 4 (при использовании фильтра).

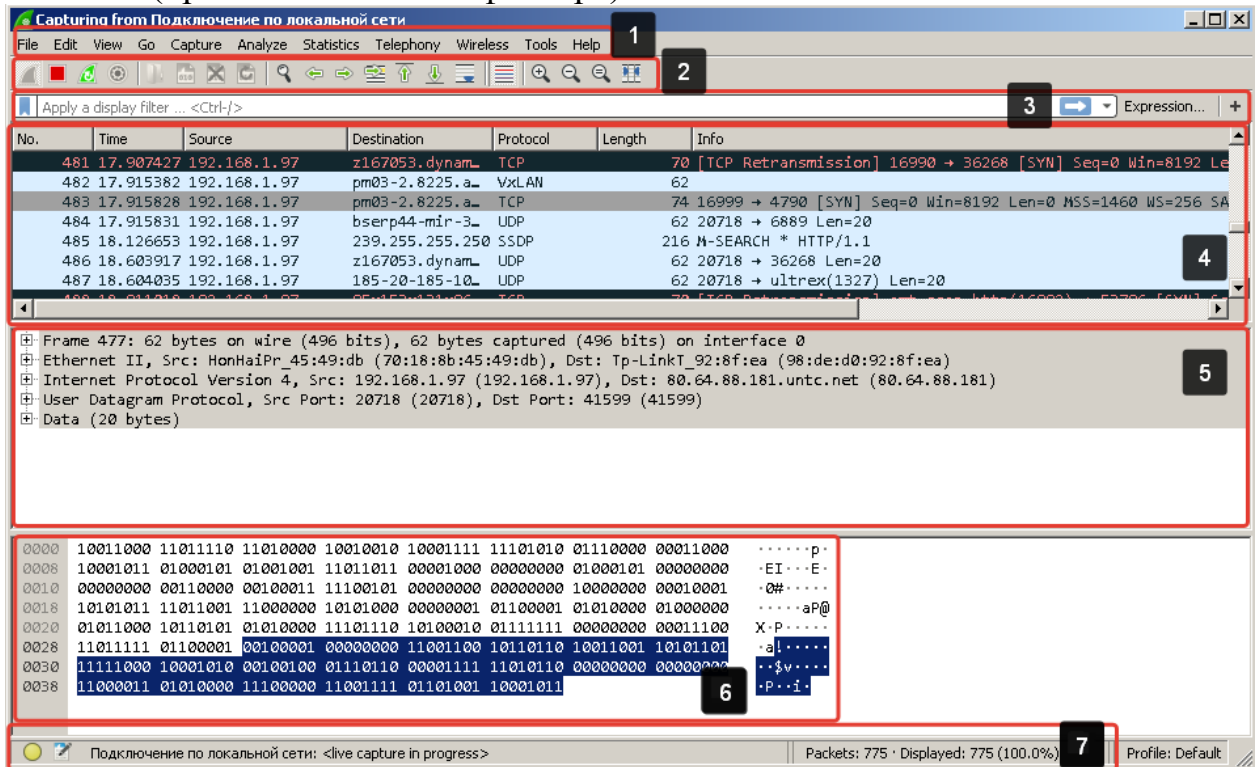


Рисунок 2 – Главное окно программы

Рассмотрим панель инструментов (Рисунок 3).



Рисунок 3 – Панель инструментов.

Кнопки 1-4 отвечают за захват трафика.

1 – Начать захват, 2- остановить, 3 – перезапустить, 4 – вызывает окно дополнительных настроек (где можно, например, выбрать другой интерфейс).

**Нажмите на кнопку 2 для остановки сбора трафика.**

Кнопки 5-8 используются для работы со снимками трафика сохраненными в файл. 5 – открыть файл, 6 – сохранить текущий захват трафика в файл, 7 закрыть текущий файл, 8 – перезагрузить текущий файл.

Кнопки 9-16 используются для передвижения между пакетами и управлением их отображением.

9 – поиск по пакетам (в том числе по содержимому). 10-11 выбрать следующий/предыдущий пакет. 12 – перейти к конкретному пакету (по номеру). 13-14 перейти в начало/конец списка. 15 – автоматически прокручивать список пакетов при получении новых. 16 – раскрашивать пакеты.

Кнопки 17-20 управляют отображением данных. 17-19 Увеличить/уменьшить/вернуть по умолчанию масштаб. 20 – автоматическое выравнивание ширины столбцов.

Поэкспериментируйте с различными кнопками управления. Выясните для чего они используются и как работают.

Попрактикуйтесь начинать сбор трафика и останавливать его. Сохранять собранный трафик в файл и загружать его из файла.

## 2. Фильтрация трафика.

Wireshark поддерживает гибкую систему фильтров. Она работает крайне просто. В поле 3 на рисунке 2 необходимо ввести условие фильтрации, например, название протокола и нажать Enter. Для отмены фильтра, достаточно очистить строку условия (нажав на крестик в этой же строке).

1) Запустите сбор трафика. Запустите на виртуальной машине браузер и перейдите по адресу <http://ncfu.ru>. После загрузки страницы в браузере, остановить сбор трафика.

2) Теперь в поле фильтрации введите http и нажмите Enter. В списке должны отобразиться http пакеты. Рисунок 4. Определите сколько % пакетов от общего числа попали под этот фильтр (см. в строке состояния)

No.	Time	Source	Destination	Protocol	Length	Info
61	77.094	10.0.2.15	ncfu.ru	HTTP	379	GET
65	77.157	ncfu.ru	10.0.2.15	HTTP	596	HTTP
72	77.362	10.0.2.15	ncfu.ru	HTTP	383	GET
97	77.596	ncfu.ru	10.0.2.15	HTTP	289	HTTP
99	77.810	10.0.2.15	ncfu.ru	HTTP	396	GET
113	77.887	10.0.2.15	ncfu.ru	HTTP	398	GET
114	77.887	10.0.2.15	ncfu.ru	HTTP	396	GET
119	77.888	10.0.2.15	ncfu.ru	HTTP	406	GET
138	77.976	ncfu.ru	10.0.2.15	HTTP	948	HTTP
140	77.977	10.0.2.15	ncfu.ru	HTTP	401	GET

Рисунок 4 – Пример фильтрации HTTP трафика.

3) Вспомните какие протоколы вы знаете из лабораторной работы №4 и отфильтруйте результаты по ним. Например, arp, dns, http, tcp.

4) Так же можно фильтровать пакеты по содержанию в них IP-адреса, конкретных IP-адресов отправителя и получателя, номеру порта отправителя и получателя. Для этого используются ключевые слова и операторы.

Таблица 1 - Основные ключевые слова

Основные ключевые слова	Значение
ip.src	IP-адрес отправителя
ip.dst	IP-адрес получателя

ip.addr	IP-адрес (содержится в пакете)
tcp.srcport	TCP-порт отправителя
tcp.dstport	TCP-порт получателя
tcp.port	TCP-порт (содержится в пакете)
udp.srcport	UDP-порт отправителя
udp.dstport	UDP -порт получателя
udp.port	UDP -порт (содержится в пакете)

Таблица 2 – Основные операторы сравнения

Символ	Значение
==	Равно
!=	Не равно
>	Больше
<	Меньше
>=	Больше или равно
<=	Меньше или равно

Комбинируя ключевые слова, и операторы мы можем составлять правила фильтрации.

Например,

**ip.addr == 8.8.8.8** – отобразить все пакеты отправленные или полученные с адреса 8.8.8.8

**udp.port >=50** – отобразить все пакеты полученные и переданные по протоколу udp с портом больше или равному 50

**tcp.dstport == 443** – отобразить все TCP пакеты отправленные на 443 порт

5) Поэкспериментируйте с различными вариантами фильтрации по ip и порту для протоколов tcp и udp.

6) Правило фильтрации можно инвертировать, если взять в скобки и поставить перед ним !. Например, **!(tcp.dstport == 443)**

7) Можно отфильтровать только пакеты содержащие определенный текст, для этого используется оператор **contains**. Синтаксис использования:

**Протокол contains строка.**  
Пример использования: **http contains ncfu.ru** – отобразит все http пакеты содержащие строку ncfu.ru

8) Условия можно объединять. Для этого используются операторы **and** (и) и **or** (или). Для этого, каждое условие берется в скобки и между условиями ставится оператор **and** или **or**. Например:

**(http) and (ip.addr == 195.209.244.53)** – отобразить все http пакеты отправленные и полученные с адреса 195.209.244.53

**(ip.srcaddr == 192.168.1.1) and (tcp.dstport == 80)** -- отобразить все пакеты отправленные с адреса 192.168.1.1 на 80 порт получателя.

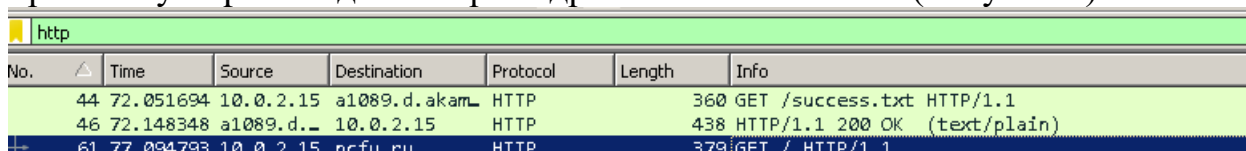
**(ip.dstaddr == 192.168.1.1) or (ip.dstaddr == 192.168.1.2)** – отобразить все пакеты адресованные узлам с адресами 192.168.1.1 ИЛИ 192.168.1.2

9) Потренируйтесь составлять сложное условие фильтрации.

### 3. Отслеживание соединения.

Кроме фильтрации трафика, Wireshark предоставляет так же удобные средства для просмотра диалогов (англ. Conversation). Этим термином обозначается обмен запросами и ответами в рамках одного соединения. Поддерживаются протоколы TCP, UDP, SSL и HTTP.

1) Для использования этой техники, сделайте фильтрацию по протоколу http и найдите запрос адресованный к ncfu.ru (Рисунок 5).



No.	Time	Source	Destination	Protocol	Length	Info
44	72.051694	10.0.2.15	a1089.d.akam	HTTP	360	GET /success.txt HTTP/1.1
46	72.148348	a1089.d.	10.0.2.15	HTTP	438	HTTP/1.1 200 OK (text/plain)
61	77.094793	10.0.2.15	ncfu.ru	HTTP	379	GET / HTTP/1.1

Рисунок 5

Теперь кликните правой кнопкой мыши на этом пакете и выберете раздел Follow(следовать) – HTTP Stream (HTTP поток). Рисунок 6.

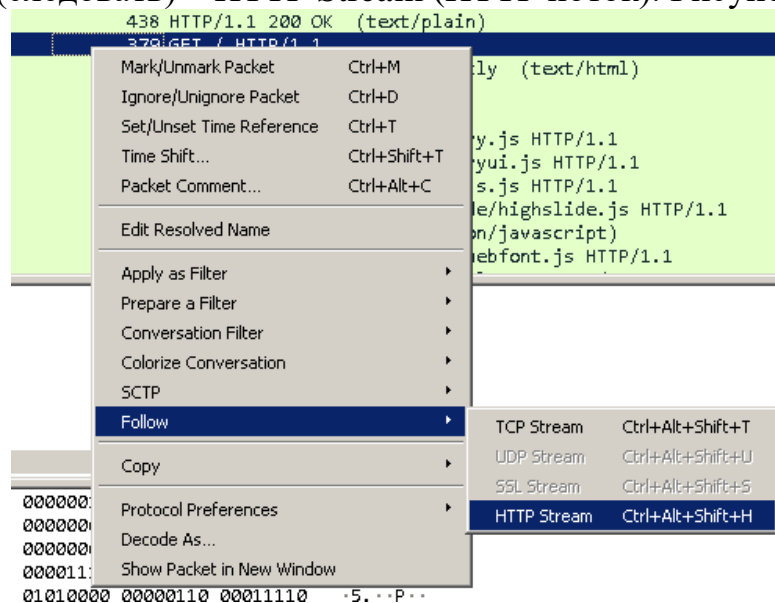


Рисунок 6

Откроется новое окно (Рисунок 7) в котором будет показан весь диалог между клиентом и сервером в рамках одного подключения.

2) Закройте окно и проделайте тоже самое, только выберите TCP Stream. Определите в чем разница.

3) Найдите пакеты UDP и попробуйте посмотреть диалоги между ними.

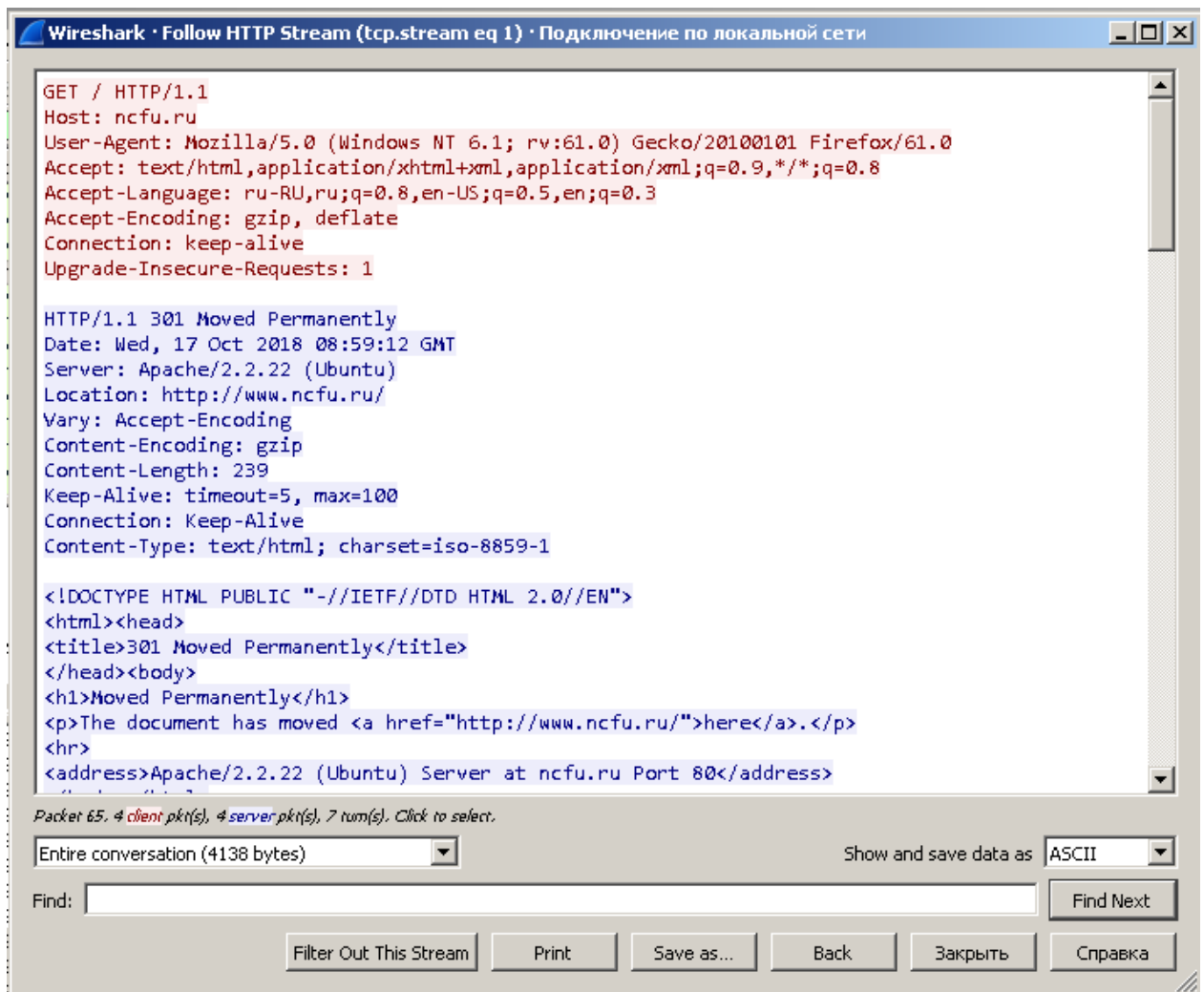


Рисунок 7 – Диалог в рамках одного HTTP соединения

#### 4. Статистика. Иерархия протоколов.

1) Wireshark содержит огромное количество инструментов для анализа статистического анализа данных. В данной работе, мы рассмотрим лишь один из них – Иерархию протоколов (Protocol Hierarchy). Этот инструмент позволяет быстро определить, какие протоколы используются в перехваченном трафике и произвести фильтрацию по ним. Это чрезвычайно важно при анализе больших объемов трафика.

2) Запустите из главного меню Wireshark Statistics - Protocol Hierarchy (Рисунок 8). Откроется окно (Рисунок 9)

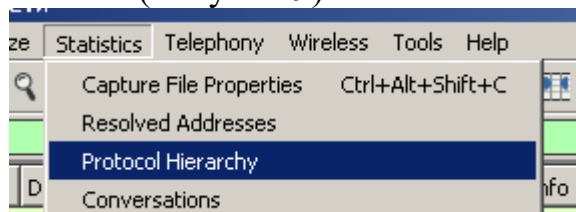


Рисунок 8

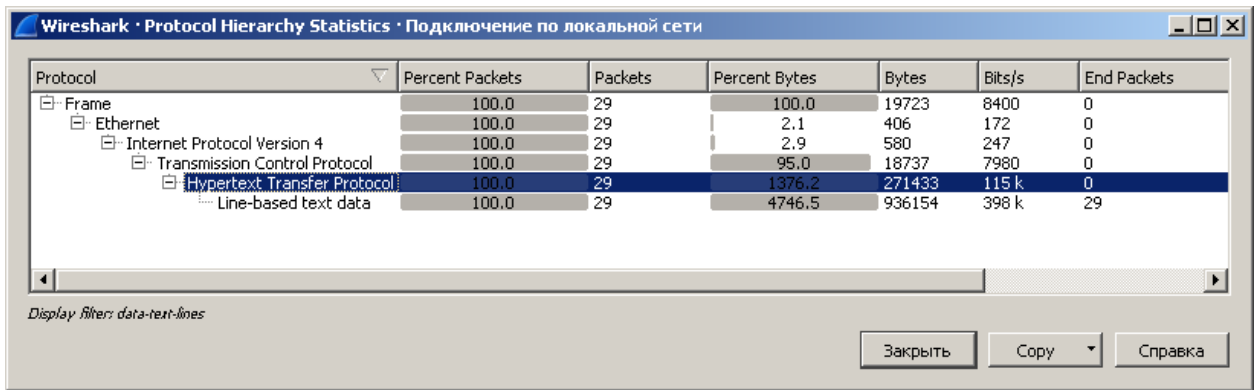


Рисунок 9 - Protocol Hierarchy

3) В открывшемся окне в виде иерархического дерева, представлены все протоколы которые встречаются в данном трафике. На рисунке 10 показан пример трафика с Telnet соединением.

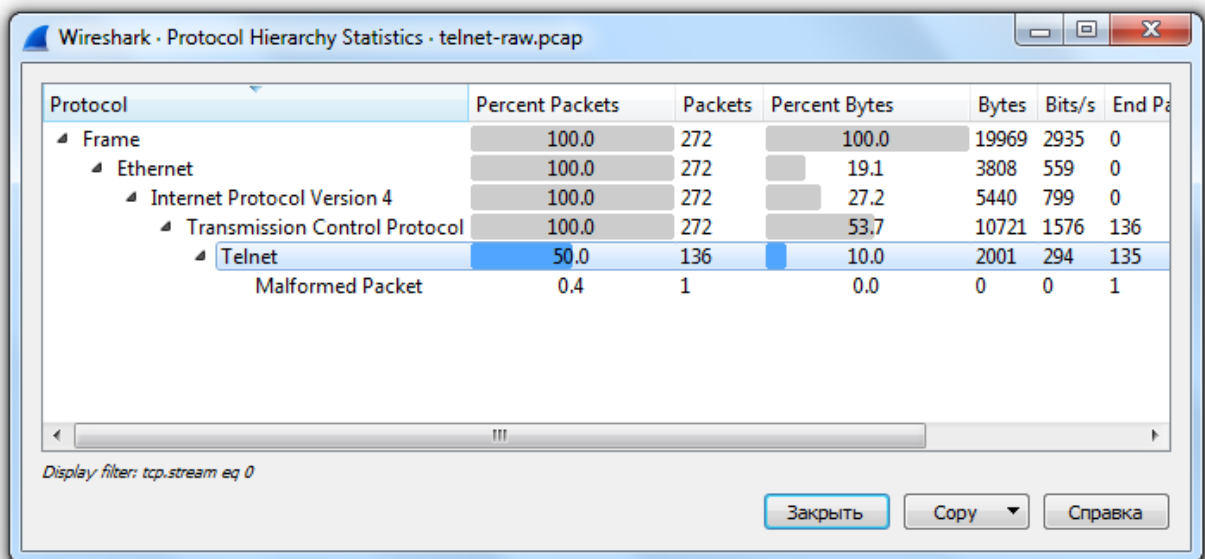


Рисунок 10 - Protocol Hierarchy – пример с Telnet

4) Для установки фильтра по данному протоколу, нажмите на нужном протоколе правой кнопкой мыши и выберите Apply as Filter – Selected и правило фильтрации по выбранному протоколу применится. (Рисунок 11).

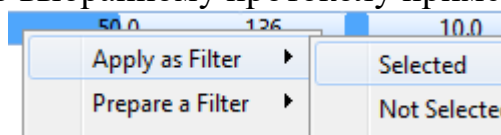


Рисунок 11

## 5. Экспорт перехваченных файлов

1) Во время анализа трафика, Wireshark автоматически находит файлы, передающиеся по незашифрованным протоколам. К ним относятся DICOM, HTTP, IMF, SMB, TFTP. Если при анализе трафика (например, в Protocol Hierarchy) вам встретится один из них, есть смысл проверить, не распознал ли в этом трафике Wireshark какие-либо файлы.

2) Откройте меню File и перейдите в раздел Export Objects. Выберите нужный протокол, в данном случае HTTP (Рисунок 12)

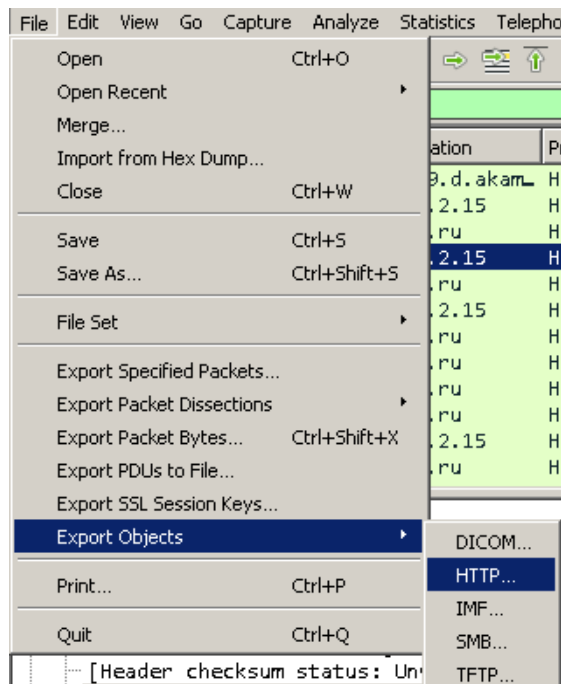


Рисунок 12 – Экспорт объектов, HTTP

3) В открывшемся окне (Рисунок 13) показаны все найденные файлы переданные по данному протоколу. Для сохранения одного файла выберите его в списке, нажмите сохранить и выберите место для сохранения. Для экспорта всех файлов, нажмите кнопку Сохранить все и выберите место для сохранения.

4) Проверьте, что файлы открываются.

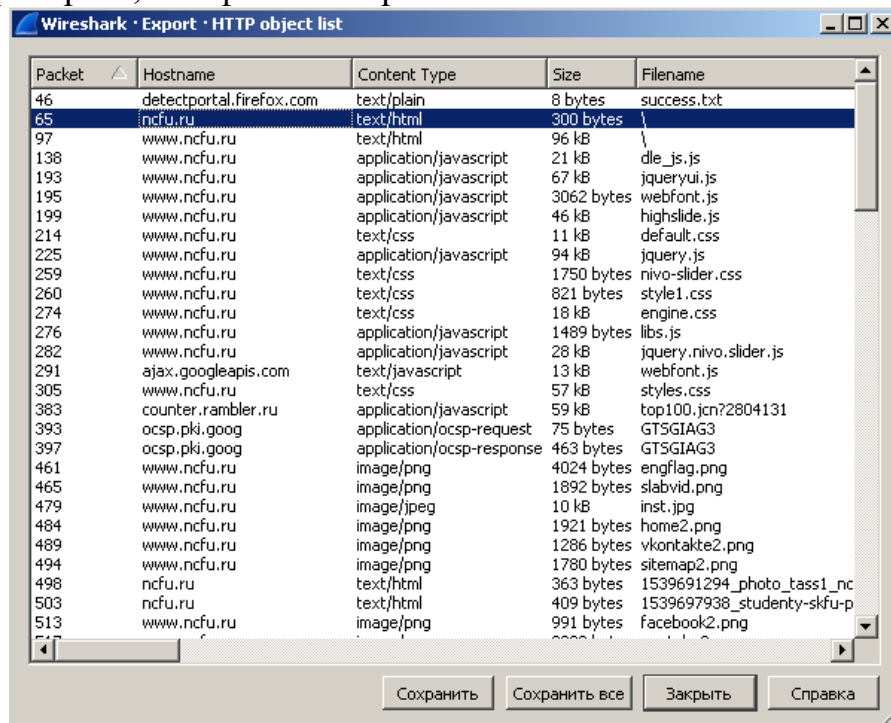


Рисунок 13 – Найденные файлы

### Самостоятельная работа.

1) ch1.pсар – TFTP, определите логин и пароль

- 2) ch2.pcap – Telnet, определите логин и пароль
- 3) ch3.pcap – Twitter – HTTP – найдите в заголовке логин и пароль
- 4) ch4.pcap – ICMP – Определите при каком TTL был достигнут хост назначения
- 5) ch5.pcap – HTTP - извлеките изображения из перехваченного трафика.

Контрольные вопросы:

1. Что такое неразборчивый режим сетевой карты?
2. Для чего используется WireShark?
3. Каковы основные элементы интерфейса программы Wireshark? Для чего они нужны?
4. Как задаются условия фильтрации трафика?
5. Как объединить условия фильтрации?
6. Что такое отслеживание соединения? Для чего оно используется?
7. Как извлечь файлы из перехваченного трафика?
8. Как определить какие протоколы используются в перехваченном трафике?

Список литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.



## Лабораторная работа №7. Установка и настройка VPN сервера.

### Цель работы:

Изучить технологии настройки и установки VPN-сервера для защиты информации на компьютере во внутренней сети.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть:

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

SoftEther VPN Server позволяет легко и быстро развернуть VPN сервер на Windows. Это позволяет объединить различные устройства, сервера и компьютеры в одну сеть (виртуальную). При этом все эти устройства могут физически находиться где угодно в мире. В данной лабораторной работе рассмотрена установка и настройка SoftEther VPN Server на Windows. SoftEther VPN Server является freeware продуктом.

Обычно VPN сервер используют для организации удалённого доступа в сеть предприятия из дома или других удалённых сетей (офисов) организации. Так же в эту сеть могут подключаться любые другие устройства которым разрешен доступ, например мобильный телефон. Т.е. можно с мобильного

телефона войти на рабочий стол своего рабочего компьютера. Поэтому, часто, VPN сервер – это центральный узел, к которому подключаются клиенты, чтобы получить доступ во внутреннюю сеть предприятия.

### Оборудование и материалы.

Персональный компьютер, 2 виртуальные машины под управлением Windows 7.

### Указания по технике безопасности:

Соответствуют технике безопасности по работе с компьютерной техникой.

### Задания

Топология создаваемой в данной работе сети приведена на рисунке 1.



Рисунок 1 – Схема виртуальной сети.

Целью данной работы, является организация доступа в Интернет для клиентской машины, находящейся во внутренней сети. В условиях данного эксперимента мы считаем “внутреннюю сеть” не безопасной и “поверх” нее настроим зашифрованный VPN-туннель. Поскольку SoftEther VPN предоставляет кучу дополнительных возможностей, это будет VPN с собственным DHCP и NAT.

Для выполнения работы потребуется:

- 2 виртуальные машины под управлением Windows 7

### **Конфигурация виртуальных машин.**

#### **Конфигурация шлюза.**

- Переименуйте одну виртуальную машину в GATE или в Шлюз.
- Переименуйте вторую виртуальную машину в Client или Клиент.
- В виртуальной машине Шлюз установите две сетевые карты. Первой сетевой карте установите режим Внутренняя сеть и имя сети intnet2 (Рисунок 2). Второй сетевой карте установите режим NAT. (Рисунок 3)

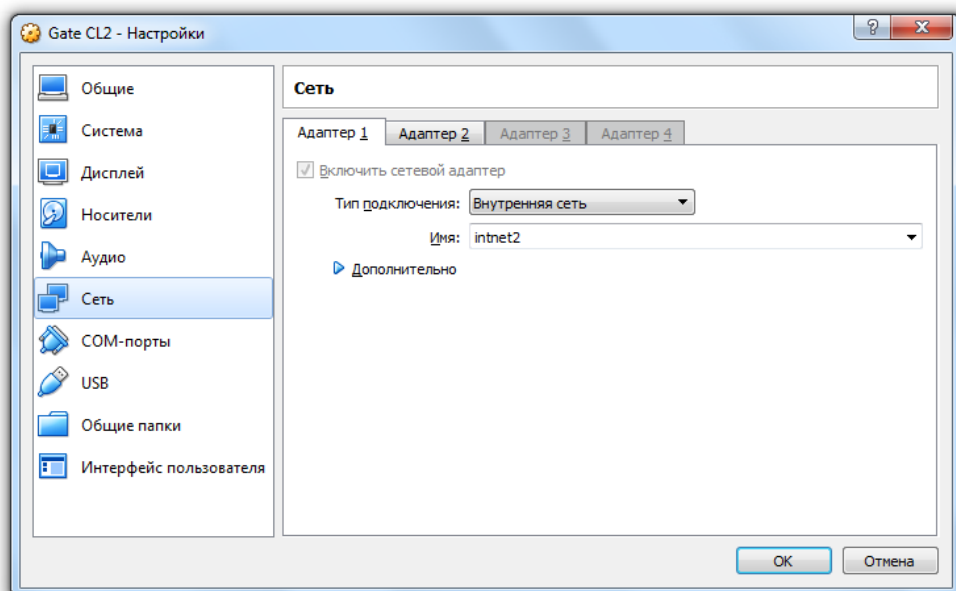


Рисунок 2 – Шлюз – сетевая карта 1

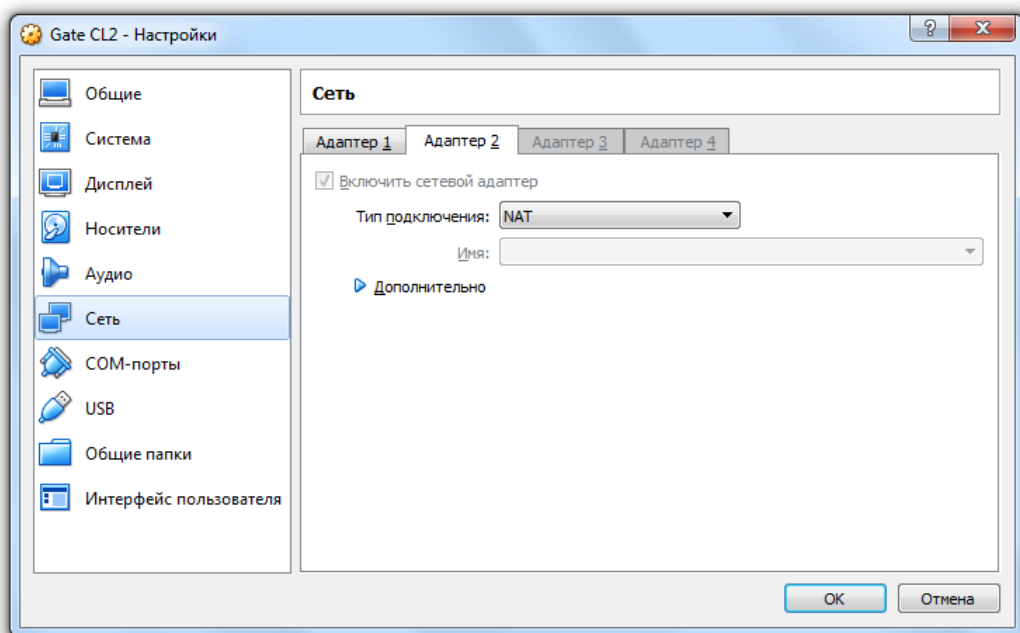


Рисунок 3 – Шлюз – сетевая карта 2

- Запустите виртуальную машину Шлюз
- Зайдите в настройки IP-адреса “Подключение по локальной сети” и установите IP-адрес 192.168.10.1 маска 255.255.255.0 (Рисунок 4)

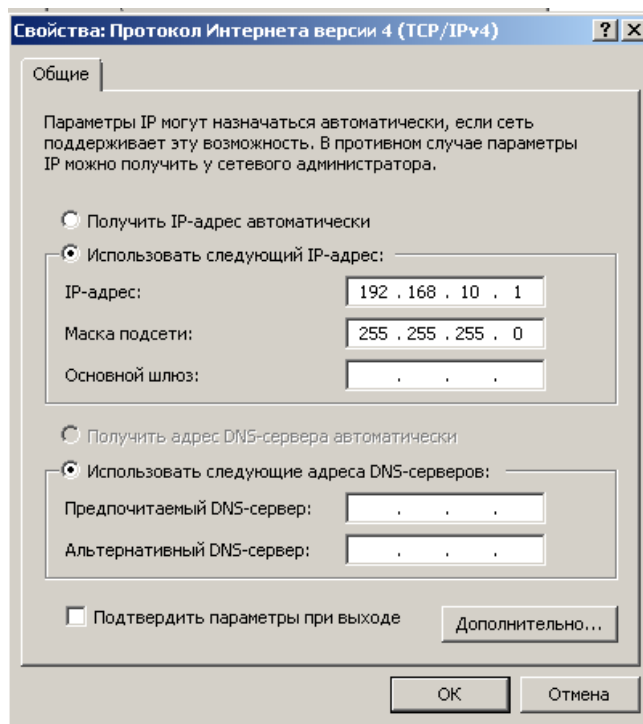


Рисунок 4 - Первый сетевой адаптер

- Зайдите в настройки IP-адреса “Подключение по локальной сети 2” и установите IP-адрес “получать IP-адрес автоматически” и “получить адрес DNS-сервера автоматически” (Рисунок 5)

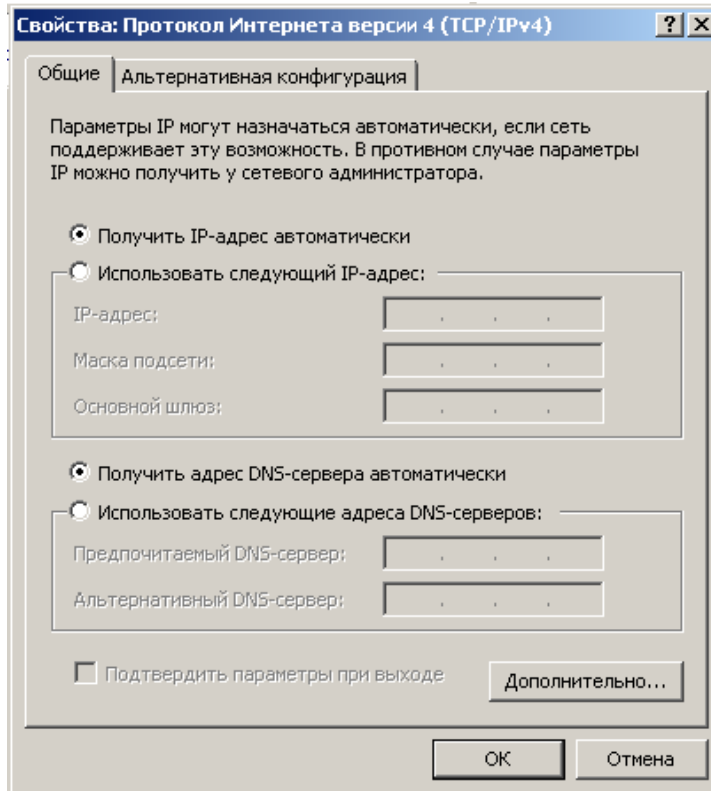


Рисунок 5 – Второй сетевой адаптер

- Отключите все профили брандмауэра Windows (Рисунок 6)

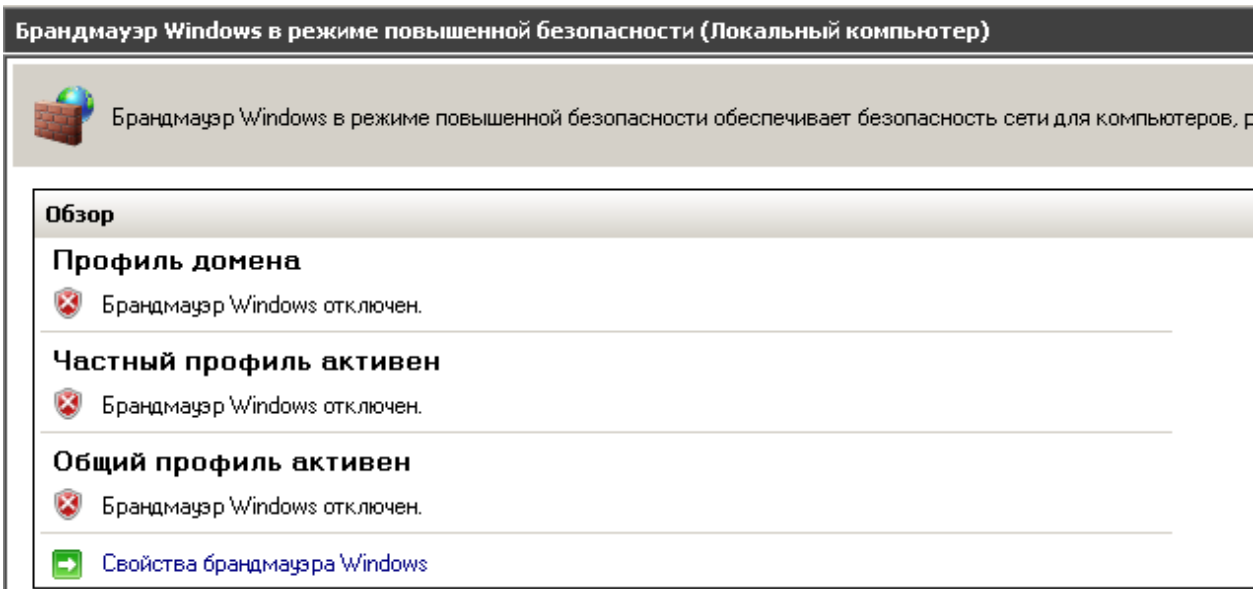
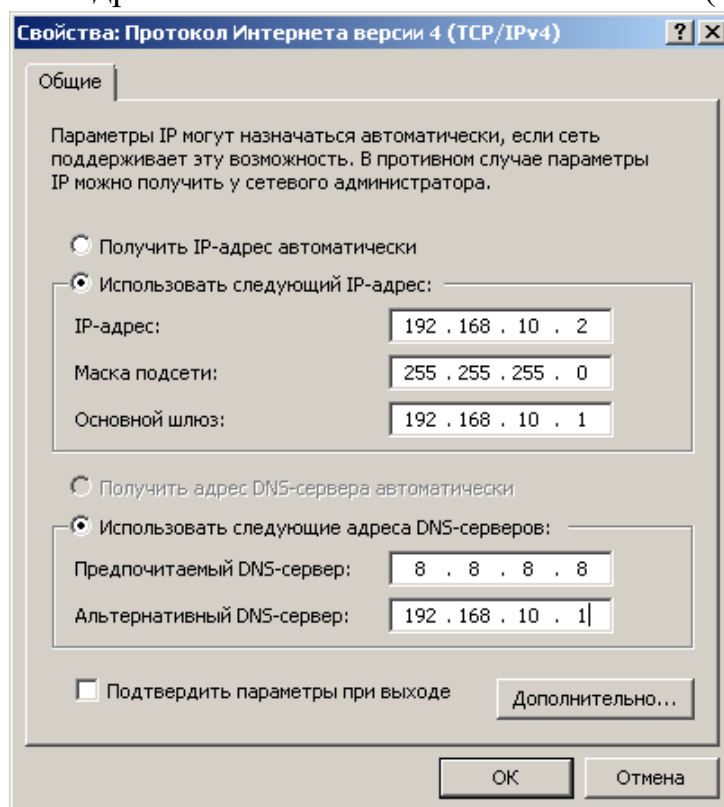


Рисунок 6 – Отключение брандмауэра Windows

- С помощью команды ping проверьте доступность узлов 8.8.8.8 и ya.ru. Они должны быть доступны.

