МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине «Программно-аппаратные средства защиты информации»
для студентов направления подготовки /специальности
10.03.01 Информационная безопасность
шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Введение

Целью методических рекомендаций по изучению дисциплины является закрепление и углубление знаний, полученных при изучении теоретического материала по дисциплине «Программно-аппаратные средства защиты информации».

Целью проведения практических занятий является:

1. Обобщение, систематизация, закрепление полученных теоретических знаний по темам конкретным требованиям дисциплины
2. Формирование умений применять полученные знания на практике
3. Выработка оптимальных решений при решении практических задач предметной области

Данное пособие содержит весь необходимый материал для выполнения практических работ с целью освоения курса «Программно-аппаратные средства вычислительной техники».

Методические рекомендации призваны обеспечить эффективность самостоятельной работы студентов с литературой, на основе рациональной организации ее изучения, облегчить подготовку студентов к сдаче экзамена, сориентировать их в направлении изучения материала по поставленным вопросам, дать возможность отработать навыки составления и оформления различных видов документов, как под контролем преподавателя, так и самостоятельно.

Перед подготовкой к занятию студенты должны ознакомиться с планом практического (семинарского) занятия, а также с учебной программой по данной теме, что поможет студенту сориентироваться при проработке вопроса и правильно составить план ответа; изучение конспекта лекций, разделов учебников, ознакомление с дополнительной литературой, рекомендованной к занятию. Студенты должны готовить краткий конспект ответов на все вопросы, знать определения основных понятий.

Количество часов на практические занятия по рабочей программе предусмотрено для направления подготовки 10.03.01 « Информационная безопасность» - 45 часов.

Содержание

Практическая работа 1
Сбор данных об информационной системе с помощью средств администрирования Windows.

Цель: сбор данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий *доступ* файловых ресурсах.

Знать: сбор данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий *доступ* файловых ресурсах.
Уметь: провести сбор данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий *доступ* файловых ресурсах.

Теоретическая часть

Для проведения оценки рисков необходимо провести инвентаризацию активов информационной системы (ИС). Если в ИС используются домены *Windows*, для получения данных о системе можно использовать средства администрирования, реализованные в виде оснасток консоли администрирования (Microsoft *management* console - *mmc*).

Используемые в данной работе инструменты могут быть запущены из раздела **"Администрирование"** *меню* **"Пуск"** или через **"Панель управления" (Пуск Панель управления Администрирование)**.

Из раздела **"Администрирование"** запустите **Active Directory Users and Computers**. В раскрывающемся списке объектов выберите **Ваш домен**, там откройте перечень компьютеров (*папка* **Computers** - рис. 1.).

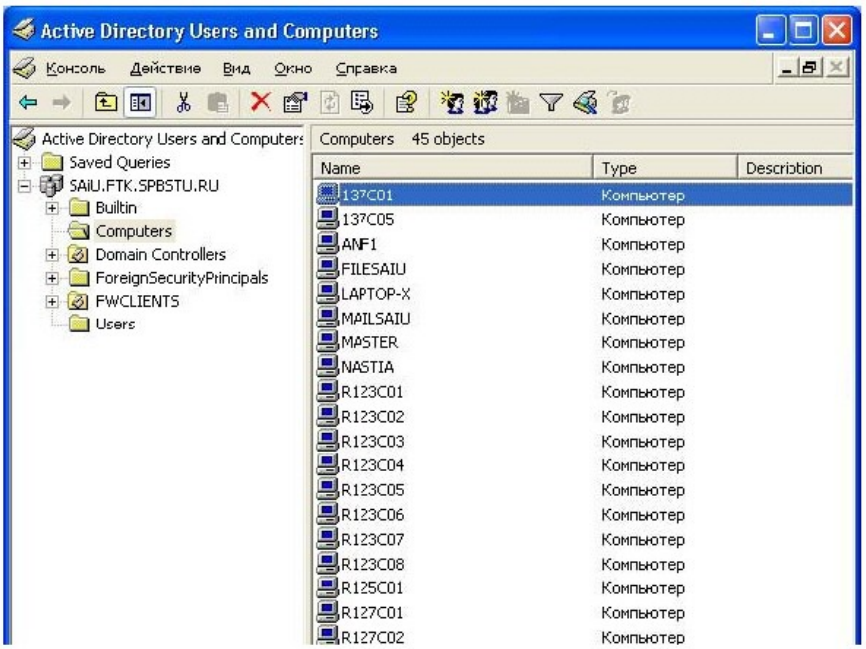

Рис. 1- Получение перечня компьютеров домена

С помощью кнопки панели инструментов **"Экспорт списка"** (на кнопке изображение списка и стрелки) *список* компьютеров можно экспортировать в *текстовый файл* для дальнейшей обработки. В свойствах компьютера отображается название и версия установленной операционной системы (рис. 2). Также там может быть дополнительная *информация*, например, описывающая *размещение*.

Аналогичные данные о контроллерах домена можно получить в разделе **Domain Controllers**. Данные о пользователях и их группах доступны в разделе **Users**. Надо отметить, что представленное распределение *по* разделам не является обязательным. В процессе администрирования могут создаваться новые *подразделения* (OU - Organization Unit) и объекты (например, пользователи или компьютеры) - помещаться в них.

Информацию о соответствии имен компьютеров IP-адресам можно получить, используя *утилиту командной строки* **nslookup** или административную оснастку **"DNS"**. Например, узнать *IP-адрес* компьютера http://comp1.mcompany.ru можно с помощью команды nslookup comp1.mcompany.ru Часто действующие настройки в сети таковы, что ip-адреса компьютерам выделяются динамически, с использованием службы **dhcp**, и могут периодически меняться. Как правило, у серверов ip-адреса постоянны.

Теперь перейдем к этапу сбора данных об информационных ресурсах, поддерживаемых на компьютере. Перечень предоставляемых в общий *доступ* папок можно получить с помощью оснастки **"Управление компьютером"**. На рис. 3 представлен пример перечня ресурсов рабочей станции, предоставляемых в общий *доступ* в служебных целях. Этот *список* можно также экспортировать в *текстовый файл*.