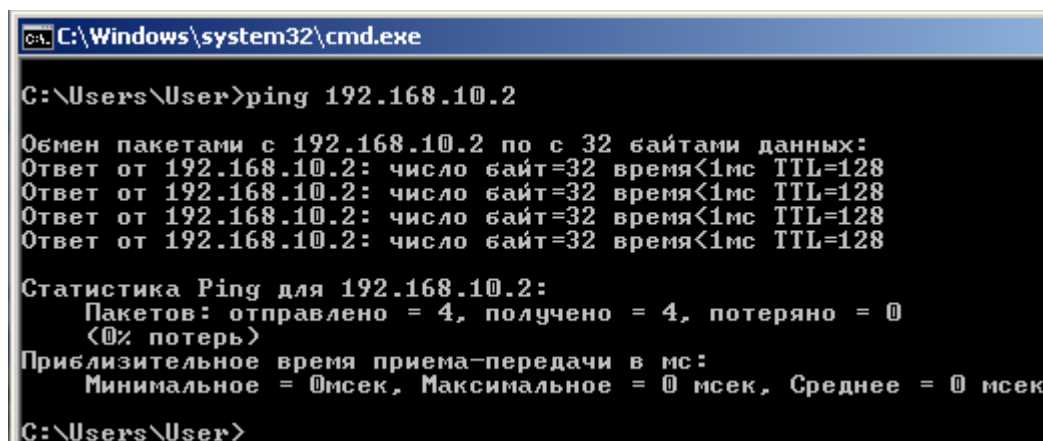
### Конфигурация клиента.

- Проверьте, что на клиентской машине включен ОДИН сетевой адаптер и установлен режим “Внутренняя сеть” (Рисунок 2)
- Запустите Windows на клиентской машине.
- Зайдите в настройки IP-адреса “Подключение по локальной сети” и установите IP-адрес 192.168.10.1 маска 255.255.255.0 (Рисунок 7)



## Рисунок 7 – Клиент - Настройка сети

- Отключите брандмауэр аналогично настройке шлюза (Рисунок 6)
- Проверьте связь со шлюзом (ping 192.168.10.1) (Рисунок 8)



```
C:\Windows\system32\cmd.exe

C:\Users\User>ping 192.168.10.2

Обмен пакетами с 192.168.10.2 по 32 байтами данных:
Ответ от 192.168.10.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.10.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\User>
```

Рисунок 8 – проверка связи

Если Ping проходит – настройка сделана правильно и можно переходить

## Установка VPN-Server

- Перейдите на виртуальную машину Шлюз.
- Загрузите установочный дистрибутив из папки \\serverbd\Студенческая\ИБ\softether-vpnserver\_vpnbridge-v4.28-9669-beta-2018.09.11-windows-x86\_x64-intel.exe и перенесите на виртуальную машину. Если это не возможно, скачайте дистрибутив по адресу [http://www.softether-download.com/files/softether/v4.28-9669-beta-2018.09.11-tree/Windows/SoftEther\\_VPN\\_Server\\_and\\_VPN\\_Bridge/softether-vpnserver\\_vpnbridge-v4.28-9669-beta-2018.09.11-windows-x86\\_x64-intel.exe](http://www.softether-download.com/files/softether/v4.28-9669-beta-2018.09.11-tree/Windows/SoftEther_VPN_Server_and_VPN_Bridge/softether-vpnserver_vpnbridge-v4.28-9669-beta-2018.09.11-windows-x86_x64-intel.exe)
- Запустите скачанный дистрибутив. На всех шагах установки нажимайте Далее и Да. На одном из шагов выберите SoftEther VPN Server (Рисунок 9)

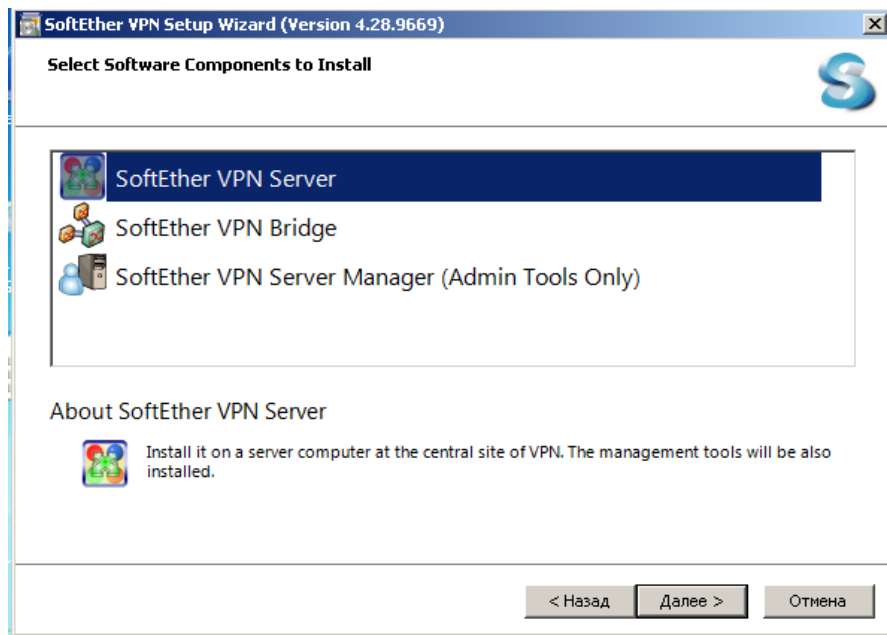


Рисунок 9 – Выбор компонентов

- После окончания установки запустится SoftEther VPN Server Manager – программа для конфигурирования VPN-серверов SoftEther (Рисунок 10). Если этого не произошло, запустите данную программу ярлыком на рабочем столе.
- Выберите в списке localhost и нажмите Connect.



Рисунок 10 - SoftEther VPN Server Manager

### Базовая конфигурация VPN-сервера

- Если все выполнено верно, то сервер при первом соединении система предложит сменить пароль администратора. Введите 123 в оба поля и нажмите ОК (Рисунок 11)



Рисунок 11 – Смена пароля.



Рисунок 12 – подтверждение успешной смены пароля

- Запустится мастер простой конфигурации VPN-сервера (Рисунок 13). На данном шаге предлагается выбрать режим работы VPN. Отметьте “Remote Access VPN Server” и нажмите ОК

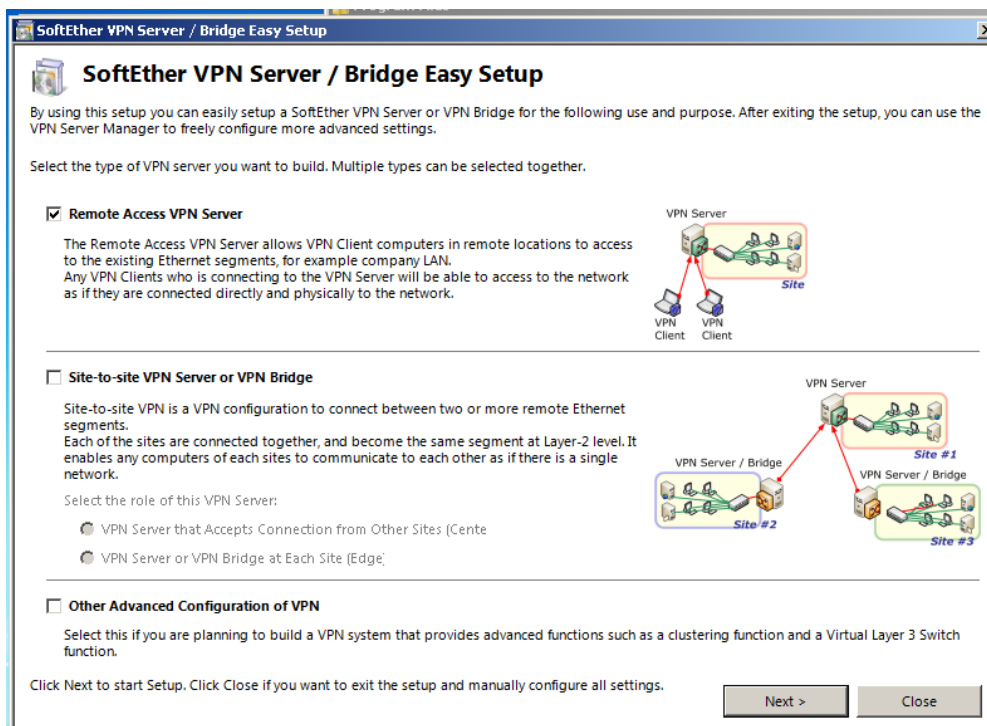


Рисунок 13 – Мастер легкой настройки

- Нажмите ОК в окне подтверждения выбора настроек. (Рисунок 14)



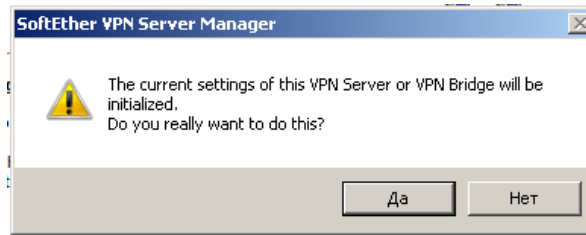


Рисунок 14 – окно подтверждения

- SoftEther объединяет настройки относящиеся к одной конфигурации VPN в хабы (Hub). В окне (Рисунок 15) укажите название хаба “VPN” и нажмите ОК

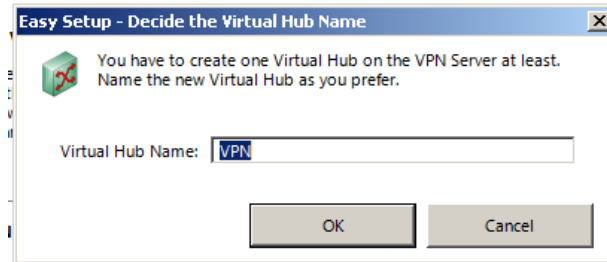


Рисунок 15 – название хаба

- Следующее окно – конфигурация IPsec (Рисунок 16). Нажмите ОК  
Следующее окно - Настройка VPN Azure Cloud, отметьте “Disable VPN Azure” и нажмите ОК

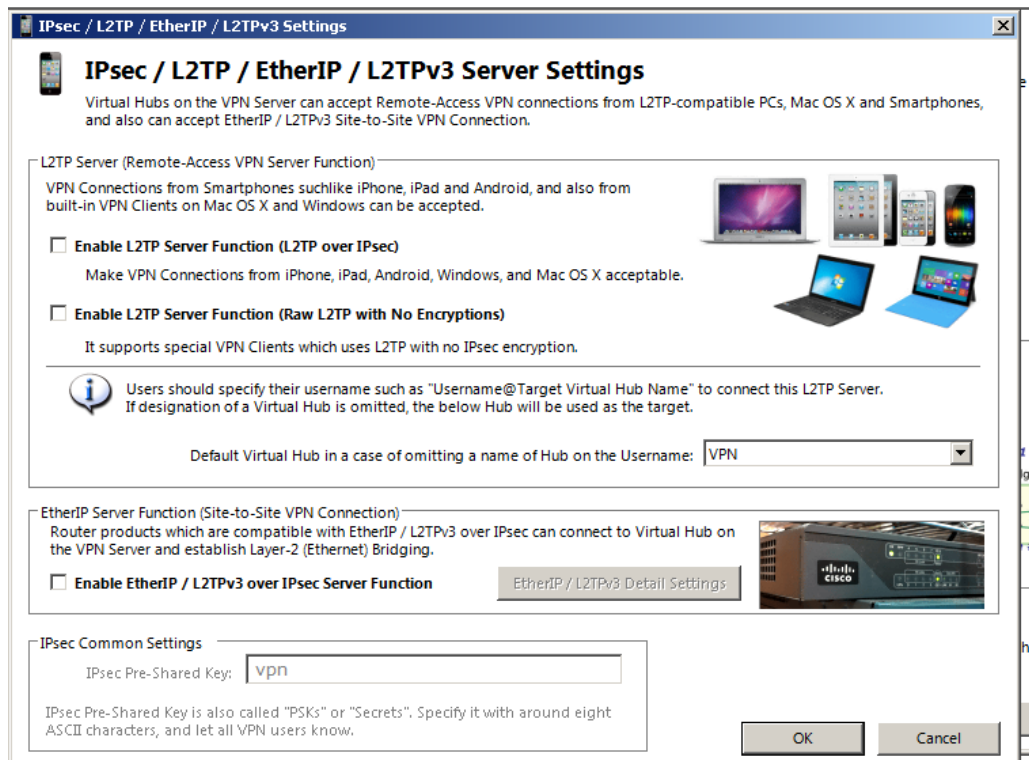


Рисунок 16 – конфигурация IPsec

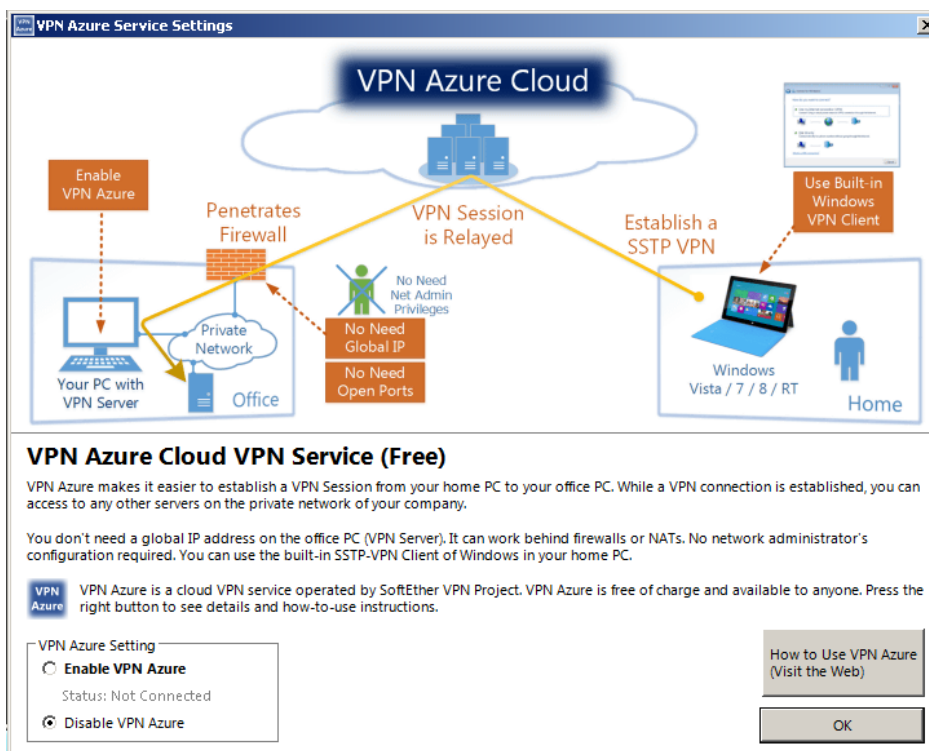


Рисунок 17 – Настройка VPN Azure Cloud

- Откроется новое окно (Рисунок 18). На данном этапе необходимо выбрать с какой внешней сетью будет коммутироваться соединение по VPN. Для этого в разделе “Step 3. Set Local Bridge” выберите “Подключение по локальной сети 2” (Сетевая карта в режиме NAT).
- Нажмите Create Users для добавления пользователя. Рисунок 19. Укажите имя пользователя user1, выберите способ аутентификации Password Authentication и задайте пароль 123. Нажмите кнопку ОК для сохранения.

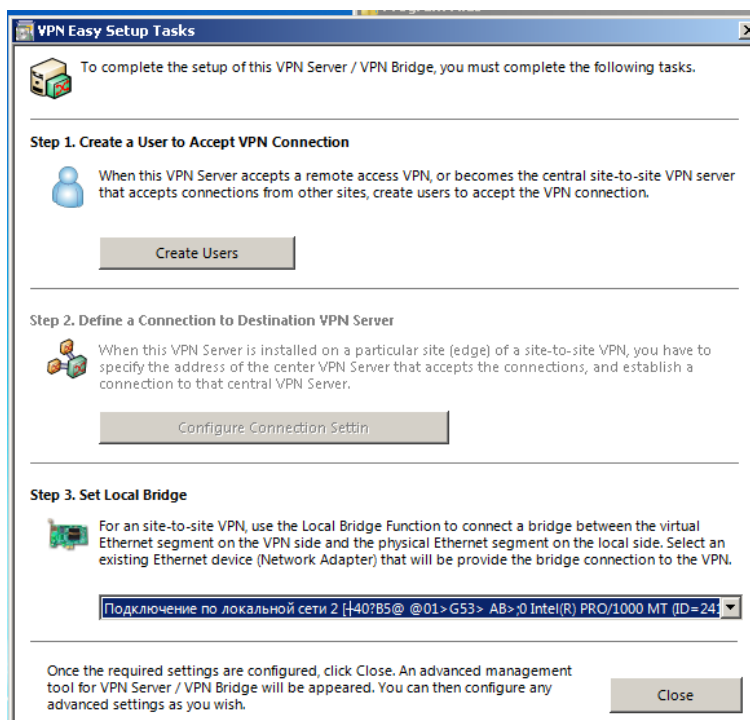


Рисунок 18 – Настройка моста и пользователей.

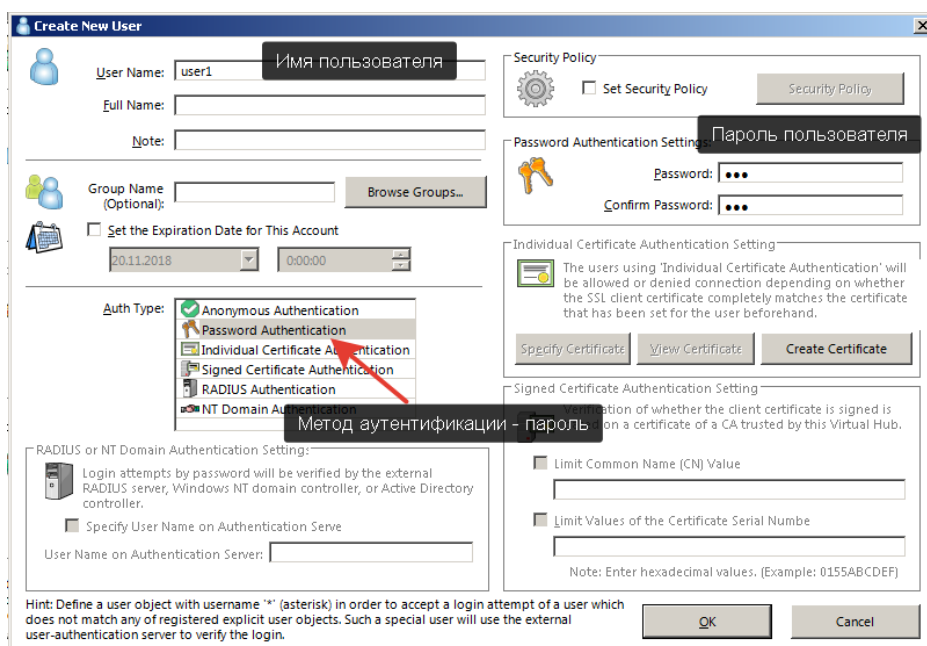


Рисунок 19 – Добавление пользователей

- Откроется окно управления пользователями. Поскольку пользователь добавлен (Рисунок 20) нажмите Exit чтобы закрыть окно.

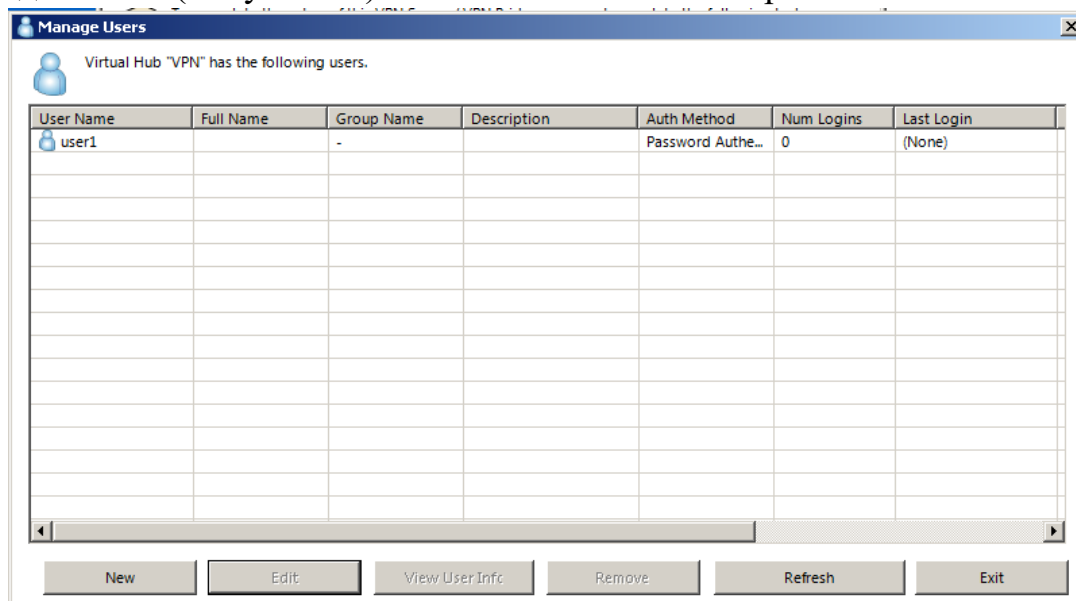


Рисунок 20 – Настройка пользователей

- В результате, вы увидите главное окно программы (Рисунок 21). Если все выполнено верно, в списке Virtual Hub Name должен быть одна строка VPN со статусом Online.

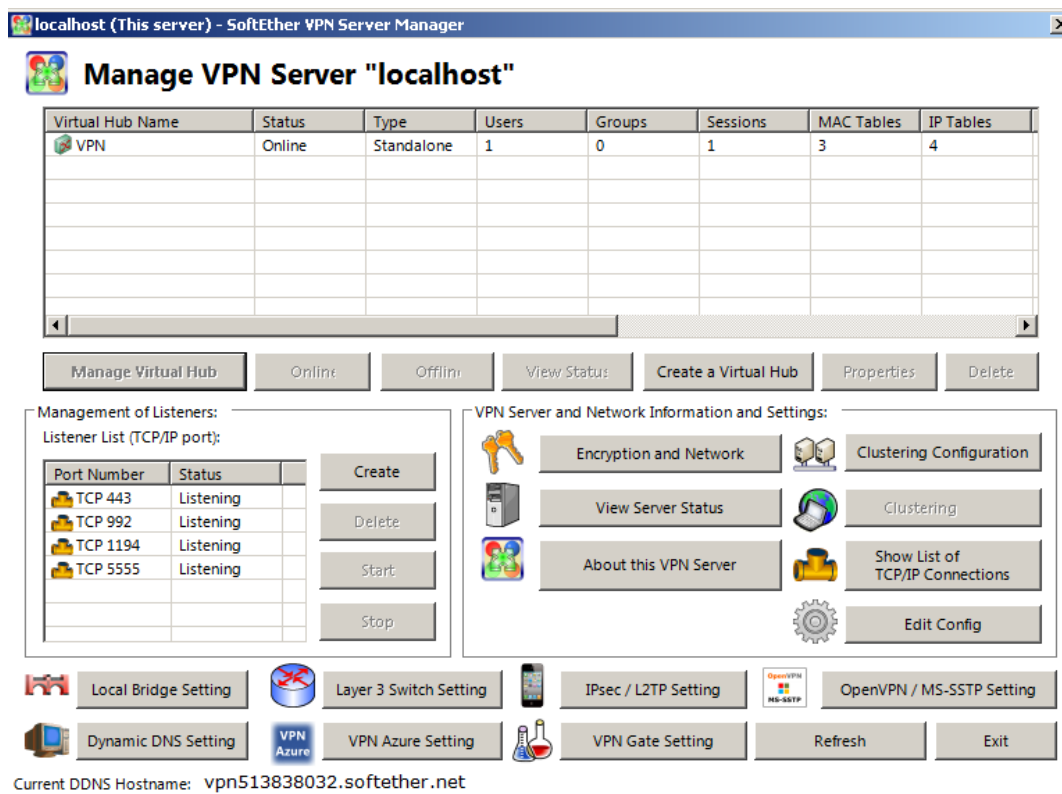


Рисунок 21 – Главная панель управления SoftEther VPN Server

## Настройка NAT и DHCP

- В главном окне программы, выделите VPN в списке Virtual Hub Name и нажмите Manage Virtual Hub (Управление виртуальным хабом) Рисунок 22.
- Откроется окно Management of Virtual Hub (Рисунок 23). В этом окне можно отредактировать настройки текущего VPN сервера. Поэкспериментируйте с различными пунктами настроек. После того как немного освоитесь, нажмите кнопку “Virtual NAT and Virtual DHCP Server” откроется окно Рисунок 24.

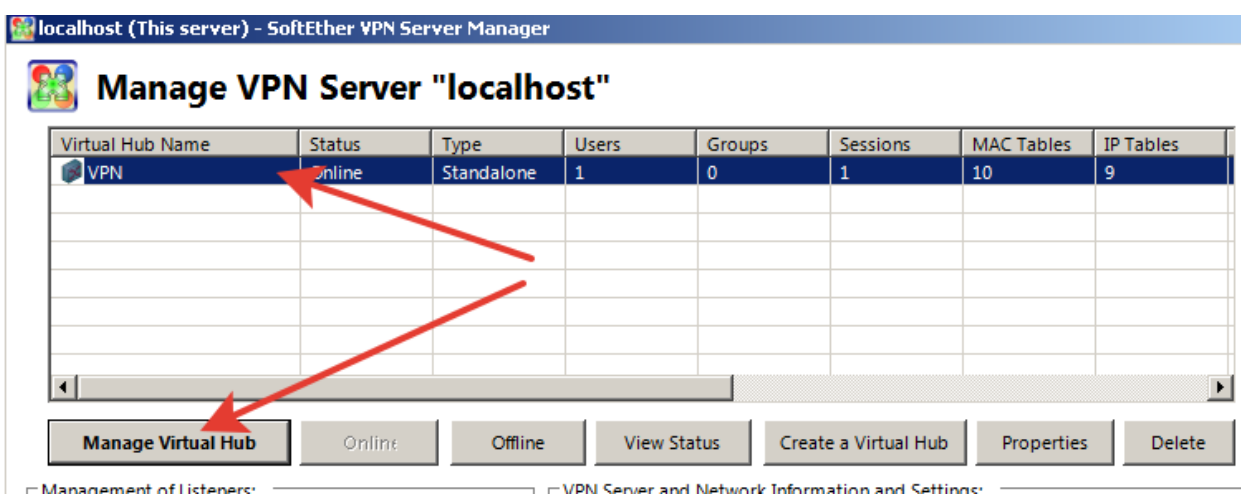


Рисунок 22 –Выбор виртуального хаба

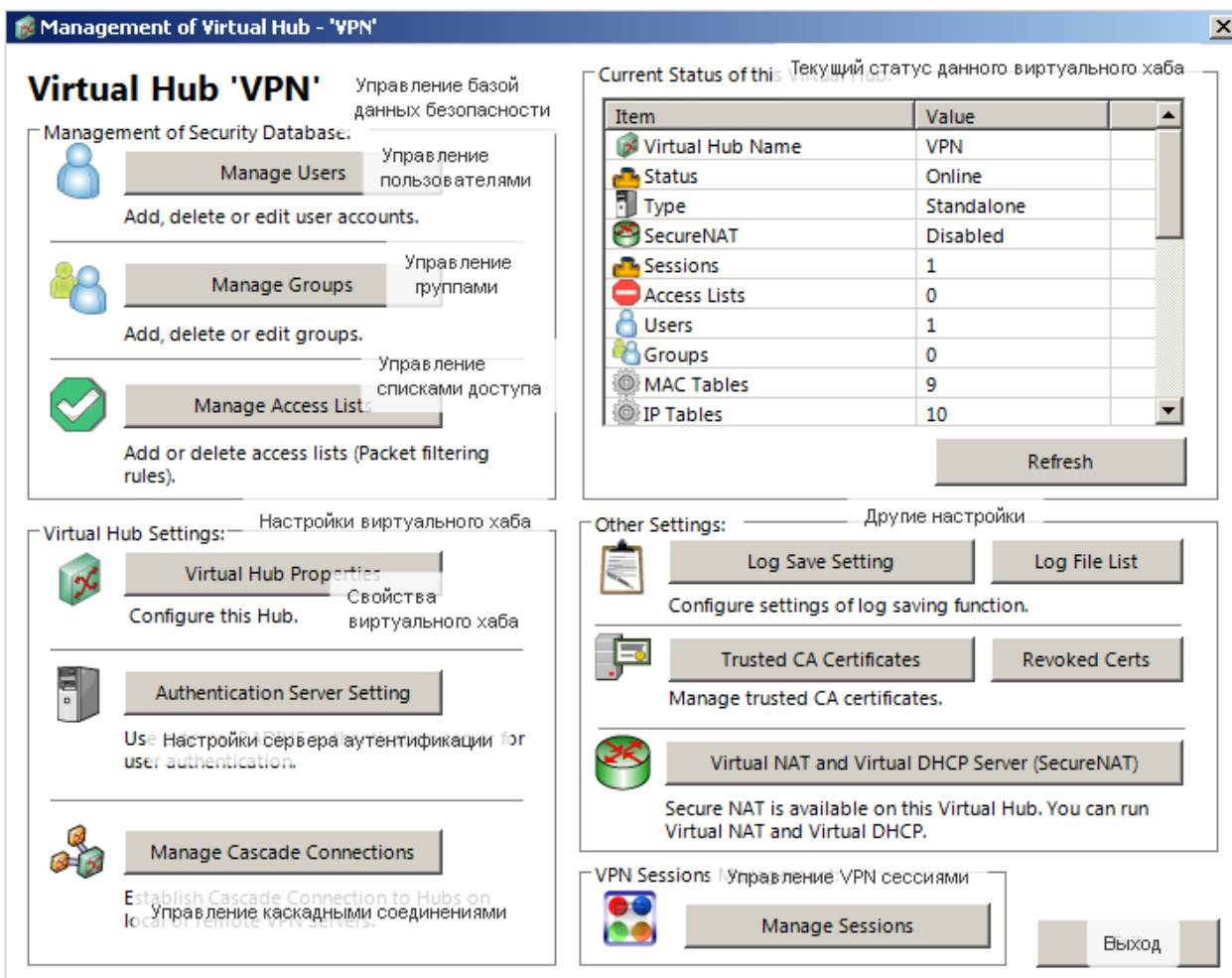


Рисунок 23 – Управление виртуальным хабом

- В данном окне (рисунок 24) Включается, отключается и конфигурируется NAT и встроенный DHCP-сервер. Нажмите кнопку SecureNAT Configuration для просмотра настроек NAT и DHCP.
- В открывшемся окне (Рисунок 25) определите какие заданы параметры виртуального хоста (ip-адрес, маска) Какие параметры заданы для DHCP сервера (диапазон адресов, маска, срок аренды). Закройте окно кнопкой ОК.

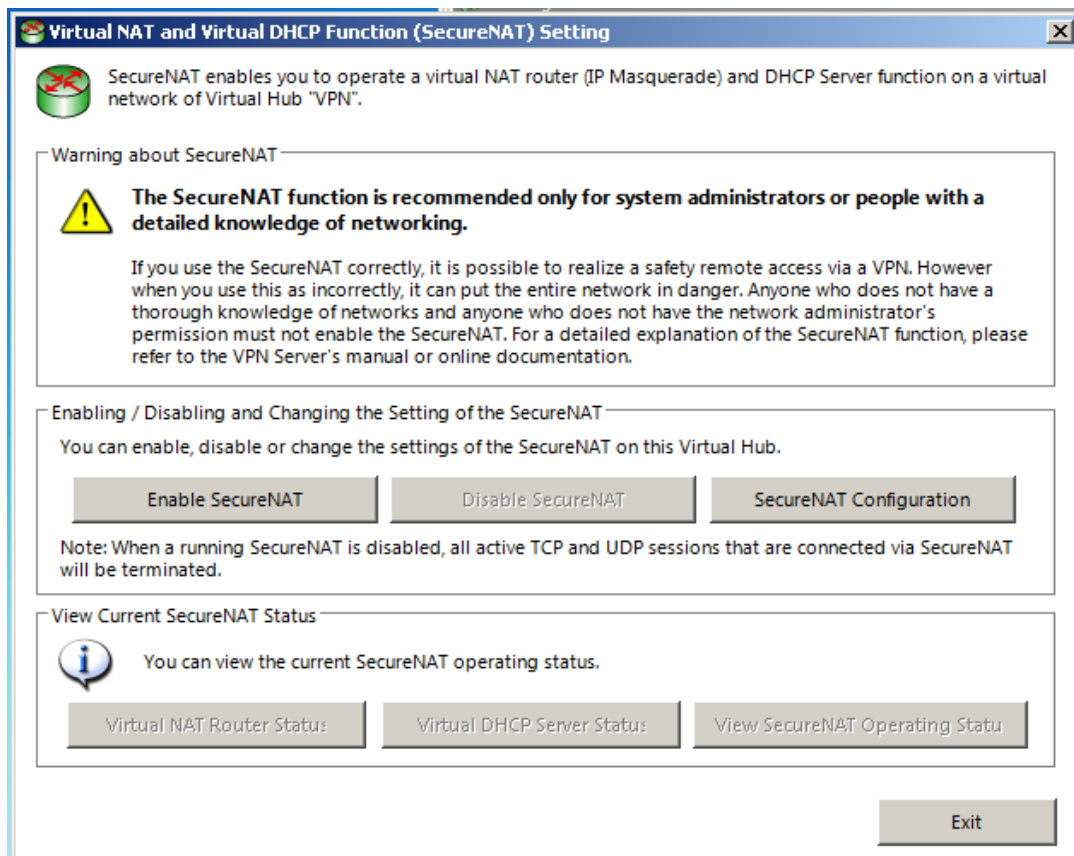


Рисунок 24 – Управление SecureNAT

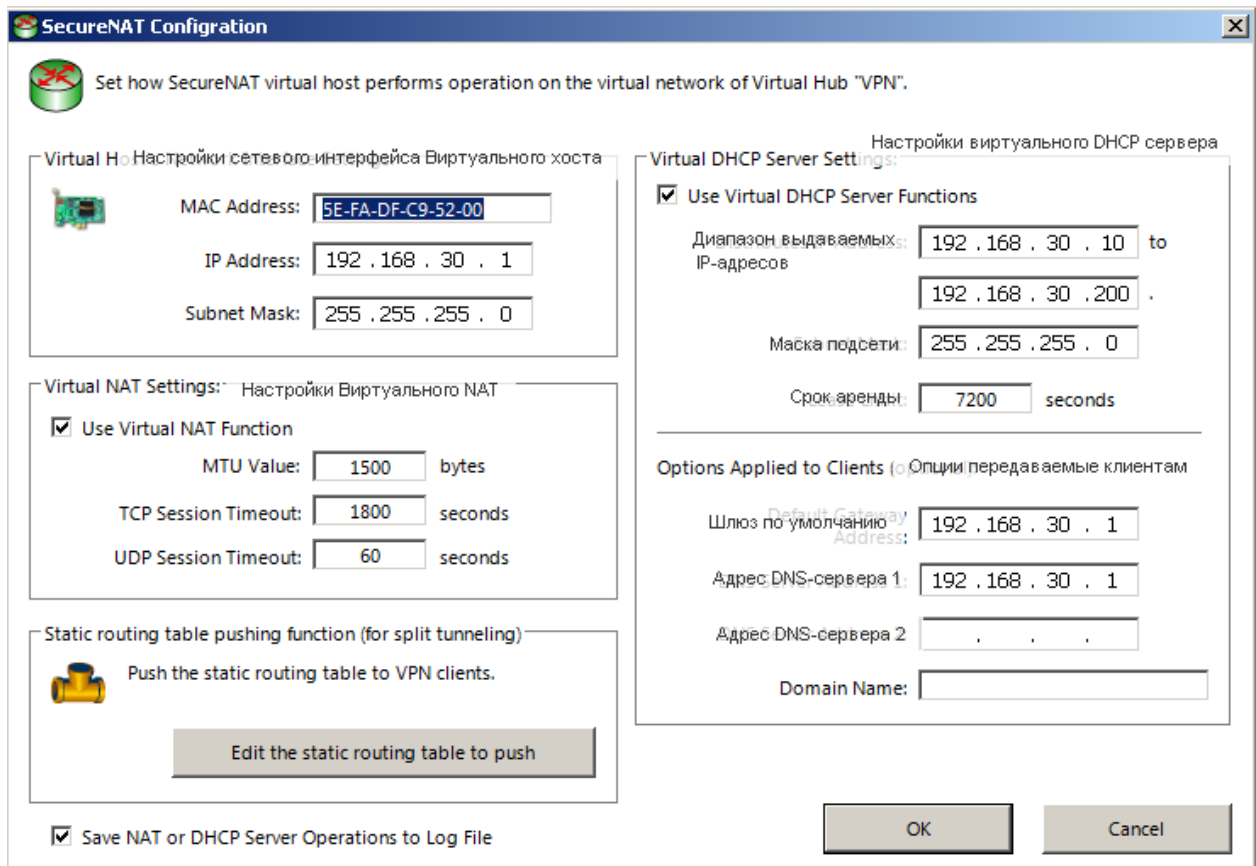
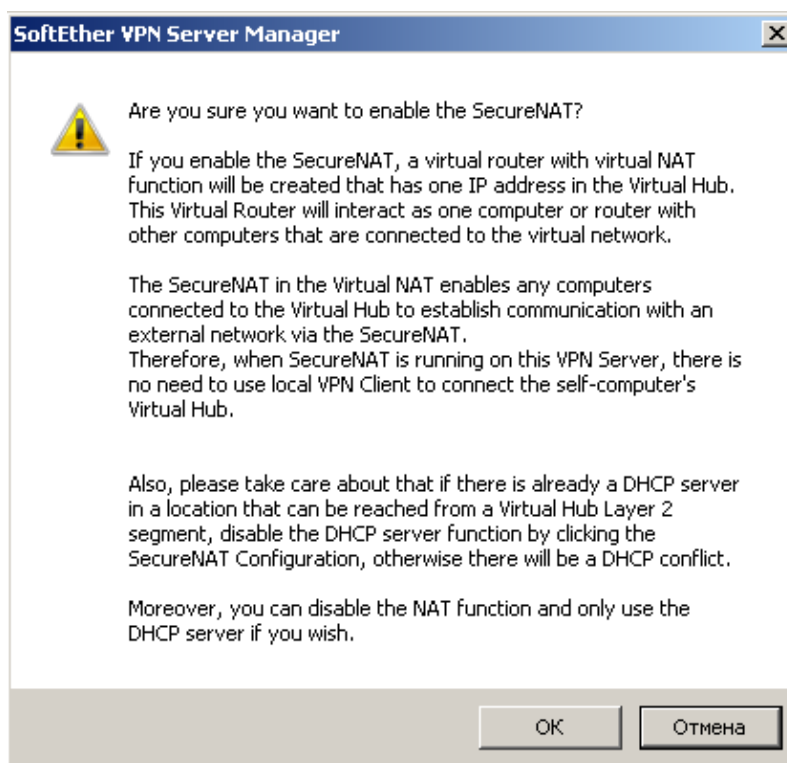


Рисунок 25 – Конфигурация SecureNAT

- Вернитесь к предыдущему окну (Рисунок 24) нажмите Enable SecureNAT для включения NAT и DHCP-сервера. При этом может

ПОЯВИТЬСЯ  
ОКНО С



подтверждением действия (Рисунок 26). Нажмите ОК. Базовая конфигурация VPN-сервера завершена.

Рисунок 26 – подтверждение включения SecureNAT

### Установка VPN-клиента

- Перейдите на виртуальную машину Клиент.
- Загрузите установочный дистрибутив из папки \\serverbd\Студенческая\ИБ\softether-vpnclient-v4.28-9669-beta-2018.09.11-windows-x86\_x64-intel.exe и перенесите на виртуальную машину. Если это не возможно, скачайте дистрибутив по адресу [https://github.com/SoftEtherVPN/SoftEtherVPN\\_Stable/releases/download/v4.28-9669-beta/softether-vpnclient-v4.28-9669-beta-2018.09.11-windows-x86\\_x64-intel.exe](https://github.com/SoftEtherVPN/SoftEtherVPN_Stable/releases/download/v4.28-9669-beta/softether-vpnclient-v4.28-9669-beta-2018.09.11-windows-x86_x64-intel.exe)
- Запустите скачанный дистрибутив. На всех шагах установки нажимайте Далее и Да. На одном из шагов выберите SoftEther VPN Client (Рисунок 27)

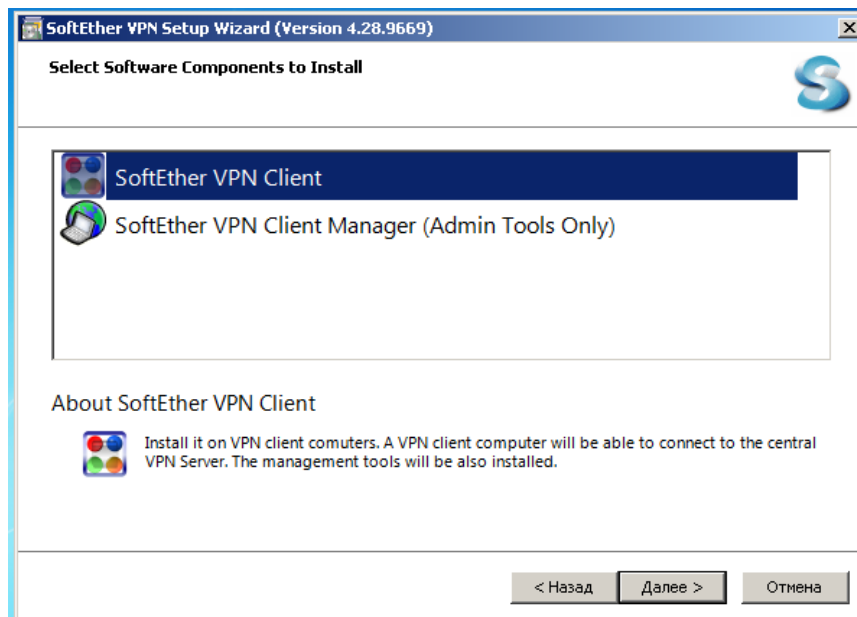


Рисунок 27 – Установка VPN-Клиента

- После установки запустится SoftEther VPN Client Manager (Рисунок 28). Это система управления VPN-соединениями. Если приложение не запустилось, запустите его ярлыком в рабочего стола.

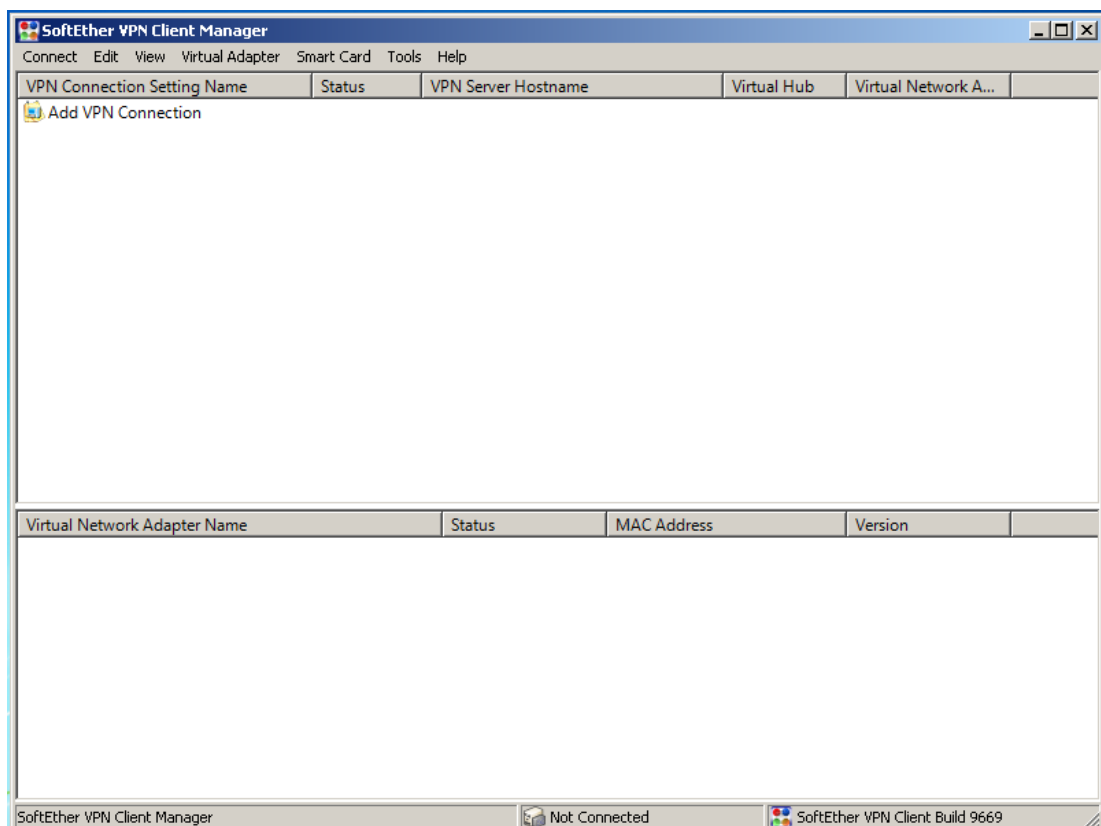


Рисунок 28 - SoftEther VPN Client Manager

- Теперь необходимо добавить новый виртуальный VPN-адаптер. Это виртуальная сетевая карта, через которую устанавливается VPN-соединение.



Для этого нажмите правой кнопкой мыши в нижней части окна и выберите “New Virtual Network Adapter” (Рисунок 29)

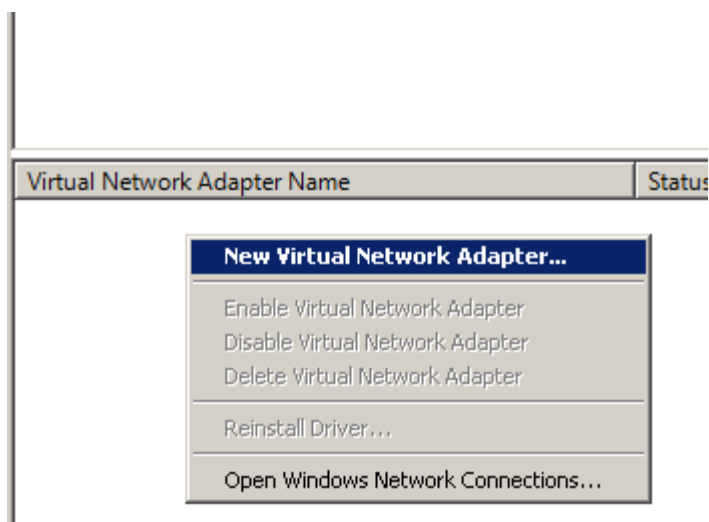


Рисунок 29 – Добавление VPN-адаптера

- Укажите название нового адаптера “VPN” Рисунок 30.

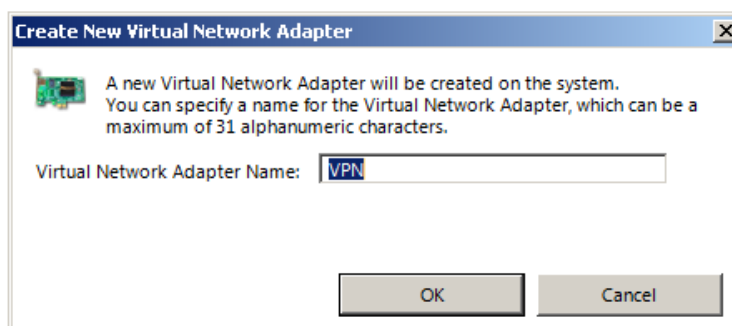


Рисунок 30 – Имя нового адаптера

- В нижней части главного окна Client Manager должен появиться новый адаптер.
- Теперь создадим VPN подключение. Для этого нажмите правой кнопкой мыши на Add VPN Connection и выберите “New VPN Connection” (Рисунок 31)

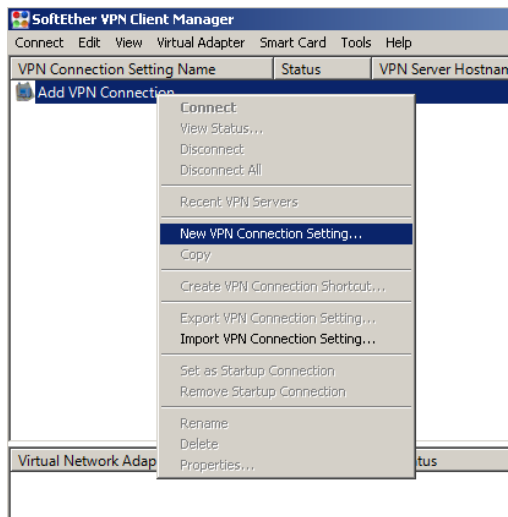


Рисунок 31 – Добавить VPN-подключение

- Откроется окно конфигурации VPN-соединения (Рисунок 32). Задайте IP-адрес VPN-сервера (192.168.10.1) порт 443. Так же укажите имя пользователя user1 пароль 123 и способ аутентификации Standart Password Authentication. Нажмите ОК для закрытия окна.

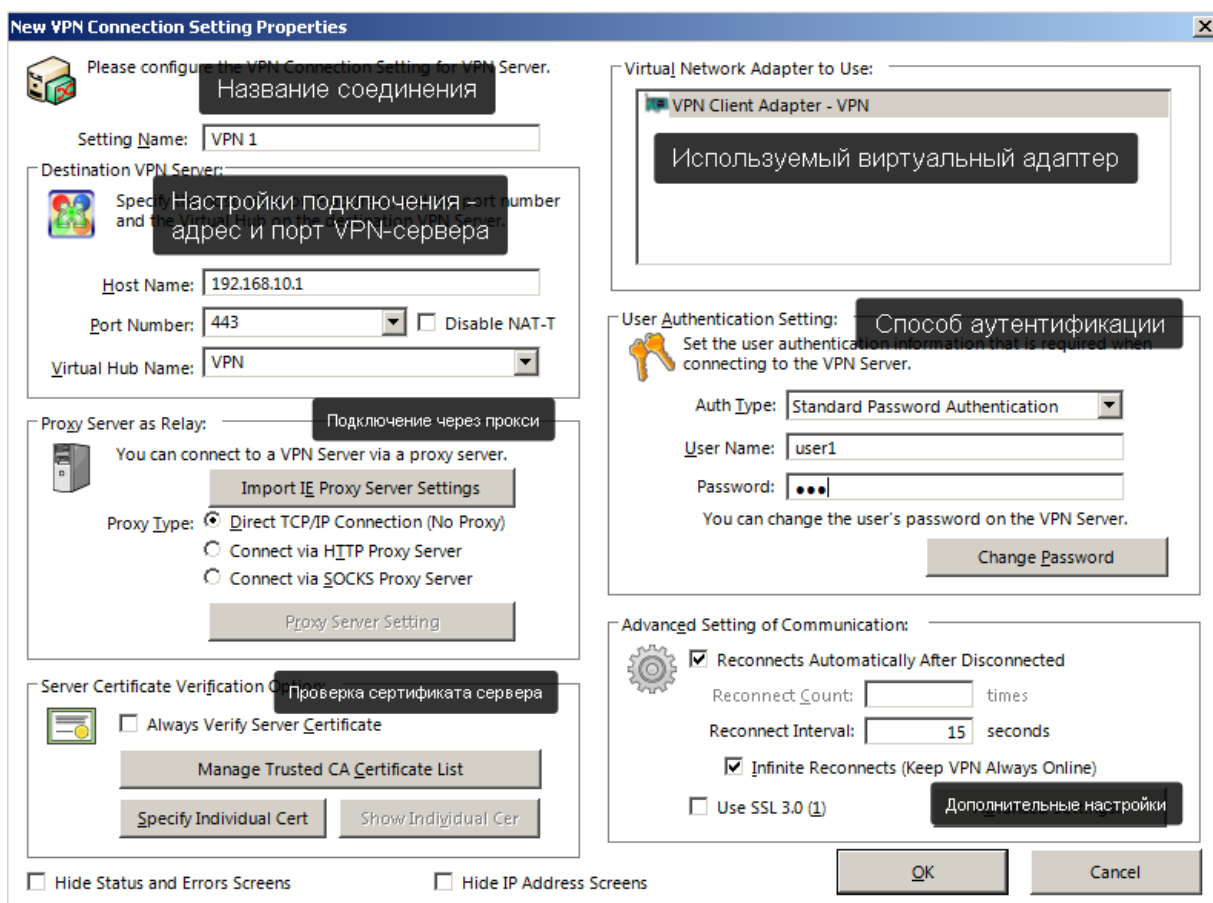


Рисунок 32 – Настройка исходящего VPN-соединения

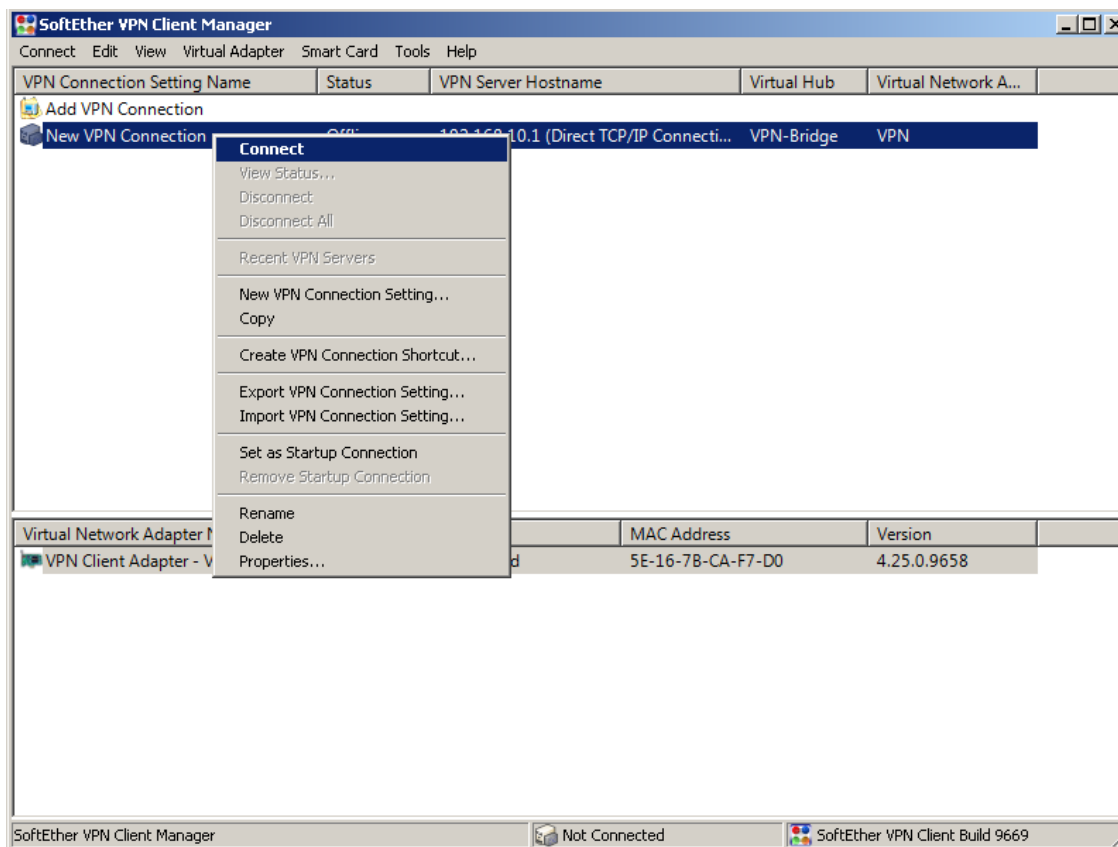


Рисунок 33 – Подключение в VPN серверу

- В главном окне программы нажмите правой кнопкой на созданное подключение и кликните на пункт Connect. (Рисунок 33). Надпись в столбце статус должна поменяться на Connected.
- Запустите на Клиенте браузер и перейдите по адресу <https://yandex.ru> если все сделано правильно, сайт откроется.

### Самостоятельная работа.

- 1) Определите какие IP-адреса используются на Клиенте
- 2) Разрешите на брандмауэре Шлюза соединение по портам использующиеся для VPN. Включите брандмауэр. Проверьте, что клиент VPN может подключиться к VPN-серверу.
- 3) Просканируйте Шлюз с помощью Zenmap. Определите какие порты открыты, и какие службы на них определяются (опция `-sV`).

### Контрольные вопросы:

1. Что такое VPN? Для чего он используется?
2. Какие виды VPN соединений существуют? Для чего они применяются?
3. Какие порты использует SoftEther Server для входящих подключений?

4. Что такое NAT? Для чего он используется?
5. Что такое DHCP? Для чего он используется?
6. Что такое SecureNAT и для чего используется?

*Список литературы:*

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## Лабораторная работа №8. Применение криптографии для безопасности данных. Использование криптосистем PGP TrueCrypt.

### Цель работы:

Изучить применение методов современной криптографической защиты для безопасности данных.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### *Теоретическая часть.*

Криптография (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в зашифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

В данной лабораторной работе рассматриваются два криптографических инструмента – GnuPG и VeraCrypt.

GNU Privacy Guard (GnuPG, GPG) — свободная программа для шифрования информации и создания электронных цифровых подписей. Разработана как альтернатива PGP и выпущена под свободной лицензией GNU General Public License. GnuPG полностью совместима со стандартом IETF OpenPGP. Текущие версии GnuPG могут взаимодействовать с PGP и другими OpenPGP-совместимыми системами.

GnuPG шифрует сообщения, используя асимметричные пары ключей, генерируемые пользователями GnuPG. Открытыми ключами можно обмениваться с другими пользователями различными путями, в том числе и через Интернет с помощью серверов ключей. Также GnuPG позволяет добавлять криптографическую цифровую подпись к сообщению, при этом целостность и отправитель сообщения могут быть проверены.

GnuPG не использует запатентованное или иначе ограниченное программное обеспечение и/или алгоритмы, включая алгоритм IDEA, который представлен в PGP почти с самого начала. GnuPG использует другие непатентованные алгоритмы CAST5, 3DES, AES, Blowfish и Twofish. Тем не менее, возможно использование в GnuPG и алгоритма IDEA с помощью дополнительного модуля.

GnuPG — это гибридное криптографическое программное обеспечение, которое использует комбинацию стандартного шифрования с помощью симметричных ключей и шифрования с открытым ключом для безопасного обмена ключами, открытый ключ получателя необходим для шифрования ключа сессии, используемого единожды. Такой режим работы является частью стандарта OpenPGP и частью PGP в его первой версии.

VeraCrypt — программное обеспечение, используемое для шифрования «на лету». VeraCrypt является бесплатным и открытым проектом, который был начат 22 июня 2013 года в качестве форка TrueCrypt. Запущен и поддерживается Mounir Idrassi, основателем компании IDRIX, в том числе в настоящее время, после того как 28 мая 2014 года было объявлено о прекращении поддержки программы TrueCrypt.

#### Оборудование и материалы.

Персональный компьютер, виртуальная машина, дистрибутив VeraCrypt Setup 1.23-Hotfix-2.exe.

#### Указания по технике безопасности:

Соответствуют технике безопасности по работе с компьютерной техникой.

### Задания

## **1. VeraCrypt**

### **1.1. Установка**

- Запустите виртуальную машину. Загрузите на нее установочный дистрибутив VeraCrypt Setup 1.23-Hotfix-2.exe и запустите его.
- Установите программу (Рисунок 1-5)

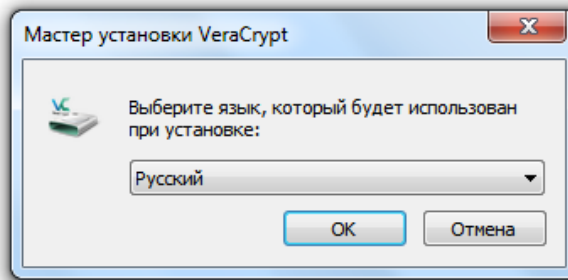


Рисунок 1 – Выбор языка

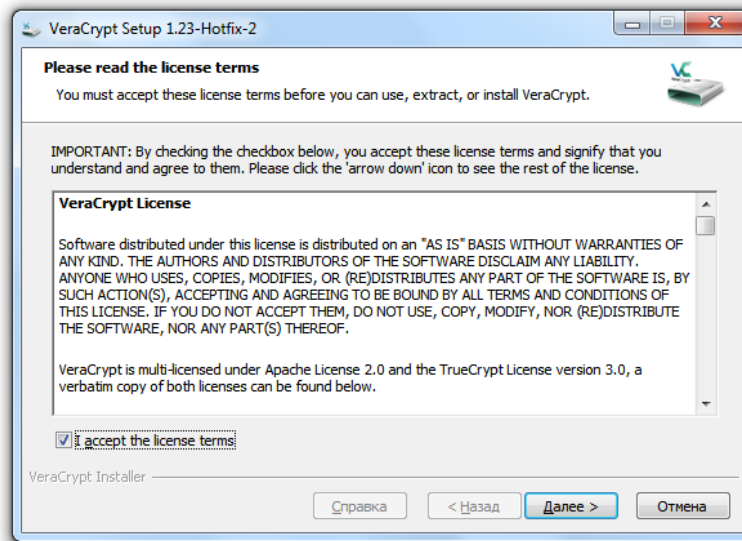


Рисунок 2 – Лицензионное соглашение

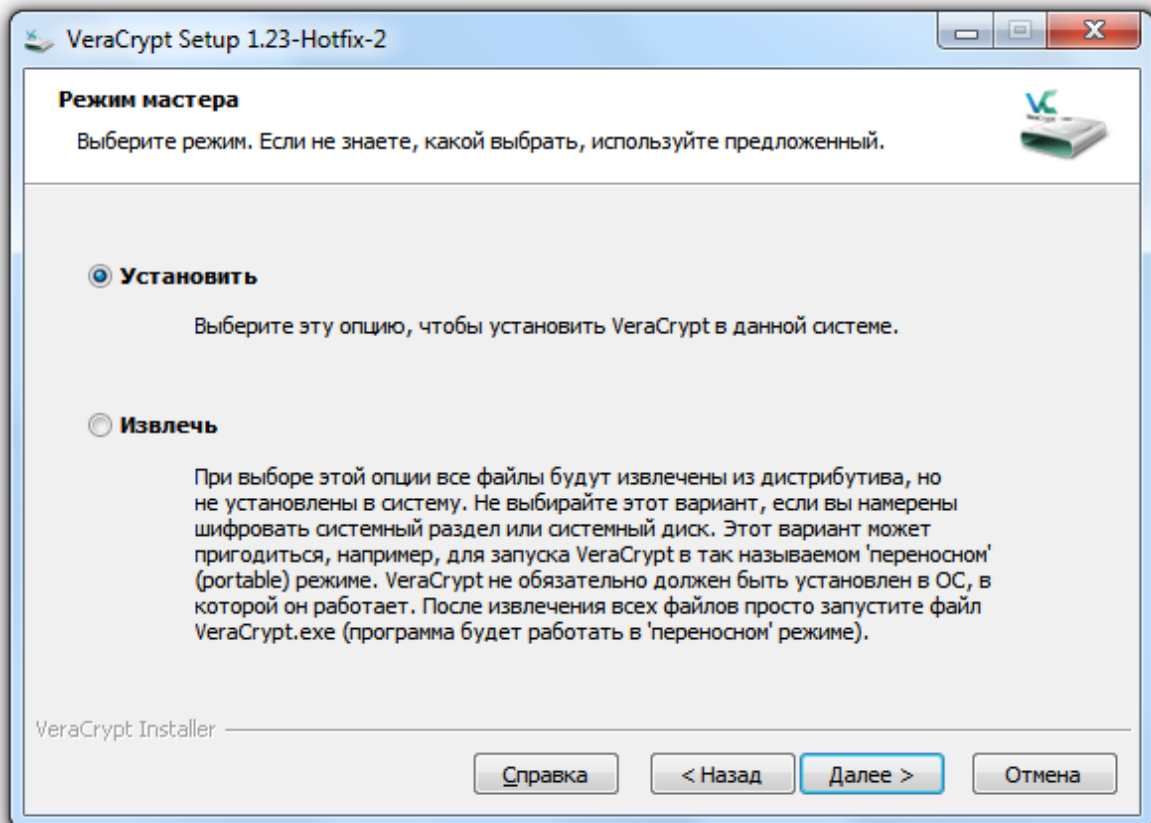


Рисунок 3 – Режим установки

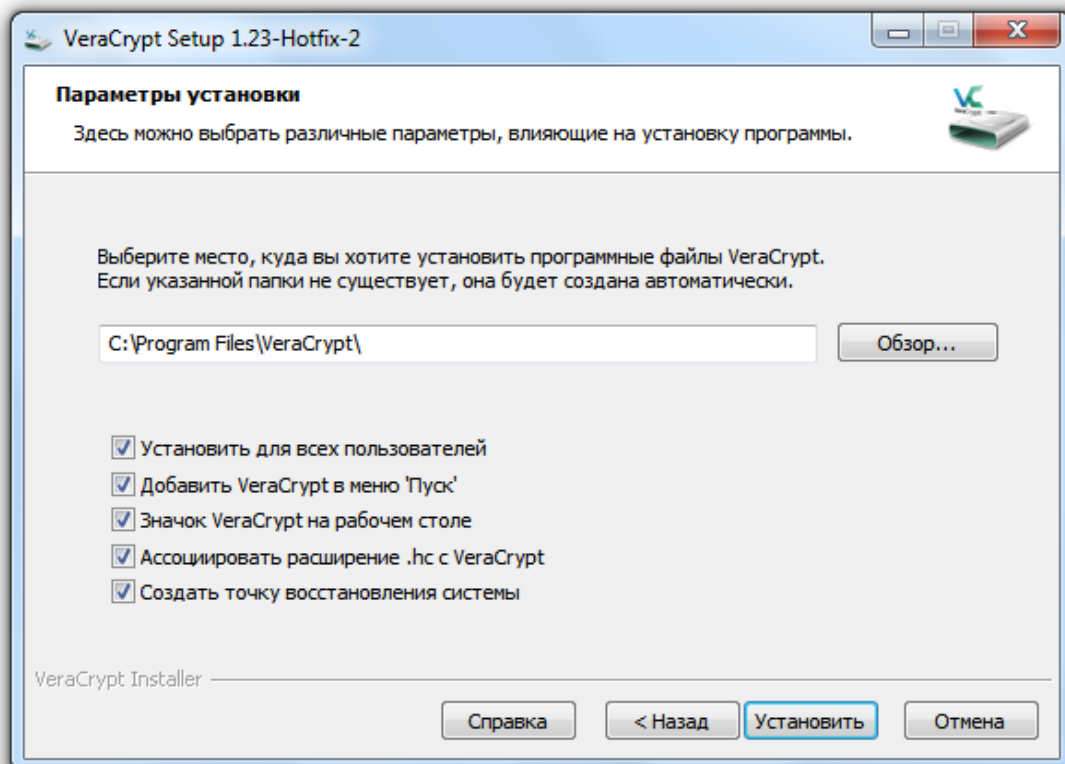


Рисунок 4 – Путь установки



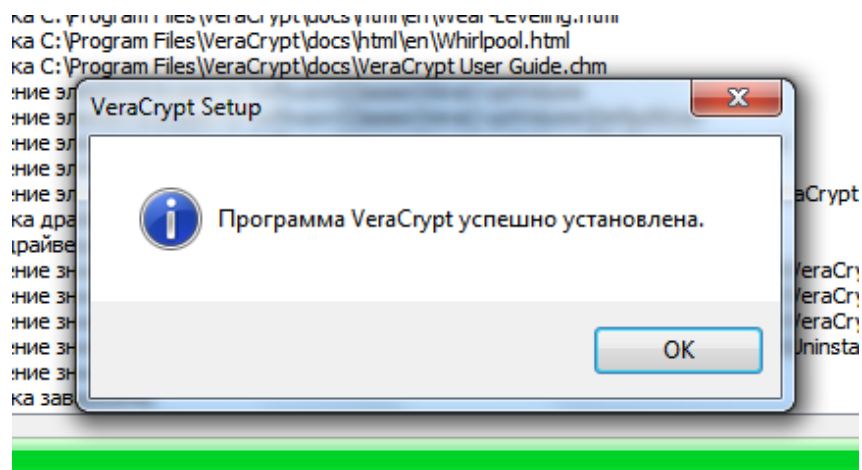


Рисунок 5 – Установка завершена

## 1.2. Локализация (если интерфейс программы на английском)

- Запустите VeraCrypt (ярлыком с рабочего стола), откроется главное окно программы (Рисунок 6).
- Включите русский язык в настройках (Рисунок 7-8)

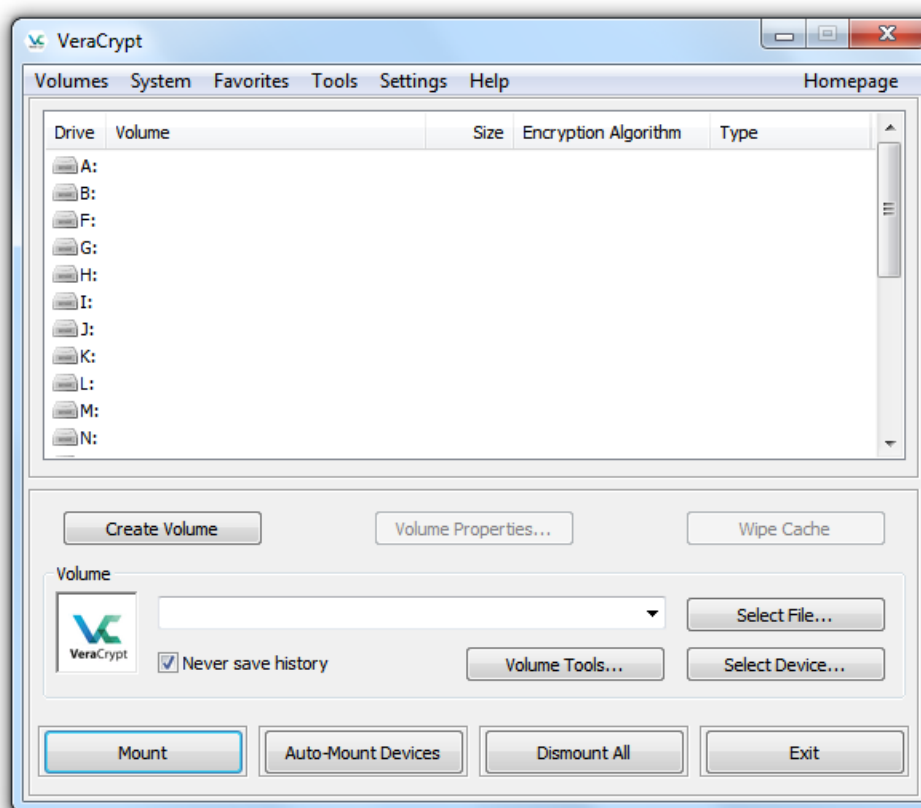


Рисунок 6 – Главное окно VeraCrypt

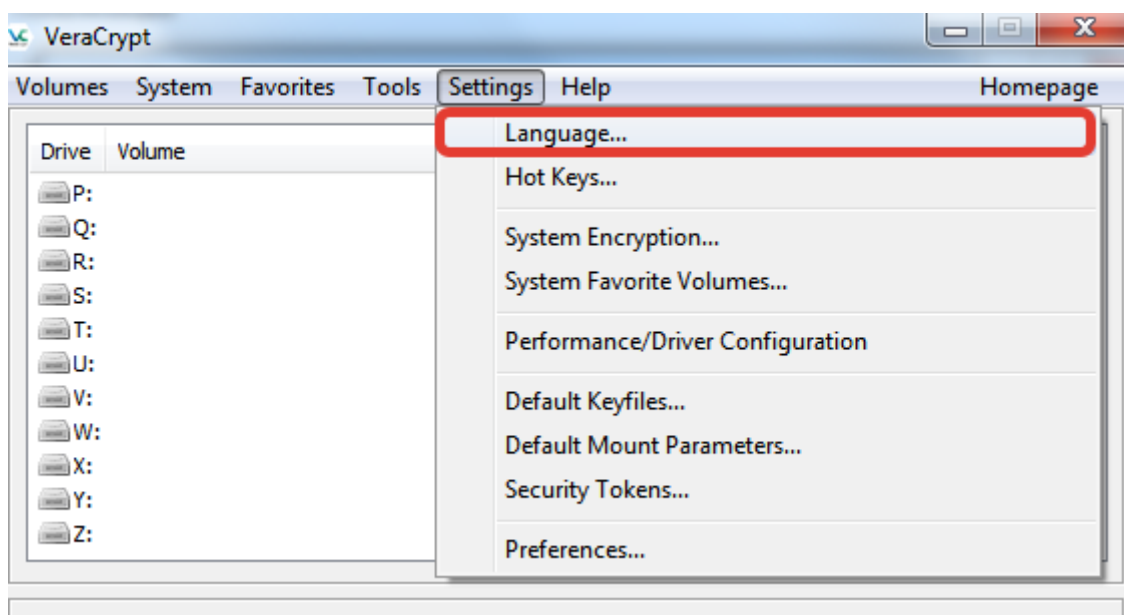


Рисунок 7 – Меню Settings -> Language

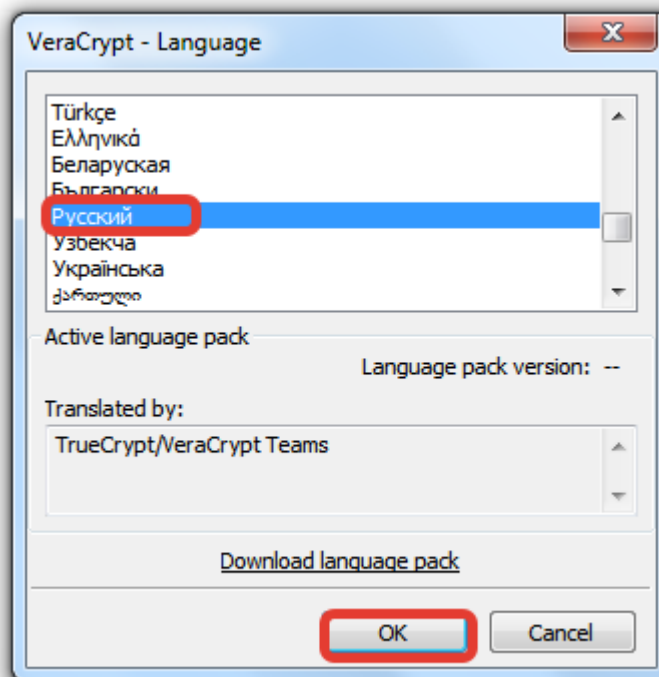


Рисунок 8 – Выбор языка

### 1.3. Создание зашифрованного контейнера

Ключевым понятием в VeraCrypt является том. Том это файл (контейнер) или физический диск/раздел диска зашифрованный VeraCrypt, подключаемый к компьютеру как внешний накопитель (как флешка). Для создания нового тома нажмите создать том (Рисунок 9).