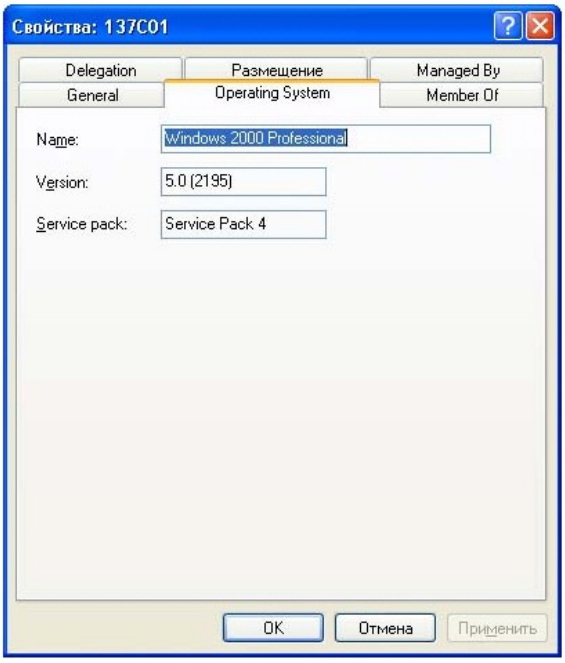

Рис. 2- Информация о компьютере

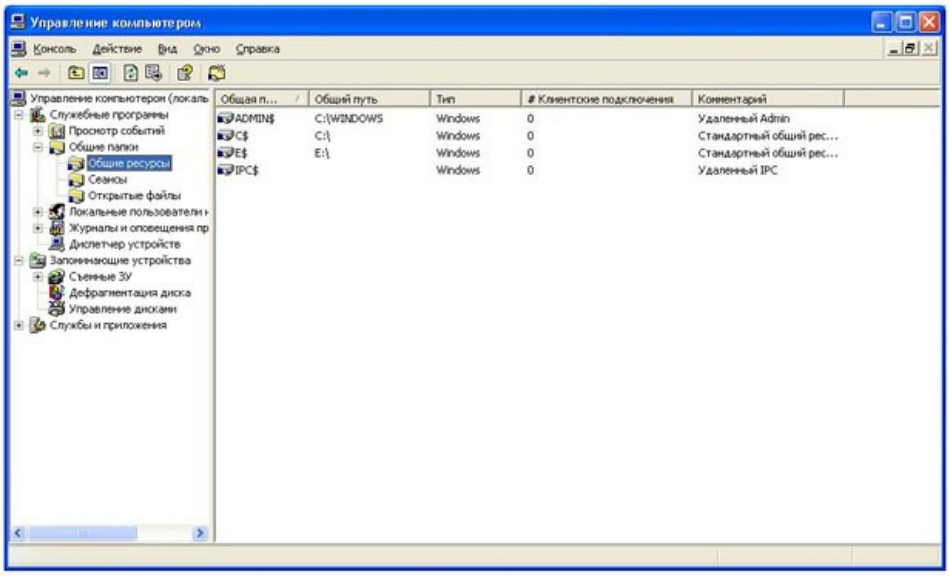

Рис. 3- Пример перечня общих ресурсов рабочей станции

Более интересен будет подобный *список* для файлового сервера. Чтобы его увидеть, надо подключить оснастку **"Управление компьютером"** для сервера. Запустите *консоль MMC* (**Пуск→Выполнить→mmc**), в *меню* выберите добавление новой оснастки (рис. 4), выберите оснастку **"Управление компьютером"** и укажите, что она будет использоваться для другого компьютера (рис. 5).

В остальном для пользователя все будет происходить так же, как и при работе с локальным компьютером.

В свойствах ресурса можно узнать о разрешениях, которые установлены на него как для разделяемого ресурса (рис. 6), а на вкладке **"Безопасность"** - разрешениях файловой системы *NTFS* (если *папка* расположена на разделе с этой файловой системой, а не с *FAT*).

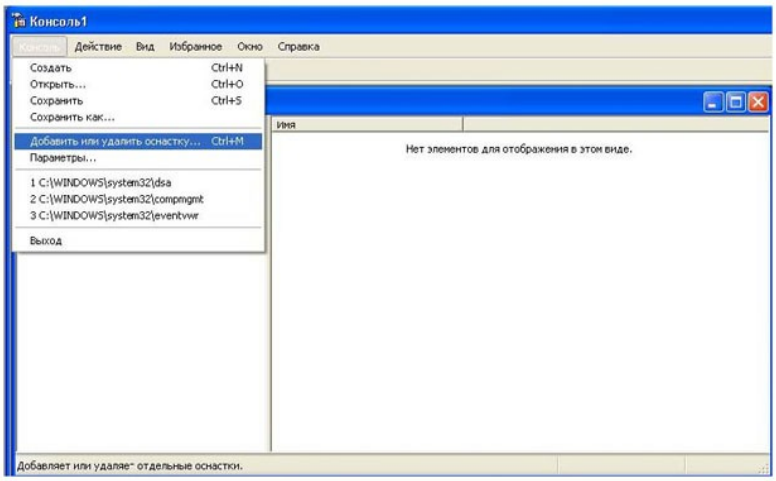

Рис. 4- Добавление новой оснастки

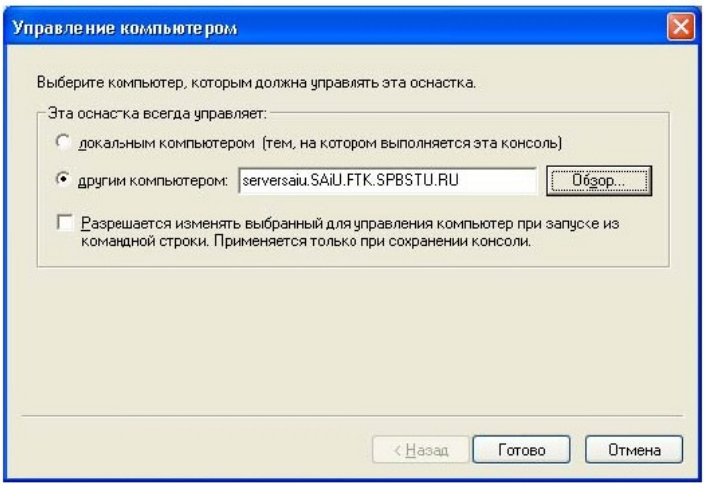

Рис. 5- Выбор компьютера

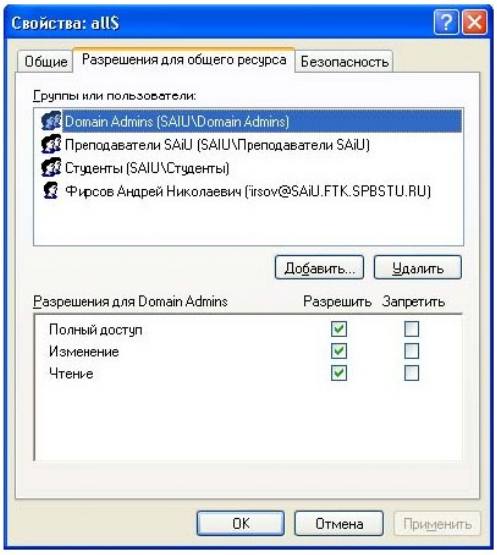

Рис. 6- Разрешения

Вопросы:

1. Линии связей локальных сетей.
2. Обеспечение секретности передаваемой информации в локальных сетях.
3. Типы линий связи локальных сетей.
4. Бескабельные каналы связи локальных сетей.
5. Базовые технологии локальных сетей.
6. Нестандартные топологии локальных сетей.
7. Согласование и экранирование линий связи.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 2

Сбор данных о топологии сети с помощью средства администрирования сетей.

Цель: Изучение различных вариантов сбора данных о топологии сети с помощью средств администрирования сетей с помощью *3Com Network Supervisor* .

Знать: топологию сети; средства администрирования сетей с помощью *3Com Network Supervisor* .

Уметь: производить выбор документируемой сети; соединения по типам подключений; свойства коммутатора; средства удаленного администрирования.

Актуальность темы объясняется особенностями подготовки бакалавров по инженерным направлениям.

Теоретическая часть

Продолжая тему инвентаризации активов информационной системы (ИС), перейдем к рассмотрению средств, позволяющих получить данные о составе и топологии сети. В качестве примера в данной лабораторной работе будет использоваться *утилита 3Com Network Supervisor*, которую можно бесплатно получить с сайта компании *3Com* (http://www.3com.com). Аналогичные *по* функциональности продукты есть и у других производителей сетевого оборудования.

При запуске программы предлагается выбор - строить новую карту сети или открыть существующую. При выборе создания новой карты надо указать, какая *подсеть* документируется (рис. 1). На рисунке выбрана локальная *подсеть*, т.е. та ip-*сеть*, к которой относится *компьютер*, на котором выполняется *3Com Network Supervisor*.

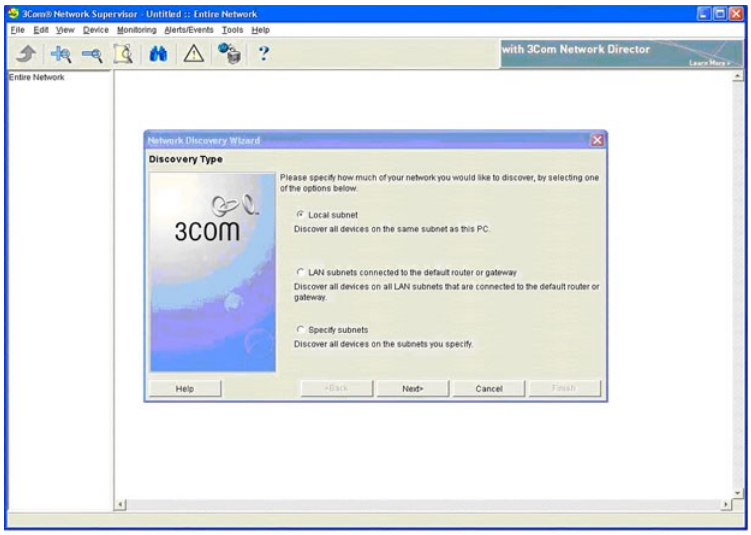

Рис. 1- Выбор документируемой сети

На рис. 2 представлен пример карты сети, которую строит *утилита*. Надо отметить, что наиболее информативна такая карта будет в том случае, если в сети используется управляемое сетевое оборудование *3Com*, поддерживающее, в частности, протокол *SNMP*. В то же время, польза от составления карты будет и в случае отсутствия в сети подобного оборудования.

Для того, чтобы это продемонстрировать, были сделаны следующие настройки. Каждому из компьютеров были присвоены ip-адреса из двух сетей класса С - 192.168.1.0 и

192.168.100.0. Управляемому коммутатору *3Com* SuperStack II *Switch* 3000 назначен *адрес* 192.168.100.6, т.е. он "виден" только при построении карты сети 192.168.100.0. *DNS* серверы доступны только в сети 192.168.1.0, поэтому на рисунках, относящихся ко второй сети, компьютеры идентифицируются только ip-адресами. Карта сети 192.168.1.0 представлена на рис. 3.

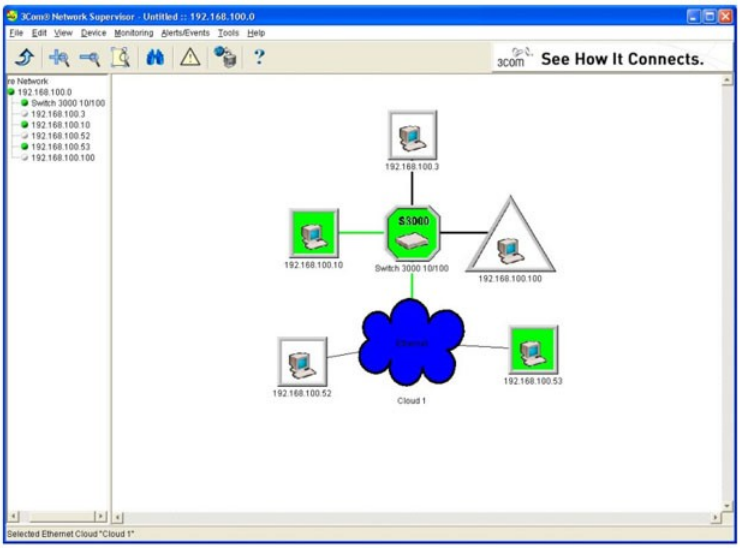

Рис. 2- Карта сети 192.168.100.0. Cloud 1 скрывает неуправляемый коммутатор

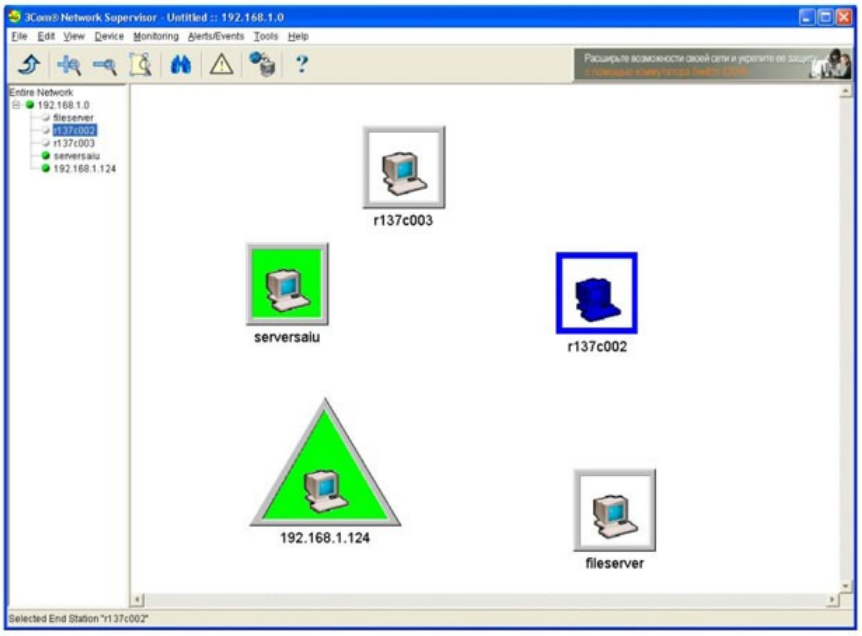

Рис. 3- Карта сети 192.168.1.0. Информация от управляемого коммутатора недоступна

Для выбранного узла можно потребовать провести *мониторинг* загрузки различных сетевых сервисов или обратиться к средствам *удаленного администрирования*, использующим протоколы http, telnet или *ssh* (рис.4,5).