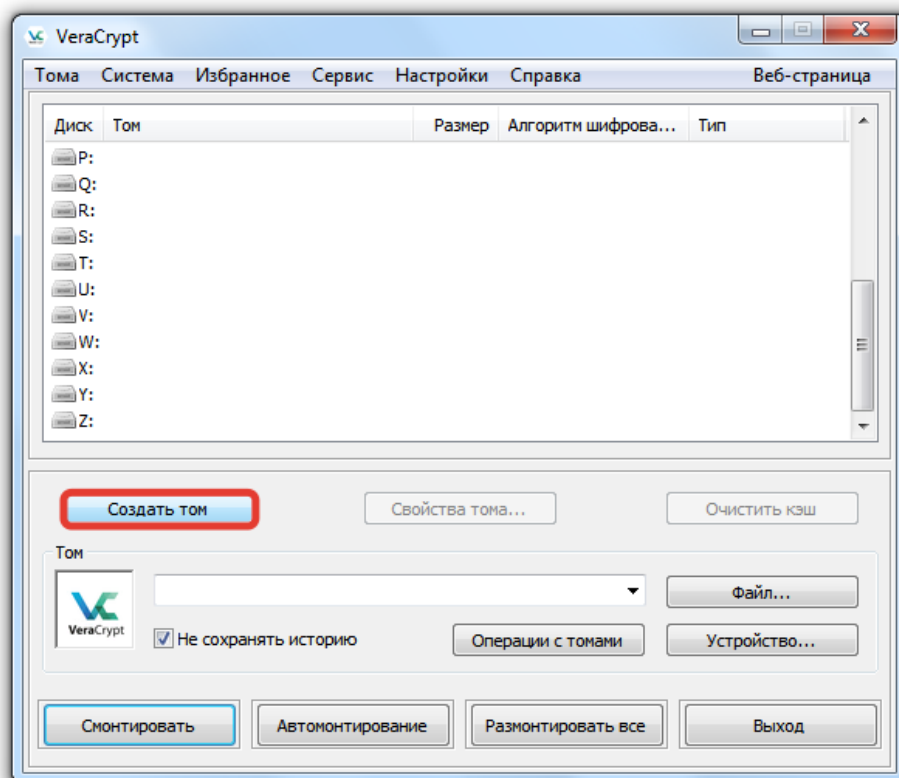


Рисунок 9 – Создание тома

Запустится мастер создания томов (Рисунок 10). Выберите “Создать зашифрованный файловый контейнер” (наш зашифрованный том будет храниться в файле) и нажмите далее.

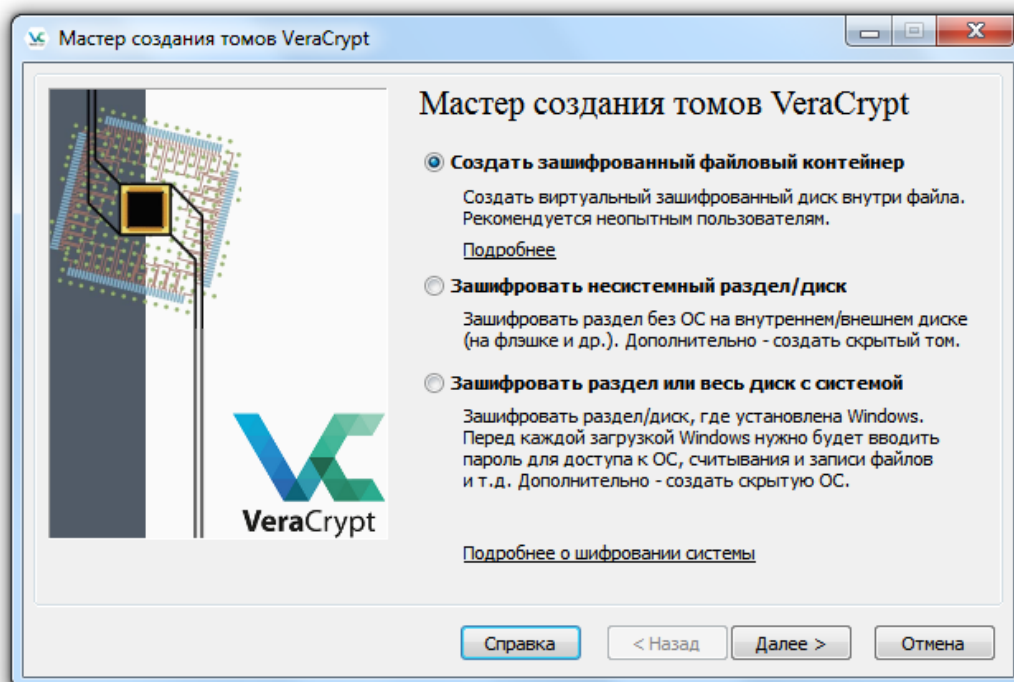


Рисунок 10 – Выбор типа контейнера

На следующем шаге требуется выбрать тип тома. Прочтите описание, выберите “Обычный том” и нажмите Далее. (Рисунок 11)

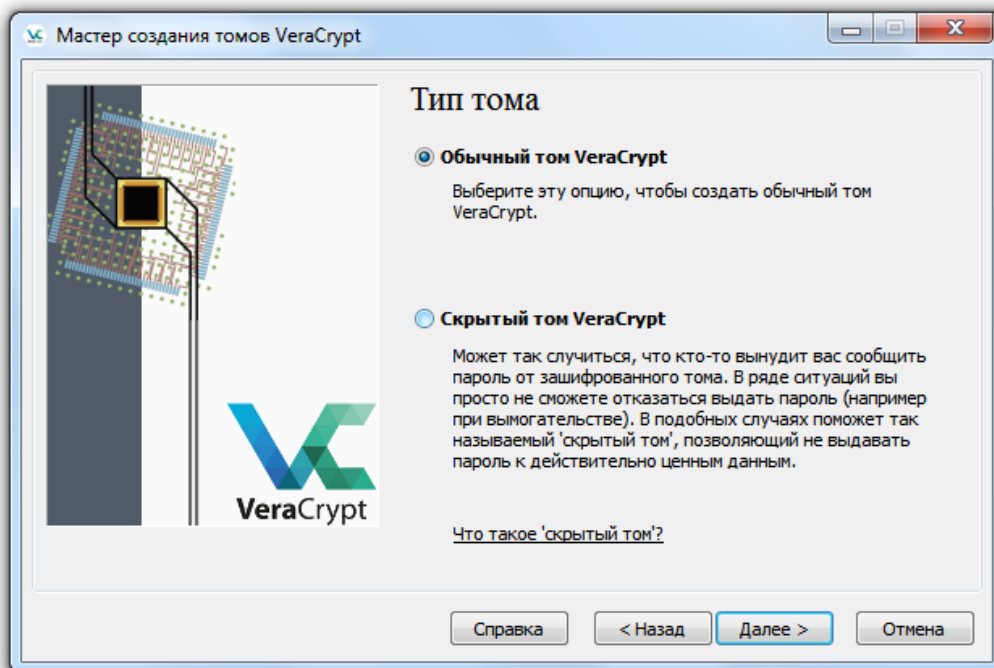


Рисунок 11 – Выбор типа тома

Поскольку том размещается в обычном файле укажите его имя и местоположение. Можете создать его на рабочем столе, с именем “SecretDisk” (Рисунок 12)

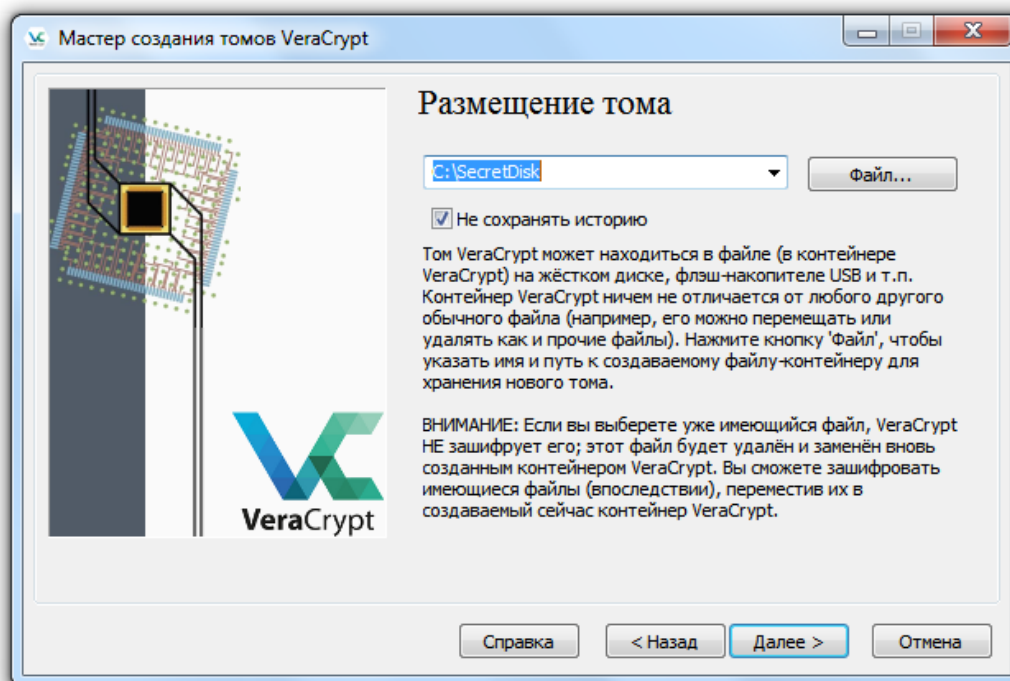


Рисунок 12 – Размещение тома

На следующем шаге выбирается алгоритм шифрования и хэширования. Укажите AES и SHA-512 и нажмите далее. (Рисунок 13)

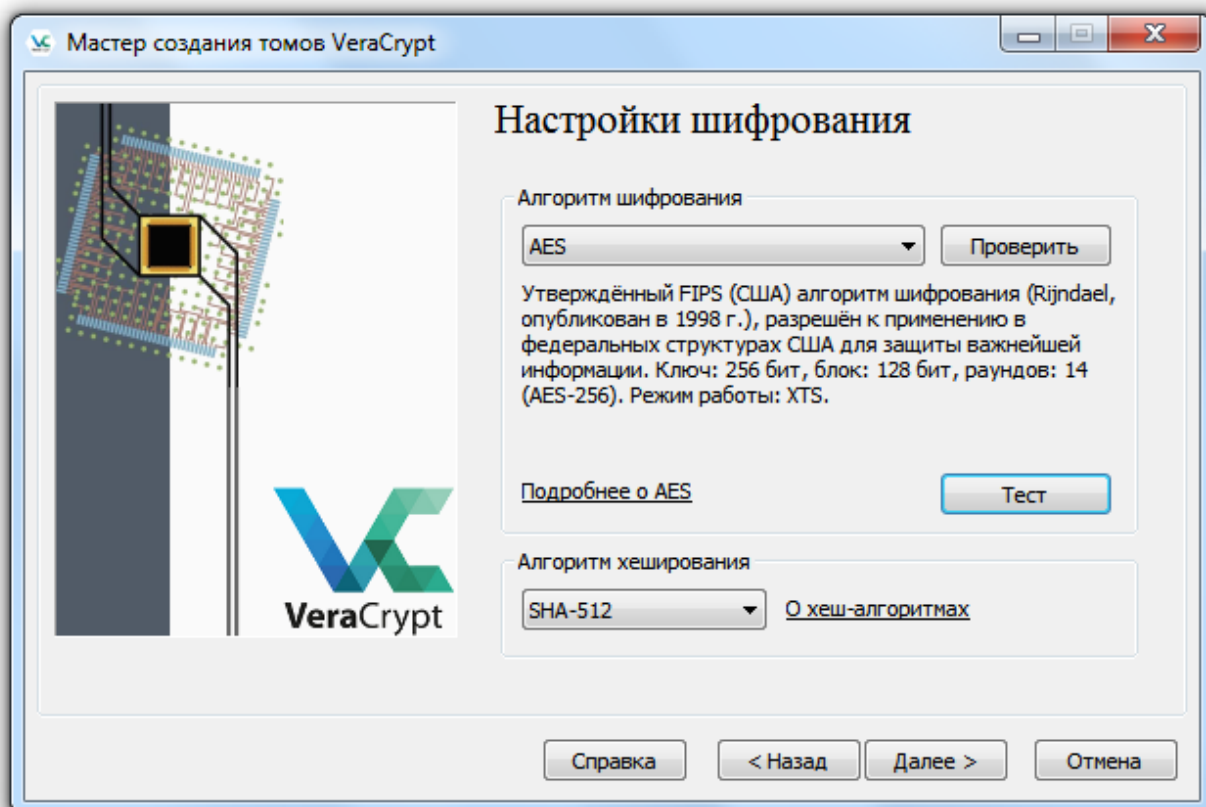


Рисунок 13 – Настройки шифрования

На этом шаге задайте размер накопителя. В данном примере 20 МБ.

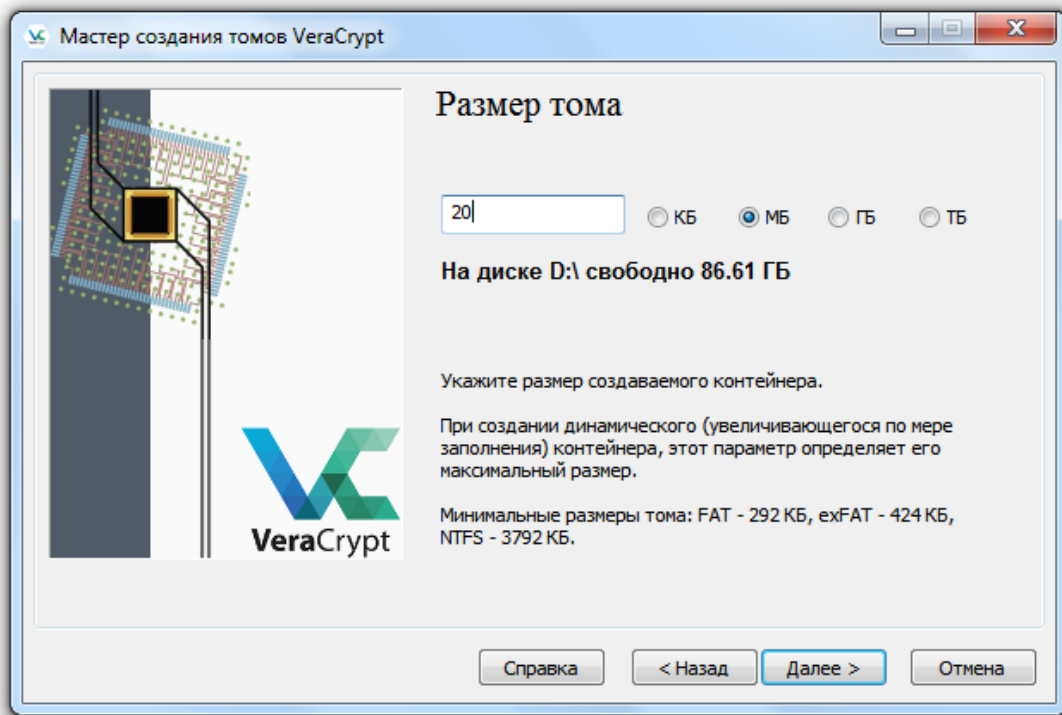


Рисунок 14 – Размер шифрованного тома

Теперь укажите тип файловой системы для тома (NTFS) и двигайте мышью в окне программы для генерации случайных чисел которые используются для шифрования данных.

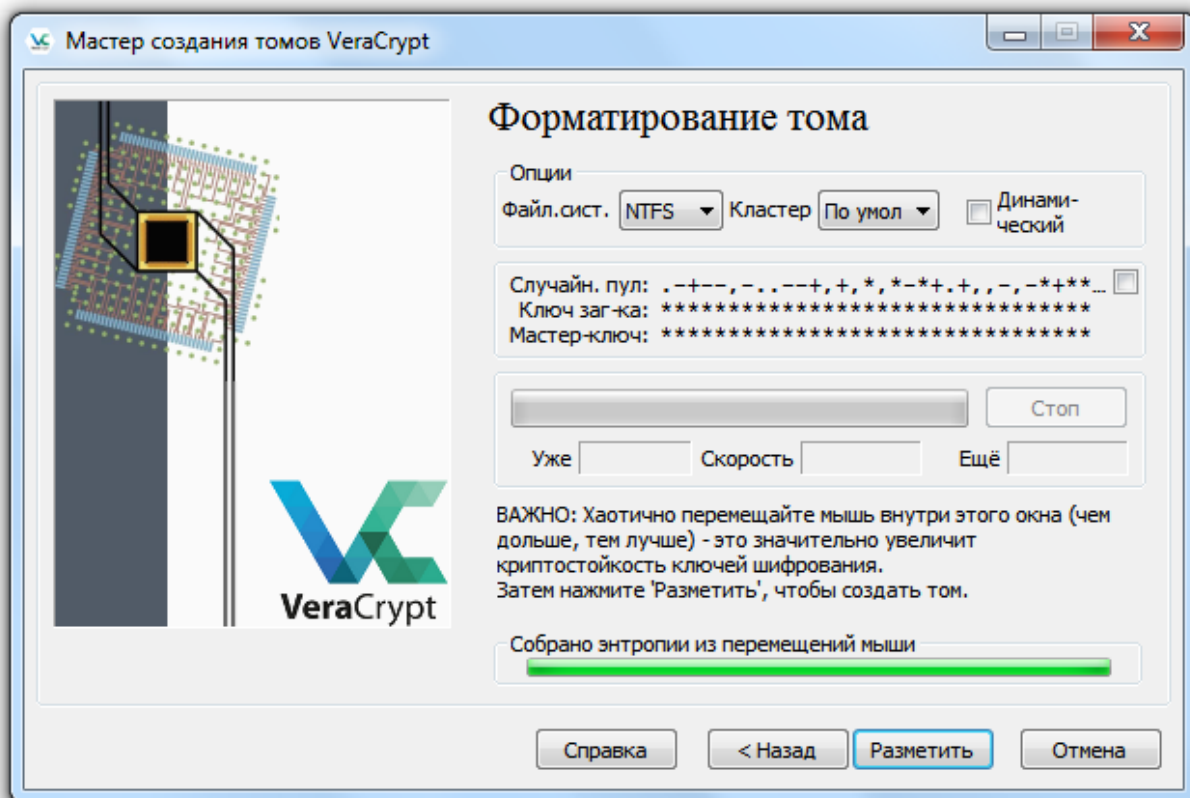


Рисунок 15 – Файловая система

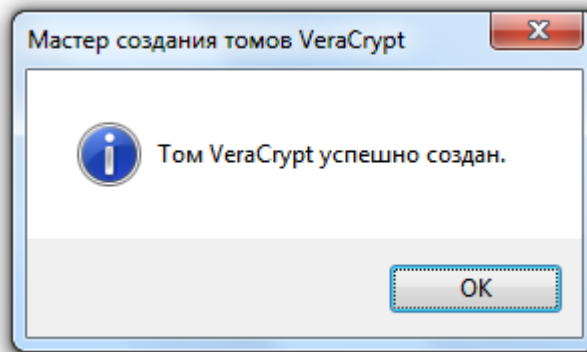


Рисунок 16 – Том создан

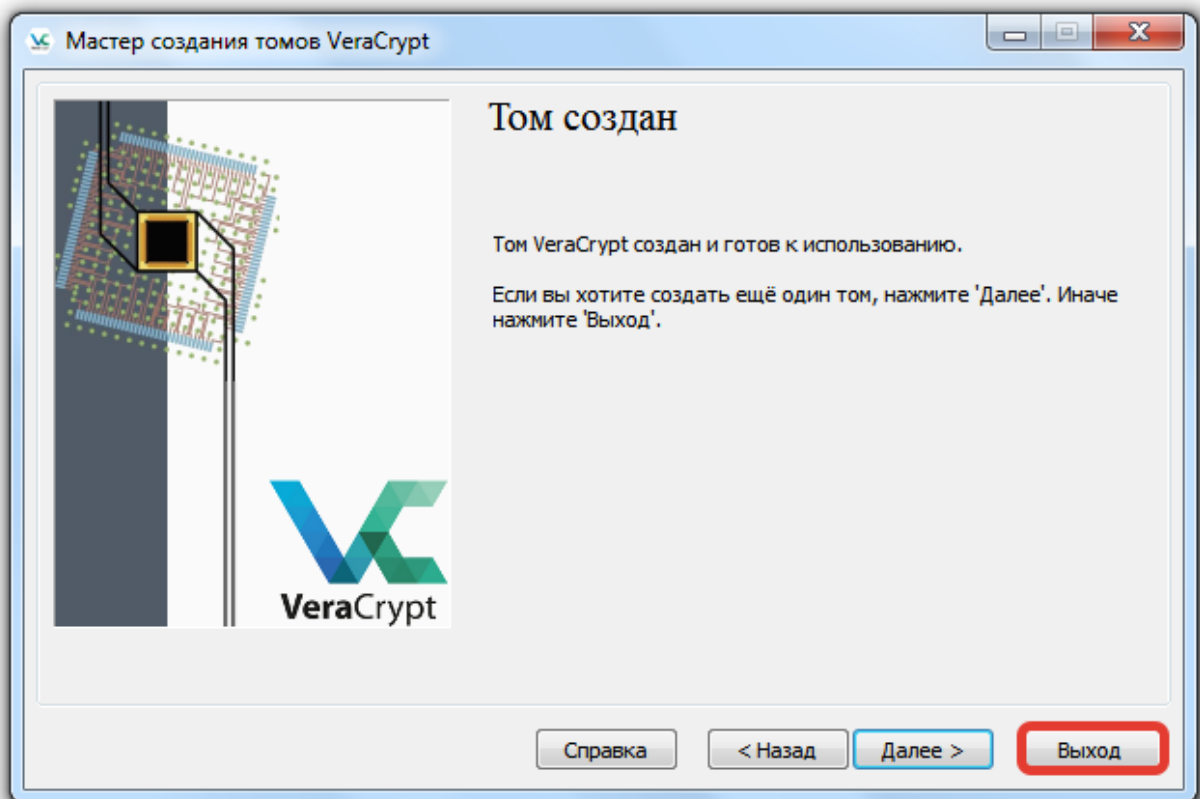


Рисунок 17 – Завершение создания тома

После того как том создан, нажмите Выход.

#### 1.4. Подключение и отключение контейнера

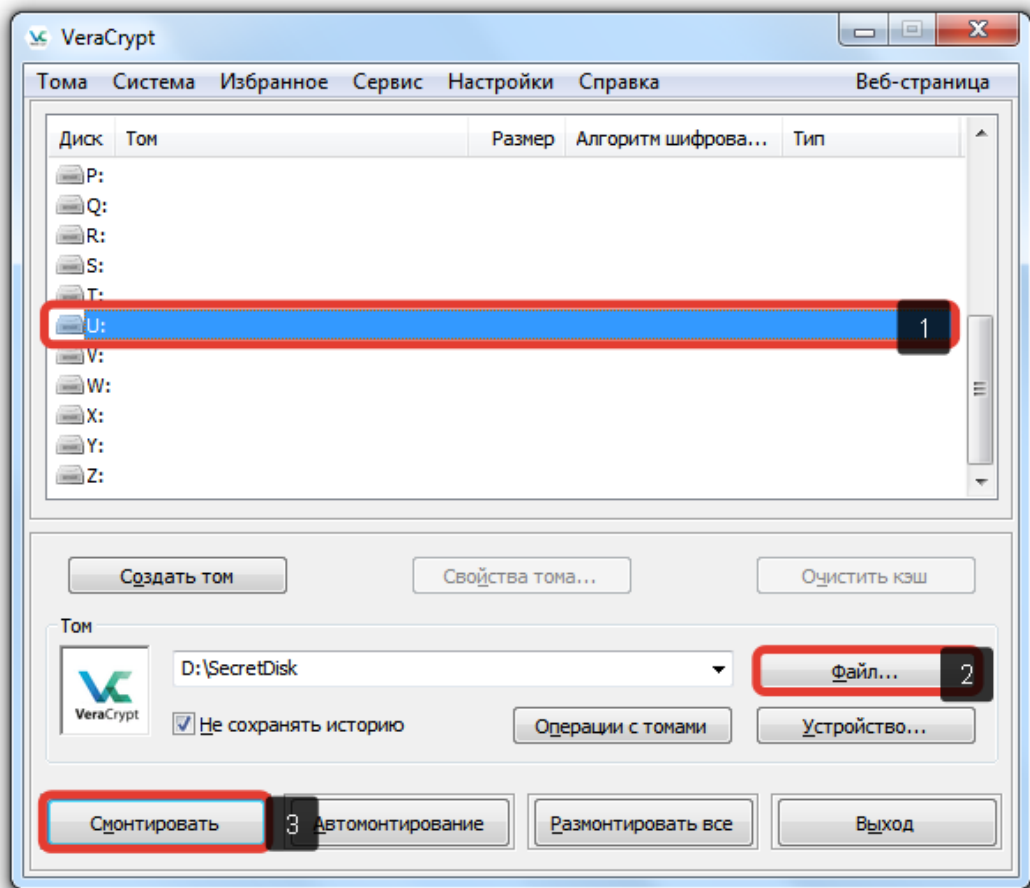


Рисунок 18 – Подключение зашифрованного тома

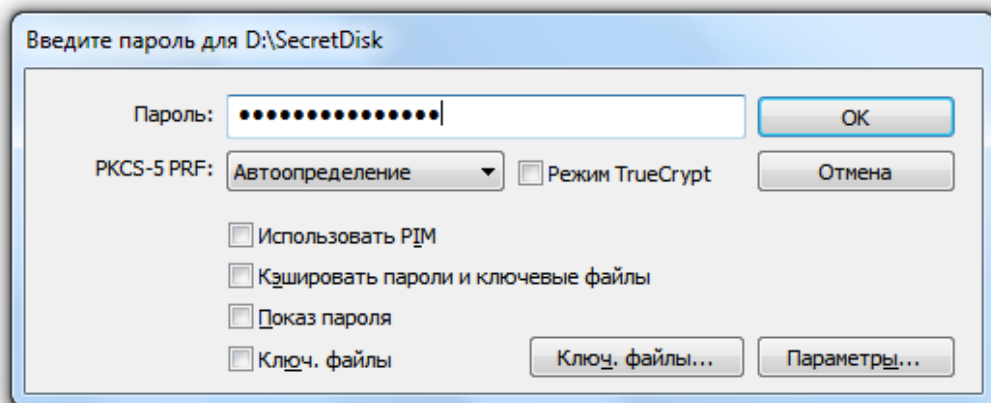


Рисунок 19 – Ввод пароля



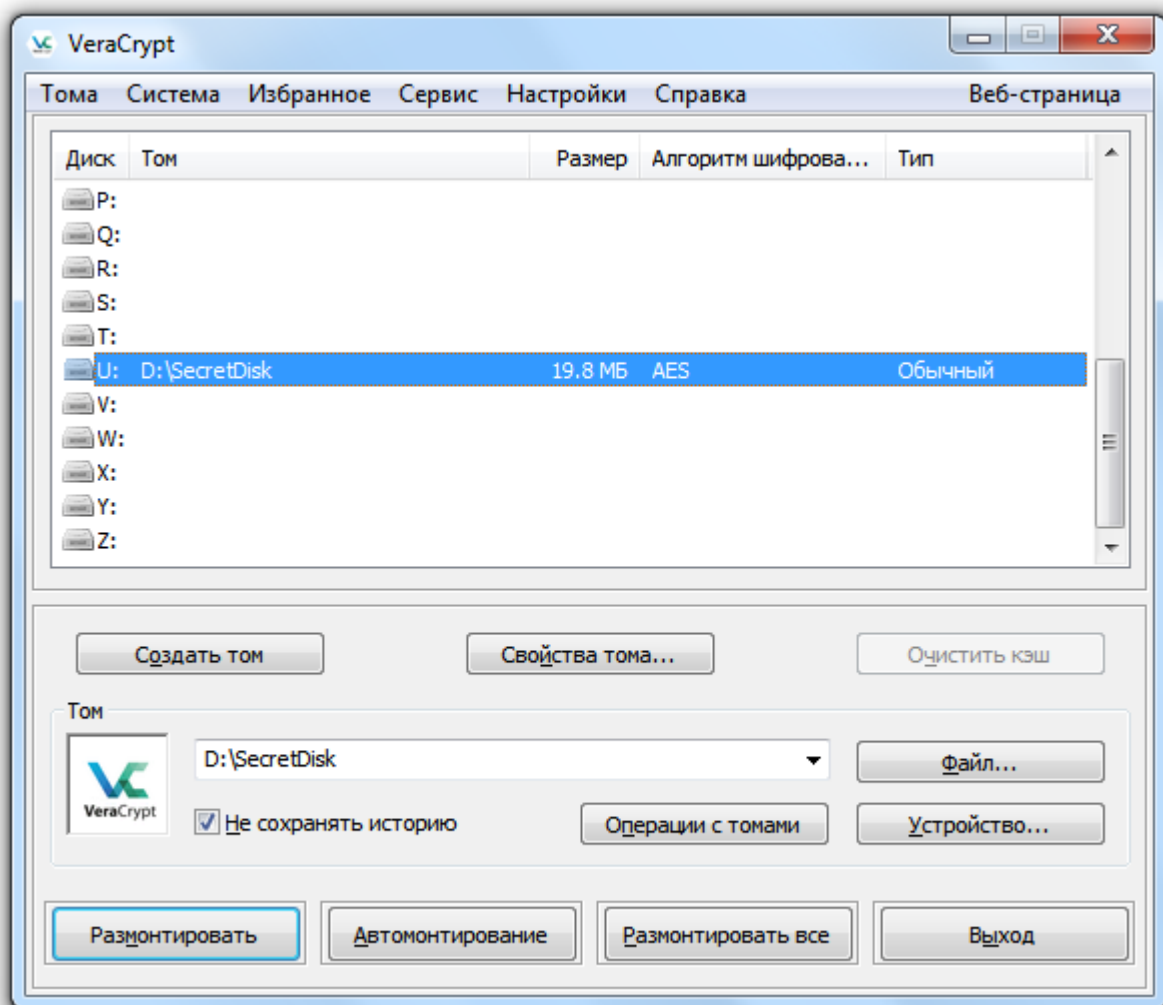


Рисунок 20 – Том подключен

Самостоятельно задание – создайте зашифрованный том размером 300 Мб, алгоритм шифрования Twofish, алгоритм хэширования SHA-256, файловая система NTFS.

## 2. **GnuPG**

Криптосистема PGP позволяет решить проблему передачи ключа по открытому каналу, т.к. для шифрования и расшифровки используются различные ключи. Кроме этого, эта система позволяет подтвердить авторство и целостность переданного документа. Для этого используется электронная подпись.

Целостность информации – это означает, что данные не были изменены. Авторство удостоверяется использованием приватного ключа, подразумевается, что приватный ключ шифрования есть только у его владельца.

Электронная подпись – это контрольная сумма файла (как правило хэш) зашифрованная с помощью приватного ключа. С помощью публичного ключа, ее можно расшифровать и проверить, если контрольная сумма в электронной подписи совпадает с текущей контрольной суммой переданного документа, то можно заключить, что документ подлинный и изменений в него не вносилось.

### 2.1. **Установка GnuPG**

Запустите виртуальную машину. Загрузите на нее установочный дистрибутив GnuPG `gpg4win-3.1.5.exe` и запустите его. Процесс установки приведен на Рисунках 21-26.