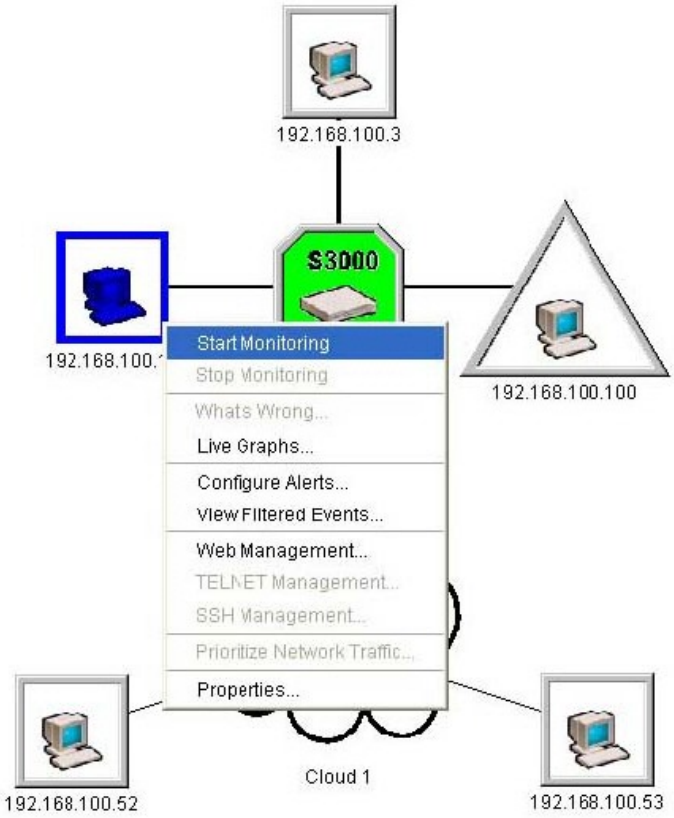

Рис. 4- Функции, доступные для выбранного узла

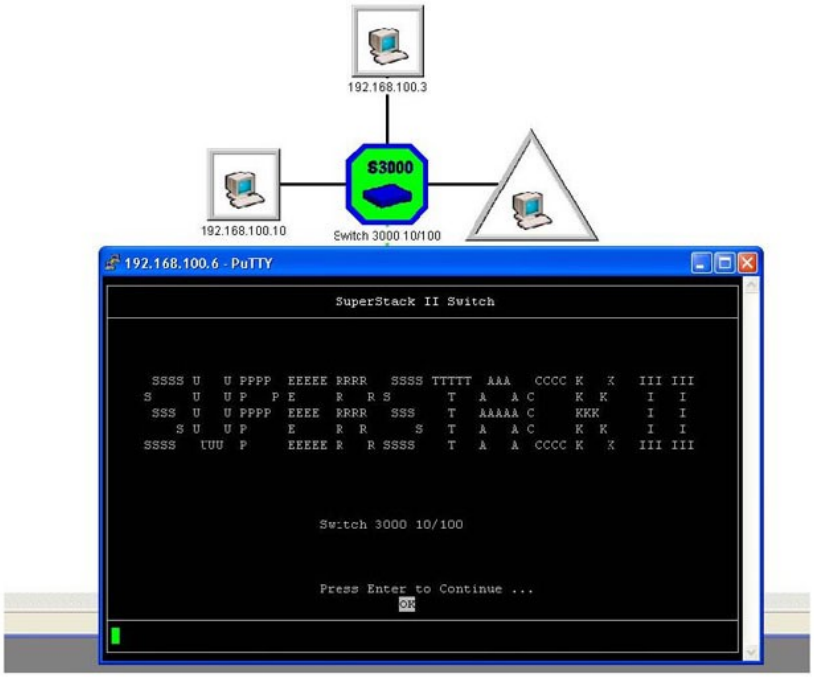

Рис. 5- Запуск удаленного терминала для администрирования коммутатора Switch 3000

Функция поиска (кнопка панели инструментов с изображением бинокля) позволяет, в частности, отобразить информацию о типах используемых сетевых подключений (рис. 6,7).

Через свойства управляемого коммутатора доступна *информация* о том, к какому порту какой узел подключен и графики загрузки (рис. 8,9).

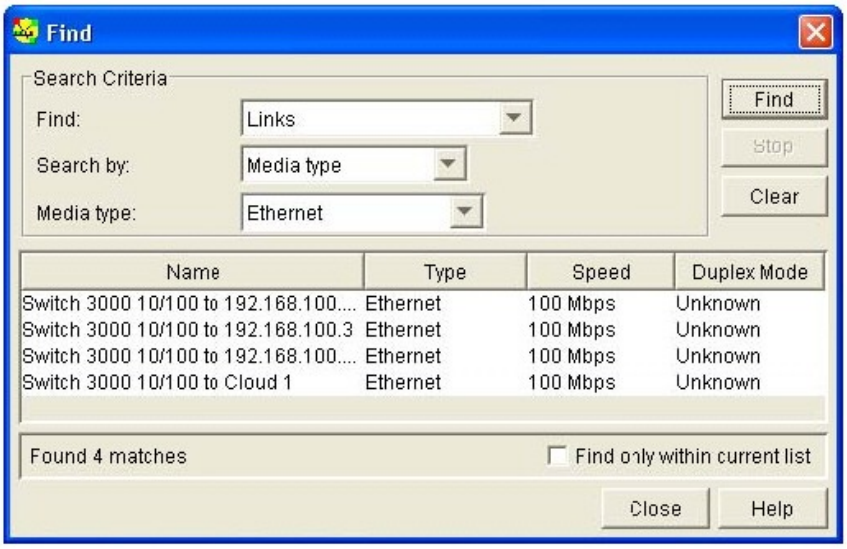

Рис. 6- Соединения по типам подключений. Ethernet

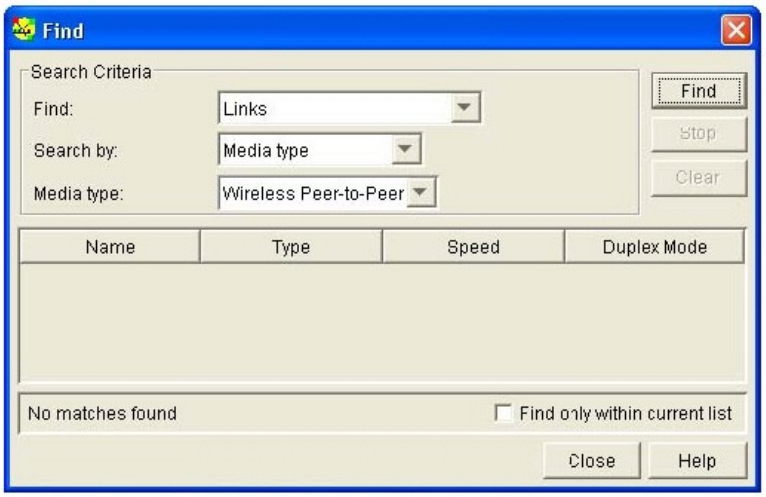

Рис. 7- Соединения по типам подключений. Беспроводные подключения (отсутствуют)

Собранная *информация* может отображаться в виде отчетов, формируемых в формате *HTML*. *Опция* доступна через *меню* **Tools пункт Reports**. Для задач, связанных с инвентаризацией системы, наибольший интерес представляют отчеты **Inventory Report** и **Topology Report**.

Отчет *по* топологии сети 192.168.1.0 состоит из записи "Нет данных", т.к. данные о топологии *программа 3Com Network Supervisor* получить не смогла (в этой сети управляемый *коммутатор* "невидим", т.к. его *адрес* принадлежит другой ip-сети).