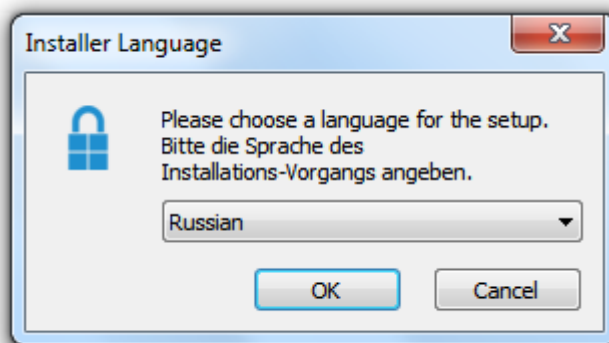


Рисунок 21 – Выбор языка установки

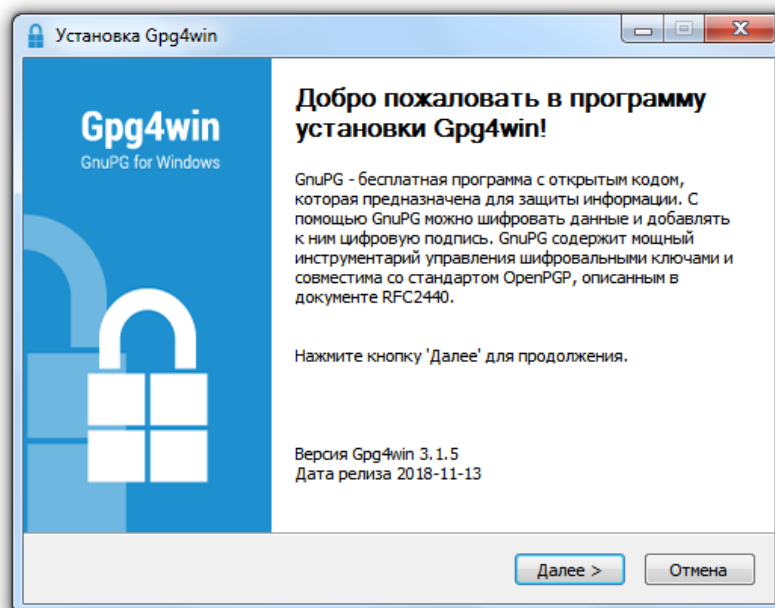


Рисунок 22 – Установка Gpg4Win

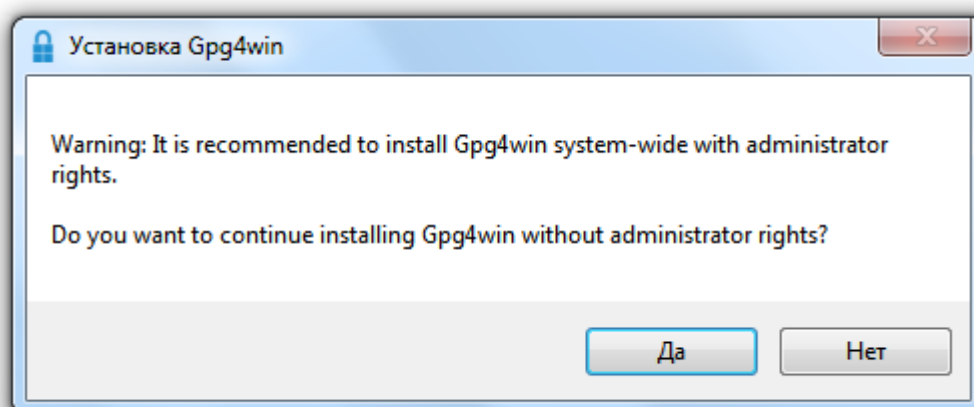


Рисунок 23 – Запрос прав администратора

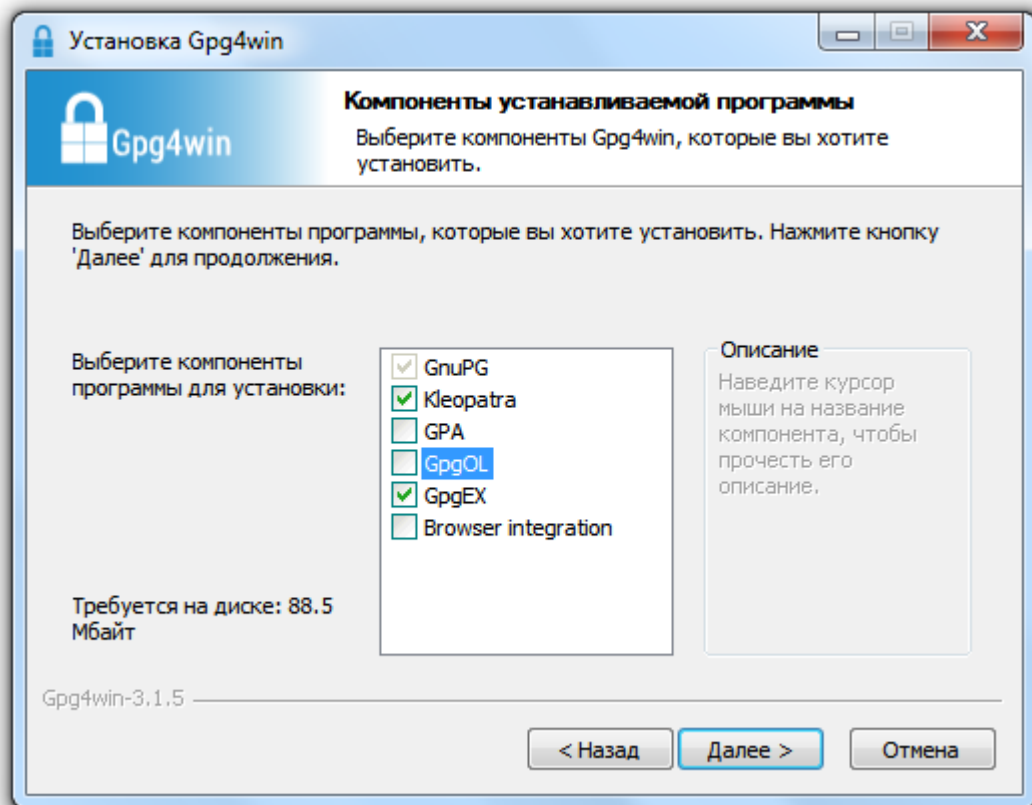


Рисунок 24 – Выбор компонентов

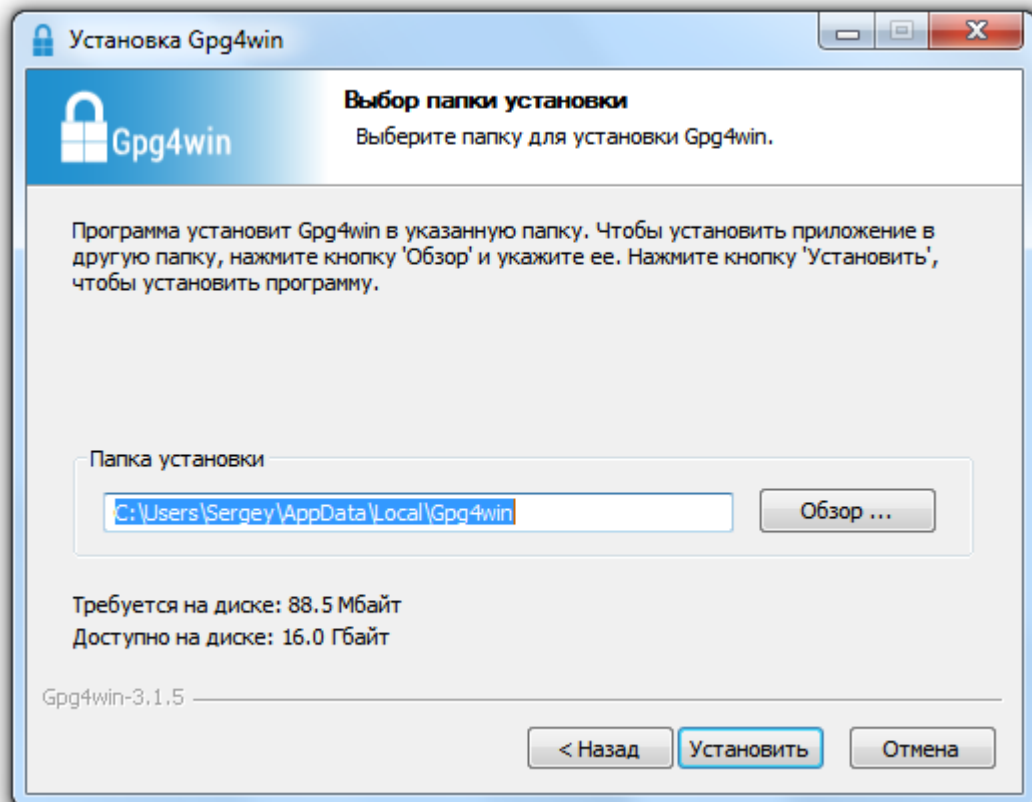


Рисунок 25 – Путь установки

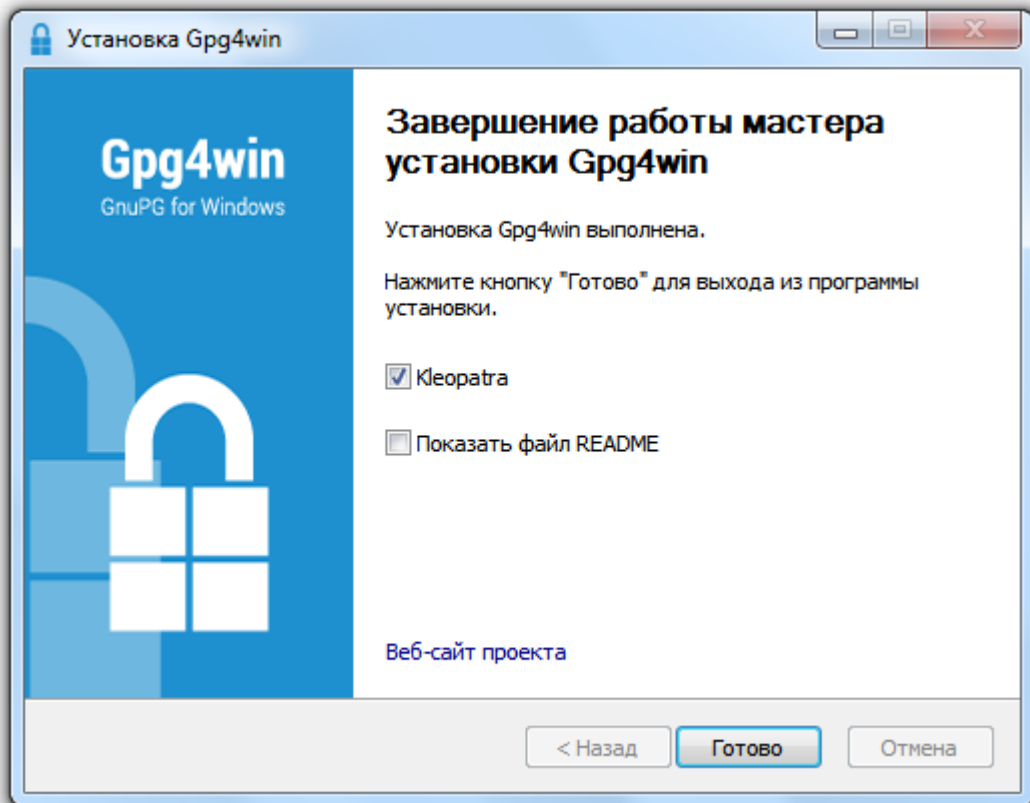


Рисунок 26 – Установка завершена

## 2.2 Генерация пары ключей и импорт ключей

Для шифрования и создания электронной подписи файлов, требуется создать личную пару ключей. Процесс приведен на рисунках 27-32 . Используйте свое ФИО при создании пары ключей (Рисунок 29). В целях безопасности, приватный ключ шифруется симметричным алгоритмом, на шаге показанном на рисунке 31 введите пароль 1234567890.

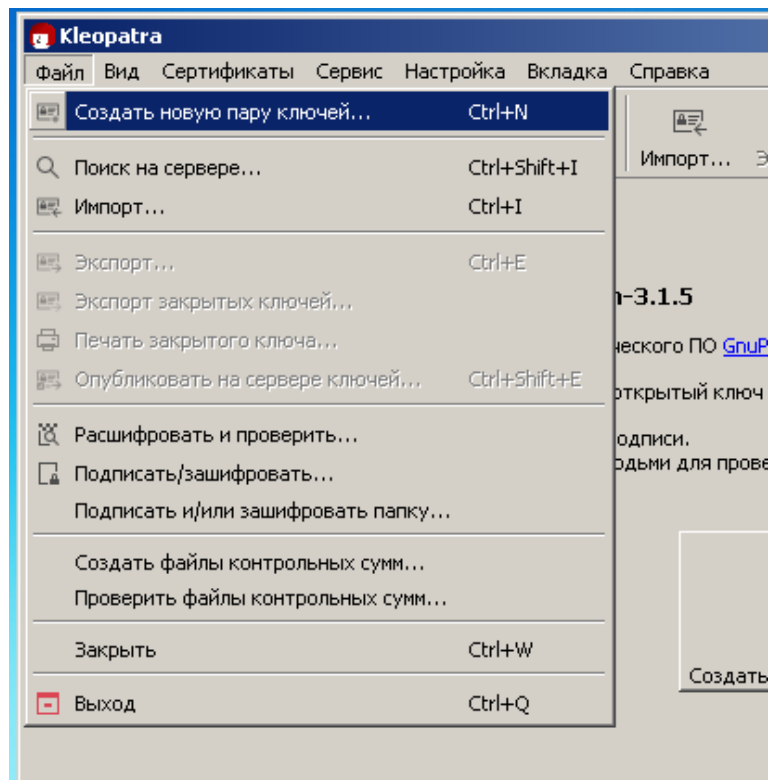


Рисунок 27 – Создание новой пары ключей

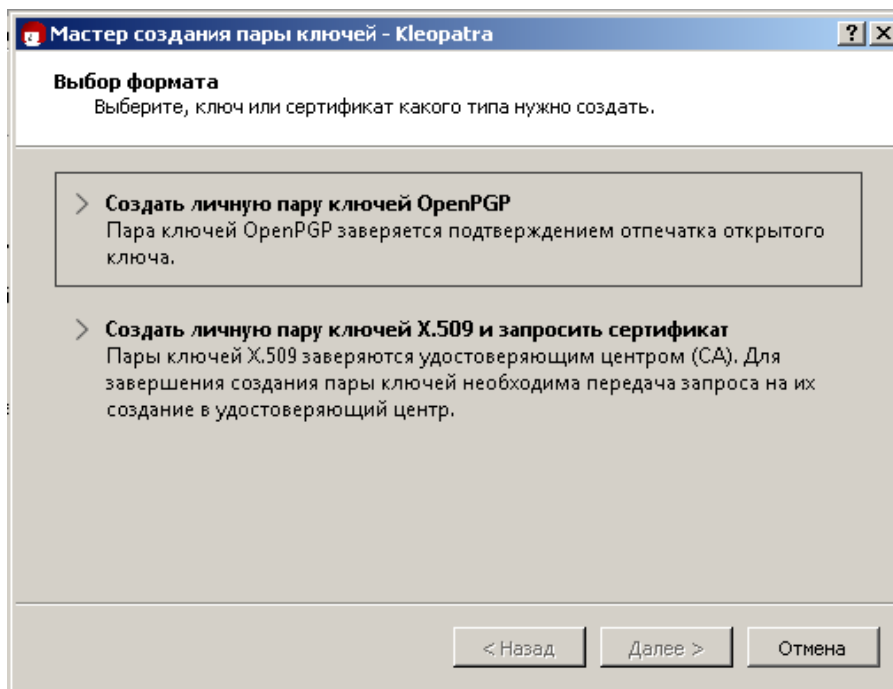


Рисунок 28 – Выбор формата ключей

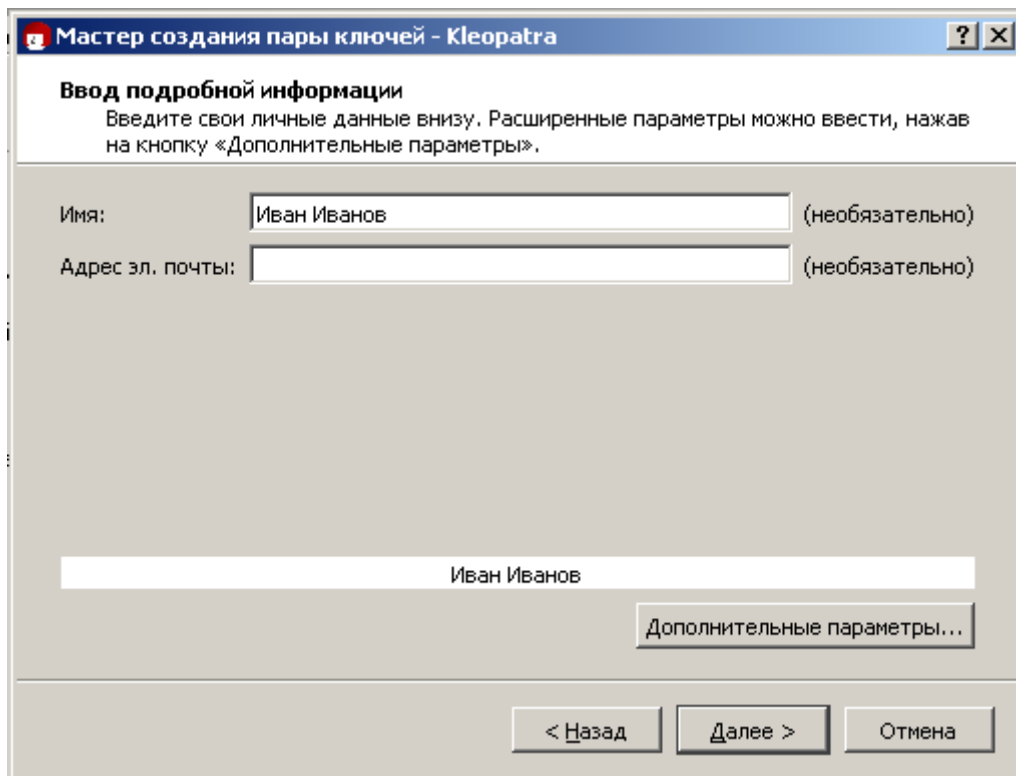


Рисунок 29 – Ввод информации о владельце ключей

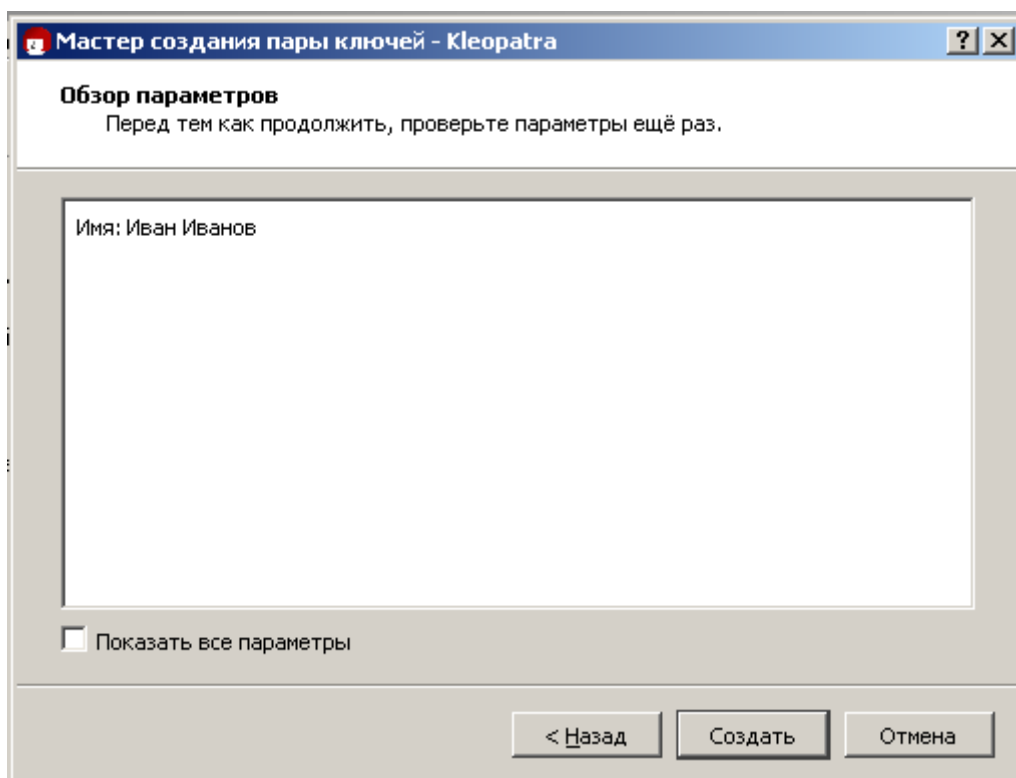


Рисунок 30 – Просмотр параметров

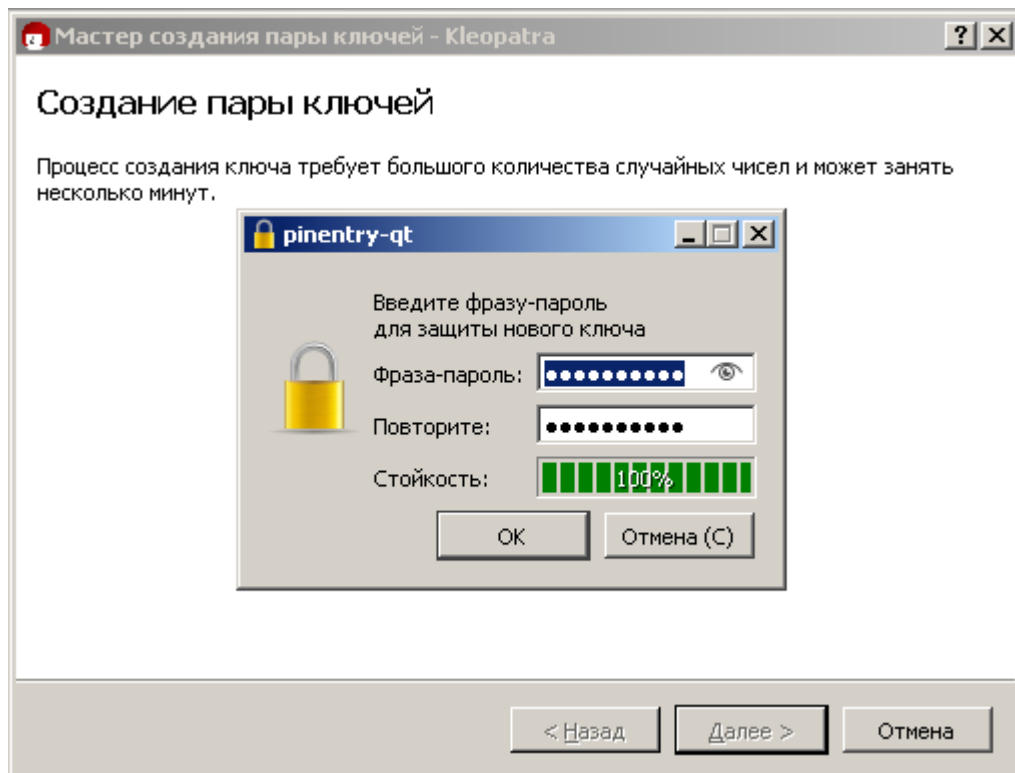


Рисунок 31 – Ввод пароля для шифрования приватного ключа

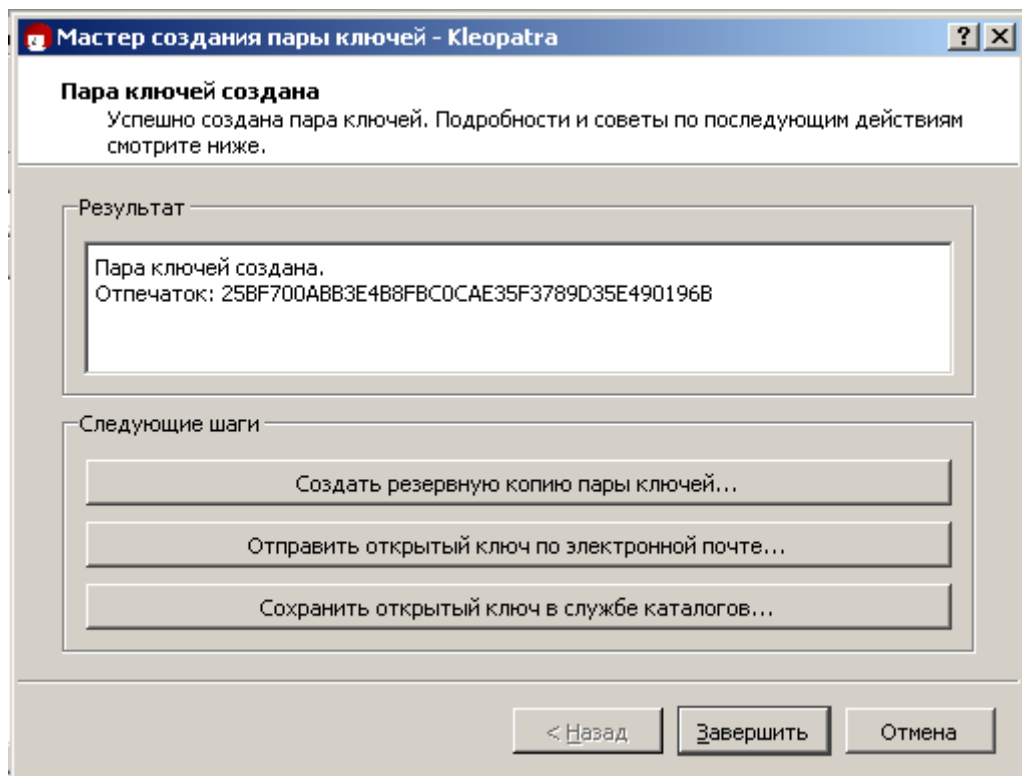


Рисунок 32 – Завершение создания ключей

Завершите создание ключа нажав на кнопку Завершить. В списке в главном окне программы должна появиться строка с новой парой ключей,



выделенной жирным шрифтом. Это означает, что пара полная (содержит приватный и публичные ключи).

### 2.3 Шифрование, расшифровка и цифровая подпись с использованием своей пары ключей

Создайте на рабочем столе текстовый файл с любым текстом. В данном примере используется файл “Секретный файл.txt” с содержанием “Это любой текст”.

Нажмите на кнопку “Подписать/зашифровать” в главном окне программы (Рисунок 33)

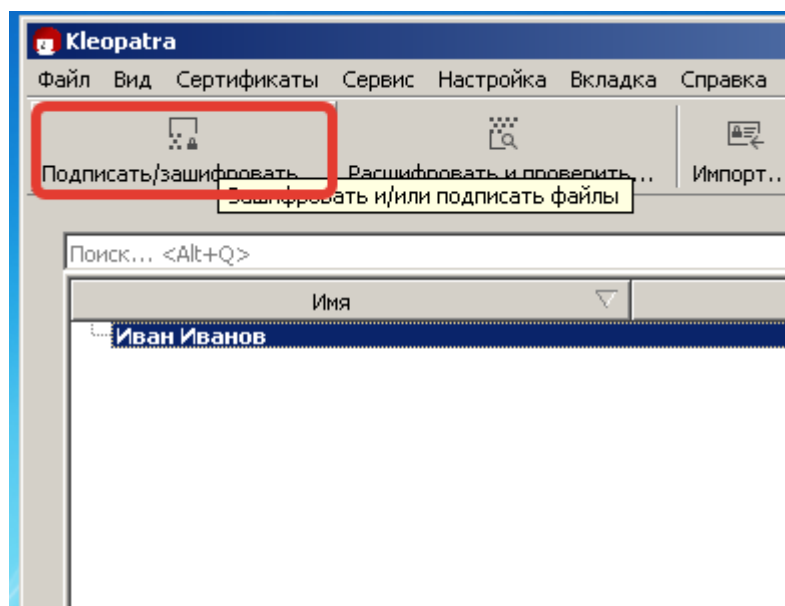


Рисунок 33 – Кнопка подписать/зашифровать

Откроется окно выбора файлов. Перейдите на рабочий стол и выберите созданный ранее текстовый файл (Рисунок 34).

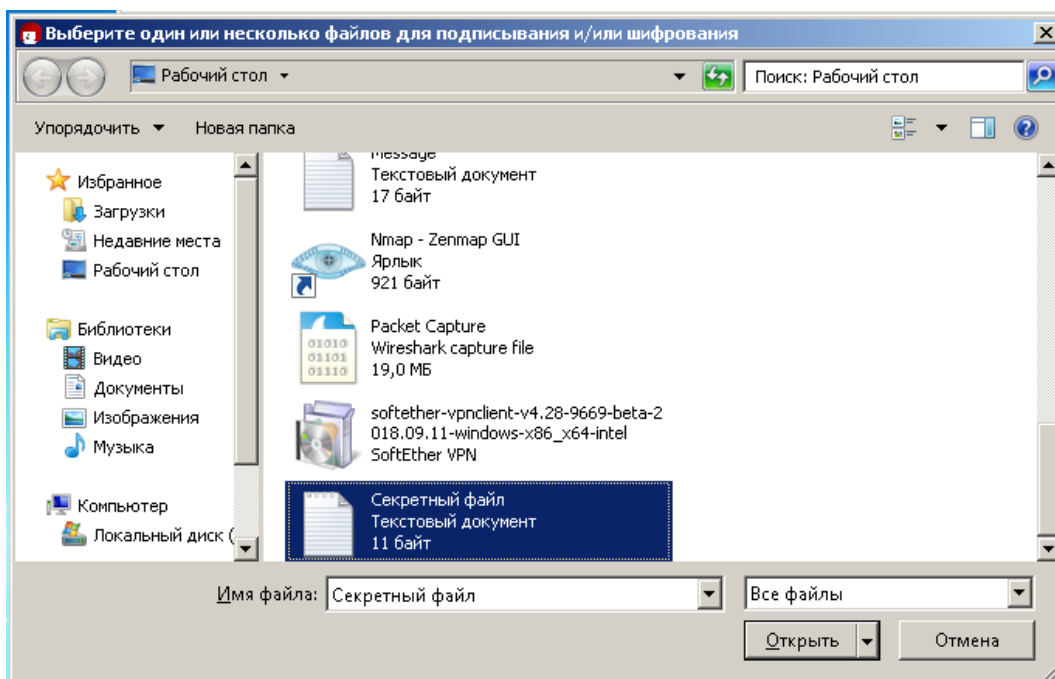


Рисунок 34 – Выбор файла для шифрования или подписания

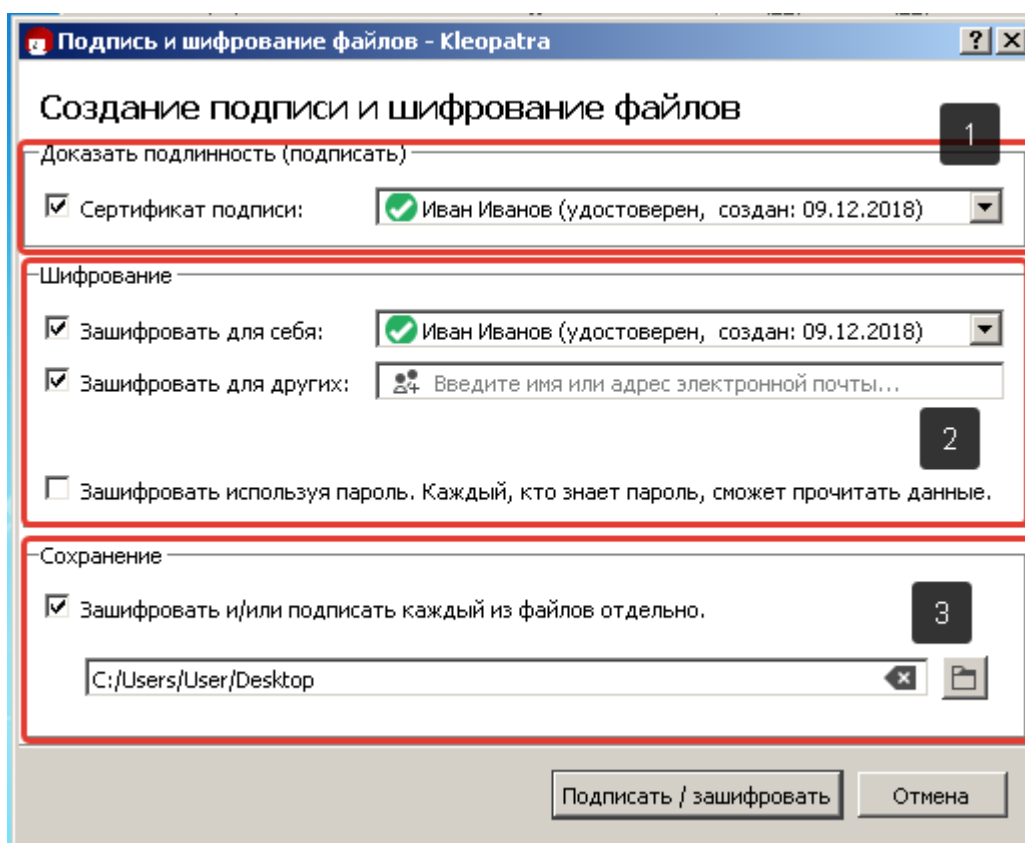


Рисунок 35 – Настройки шифрования/подписи файлов

Откроется окно (Рисунок 35). В данном окне задаются настройки подписания и шифрования файлов. Окно разделено на три блока. 1 – нужно ли подписать выбранный файл. 2 – нужно ли зашифровать выбранный файл, если да то с использованием каких публичных ключей? 3) Если на

предыдущем шаге выбрать несколько файлов, то программа автоматически объединит их в один архив который зашифрует\подпишет. Если нужно получить отдельные зашифрованные файлы и\или подписи, то нужно поставить эту галочку.

Выставьте настройки согласно рисунку 35 и нажмите Подписать.

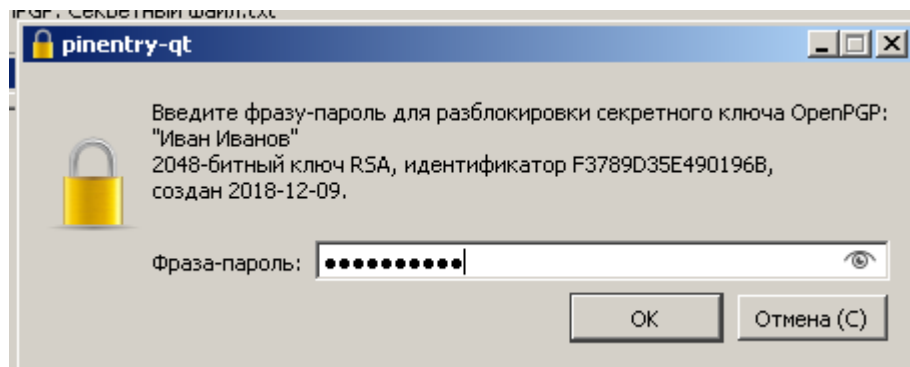


Рисунок 36 – Пароль подтверждение.

Поскольку приватный ключ хранится в зашифрованном виде, для его использования его нужно расшифровать. Именно для этого появится окно с запросом, как на рисунке 36. Введите пароль который указали при создании ключевой пары и нажмите ОК. Если все сделано правильно появится окно аналогичное Рисунку 37.

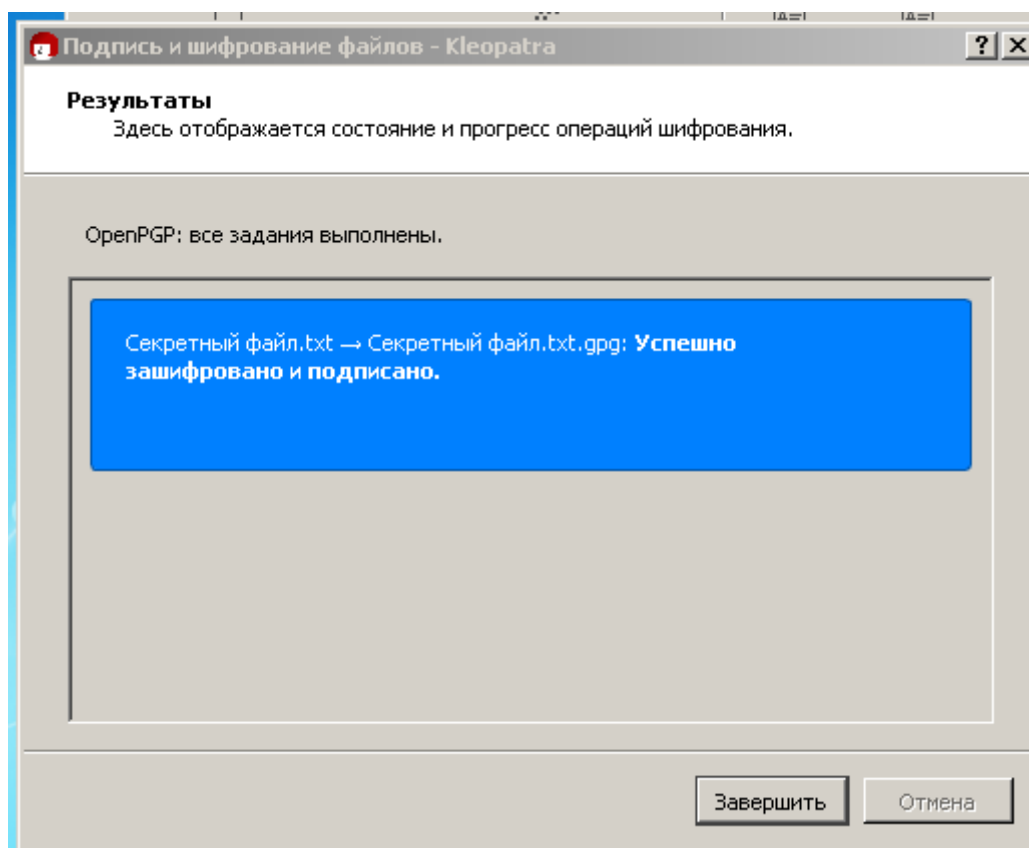


Рисунок 37 – Шифрование успешно завершено.

Теперь расшифруем зашифрованный файл. Для этого нажмите на кнопку “Расшифровать и проверить” в главном окне программы. (Рисунок 38) и выберите находящийся на рабочем столе зашифрованный файл. Он будет называться так же как и созданный вами документ, но с форматом “OpenPGP Binary File” (Рисунок 39).

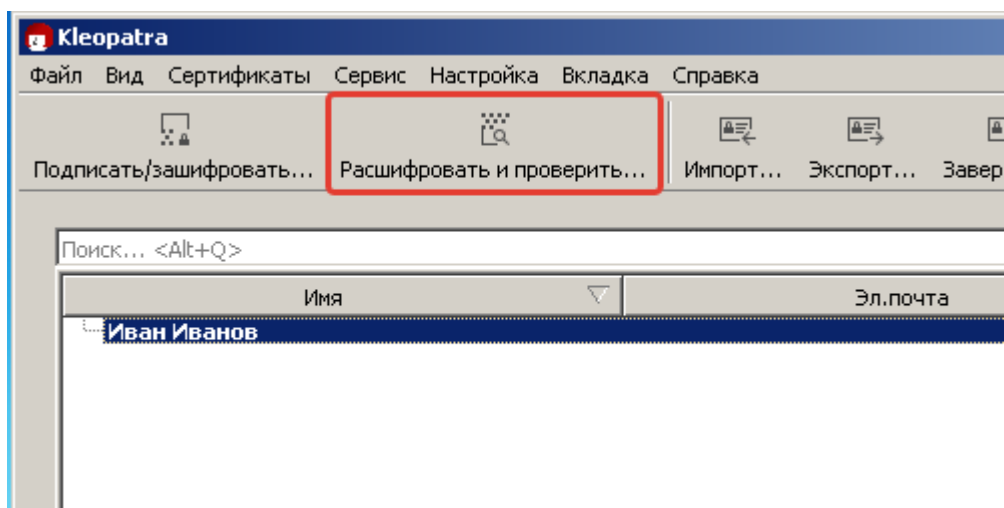


Рисунок 38 – Кнопка расшифровать и проверить подпись файла

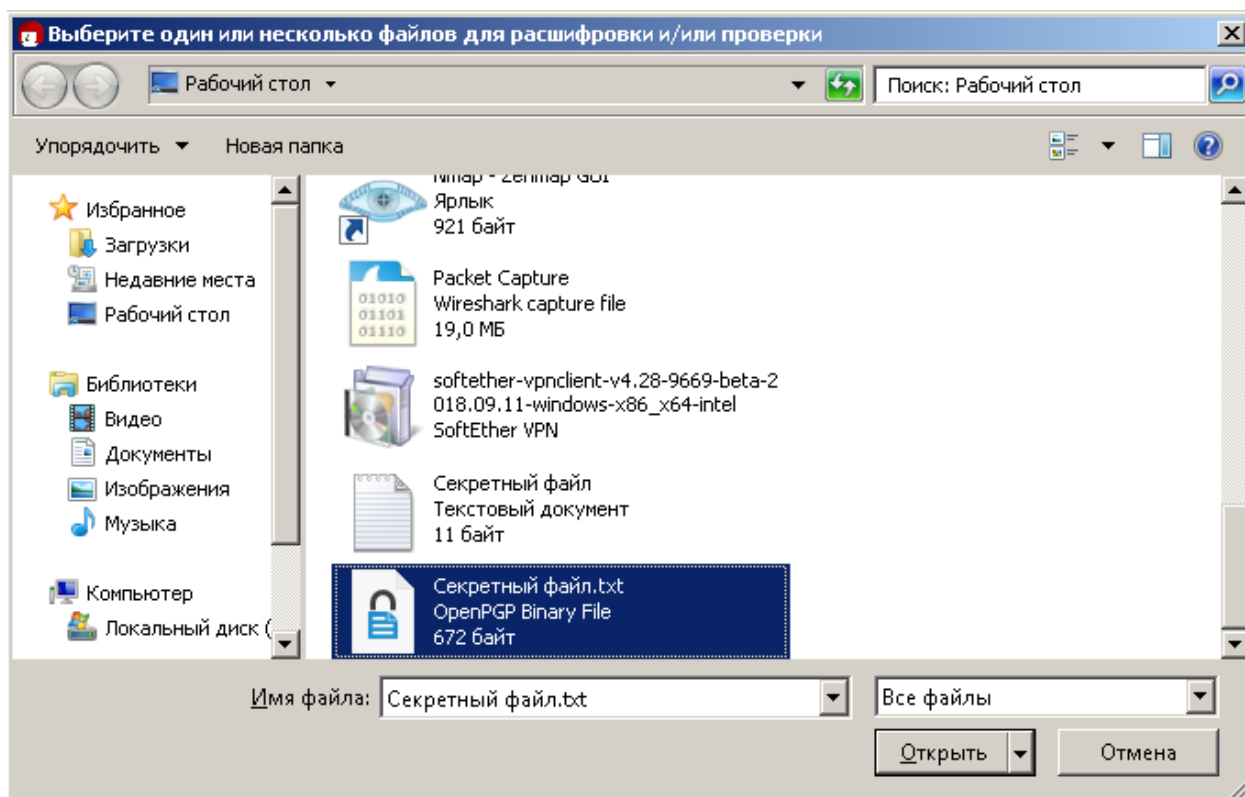


Рисунок 39 – Выбор зашифрованного файла

Откроется окно (Рисунок 40). Поскольку файл содержит электронную подпись, программа информирует о том, что подпись в документе есть, и она корректна. Для сохранения расшифрованного файла нажмите “Сохранить все”. Если появится запрос о перезаписи – нажмите да.