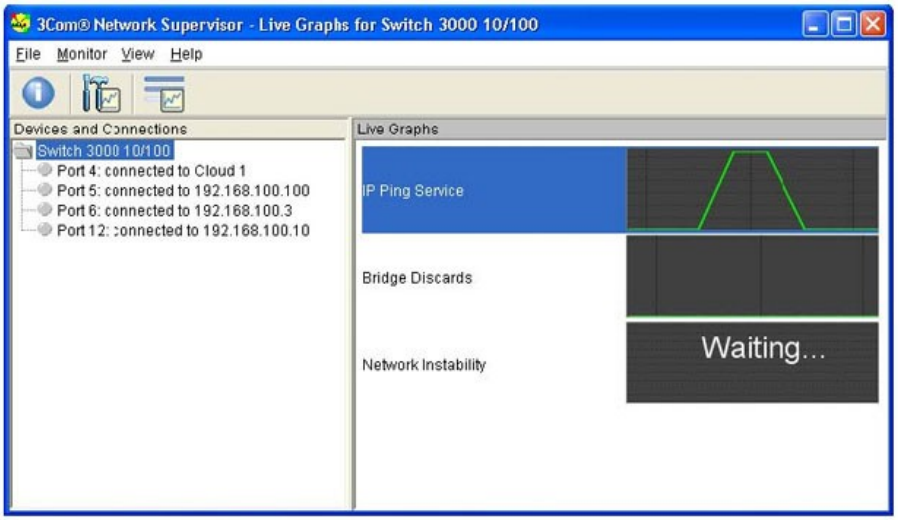

Рис.8- Данные о подключениях и графики

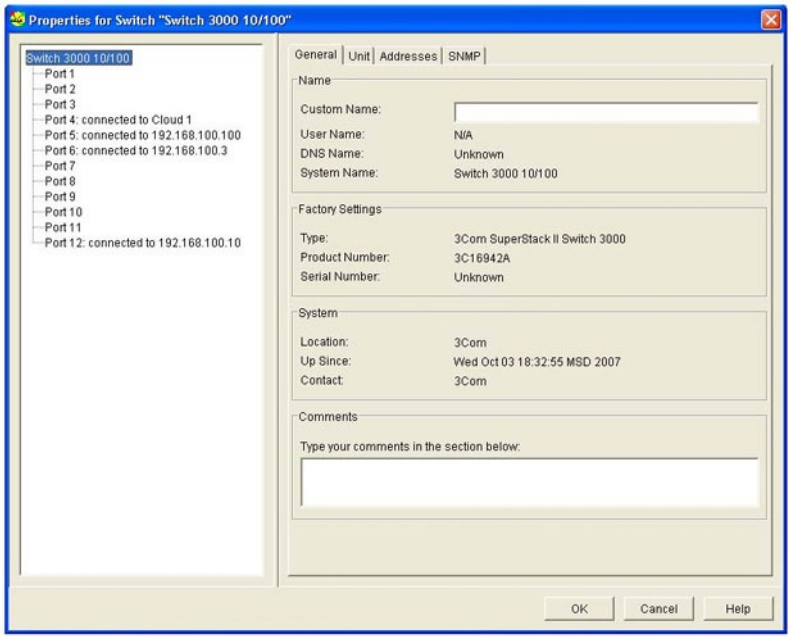

Рис. 9- Свойства коммутатора

Вопросы

1. С помощью *3Com Network Supervisor* постройте карту сети учебной лаборатории.
2. Опишите узлы сети, используемые типы соединений.
3. Опишите доступные средства *удаленного администрирования*.
4. Перечислите используемые сетевые устройства.
5. Укажите, какие последствия будут при выходе из строя (или некорректной работе) каждого из сетевого устройства.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-

7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

3. http://www.biblioclub.ru/ - электронная библиотека
4. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 3.
Идентификация и аутентификация систем семейства Microsoft Windows.

Цель работы: изучить способы идентификации и аутентификации систем семейства Microsoft Windows.

Знать: систему идентификации и аутентификации; двухфакторную аутентификацию; утилиты Microsoft Baseline Security Analyzer; проверку администраторами безопасности качества используемых паролей путем имитации атак; ограничение числа неудачных попыток ввода пароля.

Уметь: оперировать с парольными системами аутентификации; учетной записью пользователя.

Теоретическая часть.

В данной теме будут рассмотрены некоторые технические меры повышения защищенности систем. Выбор рассматриваемых мер обусловлен возможностью их реализации встроенными средствами операционных систем семейства Microsoft *Windows*. Соответственно, уровень защищенности может быть повышен без дополнительных затрат на специализированные средства защиты.

Рассматриваемые вопросы можно разделить на две группы:

- вопросы, связанные с *идентификацией и аутентификацией* пользователей;
- защита передаваемых сообщений.

Идентификация и аутентификация

Идентификация - присвоение пользователям идентификаторов (уникальных имен или меток) под которыми система "знает" пользователя. Кроме идентификации пользователей, может проводиться *идентификация* групп пользователей, ресурсов ИС и т.д.

Идентификация нужна и для других системных задач, например, для ведения журналов событий. В большинстве случаев *идентификация* сопровождается аутентификацией.

Аутентификация - установление подлинности - проверка принадлежности пользователю предъявленного им идентификатора. Например, в начале сеанса работы в ИС *пользователь* вводит имя и *пароль*. На основании этих данных система проводит идентификацию (*по* имени пользователя) и аутентификацию (сопоставляя *имя пользователя* и введенный *пароль*).

Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от несанкционированного доступа (НСД) любой информационной системы. В соответствии с рассмотренной ранее моделью многоуровневой защиты, *аутентификация* пользователя компьютера относится к уровню защиты узлов.

Обычно выделяют 3 группы методов аутентификации.

1. Аутентификация по наличию у пользователя уникального объекта заданного типа. Иногда этот класс методов аутентификации называют по-английски "I have" ("у меня есть"). В качестве примера можно привести аутентификацию с помощью смарт-карт или электронных USB-ключей.

2. Аутентификация, основанная на том, что пользователю известна некоторая конфиденциальная информация - "I know" ("я знаю"). Например, аутентификация по паролю. Более подробно парольные системы рассматриваются далее в этом разделе.

3. Аутентификация пользователя по его собственным уникальным характеристикам - "I am" ("я есть"). Эти методы также называются биометрическими.

Нередко используются комбинированные схемы аутентификации, объединяющие методы разных классов. Например, двухфакторная *аутентификация - пользователь* предъявляет системе смарт-карту и вводит пин-код для ее активации.

Наиболее распространенными на данный момент являются парольные *системы аутентификации*. У пользователя есть *идентификатор* и *пароль*, т.е. секретная *информация*, известная только пользователю (и возможно - системе), которая используется для прохождения аутентификации.

В зависимости от реализации системы, *пароль* может быть одноразовым или многоразовым. Операционные системы, как правило, проводят аутентификацию с использованием многоразовых паролей. Совокупность идентификатора, пароля и, возможно, дополнительной информации, служащей для описания пользователя составляют **учетную запись пользователя**.

Если нарушитель узнал *пароль* легального пользователя, то он может, например, войти в систему под его учетной записью и получить *доступ* к конфиденциальным данным. Поэтому безопасности паролей следует уделять особой внимание.

Как отмечалось при рассмотрении стандарта *ISO 17799*, рекомендуется, чтобы пользователи системы подписывали документ о сохранении конфиденциальности пароля. Но нарушитель также может попытаться подобрать *пароль*, угадать его, перехватить и т.д. Рассмотрим некоторые рекомендации *по* администрированию парольной системы, позволяющие снизить *вероятность* реализации подобных угроз.

1. Задание минимальной длины используемых в системе паролей. Это усложняет атаку путем подбора паролей. Как правило, рекомендуют устанавливать минимальную длину в 6-8 символов.
2. Установка требования использовать в пароле разные группы символов - большие и маленькие буквы, цифры, специальные символы. Это также усложняет подбор.
3. Периодическая проверка *администраторами безопасности* качества используемых паролей путем *имитации атак*, таких как подбор паролей "по словарю" (т.е. проверка на использование в качестве пароля слов естественного языка и простых комбинаций символов, таких как "1234").
4. Установка максимального и минимального сроков жизни пароля, использование механизма принудительной смены старых паролей.
5. Ограничение числа неудачных попыток ввода пароля (блокирование учетной записи после заданного числа неудачных попыток войти в систему).
6. Ведение журнала истории паролей, чтобы пользователи, после принудительной смены пароля, не могли вновь выбрать себе старый, возможно скомпрометированный пароль.

Современные операционные системы семейства *Windows* позволяют делать установки, автоматически контролирующие выполнение требований 1,2,4-6. При использовании домена *Windows*, эти требования можно распространить на все компьютеры, входящие в *домен* и таким образом повысить защищенность всей сети.

Но при внедрении новых механизмов защиты могут появиться и нежелательные последствия. Например, требования "сложности" паролей могут поставить в *тупик* недостаточно подготовленного пользователя. В данном случае потребуется объяснить, что с точки зрения операционной системы *Windows* надежный *пароль* содержит 3 из 4 групп символов (большие буквы, малые буквы, цифры, служебные знаки).

Аналогичным образом, надо подготовить пользователей и к внедрению блокировки учетных записей после нескольких неудачных попыток ввода пароля. Требуется объяснить пользователям, что происходит, а сами правила блокировки должны быть хорошо продуманы. Например, если высока *вероятность* того, что *пользователь* заблокирует

свою *запись* в период отсутствия администратора, лучше ставить блокировку не насовсем, а на какой-то срок (30 минут, час и т.д.).

Это приводит к тому, что должна быть разработана политика *управления паролями*, сопровождающие ее документы, а потом уже проведено внедрение.

При использовании ОС семейства *Windows*, выявить учетные записи со слабыми или отсутствующими паролями можно, например, с помощью утилиты Microsoft *Baseline Security Analyzer*. Она же позволяет выявить и другие ошибки администрирования. Вопросам использования этой утилиты, а также настройке политики паролей посвящена данная лабораторная работа.

Вопросы:

1. Система идентификации и аутентификации.
2. Утилиты Microsoft Baseline Security Analyzer.
3. Двухфакторная аутентификация.
4. Парольные системы аутентификации.
5. Учетная запись пользователя.
6. Задание минимальной длины используемых в системе паролей.
7. Проверка администраторами безопасности качества используемых паролей путем имитации атак.
8. Ограничение числа неудачных попыток ввода пароля.
9. Журнал истории паролей.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 4.
Аутентификация по протоколу Kerberos.

Цель: изучение стандарта системы централизованной аутентификации и распределения ключей в рамках операционной системы Windows.

Знать: аутентификацию с использованием протокола Kerberos v.5; централизованное распределение ключей симметричного шифрования; Серверную часть Kerberos как центр распределения ключей.

Уметь: применять протокол Kerberos; производить взаимодействие между Kerberos-областями.

Актуальность темы изучение стандарта системы централизованной аутентификации и распределения ключей в рамках операционной системы Windows.

Теоретическая часть

Протокол Kerberos был разработан в Массачусетском технологическом институте в середине 1980-х годов и сейчас является фактическим стандартом системы централизованной аутентификации и *распределения ключей* симметричного шифрования. Поддерживается операционными системами семейства Unix, *Windows* (начиная с *Windows*'2000), есть реализации для *Mac* OS.

В сетях *Windows* (начиная с *Windows*'2000 Serv.) *аутентификация по* протоколу Kerberos v.5 (*RFC* 1510) реализована на уровне доменов. Kerberos является основным протоколом аутентификации в домене, но в целях обеспечения совместимости с с предыдущими версиями, также поддерживается протокол *NTLM*.

Перед тем, как рассмотреть порядок работы Kerberos, разберем зачем он изначально разрабатывался. **Централизованное** *распределение ключей* симметричного шифрования подразумевает, что у каждого абонента сети есть только один основной *ключ*, который используется для взаимодействия с *центром распределения ключей* (сервером ключей). Чтобы получить *ключ* шифрования для защиты обмена данными с другим абонентом, *пользователь* обращается к серверу ключей, который назначает этому пользователю и соответствующему абоненту сеансовый *симметричный ключ*.

Протокол Kerberos обеспечивает *распределение ключей* симметричного шифрования и проверку подлинности пользователей, работающих в незащищенной сети. Реализация Kerberos - это программная система, построенная *по* архитектуре "клиент-*сервер*". Клиентская часть устанавливается на все компьютеры защищаемой сети, кроме тех, на которые устанавливаются компоненты сервера Kerberos. В роли клиентов Kerberos могут, в частности, выступать и сетевые серверы (файловые серверы, *серверы печати* и т.д.).

Серверная часть Kerberos называется *центром распределения ключей* (англ. Key *Distribution Center*, сокр. *KDC*) и состоит из двух *компонент*:

- сервер аутентификации (англ. *Authentication Server*, сокр. AS);
- сервер выдачи разрешений (англ. *Ticket* Granting Server, сокр. *TGS*).

Каждому субъекту сети *сервер* Kerberos назначает разделяемый с ним *ключ* симметричного шифрования и поддерживает базу данных субъектов и их секретных ключей. Схема функционирования протокола Kerberos представлена на рис. 1.

Пусть клиент C собирается начать взаимодействие с сервером SS (англ. *Service Server - сервер*, предоставляющий сетевые сервисы). В несколько упрощенном виде, протокол предполагает следующие шаги:

1. C→AS: {c}.

Клиент C посылает серверу аутентификации AS свой идентификатор c (идентификатор передается открытым текстом).

2. AS→C: {{TGT}K_{AS_TGS}, K_{C_TGS}}K_C,

где:

- K_C - основной ключ C ;
- K_{C_TGS} - ключ, выдаваемый C для доступа к серверу выдачи разрешений *TGS* ;
- {TGT} - *Ticket* Granting *Ticket* - билет на доступ к серверу выдачи разрешений

{TGT}={c,*tgs*,t_1,p_1, K_{C_TGS}}, где *tgs* - идентификатор сервера выдачи разрешений, t_1 - отметка времени, p_1 - *период действия* билета.

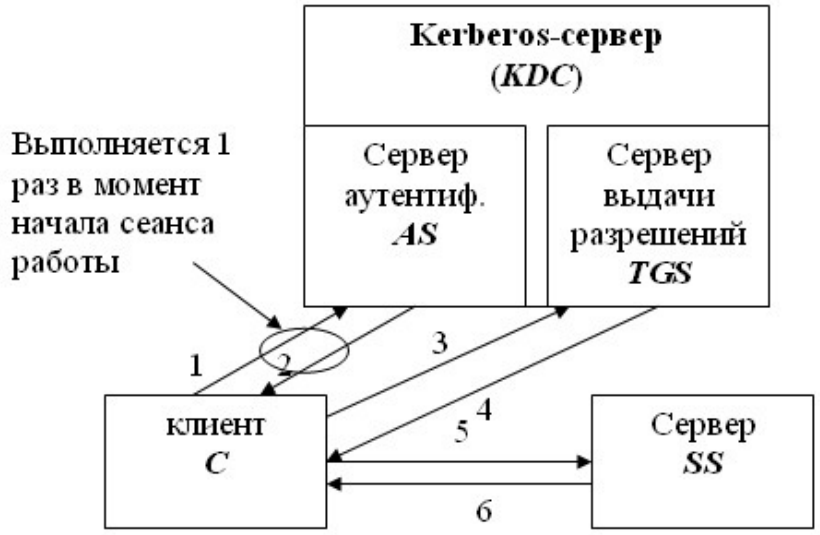

Рис. 1- Протокол Kerberos

Запись $\{\cdot\}K_X$ здесь и далее означает, что содержимое фигурных скобок зашифровано на ключе K_X.

На этом шаге сервер аутентификации AS, проверив, что клиент C имеется в его базе, возвращает ему билет для доступа к серверу выдачи разрешений и ключ для взаимодействия с сервером выдачи разрешений. Вся посылка зашифрована на ключе клиента C. Таким образом, даже если на первом шаге взаимодействия идентификатор с послал не клиент C, а нарушитель X, то полученную от AS-посылку X расшифровать не сможет.

Получить доступ к содержимому билета TGT не может не только нарушитель, но и клиент C, т.к. билет зашифрован на ключе, который распределили между собой сервер аутентификации и сервер выдачи разрешений.

3. C→*TGS*: {TGT}K_{AS_TGS}, {Aut_1} K_{C_TGS}, {ID}

где {Aut_1} - аутентификационный блок - Aut_1 = {c,t_2}, t_2 - метка времени; ID - идентификатор запрашиваемого сервиса (в частности, это может быть идентификатор сервера SS).

Клиент C на этот раз обращается к серверу выдачи разрешений TGS. Он пересылает полученный от AS билет, зашифрованный на ключе K_{AS_TGS}, и аутентификационный блок, содержащий идентификатор c и метку времени, показывающую, когда была сформирована посылка. Сервер выдачи разрешений расшифровывает билет TGT и получает из него информацию о том, кому был выдан билет, когда и на какой срок, ключ шифрования, сгенерированный сервером AS для взаимодействия между клиентом C и сервером *TGS*. С помощью этого ключа расшифровывается аутентификационный блок. Если метка в блоке совпадает с меткой в билете, это доказывает, что посылку сгенерировал на самом деле C (ведь только он знал ключ K_{C_TGS} и мог правильно зашифровать свой идентификатор). Далее делается проверка времени действия билета и времени оправления

посылки **3**). Если проверка проходит и действующая в системе политика позволяет клиенту C обращаться к клиенту SS, тогда выполняется шаг **4**).