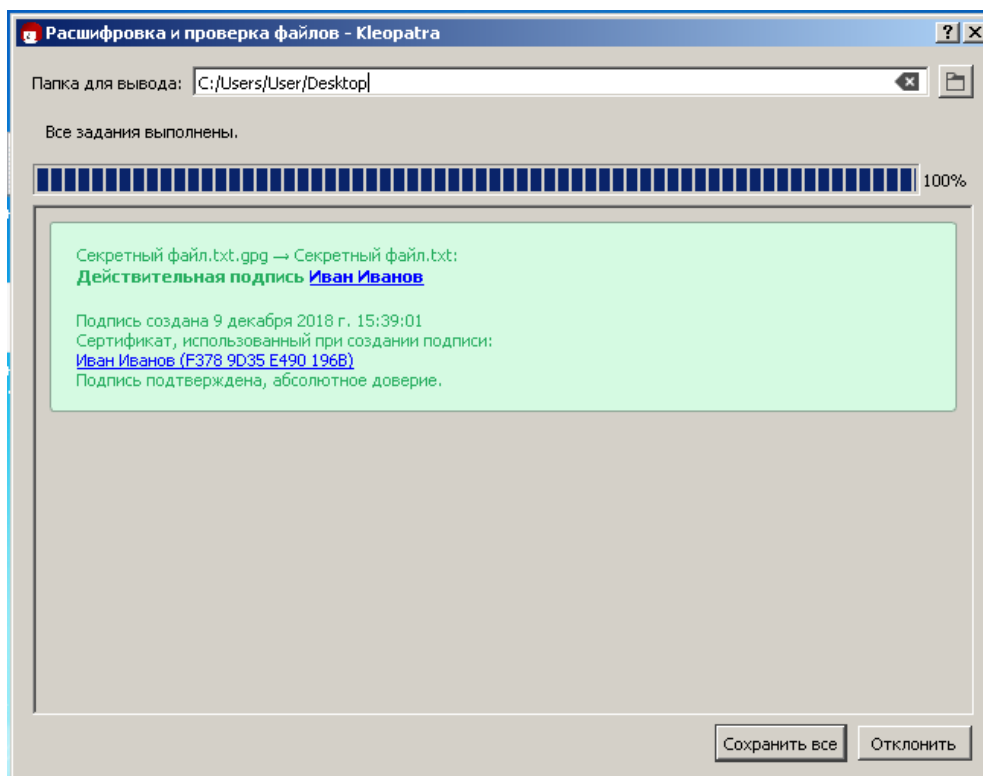


Рисунок 40 – Расшифровка и проверка подписи файла.

Теперь рассмотрим применение исключительно цифровой подписи.

Снова нажмите на кнопку “Подписать и шифрование файла” и выберите свой созданный файл (в примере это “Секретный файл.txt”). Откроется уже знакомое окно (Рисунок 41). Отметьте только сертификат подписи, а остальные галочки снимите. В этом случае создастся файл подписи (расширение .sig). Нажмите Подписать.

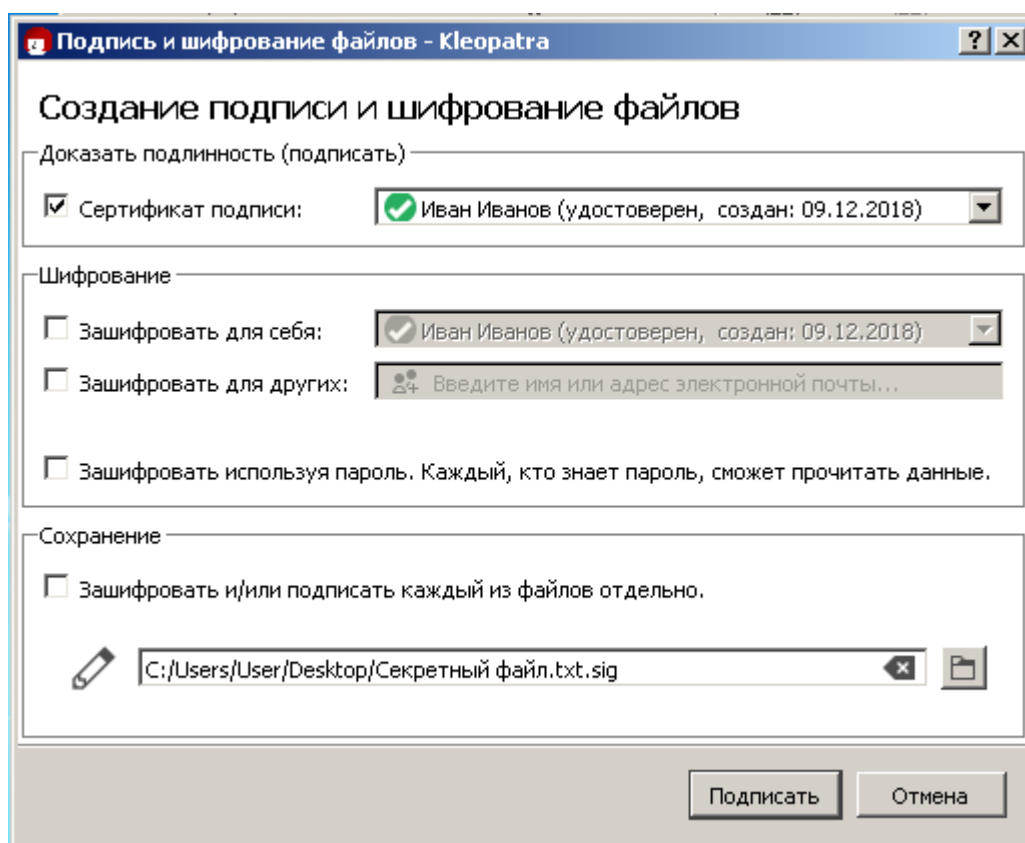


Рисунок 41 – Создание электронной подписи

Теперь проверим подпись. Нажмите кнопку “Проверить и расшифровать” и выберите получившийся файл подписи (OpenPGP Signature) Рисунок 42.

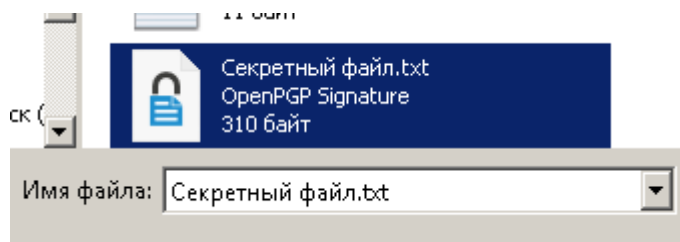


Рисунок 42 – Выбор файла подписи.

Проверка должна пройти успешно – Рисунок 43.

Теперь измените текст в текстовом файле, сохраните и повторите проверку подписи. Поскольку исходный файл изменился появится ошибка “Неверная подпись”. Как правило, это означает, что подписанный файл изменился и доверять ему нельзя.

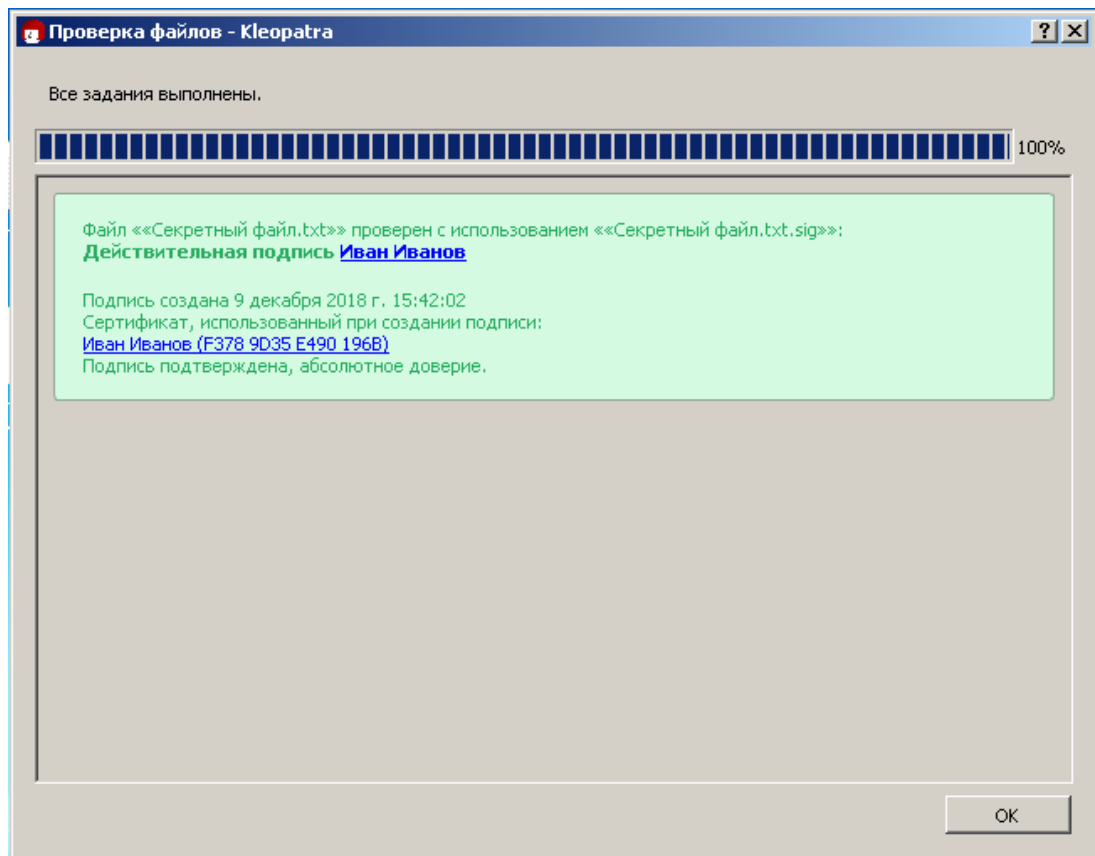


Рисунок 43 – Положительный результат проверки подписи

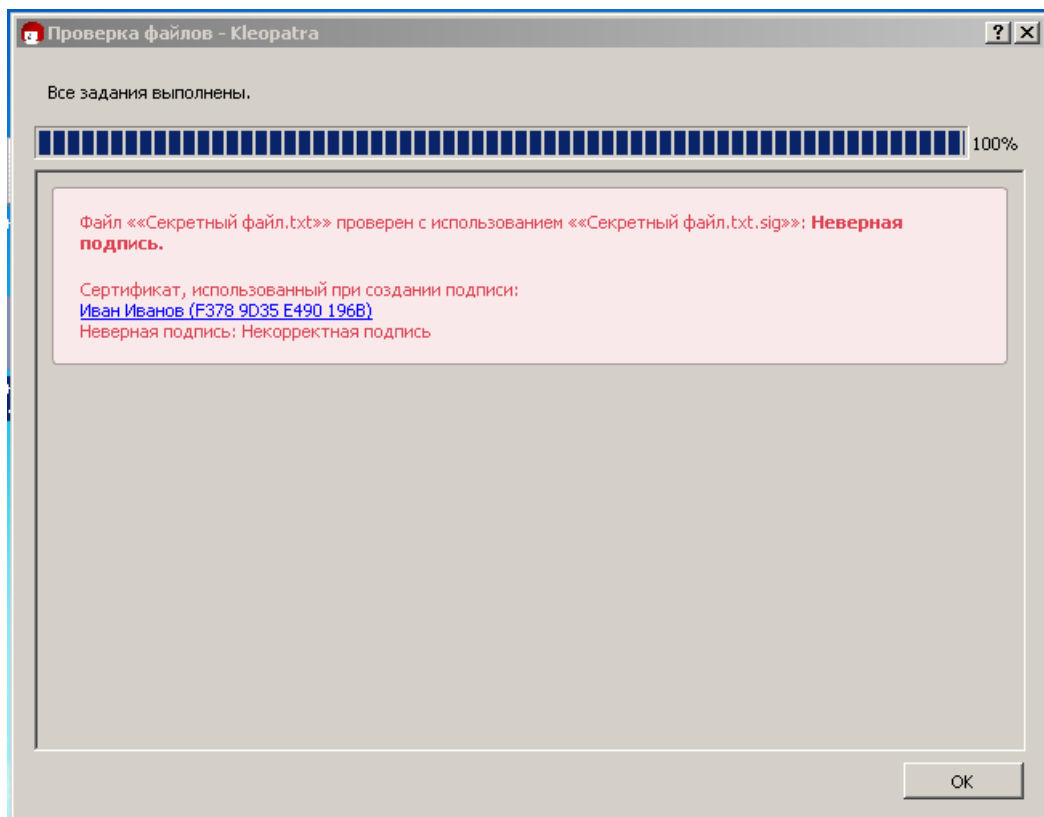


Рисунок 44 – Отрицательный результат проверки подписи

## 2.4 Импорт чужого публичного ключа.

Как мы уже знаем, публичный ключ нужен для шифрования документов и для проверки авторства документа. Для того чтобы зашифровать документ для другого человека нужно добавить его публичный ключ в программу.

Нажмите “Импорт...” на панели главного окна и выберите из папки Lab9 файл “Lab 9 – Public Teacher Key” (формат OpenPGP Text File) Рисунок 45. При экспорте сертификата требуется подтвердить его подлинность. Для этого нужно каким-то образом связаться с владельцем ключа и сверить правильность контрольной суммы ключа. В нашем случае следуйте рисункам 46-49.

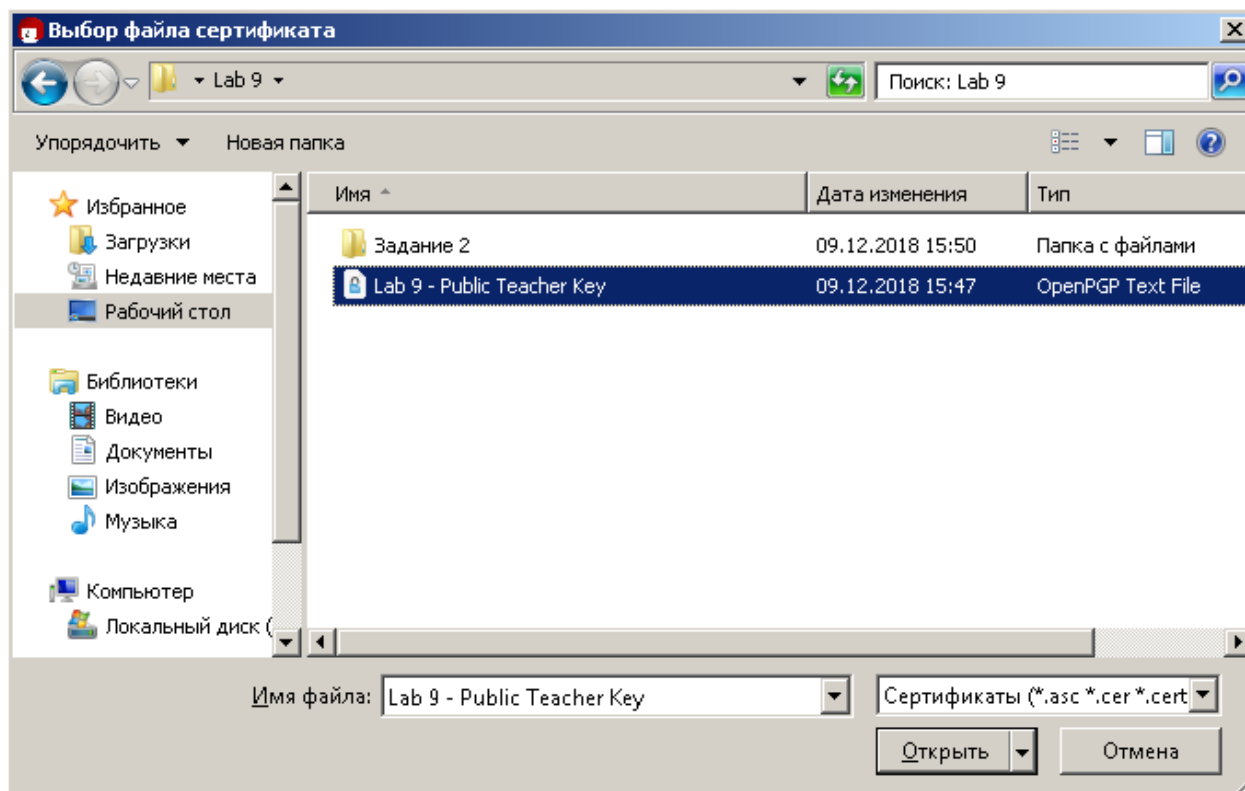


Рисунок 45 – Выбор файла публичного ключа



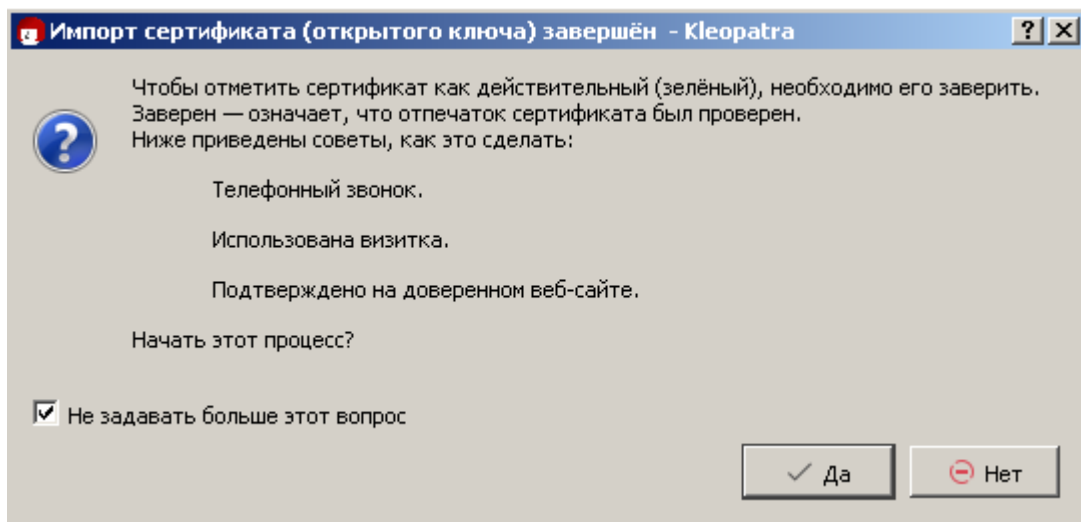


Рисунок 46 – Подтверждение импорта ключа

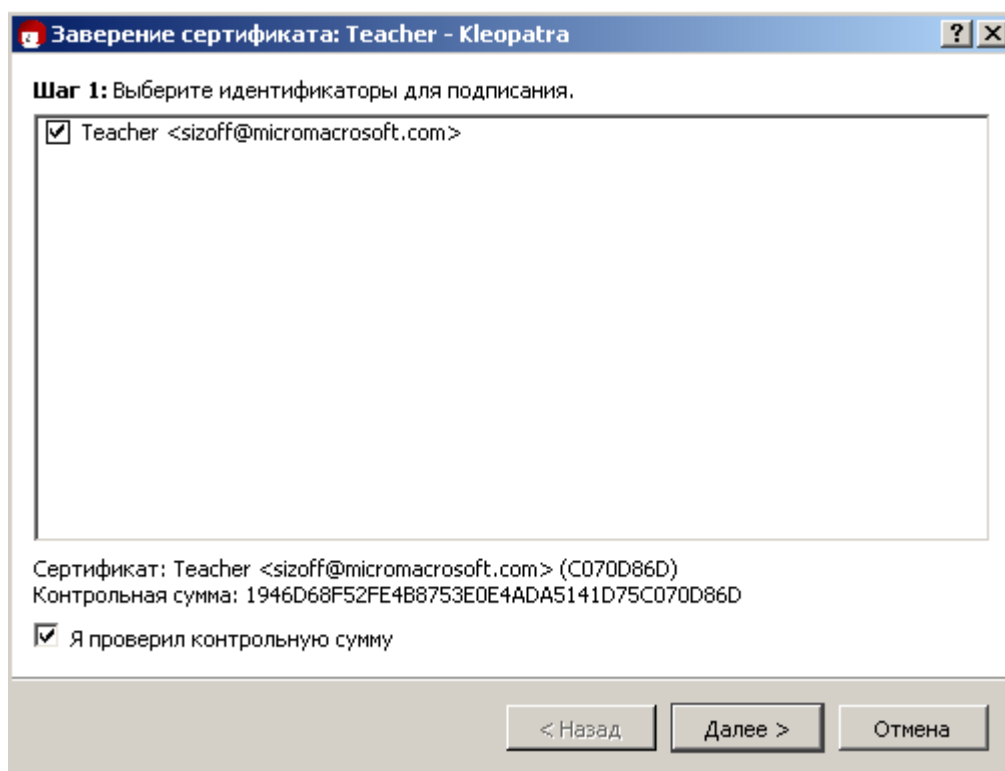


Рисунок 47 – Подтверждение контрольной суммы ключа

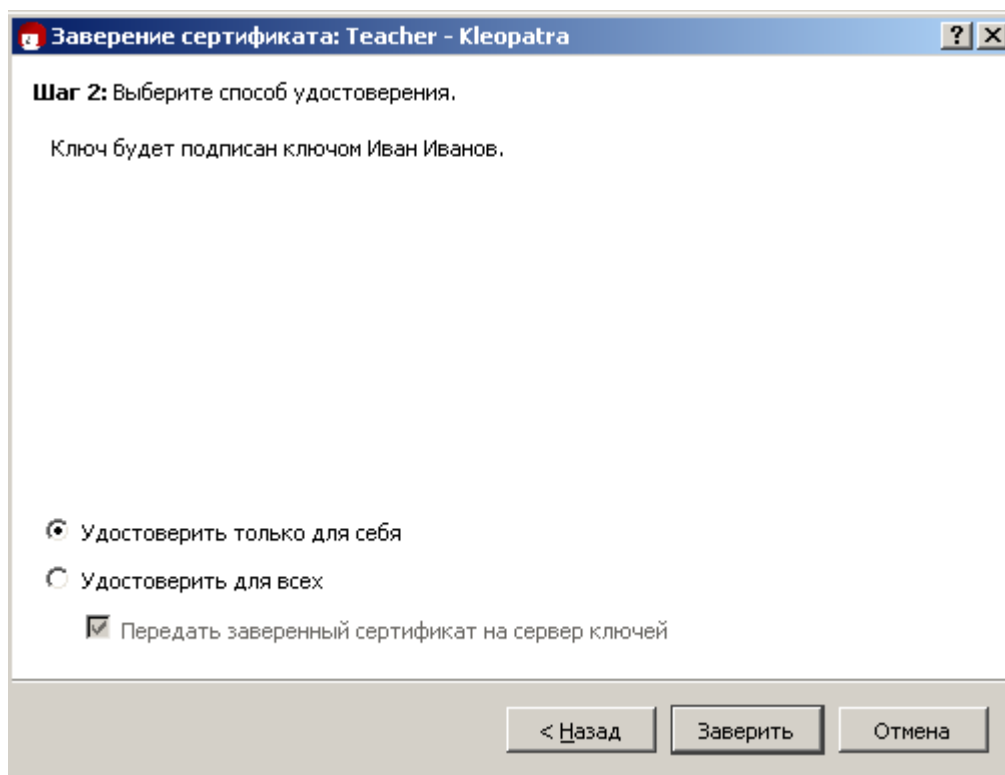


Рисунок 48 – Заверение сертификата ключа

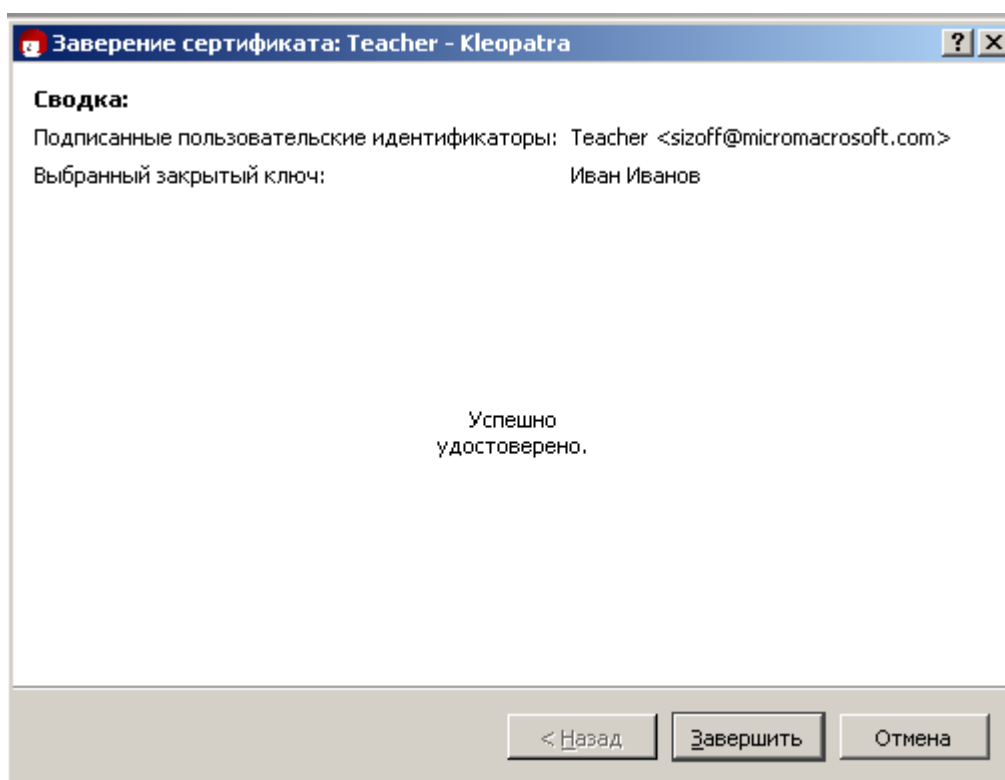


Рисунок 49 – Ключ заверен.

В списке появится еще одна подпись – Teacher.

## 2.5 Проверка подписи документа с использованием чужого публичного ключа

В папке Lab 9 содержится файл “Lab 9 – Secret.txt” и его цифровая подпись. Проверьте цифровую подпись данного файла Рисунки 50-51

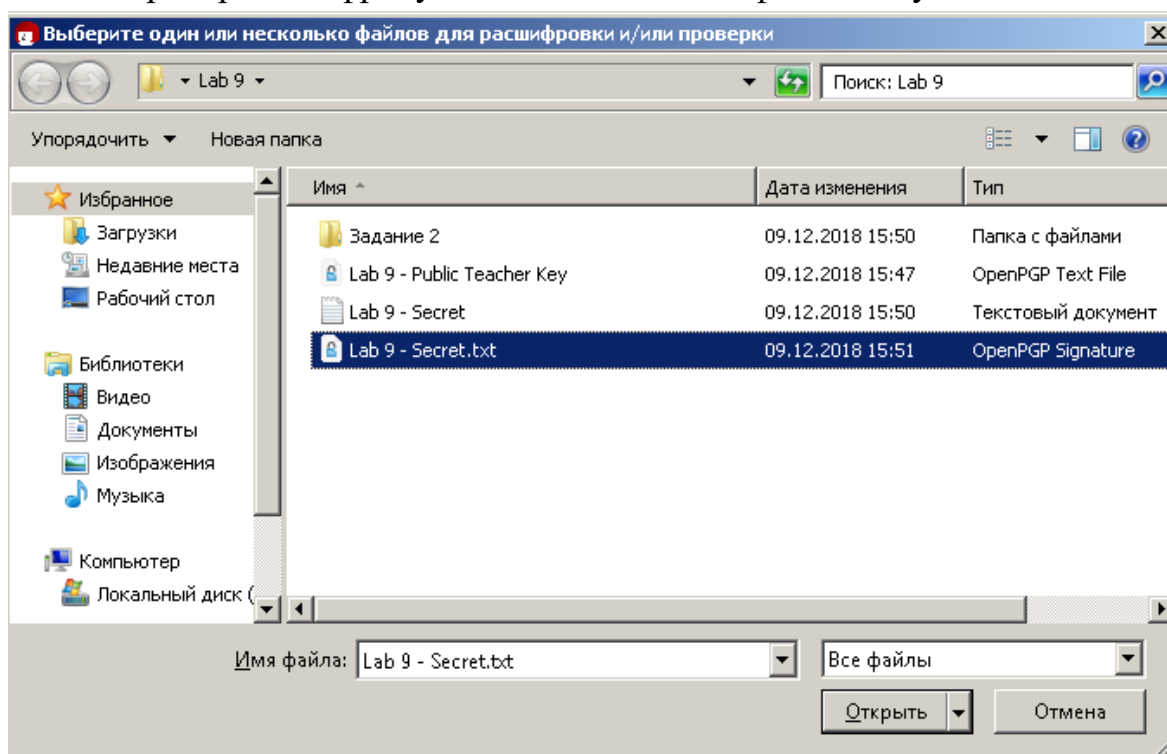


Рисунок 50 – Проверка подписи файла

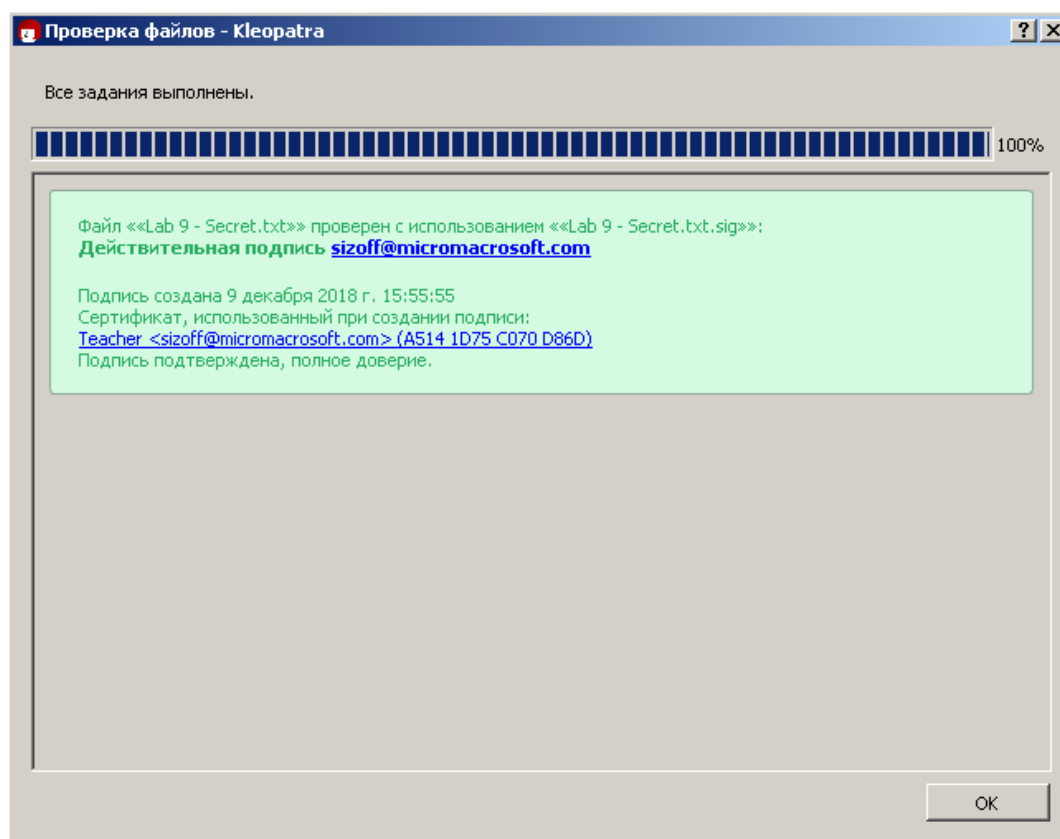


Рисунок 51 – Проверка подписи прошла успешно

Обратите внимание на то, каким сертификатом подписан файл. Попробуйте изменить текст в “Lab 9 – Secret.txt” и повторите проверку. Что-то изменилось? Почему?

## 2.6 Шифрование документа с использованием чужого публичного ключа

Предположим, что вам надо переслать какой-то файл владельцу ключа Teacher. Для этого файл нужно зашифровать с использованием его публичного ключа.

Нажмите “Подписать/зашифровать” и выберите ранее созданный на рабочем столе файл (Рисунок 52).

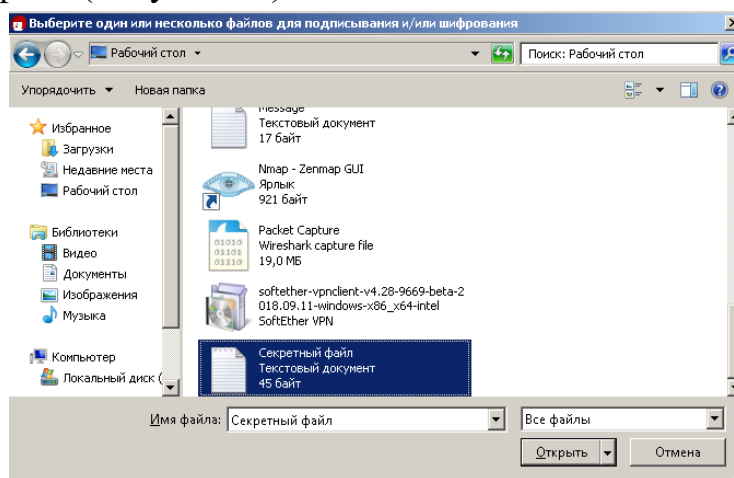


Рисунок 52 – Выбор файла для шифрования

Теперь необходимо указать для кого шифруется файл. Начните вводить имя адресата или адрес почты и соответствующем поле. Если указать несколько адресатов, то каждый из них сможет расшифровать файл. Укажите настройки как показано на рисунке Рисунок 53 и нажмите Шифрование.

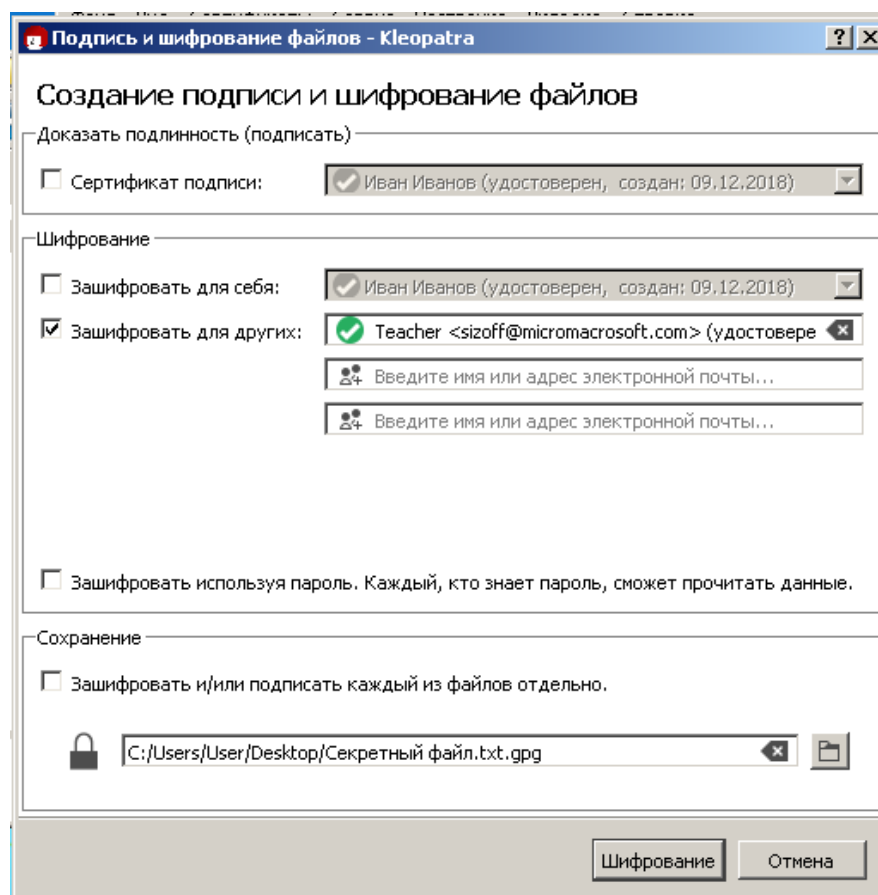


Рисунок 53 – Шифрование чужим публичным ключом

В папке с исходным файлом появится файл с расширением gpg, попробуйте его расшифровать. Должна отобразиться ошибка как на рисунке 54.