4. *TGS*→C: $\{\{TGS\}K_{TGS\_SS}, K_{C\_SS}\}K_{C\_TGS}$,

где K_{C_SS} - ключ для взаимодействия C и SS, {*TGS*} - *Ticket* Granting Service - билет для доступа к SS (обратите внимание, что такой же аббревиатурой в описании протокола обозначается и сервер выдачи разрешений). $\{TGS\} = \{c, ss, t_3, p_2, K_{C\_SS}\}$.

Сейчас сервер выдачи разрешений *TGS* посылает клиенту C ключ шифрования и билет, необходимые для доступа к серверу SS. Структура билета такая же, как на шаге 2): идентификатор того, кому выдали билет; идентификатор того, для кого выдали билет; отметка времени; *период действия*; ключ шифрования.

5. C→SS: $\{TGS\}K_{TGS\_SS}$, $\{Aut_2\}\ K_{C\_SS}$

где $Aut_2 = \{c, t_4\}$.

Клиент C посылает билет, полученный от сервера выдачи разрешений, и свой аутентификационный блок серверу SS, с которым хочет установить сеанс защищенного взаимодействия. Предполагается, что SS уже зарегистрировался в системе и распределил с сервером *TGS* ключ шифрования K_{TGS_SS}. Имея этот ключ, он может расшифровать билет, получить ключ шифрования K_{C_SS} и проверить подлинность *отправителя сообщения*.

6. SS→C: $\{t_4+1\}K_{C\_SS}$

Смысл последнего шага заключается в том, что теперь уже SS должен доказать C свою подлинность. Он может сделать это, показав, что правильно расшифровал предыдущее сообщение. Вот поэтому, SS берет отметку времени из аутентификационного блока C, изменяет ее заранее определенным образом (увеличивает на 1), шифрует на ключе K_{C_SS} и возвращает C.

Если все шаги выполнены правильно и все проверки прошли успешно, то стороны взаимодействия C и SS, во-первых, удостоверились в подлинности друг друга, а во-вторых, получили *ключ* шифрования для защиты сеанса связи - *ключ* K_{C_SS}.

Нужно отметить, что в процессе сеанса работы клиент проходит шаги 1) и 2) только один раз. Когда нужно получить билет на *доступ* к другому серверу (назовем его SS1), клиент C обращается к серверу выдачи разрешений *TGS* с уже имеющимся у него билетом, т.е. протокол выполняется начиная с шага 3).

При использовании протокола Kerberos компьютерная *сеть* логически делится на области действия серверов Kerberos. Kerberos-область - это участок сети, пользователи и серверы которого зарегистрированы в базе данных одного сервера Kerberos (или в одной базе, разделяемой несколькими серверами). Одна область может охватывать сегмент локальной сети, всю локальную *сеть* или объединять несколько связанных локальных сетей. Схема взаимодействия между Kerberos-областями представлена на рис. 2.

Для взаимодействия между областями, должна быть осуществлена взаимная *регистрация* серверов Kerberos, в процессе которой *сервер* выдачи разрешений одной области регистрируется в качестве клиента в другой области (т.е. заносится в базу сервера аутентификации и разделяет с ним *ключ*).

После установки взаимных соглашений, клиент из области 1 (пусть это будет K_{11}) может установить *сеанс* взаимодействия с клиентом из области 2 (например, K_{21}). Для этого K_{11} должен получить у своего сервера выдачи разрешений билет на *доступ* к Kerberos-серверу, с клиентом которого он хочет установить взаимодействие (т.е. серверу Kerberos KDC2). Полученный билет содержит отметку о том, в какой области зарегистрирован владелец билета. Билет шифруется на ключе, разделенном между серверами KDC1 и KDC2. При успешной расшифровке билета, удаленный Kerberos-*сервер* может быть уверен, что билет выдан клиенту Kerberos-области, с которой установлены *доверительные отношения*. Далее протокол работает как обычно.

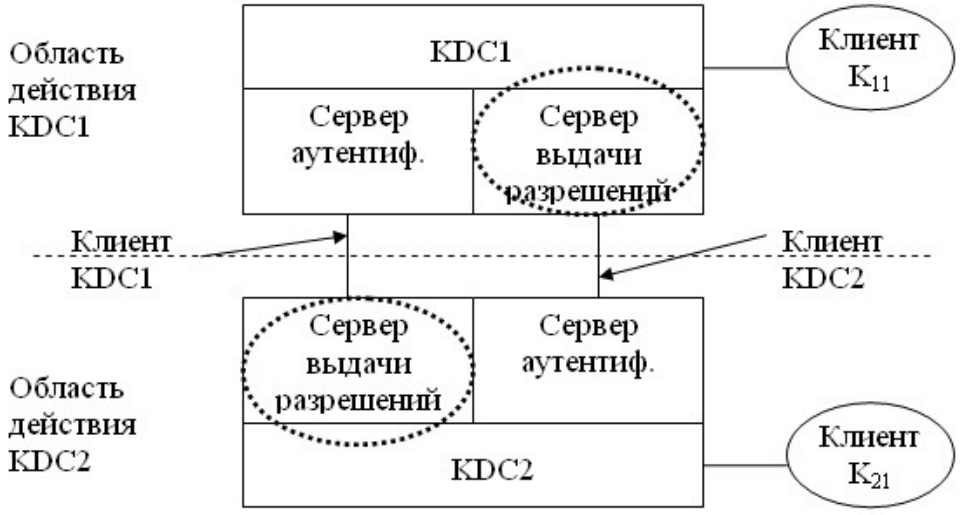

Рис. 2- Взаимодействие между Kerberos-областями

Кроме рассмотренных, Kerberos предоставляет еще ряд дополнительных возможностей. Например, указанный в структуре билета *параметр* p(период времени) задается парой значений "время начала действия" - "время окончания действия", что позволяет получать билеты *отложенного действия*.

Имеется тип билета "с правом передачи", что позволяет, например, серверу выполнять действия от имени обратившегося к нему клиента.

Два слова об аутентификации. Если Kerberos - протокол *распределения ключей*, корректно ли использовать его для аутентификации?! Но как отмечалось выше, если все стадии протокола прошли успешно, взаимодействующие стороны не только распределили *ключ*, но и убедились в подлинности друг друга, иными словами - аутентифицировали друг друга.

Что касается реализации протокола Kerberos в *Windows*, то надо отметить следующее.

1. Ключ пользователя генерируется на базе его пароля. Таким образом, при использовании слабых паролей эффект от надежной защиты процесса аутентификации будет сведен к нулю.

2. В роли Kerberos-серверов выступают контроллеры домена, на каждом из которых должна работать служба Kerberos Key Distribution Center (*KDC*). Роль хранилища информации о пользователях и паролях берет на себя служба каталога Active Directory. Ключ, который разделяют между собой сервер аутентификации и сервер выдачи разрешений формируется на основе пароля служебной учетной записи **krbtgt** - эта запись автоматически создается при организации домена и всегда заблокирована.

3. Microsoft в своих ОС использует расширение Kerberos для применения криптографии с открытым ключом. Это позволяет осуществлять регистрацию в домене и с помощью смарт-карт, хранящих ключевую информацию и цифровой *сертификат пользователя*.

4. Использование Kerberos требует синхронизации внутренних часов компьютеров, входящих в домен Windows.

Для увеличения уровня защищенности процесса аутентификации пользователей, рекомендуется отключить использование менее надежного протокола *NTLM* и оставить только Kerberos (если использования *NTLM* не требуют устаревшие клиентские ОС).