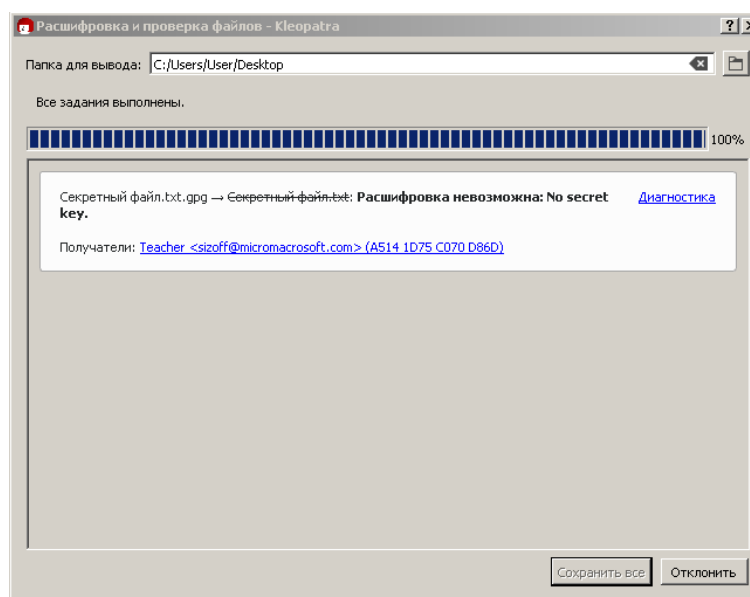


Рисунок 54 – Ошибка расшифровки файла

## 2.7 Импорт чужого приватного ключа

Расшифровка не удалась, поскольку у нас в программе нет приватного ключа для Teacher. Импортируйте его в программу так же как ранее публичный ключ. Приватный ключ находится в папке Lab 9 – Задание 2 в файле “Lab 9 – Private Teacher Key” (OpenPGP Binary File) (Рисунки 55-56)

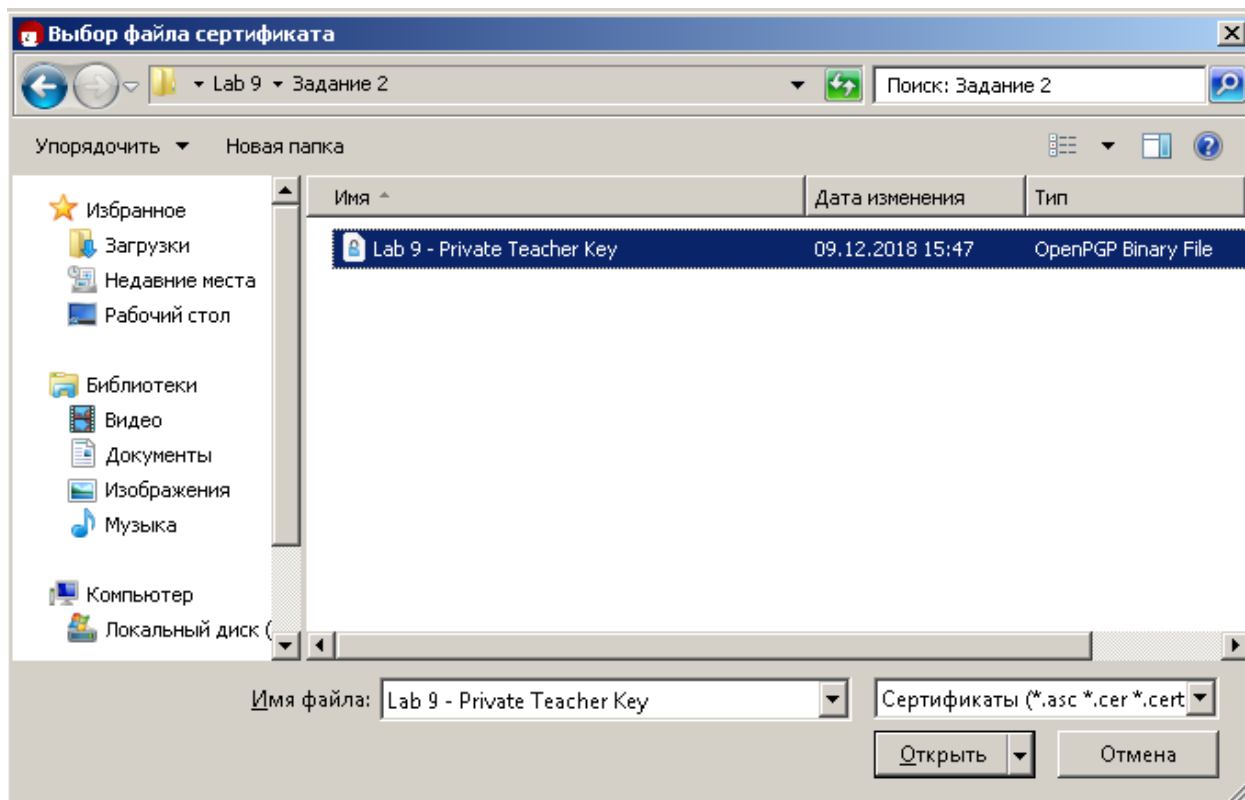


Рисунок 55 – Выбор приватного ключа.

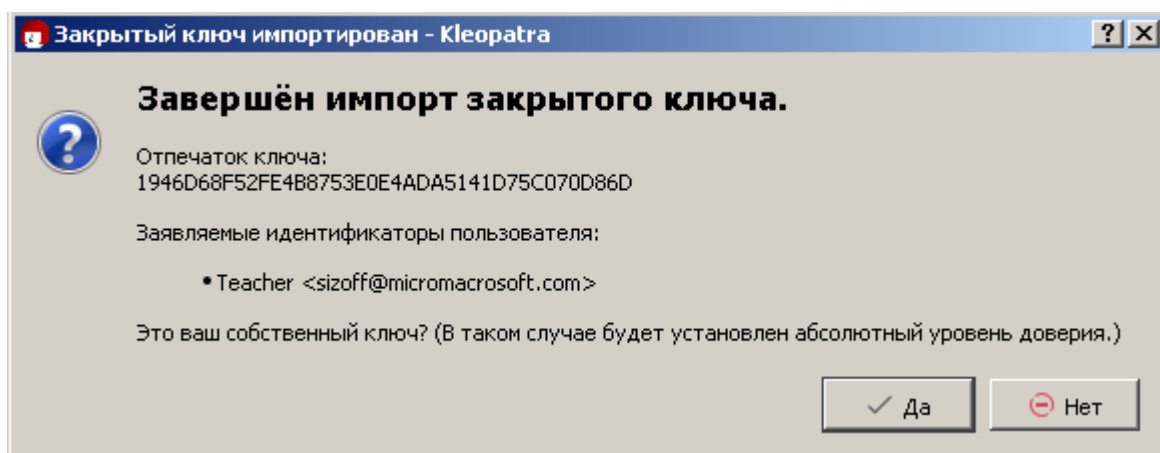


Рисунок 56 – Подтверждение импорта

### Самостоятельное задание.

Попробуйте снова расшифровать файл из предыдущего задания. Расшифровка должна пройти успешно.

Расшифруйте файл Lab 9 - Задание 2.pdf.gpg и внимательно изучите его содержимое, подготовьте ответы на вопросы.

Экспортируйте из программы пару ключей созданные вами в начале данного раздела.

*Контрольные вопросы:*

1. Что такое шифрование?
2. Чем отличается симметричное шифрование от асимметричного?
3. Что такое хэш-функция? Каковы ее свойства?
4. Что такое цифровая подпись? Для чего она используется?
5. Для чего используется приложение VeraCrypt? Какой тип шифрования она использует?
6. Для чего используется приложение GnuPG? Какой тип шифрования она использует?

*Список литературы:*

5. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
6. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
7. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
8. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## Лабораторная работа №9. Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft Baseline Security.

### Цель работы:

Изучить настройку которая позволит запускать MBSA периодически, в автоматическом режиме и отправлять отчеты на адреса электронной почты. Это позволит в значительной степени увеличить уровень информированности о состоянии безопасности в корпоративной сети.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть:

В рамках корпоративной инфраструктуры требуется иметь актуальную информацию о состоянии уровня безопасности. Несмотря на то, что на рынке присутствуют достойные продукты, позволяющие производить автоматическое сканирование по заданным шаблонам, они обладают достаточно высокой ценой. Компания Microsoft выпустила продукт под названием Microsoft Baseline Security Analyzer, который производит проверку продуктов Microsoft на наличие уязвимостей.

Основная задача данной работы - предоставить материал, который позволит запускать MBSA периодически, в автоматическом режиме и отправлять отчеты на адреса электронной почты. Это позволит в значительной степени увеличить уровень информированности о состоянии безопасности в корпоративной сети.

В рамках MBSA существует возможность запуска сканирования через командную строку – mbsacli.exe. Команда имеет ряд ключей которые позволят управлять сканированием.

/target		Проверка домена \ компьютера по имени
/target	IP адрес	Проверка по IP адресу
/r	Начальный IP адрес – конечный IP адрес	Проверка диапазона IP адресов
/listfile	Имя файла.txt	Проверка по файлу со списком IP адресов



/d	Имя домена	Проверка домена
/n	Опции	Выбор какую проверку не выполнять. Варианты: "OS"(операционная система), "SQL"(SQL сервер), "IIS"(веб-сервер ISS), "Updates"(обновления), "Password"(пароли). при наборе необходимо использовать "+" без пробела. Пример: OS+SQL+ISS+Updates+Password
/wa		Показывать только обновления, одобренные на WSUS.
/wi		Показать все обновления, даже если они не приняты на WSUS.
/nvc		Не проверять новую версия MBSA
/o	Имя файла	Шаблон названия отчета. имеет параметры: %D% - имя домена, %C% имя компьютера, %T% - время, %IP% - IP адрес. По умолчанию: %D% - %C% (%T%).
/qp		Не показывать процесс проверки.
/qt		Не показывать отчет при проверки одного компьютера.
/qe		Не показывать отчет ошибок.
/qr		Не показывать отчет.
/q		Не показывать все из вышеперечисленного
/unicode		Отчет в ЮНИКОДе
/u	Имя пользователя	Имя пользователя используемого при сканировании.
/p	Пароль пользователя	Пароль пользователя используемого при сканировании.
/catalog	Имя файла	Указывает источник данных который содержит информацию о доступных обновлений безопасности.
/ia		Обновления с учетом условий Windows Update Agent
/mu		Проверка с учетом обновлений сайта Microsoft Update.
/nd		Не скачивать обновления с сайта Microsoft Update при проверке.
/xmlout		Запуск проверки в режиме только для обновления с использованием только mbsacli.exe и wusscan.dll. Этот ключ может быть использован только с ключами: /catalog, /wa, /wi, /nvc, /unicode.
/l		Показать все отчеты.

/ls		Показать отчеты за последнее сканирование
/lr	Имя файла	Показать общий отчет.
/ld	Имя файла	Показать детализированный отчет
/rd	Имя директории	Директория для сохранения отчетов проверки.

Имея в распоряжении информацию по ключам, используемых командой `mbsacli.exe`, мы можем составить свой сценарий сканирования согласно нашим требованиям. Задача ставится следующим образом: необходимо провести проверку компьютеров (диапазон IP адресов) с использованием данных службы WSUS и сохранением отчета в определенной директории формат отчета: имя компьютера – время. Команда будет выглядеть следующим образом:

```
mbsacli.exe /r [начальный IP адрес]-[конечный IP адрес] /q /wa /o %IP%-%T% /u [Домен/имя пользователя] /p [пароль пользователя] /rd [директория, куда будут сохраняться отчеты]
```

Через некоторое время появятся отчеты об узлах в диапазоне IP адресов.

В рамках данной задачи будут отображены основные проблемы, связанные с безопасностью, которые будет необходимо изучить администраторам для устранения уязвимостей.

Но очень часто в рамках WSUS отсутствуют некоторые достаточно критичные обновления для систем. MBSA позволит выявить эти проблемы. Достаточно выше приведенную команду запустить с ключом `/tu` вместо `/wa`. В файлы отчета в Issue – Windows Security Updates будут показаны какие обновления необходимы для данного компьютера.

### Оборудование и материалы.

Персональный компьютер, программа Microsoft Baseline Security Analyzer.

### Указания по технике безопасности:

Соответствуют технике безопасности по работе с компьютерной техникой.

### Задания

#### **Автоматизация проверки**

Как было показано выше, необходимо иметь два отчета, которые показывают разницу между установленными обновлениями со службы WSUS и имеющимся обновлениями на сервере Microsoft Update. Для этого необходимо использовать две различные папки хранения отчетов разбитые по датам сканирования.

Файл исполнения (.bat) для проверки MBSA с использованием службы WSUS будет выглядеть так:

```
@echo off
cd {Папка хранения отчетов}/WSUS
MD %date:~-10%
cd "C:\Program Files\Microsoft Baseline Security Analyzer 2"
mbsacli.exe /r [начальныйIP]-[конечныйIP] /q /wa /rd c:/
{Папка хранения отчетов}/WSUS/%date:~-10%
```

Файл исполнения (.bat) для проверки MBSA с использованием сервера Microsoft Update будет выглядеть так:

```
@echo off
cd {Папка хранения отчетов}/MU
MD %date:~-10%
cd "C:\Program Files\Microsoft Baseline Security Analyzer 2"
mbsacli.exe /r [начальныйIP]-[конечныйIP] /q /mu /rd c:/
{Папка хранения отчетов}/MU/%date:~-10%
```

Bat-файлы различны между собой ключами /wa или /mu, задающие область сравнения обновлений, и папками, в которые необходимо сохранять отчеты.

В bat-файлах отсутствуют ключи /u и /p с параметрами имя пользователя и пароль. Это сделано по причине отсутствия необходимости хранения паролей в открытом виде в bat-файлах. Для безопасности необходимо использовать «Планировщик задач», в котором настраивается: от имени какого пользователя будет исполняться bat-файл.

В рамках системы Microsoft Windows присутствует «Планировщик заданий», который позволяет выполнять необходимые действия в определенное время. Также он позволяет добавлять необходимые аргументы. В нашем случае это два ключа /u и /p с параметрами Имя пользователя и пароль

Для этого создаем новую задачу выбирая пункт «Создать простую задачу» и даем описание к ней (рис. 1).

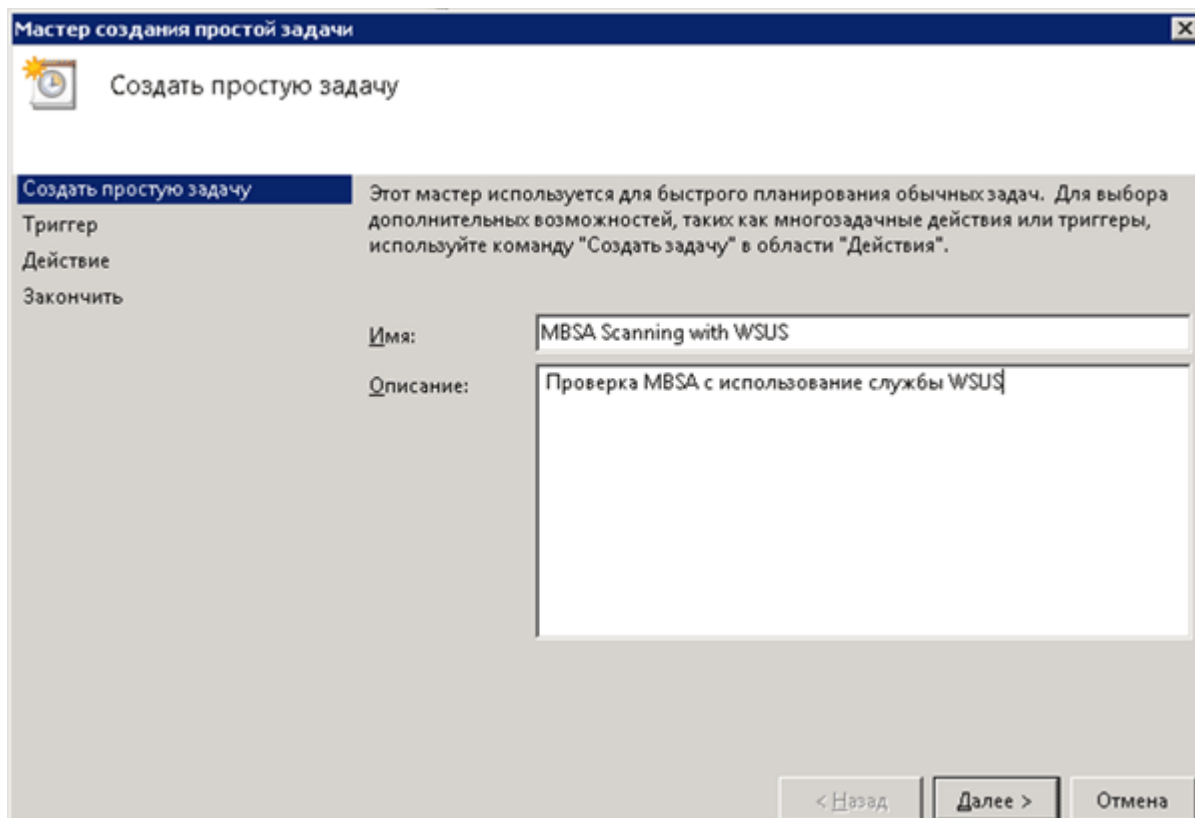


рис. 1

В окне «Триггер задачи» устанавливаем периодичность проведения проверки (достаточно раз в неделю)(рис. 2).

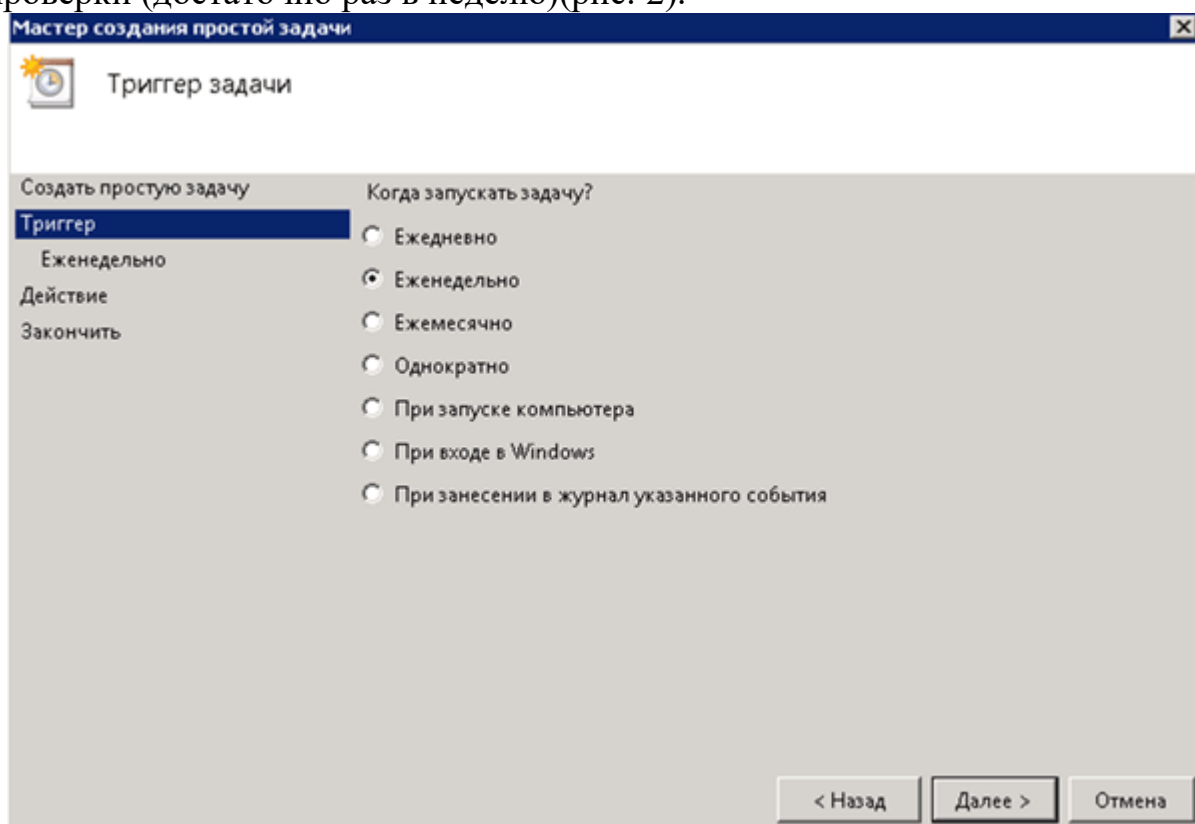


рис. 2

В окне «Еженедельно» устанавливаем время проведения проверки (время должно быть рабочее, так как сканируемый компьютер должен быть включен. (рис. 3).

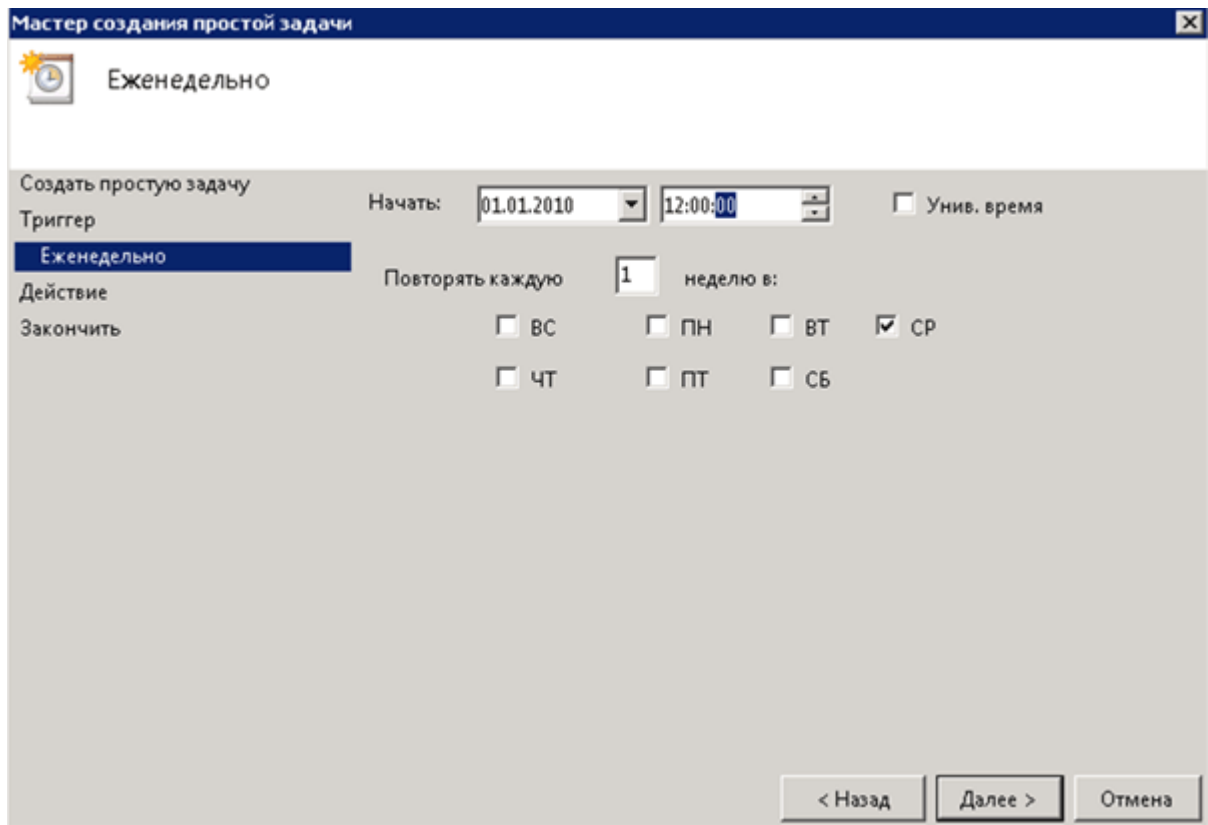


рис. 3

В окне «Действие» выбираем действие «Запустить программу». (рис. 4).

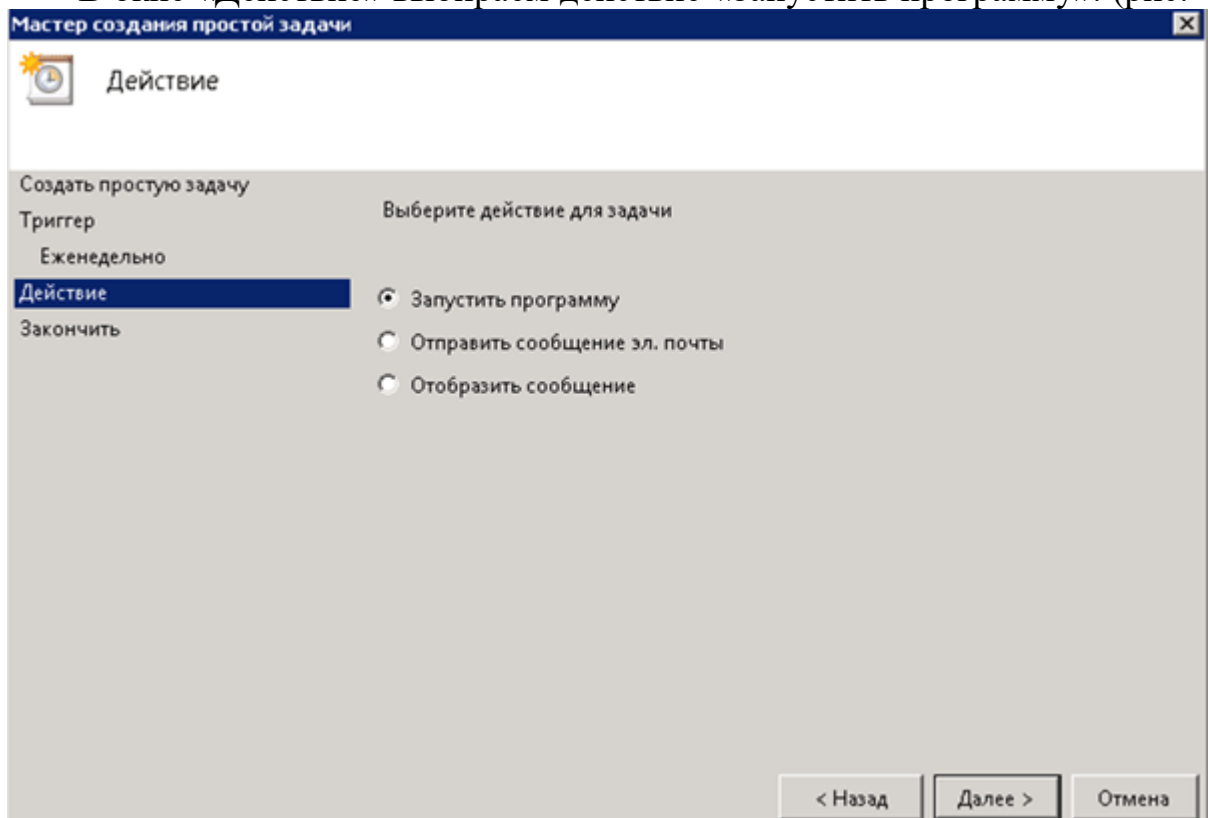


рис. 4

В окне «Запуск программы» выбираем через кнопку «Обзор», bat-файл предназначенный для сканирования с использованием WSUS (рис. 5).

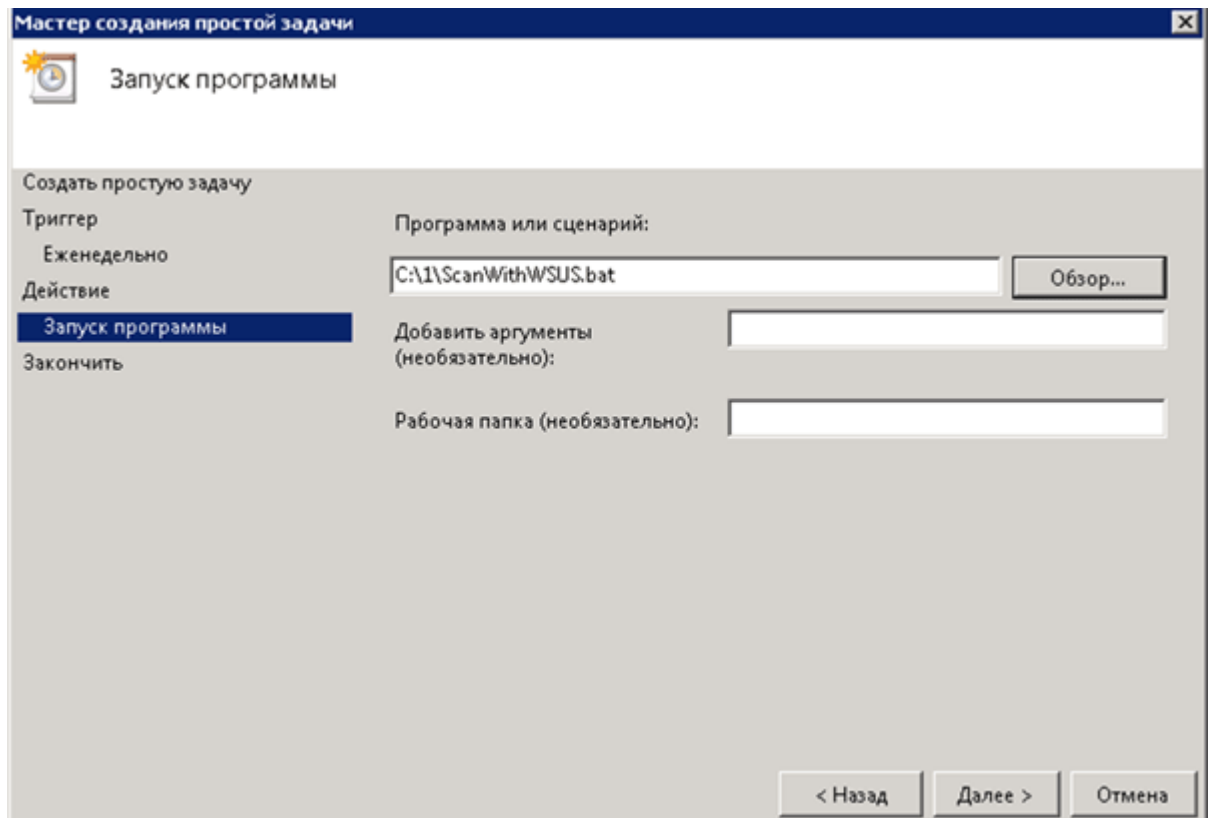


рис. 5

После создания задачи необходимо открыть её свойства и во вкладке «Общие» указать пункт «Выполнять вне зависимости от регистрации пользователя», что позволит выполнять задачи без необходимости регистрации в системе, например на сервере (рис. 6)

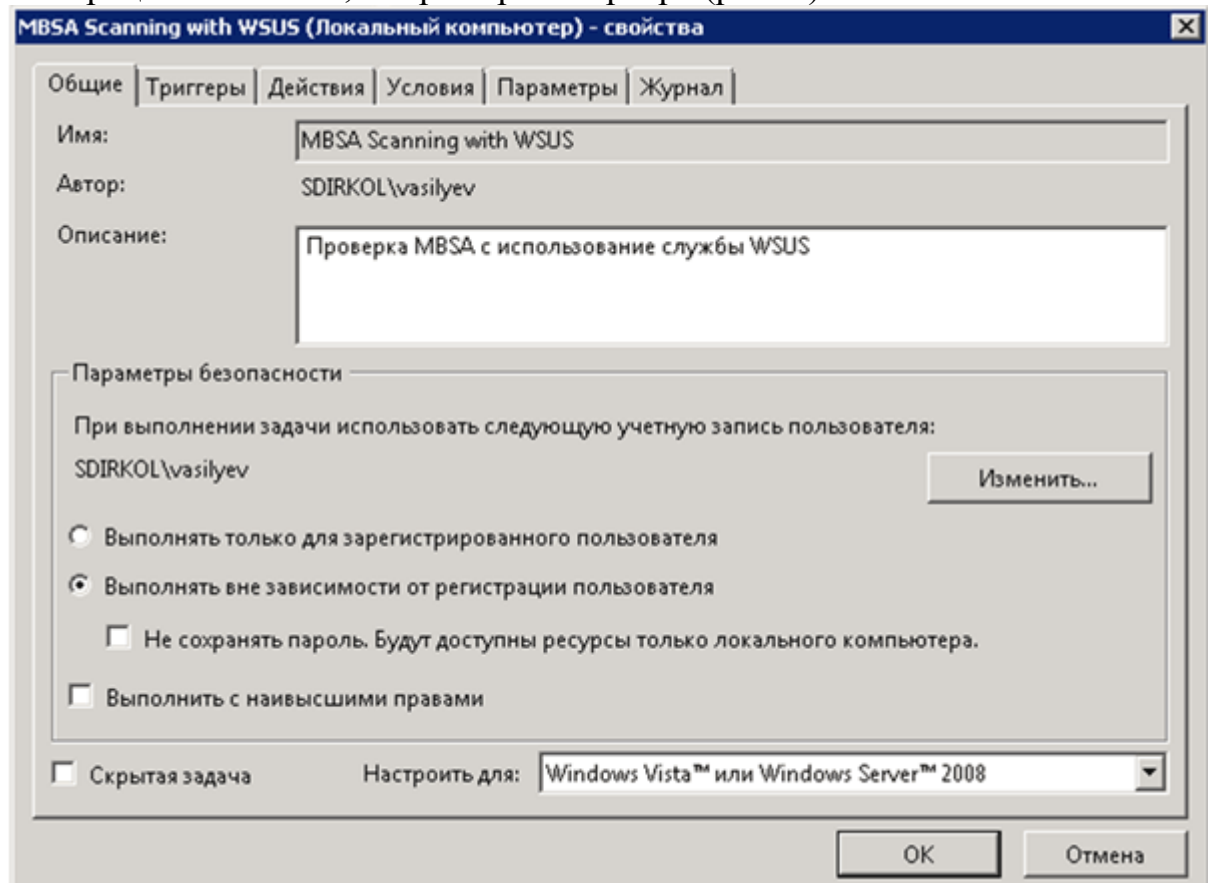


рис. 6

Продельываем вышеперечисленные действия для создания второй задачи проверки с использованием обновлений с сервера Microsoft Update и указанием соответствующего bat-файла.

Заключение. Продукт Microsoft Baseline Security Analyzer не обладает богатым функционалом из-за своей «бесплатности», но благодаря использованию в командной строке различных ключей с параметрами, позволяет повысить уровень информативности о состоянии безопасности и получить информацию для устранения уязвимостей в корпоративной среде.

Также управление через командную строку позволяет администраторам автоматизировать процесс получения необходимых отчетов о состоянии безопасности.

### **Контрольные вопросы**

1. Автоматическое сканирование по заданным шаблонам.
2. Проверка продуктов Microsoft на наличие уязвимостей – Microsoft Baseline Security Analyzer.
3. Составление сценария сканирования по определенным требованиям.
4. Автоматизация проверки.

### *Список литературы:*

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## Лабораторная работа №10. Системы разграничения доступа.

Цель работы: Освоение средств защищенных версий операционной системы Windows, предназначенных для разграничения доступа субъектов к папкам и файлам; разграничения доступа субъектов к принтерам; разграничения доступа к разделам реестра; обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### *Теоретическая часть.*

Существуют критерии определения безопасности компьютерных систем (КС), составляющие основу международного стандарта Common Criteria, опубликованного в 2005 году.

«Критерии» устанавливают основные условия для оценки эффективности средств компьютерной безопасности АС.

Под *политикой безопасности* (ПБ) понимается совокупность норм, правил и практических рекомендаций, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от заданного множества угроз и составляет необходимое условие безопасности КС.

Политики безопасности должны быть подробными, четко определёнными и обязательными для КС. Есть две основные политики безопасности:

- **мандатная политика безопасности** — обязательные правила управления доступом, напрямую основанные на индивидуальном разрешении на доступ к информации и уровне конфиденциальности запрашиваемой информации.

- **дискреционная политика безопасности** — предоставляет непротиворечивый набор правил для управления и ограничения доступа, основанный на идентификации тех пользователей, которые намерены получить только необходимую им информацию.

В качестве обязательных функций сервиса управления доступом к информации в АС выделяются:

- аутентификация — процесс распознавания пользователя;
- авторизация — проверка разрешения пользователю на получение информации определённого рода;



- аудит — отслеживание действий аутентифицированных пользователей, при которых затрагивается безопасность.

Основная цель создания ПБ информационной системы – определение условий, которым должно подчиняться поведение подсистемы безопасности.

Компьютерная система должна содержать аппаратные и/или программные механизмы, которые могут определять обеспечивается ли достаточная уверенность в том, что система защиты выполняет необходимые требования. Существуют следующие гарантии безопасности.

Операционная гарантия — уверенность в том, что реализация спроектированной системы обеспечивает осуществление принятой стратегии защиты системы. Сюда относятся *системная архитектура, целостность системы, анализ скрытых каналов, безопасное управление возможностями и безопасное восстановление*.

Гарантия жизненного цикла — уверенность в том, что система разработана и поддерживается в соответствии с формализованными и жестко контролируемыми критериями функционирования. Сюда относятся *тестирование безопасности, задание на проектирование и его проверка, управление настройками и соответствие параметров системы заявленным*.

Гарантии непрерывной защиты — надёжные механизмы, обеспечивающие непрерывную защиту основных средств от преступных и/или несанкционированных действий.

Критерии делятся на 4 раздела: D, C, B и A, из которых наивысшей безопасностью обладает раздел A. Каждый раздел представляет собой значительные отличия в доверии индивидуальным пользователям или организациям. Разделы C, B и A иерархически разбиты на серии подразделов, называемые классами: C1, C2, B1, B2, B3 и A1. Каждый раздел и класс расширяет или дополняет требования указанные в предшествующем разделе или классе. Не останавливаясь подробно на организации доступа внутри классов, отметим основные моменты:

Раздел **D** характеризуется организацией минимальной защиты.

Раздел **C** характеризуется организацией *дискреционной защиты*.

Раздел **B** характеризуется *организацией мандатной защиты*.

Раздел **A** характеризуется *проверенной защитой*.

### Дискреционные политики безопасности

Возможны следующие подходы к построению дискреционного управления доступом:

1. Каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту

2. Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.

3. Смешанный вариант построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и (или) изменения его владельца.

Именно такой смешанный вариант реализован в большинстве операционных систем, например, в классических UNIX-системах или в системах Windows.

Дискреционное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Исходная политика избирательного разграничения доступа к информации (дискреционная модель) формируется путем задания администратором набора троек следующего вида:

$$(S_i, O_j, T_k), i = \overline{1, N}, j = \overline{1, M}, k = \overline{1, K},$$

где  $S_i \in S$  - субъект доступа,  $O_j \in O$  - объект доступа,  $T_k \subset T$  - множество прав доступа, которыми наделен субъект  $S_i$  к объекту  $O_j$  (например, чтение, запись, исполнение и т.д.) [7].

При формировании дискреционной политики безопасности обычно формируют дискреционную матрицу доступов  $M_{N \times M}$ , строки которой соответствуют субъектам системы, столбцы – объектам, а в ячейках матрицы хранят множество типов доступов. Пример данной матрицы представлен в таблице 2.1.

Табл. 2.1. Дискреционная матрица доступа

Объект / Субъект	Файл_1	Файл_2	Файл_3	CD-RW
<b>Администратор</b>	Полные права	Полные права	Полные права	Полные права
<b>Гость</b>	Запрет	Чтение	Чтение	Запрет
<b>Пользователь_1</b>	Чтение, передача прав	Чтение, запись	Полные права	Полный запрет

Для матрицы доступа, представленной в таблице 2.1, Пользователь\_1 имеет права на чтение и запись в Файл\_2. Передавать эти права другому пользователю он не может, но может передавать права на чтение файла 1, имеет полные права при работе в файлом 3 и не имеет доступа к лиску **CD-RW**.

Мандатные политики безопасности

Мандатные модели управления доступом были созданы по результатам анализа правил секретного документооборота, принятых в государственных и правительственных учреждениях многих стран.

Мандатное управление доступом — разграничение доступасубъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся вобъектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Мандатная модель управления доступом, помимо дискреционной, является основой реализации разграничительной политики доступа к ресурсам при защите секретной информации. При этом данная модель доступа практически не используется "в чистом виде", обычно на практике она дополняется элементами дискреционной модели доступа.

*Исходная мандатная политика безопасности* строится на базе следующей совокупности аксиом, определяющих правило разграничения доступа субъектов к обрабатываемой информации:

1. Вводится множество атрибутов (уровней) безопасности  $A$ , элементы которого упорядочены с помощью установленного отношения доминирования. Например, для России характерно использование следующего множества уровней безопасности  $A = \{\text{открыто (O), конфиденциально (K), секретно (C), совершенно секретно (CC), особая важность (OB)}\}$ .

2. Каждому объекту  $O_j \in O$  КС ставится в соответствие атрибут безопасности  $x_{O_j} \in A$ , который соответствует ценности объекта  $O_j$  и называется егоуровнем (*грифом*) конфиденциальности.

3. Каждому субъекту  $S_i \in S$  КС ставится в соответствие атрибут безопасности  $x_{S_i} \in A$ , который называетсяуровнем допуска субъекта и равен максимальному из уровней конфиденциальности объектов, к которому субъект  $S_i$  будет иметь допуск.

4. Если субъект  $S_i$  имеет уровень допуска  $x_{S_i}$ , а объект  $O_j$  имеет уровень конфиденциальности  $x_{O_j}$ , то  $S_i$  будет иметь допуск к  $O_j$  тогда и только тогда, когда  $x_{S_i} \geq x_{O_j}$ .

Основным недостатком исходной мандатной политики безопасности является то, что в ней не различаются типы доступа вида «чтение» и «запись». Это создает потенциальную возможность утечки информации сверху вниз, например, путем запуска в КС программной закладки с максимальным уровнем допуска, способной записывать информацию из объектов с верхних уровней конфиденциальности в объекты с более низкими уровнями, откуда она может быть прочитана субъектами с низким уровнем допуска.

*Практическая часть:*

1. После собеседования с преподавателем и получения допуска к работе войти в систему с указанным общим именем учетной записи (с правами обычного пользователя).
2. Освоить средства разграничения доступа пользователей к папкам:
  - выполнить команду «Общий доступ и безопасность» контекстного меню папки, содержащей отчеты студентов о выполненных лабораторных работах (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»;
  - открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;
  - с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);
  - включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;
  - открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;
  - открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;
  - закрыть окно дополнительных параметров безопасности и с помощью кнопки «Добавить» открыть окно выбора пользователя или группы;
  - с помощью кнопок «Дополнительно» и «Поиск» открыть список зарегистрированных пользователей и групп и выбрать пользователя с именем своей индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
  - назначить ему права на полный доступ к папке с отчетами о выполненных лабораторных работах;
  - включить в отчет копии экранных форм, использованных при выполнении заданий данного пункта.
3. Освоить средства разграничения доступа пользователей к файлам:
  - выполнить команду «Свойства» контекстного меню файла с одним из отчетов о ранее выполненных лабораторных работах;
  - повторить все задания п. 2, но применительно не к папке, а к файлу;
  - включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам.
4. Освоить средства разграничения доступа к принтерам:
  - выполнить команду «Принтеры и факсы» меню «Пуск»;

- выполнить команду «Свойства» контекстного меню установленного в системе принтера;
- повторить все задания п. 2, но применительно не к папке, а к принтеру (кроме добавления нового субъекта к списку управления доступом);
- включить в отчет ответ на вопрос, в чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам.

5. Освоить средства разграничения доступа к разделам реестра операционной системы:

- с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);
- с помощью команды «Разрешения» меню «Правка» редактора реестра определить и включить в отчет сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита (аналогично п. 2);
- включить в отчет копии экранных форм, использованных при выполнении данного пункта, и ответ на вопрос, в чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам.

5. Освоить средства обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы:

- выполнить команду «Свойства» контекстного меню папки, содержащей отчеты о ранее выполненных лабораторных работах, и на вкладке «Общие» окна свойств нажать кнопку «Другие»;
- включить выключатель «Шифровать содержимое для защиты данных», нажать кнопку «Применить» и в окне подтверждения изменения атрибутов нажать кнопку «Ok»;
- включить в отчет ответ на вопрос, как визуально выделяются имена зашифрованных файлов и папок;
- выполнить команду «Свойства» контекстного меню папки с отчетами о ранее выполненных лабораторных работах;
- нажать кнопку «Другие» и включить в отчет ответ на вопрос, доступна ли кнопка «Подробно»;
- повторить два предыдущих пункта для одного из файлов с отчетами о ранее выполненных лабораторных работах;
- выйти из системы и войти повторно под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- создать произвольный файл (например, с копией описания данной лабораторной работы) в папке «Мои документы» и обеспечить шифрование этого файла;

- выйти из системы и снова войти под именем общей учетной записи, под которой работали первоначально;
- выполнить команду «Свойства» контекстного меню одного из файлов с отчетами о ранее выполненных лабораторных работах, нажать последовательно кнопки «Другие» и «Подробно»;
- в окне подробностей шифрования нажать кнопку «Добавить» и в окне выбора пользователя выбрать имя индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- повторить два предыдущих пункта для всех файлов с отчетами о ранее выполненных работах;
- снова выйти из системы и войти повторно под именем индивидуальной учетной записи, созданной при выполнении лабораторной работы №1;
- убедиться, что под индивидуальной учетной записью можно просматривать и редактировать отчеты о ранее выполненных лабораторных работах;
- включить в отчет копии экранных форм, использованных при выполнении данного пункта, сведения о порядке использования шифрующей файловой системы и ответы на вопросы
  - как формируется список пользователей, из которого возможен выбор субъектов для совместного доступа к зашифрованным файлам;
  - связан ли этот список с зарегистрированными в системе пользователями и группами;
  - каковы функции агента восстановления зашифрованных файлов и как он может быть назначен (воспользуйтесь Справкой Windows).

Ознакомиться с правами доступа к файлам и папкам, назначаемым операционной системой по умолчанию:

- выполнить команду «Общий доступ и безопасность» (команду «Свойства») контекстного меню одной из папок с документами зарегистрированного в системе пользователя (например, «Документы - Пользователь компьютерного класса») и открыть вкладку «Безопасность»;
- включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце;
- повторить два предыдущих пункта для папки с документами другого зарегистрированного пользователя;
- повторить два предыдущих пункта для папки «Общие документы»;
- включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и ответы на вопросы
  - как обеспечивается операционной системой разграничение доступа к личным документам пользователей (по умолчанию);

- где (по умолчанию) должны находиться документы, предназначенные для совместного использования.

*Контрольные вопросы:*

1. какая политика безопасности лежит в основе разграничения доступа к объектам в защищенных версиях операционной системы Windows?
2. в чем уязвимость принятой в защищенных версиях операционной системы Windows политики разграничения доступа (приведите примеры)?
3. как работает механизм наследования при определении прав на доступ субъектов к объектам в защищенных версиях операционной системы Windows?
4. какие дополнительные возможности разграничения доступа к информационным ресурсам предоставляет шифрующая файловая система?
5. насколько, на Ваш взгляд, удобно использование шифрующей файловой системы (в том числе при необходимости совместной работы над документами)?
6. какой стандартный механизм работы с личными и общими документами предлагается в защищенных версиях операционной системы Windows и насколько, на Ваш взгляд, он удобен?

*Список литературы:*

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## **Лабораторная работа №11. Управление доступом.**

### Цель работы:

Научиться управлять пользователями, группами и компьютерами домена. Данные операции составляют основу повседневной работы администратора компьютерной сети предприятия.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### *Теоретическая часть.*

Для достижения поставленной цели рассматриваются следующие объекты домена и операции управления ими:

- Учетные записи пользователей и компьютеров
- Управление пользователями
- Управление группами
- Управление компьютерами

### **Учетные записи пользователя и компьютера**

Учетные записи пользователей и учетные записи компьютеров в Active Directory представляют собой физические объекты, как компьютер или пользователь.

Группы, а также учетные записи пользователей и компьютеров называются участниками безопасности. Участники безопасности являются объектами каталогов, которым автоматически назначают коды безопасности (SID) для доступа к ресурсам домена.

Учетная запись пользователя или компьютера используется для следующих целей:

- Проверка подлинности пользователя или компьютера.
- Разрешение или запрещение доступа к ресурсам домена.



- Аудит действий, выполняемых с использованием учетной записи пользователя или компьютера. Аудит помогает при наблюдении за безопасностью учетных записей.

### **Учетные записи пользователей**

Учетные записи пользователей, созданные автоматически при установке домена, называются встроенными учетными записями пользователей. После установки Active Directory контейнер Users, расположенный в оснастке Active Directory — пользователи и компьютеры, отображает встроенные учетные записи пользователей: «Администратор», «Гость» .

Учетная запись администратора имеет самые большие права и разрешения в домене, а учетная запись гостя — ограниченные права и разрешения.

- Учетная запись «Администратор»

При помощи учетной записи «Администратор» можно полностью контролировать домен, назначать права пользователей и разрешения управления доступом для пользователей домена. Эта запись должна использоваться только для задач, выполнение которых требует учетных данных администратора. По умолчанию учетная запись «Администратор» назначается членом групп Администраторы, Администраторы домена, Администраторы предприятия, Владельцы-создатели групповой политики и Администраторы схемы в Active Directory. Она не может быть удалена или перемещена из группы «Администраторы», но ее настоятельно рекомендуется переименовать. Поскольку коды безопасности (SID) учетных записей сохраняются, переименованная учетная запись сохраняет все остальные свойства, в том числе описание, пароль, принадлежность к группам, профиль пользователя, учетную информацию, а также любые разрешения и права пользователя.

- Учетная запись «Гость»

Учетная запись Гость используется теми, кто не имеет действительной учетной записи в домене. Если учетная запись пользователя отключена (но не удалена), он также может воспользоваться учетной записью «Гость». Учетная запись «Гость» не требует пароля.

Учетной записи «Гость», как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. По умолчанию учетная запись «Гость» является членом встроенной группы Гости и глобальной группы Гости домена, позволяющих пользователям входить в

домен. По умолчанию она отключена, и рекомендуется оставить ее в этом положении.

### **Защита учетных записей пользователей**

Для обеспечения безопасности проверки подлинности пользователя следует создавать отдельные учетные записи для каждого пользователя сети, применяя для этого оснастку «Active Directory — пользователи и компьютеры». Каждая учетная запись пользователя (включая учетные записи администратора и гостя) может быть добавлена в группу для управления правами и разрешениями, назначенными этой учетной записи. Использование соответствующих этой сети учетных записей и групп позволяет проверить подлинность входящего в сеть пользователя и возможность предоставления ему разрешенных ресурсов.

Повысить защиту домена от атак можно с помощью надежных паролей и политики блокировки учетных записей. Применение политики блокировки учетных записей снижает вероятность проникновения злоумышленника в домен путем повторных попыток. Политика блокировки учетных записей позволяет установить число неудачных попыток входа в систему, после которых учетная запись отключается.

### **Параметры учетных записей**

Каждая учетная запись пользователя Active Directory имеет ряд параметров, относящихся к безопасности и определяющих, как производится проверка подлинности данной учетной записи при входе в сеть. Параметры пароля и безопасности для учетных записей можно настроить указанными ниже способами.

- Потребовать смену пароля при следующем входе в систему

Задает требование смены пользователем пароля при следующем входе в сеть. Параметр используется, когда необходима уверенность в том, что никто, кроме пользователя, не знает его пароля.

- Запретить смену пароля пользователем

Не разрешает пользователю менять пароль. Параметр используется при необходимости контролировать учетную запись пользователя, например учетную запись гостя или временную учетную запись.

- Срок действия пароля не ограничен

Снимает временные ограничения на использование пароля.

- Хранить пароль, используя обратимое шифрование

Позволяет пользователю входить в сеть Windows с компьютеров Apple.

- Отключить учетную запись

Не разрешает использовать данную учетную запись для входа в сеть. Многие администраторы используют отключенные учетные записи в качестве шаблонов для часто употребляемых учетных записей пользователей.

- Требовать смарт-карту для интерактивного входа в сеть

Требует наличия смарт-карты для входа в сеть в интерактивном режиме.

- Учетная запись доверена для делегирования

Позволяет службе использовать данную учетную запись для выполнения операций от имени других пользователей в сети.

- Учетная запись важна и не может быть делегирована
- Использовать для данной учетной записи тип шифрования

DES

Обеспечивает поддержку шифрования с алгоритмом DES (Data Encryption Standard).

### **Управление пользователями:**

Управление пользователями домена включает в себя следующие операции:

- Создание новой учетной записи пользователя
- Смена пароля пользователя
- Копирование учетной записи пользователя
- Перемещение учетной записи пользователя
- Установка времени входа
- Отключение или включение учетной записи пользователя
- Сопоставление сертификата учетной записи пользователя
- Изменение основной группы пользователя
- Удаление учетной записи пользователя

### **Создание новой учетной записи пользователя**

Чтобы создать новую учетную запись пользователя, используя интерфейс Windows, откройте оснастку Active Directory — пользователи и компьютеры.

В дереве консоли щелкните правой кнопкой мыши папку, в которую добавляется учетная запись пользователя, выделите пункт Создать, а затем выберите команду Пользователь.

В поле Имя введите имя пользователя. В поле Инициалы введите инициалы пользователя. В поле Фамилия введите фамилию пользователя.

В поле Имя входа пользователя введите имя входа пользователя, к которому добавляется суффикс UPN(@ имя домена), а если доменов в сети несколько то выберите суффикс UPN в раскрывающемся списке.

В полях Пароль и Подтверждение введите пароль пользователя, а затем выберите соответствующие параметры пароля.

Смена пароля пользователя, копирование или перемещение учетной записи пользователя, отключение или включение учетной записи, смена основной группы пользователя, а также ее удаление осуществляется выбором соответствующей операции, доступной после щелчка правой кнопкой по учетной записи пользователя.

Чтобы установить время входа, щелкните учетную запись пользователя правой кнопкой мыши и выберите команду Свойства.

На вкладке Учетная запись выберите команду Время входа и установите часы, когда пользователю разрешен или запрещен вход в систему.

## **Управление компьютерами**

Каждый компьютер, который присоединяется к домену, имеет учетную запись компьютера. Так же, как и учетные записи пользователей, учетные записи компьютеров предоставляют возможность проверки подлинности и аудита доступа компьютера к сети и к ресурсам домена. Учетная запись компьютера должна быть уникальной. Учетная запись компьютера создается при подключении компьютера к домену.

Учетные записи компьютеров и пользователей добавляются, отключаются, восстанавливаются и удаляются с помощью оснастки Active Directory — пользователи и компьютеры.

Чтобы выполнить операцию с учетной записью компьютера используя интерфейс Windows, откройте оснастку Active Directory — пользователи и

компьютеры, выберите компьютер и соответствующую команду, доступную при щелчке правой кнопкой мыши.

## **Управление группами**

Группы используются для объединения учетных записей пользователей, учетных записей компьютеров и учетных записей групп в управляемые элементы. Использование групп позволяет упростить обслуживание и администрирование сети.

В Active Directory существует два типа групп: группы распространения и группы безопасности. Группы распространения используются только приложениями электронной почты (например, Exchange) для отправки сообщений электронной почты группам пользователей. Группы распространения могут быть использованы для создания списков рассылки электронной почты, а группы безопасности для задания разрешений на использование общих ресурсов.

Группы безопасности обеспечивают эффективное управление доступом к ресурсам сети. Использование групп безопасности позволяет выполнять следующие действия:

- Назначать права пользователя группе безопасности в Active Directory.
- Назначать разрешения на использование ресурсов для групп безопасности.

Не следует путать разрешения с правами пользователей. Разрешения задаются для групп безопасности, использующих общие ресурсы. Разрешения определяют, кто может получить доступ к данному ресурсу и уровень доступа. Права пользователя, заданные для групп безопасности, определяют, что может делать член данной группы в области действий домена или на локальном компьютере рабочей группы.

Группы безопасности перечислены в избирательных таблицах управления доступом, которые определяют разрешения на ресурсы и объекты. Администраторам следует назначать разрешения для ресурсов (общих файлов, принтеров, и т. д.) группам безопасности, а не отдельным пользователям. Разрешения назначаются группе один раз, вместо назначения прав каждому отдельному пользователю. Каждая учетная запись при добавлении к группе получает права, заданные данной группе в Active Directory, и разрешения, определенные для данной группы на ресурсе.

Группы безопасности могут использоваться в качестве адресатов электронной почты, как и группы распространения. Сообщение электронной почты, отправленное группе, отправляется всем членам группы.

Управление группами включает в себя следующие операции:

- Создание новой группы
- Добавление участника группы
- Преобразование типа группы
- Изменение области действия группы
- Удаление группы
- Поиск групп, в которые входит пользователь

### **Создание новой группы**

Чтобы создать новую группу щелкните правой кнопкой мыши папку, в которую добавляется новая группа.

Выделите пункт Создать, а затем выберите команду Группа. Введите имя создаваемой группы. Задавая тип группы, выберите один из предложенных вариантов: группа безопасности или группа распространения.

Задавая область действия группы, выберите один из предложенных вариантов: локальная в домене, глобальная или универсальная (только для групп распространения).

Группы с локальной доменной областью действия могут включать учетные записи и группы с глобальной областью действия, а также группы с универсальной областью действия и группы с локальной доменной областью действия только из данного домена.

Группы с глобальной областью действия могут включать учетные записи и группы с глобальной областью действия из данного домена.

Группы с универсальной областью действия могут включать учетные записи и группы с глобальной областью действия, а также группы с универсальной областью из любого домена.

### **Добавление участника группы**

Чтобы добавить участника группы выберите команду Свойства данной группы и на вкладке «Члены групп» нажмите кнопку Добавить.

В поле Введите имена выбираемых объектов введите имя пользователя, группы или компьютера, добавляемых к выбранной группе и нажмите кнопку ОК. Можно воспользоваться кнопками «Дополнительно» и «Поиск», а затем выбрать добавляемый объект из списка доступных в домене.

### **Преобразование типа группы**

Чтобы преобразовать тип группы выберите папку, включающую группу, тип которой необходимо изменить. В области сведений щелкните правой кнопкой мыши необходимую группу и выберите команду Свойства.

На вкладке Общие в группе Тип группы выберите тип группы.

### **Изменение области действия группы**

Чтобы изменить область действия группы выберите папку, включающую группу, для которой необходимо изменить область действия. В области сведений щелкните правой кнопкой мыши необходимую группу и выберите команду Свойства.

На вкладке Общие в разделе Область действия группы выберите область действия группы.

### **Удаление группы**

Чтобы удалить группу выберите папку, включающую группу, которую необходимо удалить.

На панели сведений щелкните правой кнопкой мыши необходимую группу и выберите команду Удалить.

### **Поиск групп, в которые входит пользователь**

Чтобы найти группы, в которые входит пользователь, в дереве консоли Active Directory щелкните узел Пользователи.

Можно также выбрать папку, содержащую учетную запись пользователя. На панели сведений щелкните правой кнопкой мыши учетную запись пользователя и выберите команду Свойства. Выберите вкладку Член групп и определите, в какие группы входит данный пользователь.

### **Практическая часть:**

#### **1. Создание групп**

Создайте две группы безопасности с локальной доменной областью действия, например группу Разработчики и группу Менеджеры.

Создайте две группы безопасности с глобальной областью действия, например группу Инженеры и группу Экономисты.

#### **2. Создание учетных записей пользователей и помещение их в группы**

Создайте по одной учетной записи для каждой из созданных групп, задавая в качестве параметра человеческие имена.

Создайте одну учетную запись, которую поместите в каждую из созданных групп.

### 3. Включение групп в другие группы

Поместите глобальную группу Инженеры в локальную группу Разработчики, а глобальную группу Экономисты в локальную группу Менеджеры.

4. Создайте учетную запись для нового компьютера WorkStation1, который предполагается подключить к домену.

5. Создайте произвольную группу, учетную запись пользователя и учетную запись компьютера. Выполните с ними все описанные в теоретическом разделе работы операции по управлению ими и после показа результатов преподавателю, удалите эти временные объекты.

### *Контрольные вопросы:*

1. Какие типы групп могут быть созданы в домене?
2. Чем отличаются группы безопасности от групп распространения?
3. Назовите порядок размещения пользователей и групп в группах домена большого предприятия с несколькими доменами.
4. В чем главное отличие групп локального компьютера от групп домена?
5. Почему уровень безопасности сети на основе домена выше, чем в одноранговой сети?
6. В чем отличие глобальных и локальных доменных групп?
7. Какие группы могут быть отнесены к универсальным группам домена?
8. Как создается учетная запись компьютера в домене?
9. Как создается учетная запись пользователя домена?
10. Какими учетными записями должен обладать пользователь для того, чтобы он мог выполнить первоначальное присоединение компьютера к домену?

### *Список литературы:*

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В.



Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

## **Лабораторная работа №12. Аудит и журналы безопасности.**

### Цель работы:

Научить студентов проводить настройку аудита событий безопасности и использовать журналы безопасности для повышения защищенности системы.

### Компетенции:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

### Теоретическая часть.

Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношения к безопасности. Аудит сопровождается записью информации о контролируемых событиях в специальные журналы безопасности, контролируемые администратором. Журналы позволяют контролировать поведение и использование тех ресурсов, для которых администратор назначил проведение аудита.

Аудит по умолчанию отключен, и для его настройки и введения в действие необходимо сначала активизировать аудит через настройки, управляющие политикой безопасности домена (Групповая политика) или компьютера (Локальная политика безопасности).

Затем можно выполнить настройку выбранного типа аудита применительно к объектам системы и ее пользователям.

### Практическая часть.

Чтобы активизировать аудит на локальном компьютере или в масштабах домена, необходимо выполнить следующие действия.

Для локального компьютера на Панели управления в разделе Администрирование выберите Локальные параметры безопасности или в качестве альтернативы запустите в строке Выполнить программу `secpol.msc`.

В открывшейся оснастке (рисунок 5.1) выберите пункт Локальные политики и раскройте пункт Политика аудита. В правой части окна появится список типов действий аудита. Поначалу ни один из видов аудита не проводится и необходимо активизировать аудит.

Дважды щелкните на каждой политике, для которой необходимо активизировать аудит и затем установите флажки Успех и (или) Отказ. Аналогичные действия при управлении доменом выполняются с помощью оснастки Групповая политика безопасности в разделе Администрирование контроллера домена.

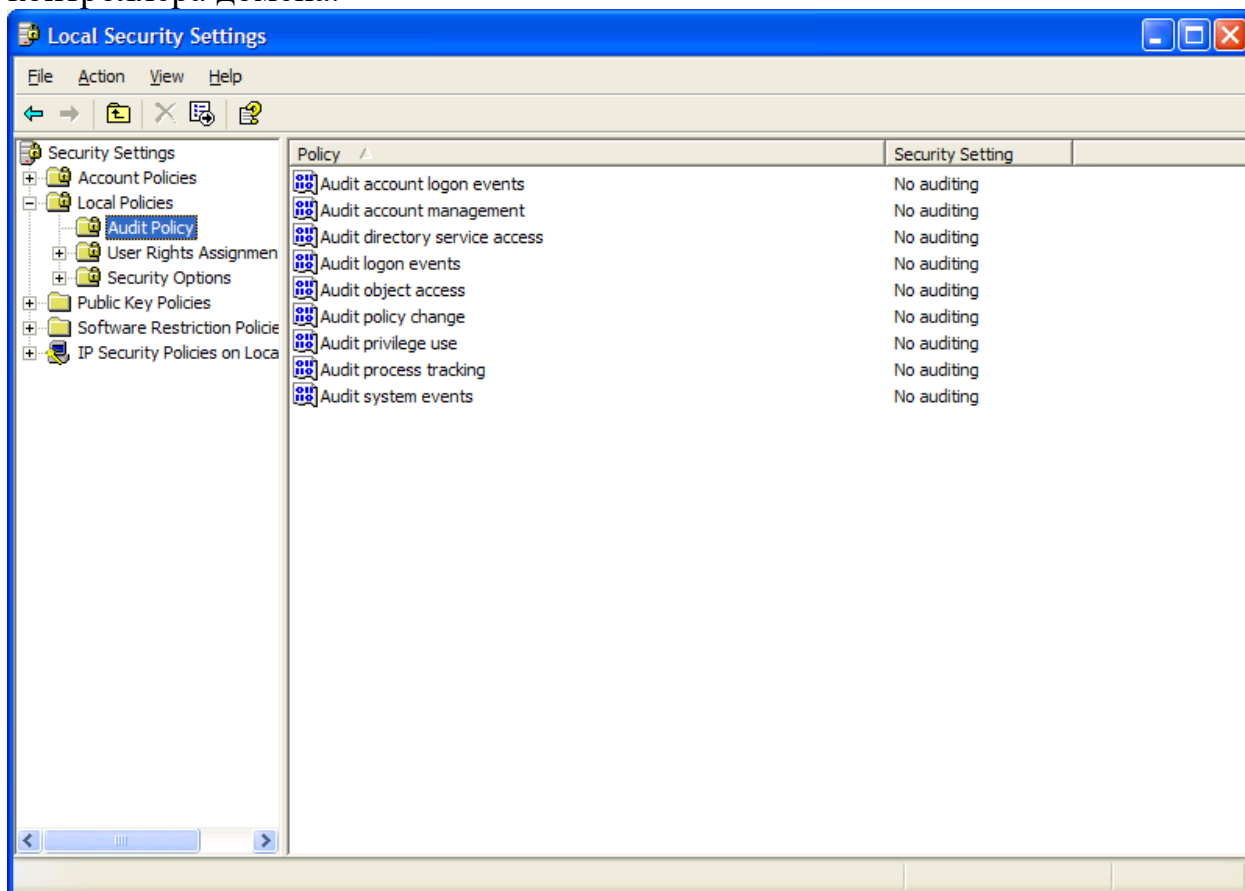


Рисунок 5.1 Выбор оснастки Локальная политика безопасности

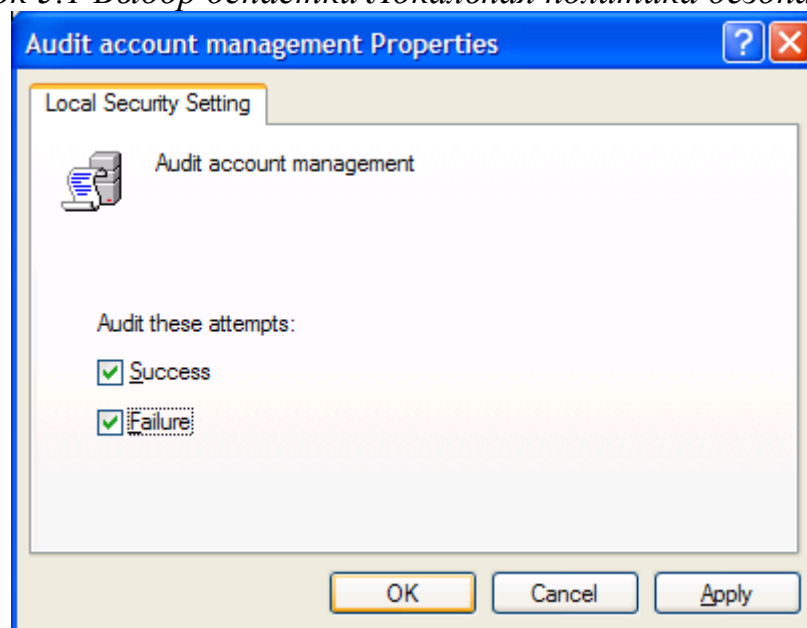


Рисунок 5.2 Установка событий для аудита

Основные события, которые могут быть подвергнуты аудиту, описываются в таблице.

Политика аудита	Описание политики
Аудит событий входа по учетной записи	Эти события возникают в контроллере домена, когда пользователь выполняет вход или выход на другом компьютере, входящем в домен
Аудит управления учетными записями	Эти события возникают при создании, изменении или удалении учетной записи или группы, переименовании, активизации или отключении учетной записи, когда задается или изменяется пароль
Аудит доступа к службе каталогов	Эти события возникают, когда выполняется доступ к объекту Active Directory
Аудит событий входа	Эти события возникают, когда пользователь выполняет вход или выход на рабочей станции или подсоединяется через сеть.
Аудит доступа к объектам	Эти события возникают, когда пользователь выполняет доступ к файлу, папке, принтеру, ключу реестра или другому объекту, для которого задан аудит
Аудит изменения политики	Эти события возникают, когда вносятся изменения в политики назначения прав пользователей, политики аудита
Аудит системных событий	Эти события возникают, когда пользователь перезагружает компьютер или завершает его работу либо при возникновении события, которое влияет на безопасность компьютера

В лабораторной работе выполняется настройка аудита для папок и файлов, т.е. выбирается тип аудита - Аудит доступа к объектам.

Для настройки аудита в качестве объекта аудита выберите папку или файл, в диалоговом окне Свойства используйте вкладку Безопасность и по кнопке Дополнительно перейдите в диалоговое окно Параметры управления доступом. Откройте вкладку Аудит (рисунок 5.3). Добавьте пользователей или группы (кнопка Добавить).

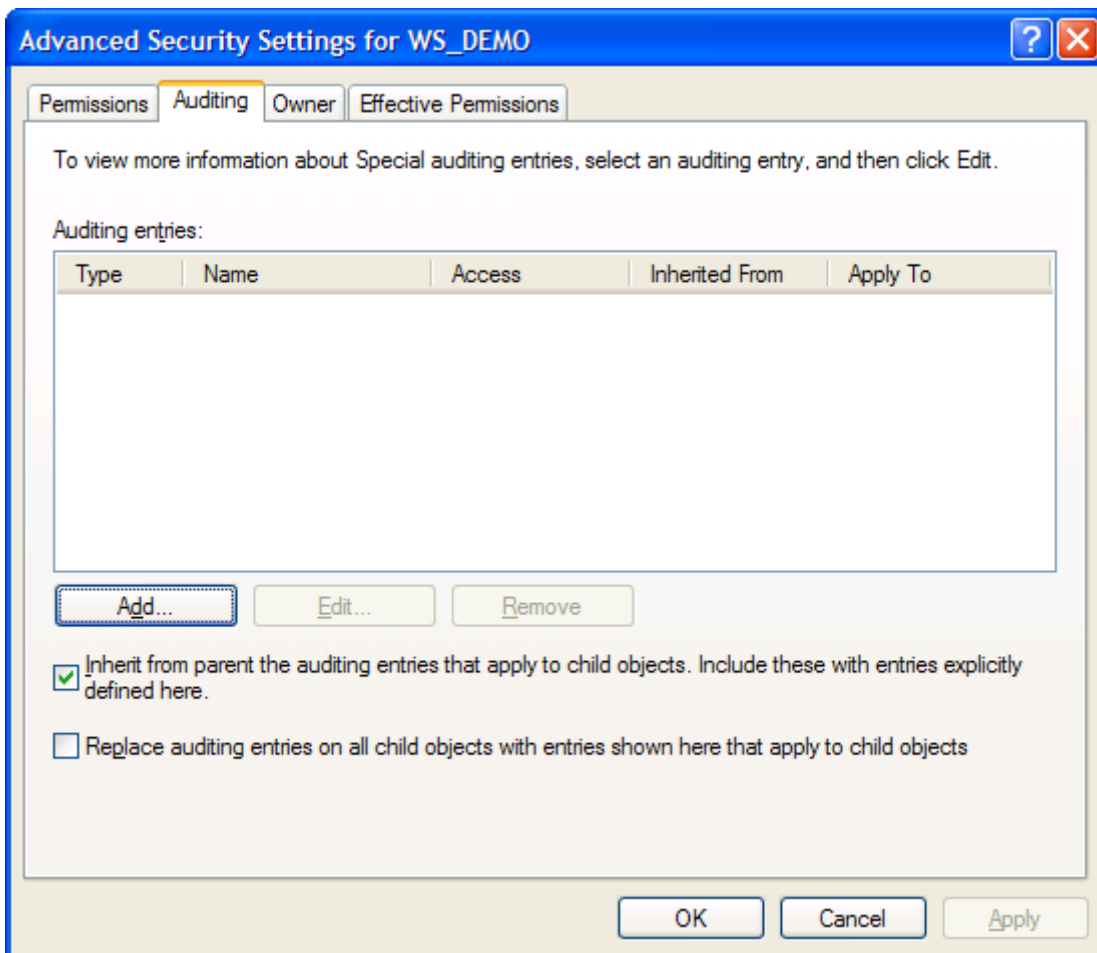


Рисунок 5.3 Выбор объектов аудита

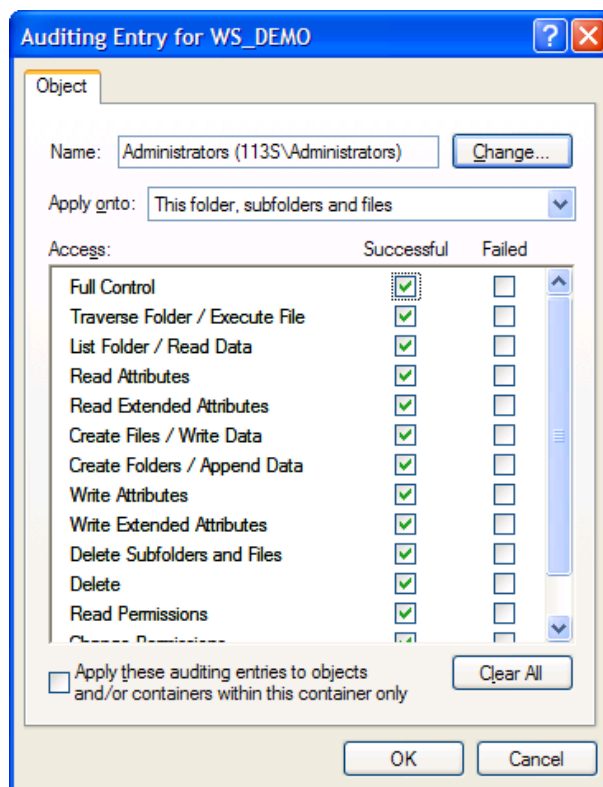
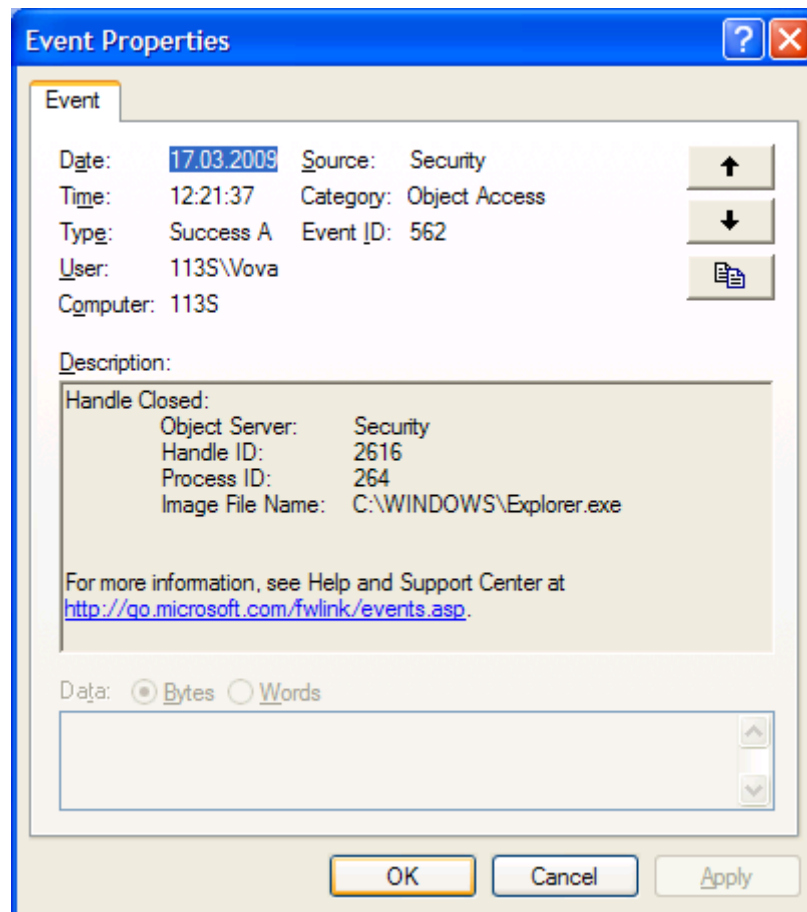


Рисунок 5.4 Установка действий, контролируемых при аудите





*Рисунок 5.6 Просмотр информации о событии безопасности*

### **Задание к лабораторной работе**

С целью освоения настройки аудита и его использования для повышения безопасности системы выполните следующие действия:

1. Войдите на виртуальную машину с учетной записью администратора
2. Активизируйте средствами политики безопасности аудит доступа к объекта (Успех и Отказ).
3. Создайте временную папку и текстовый файл внутри ее.
4. Выберите эту папку как объект аудита
5. Настройте аудит доступа к папке для администратора и пользователя компьютера, ограничив пользователя в возможных действиях с папкой и файлом, чтобы в ряде случаев происходило событие Отказ.
6. Выполните ряд типовых действий с папкой и файлом от имени администратора и затем от имени пользователя.
7. Прочитайте журнал событий Безопасности и найдите в нем записи, в которых отражены ваши действия с объектами как о имени администратора, так и от имени пользователя. Сделайте соответствующие выводы.
8. Результаты в виде экранов и текстов должны быть сохранены в файле отчета по лабораторной работе и представлены к защите.

9. Самостоятельно освоите настройку аудита для принтеров.

*Контрольные вопросы:*

1. Какова роль аудита в обеспечении безопасности компьютерной системы?
2. Где и каким образом формируется информация о событиях аудита?
3. Какая информация может быть получена в результате аудита?
4. Какие типы аудита вы знаете и для чего предназначен каждый из них?
5. Каким образом активизируется политика аудита?
6. Каким образом политика аудита применяется для выбранных объектов и пользователей?
7. В каких случаях целесообразно учитывать Успех, а когда целесообразно фиксировать Отказ?
8. Как пользоваться журналами безопасности?
9. Какие учетные записи дают право на настройку аудита и проверку результатов аудита?
10. Каким образом администратор может использовать информацию об аудите для повышения безопасности системы?

*Список литературы:*

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.