Кроме того, рекомендуется запретить администраторским учетным записям получать билеты "с правом передачи" (это убережет от некоторых угроз, связанных автоматическим запуском приложений от имени таких записей).

Вопросы:

1. Центр распределения ключей (серверная часть Kerberos).
2. Порядок взаимной *регистрации* серверов Kerberos.
3. Основные этапы реализации протокола Kerberos в *Windows*.
4. Служба Kerberos Key Distribution Center.
5. Как осуществляется взаимодействие между Kerberos-областями.
6. Централизованное распределение ключей симметричного шифрования.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 5.
Настройка локальной политики парольной безопасности операционной системы.

Цель: изучить методы повышения надежности путем практического применения рекомендаций по администрированию парольной системы операционной системы.

Знать: Администрирование парольной системы. Локальная политика безопасности операционной системы.

Уметь: применять свойства учетных записей; политику паролей и учетных записей; особенности простых и групповых учетных записей.

Актуальность темы изучении методов повышения надежности путем практического применения рекомендаций по администрированию парольной системы операционной системы.

Теоретическая часть

Локальная политика паролей. Рассмотрим, какие настройки необходимо сделать, чтобы пароли пользователей компьютера были достаточно надежны. В теоретической части курса мы рассматривали рекомендации *по* администрированию парольной системы. Потребовать их выполнения можно с помощью политики безопасности. Настройка делается через **Панель управления Windows**.

Откройте **Панель управления** ⟶ **Администрирование** ⟶ **Локальная политик а безопасности**. Выберите в списке **Политика учетных записей** и **Политика паролей**. Для *Windows* Vista экран консоли управления будет выглядеть так, как представлено на рис. 1.

Значения выбранного параметра можно изменить (рис. 2). Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит "Срок действия пароля не ограничен", установленное политикой требование максимального срока действия пароля будет игнорироваться.

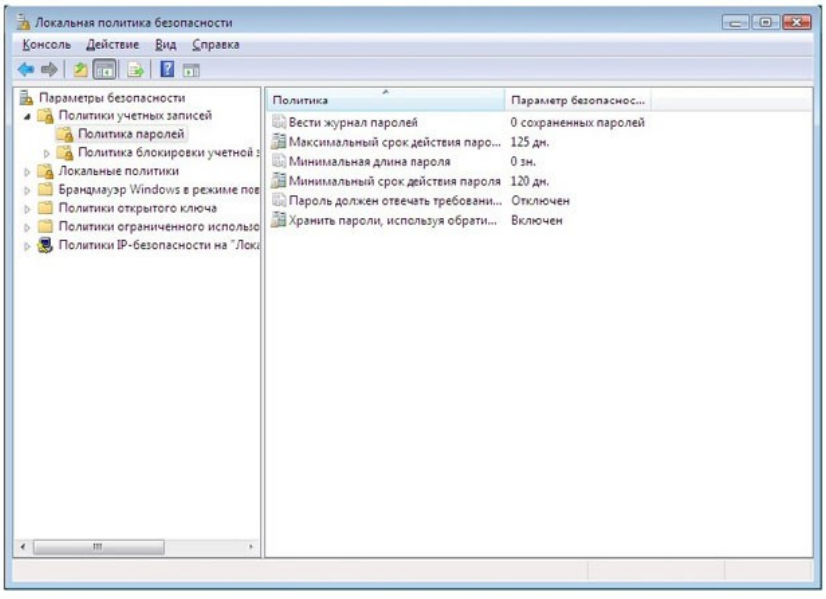

Рис. 1. Настройка политики паролей

Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в учебном классе нужна "групповая" учетная *запись*, параметры которой известны всем студентам, лучше поставить для нее **"Срок действия пароля не ограничен"** и **"Запретить смену пароля пользователем"**.

Свойства учетной записи можно посмотреть в **Панель управления** ⟶ **Администрирование** ⟶ **Управление компьютером**, там выберите **Локальные пользователи и группы** и **Пользователи** (или запустив эту же оснастку через **Пуск** ⟶ **Выполнить** ⟶ **lusrmgr.msc**).

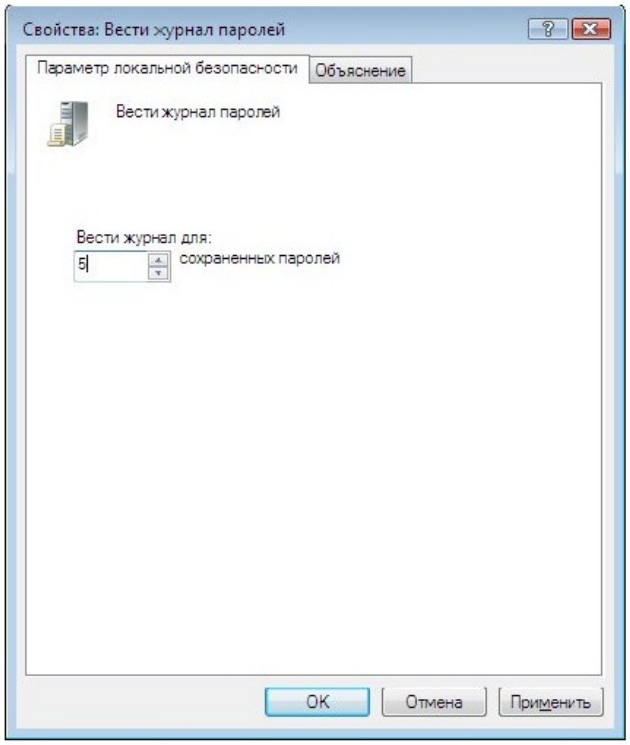

Рис. 2- Установка требования ведения журнала паролей

Вопросы:

1. Что такое политика парольной безопасности?
2. Локальная политика безопасности операционной системы.
3. Администрирование парольной системы.
4. Свойства учетной записи.
5. Особенности простых и групповых учетных записей.
6. Администрирование парольной системы.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 6.
Инфраструктура открытых ключей. Цифровые сертификаты.

Цель: Изучить инфраструктуру открытых ключей и цифровые сертификаты.

Знать: Инфраструктуру открытых ключей (*Public* Key *Infrastructure*, сокр. *PKI*); центры распределения ключей; цифровые сертификаты.

Уметь: решать проблему аутентификации ключа; применять структуру списка отозванных сертификатов; криптографический протокол; атаку типа "человек посередине" (*man* in the middle); структуру PKI; иерархию центров сертификации и клиентов; сертификат формата X.509 v.3.

Актуальность темы изучение инфраструктуры открытых ключей и цифровых сертификатов.

Теоретическая часть

Как было рассмотрено ранее, использование протокола Kerberos, позволяет провести аутентификацию и распределить ключи симметричного шифрования. Использование методов асимметричной криптографии сделало возможным безопасный обмен *криптографическими ключами* между отправителем и получателем без использования *центров распределения ключей*.

Но возникает другая проблема - как убедиться в том, что имеющийся у Вас открытый *ключ* другого абонента на самом деле принадлежит ему. Иными словами, возникает проблема аутентификации ключа. Без этого, на криптографический протокол может быть осуществлена *атака* типа "человек посередине" (*man* in the middle).

Идею данной атаки поясняет следующий пример. *Абонент* A (Алиса) хочет послать абоненту B (Боб) зашифрованное сообщение и берет его открытый *ключ* из общедоступного справочника.

Но, на самом деле, ранее нарушитель E (Ева) подменил в справочнике открытый *ключ* Боба своим открытым ключом. Теперь Ева может расшифровать те

сообщения, которые Алиса формирует для Боба, ознакомиться с их содержимым, возможно, зашифровать их на настоящем ключе Боба и переслать ему (рис. 1).

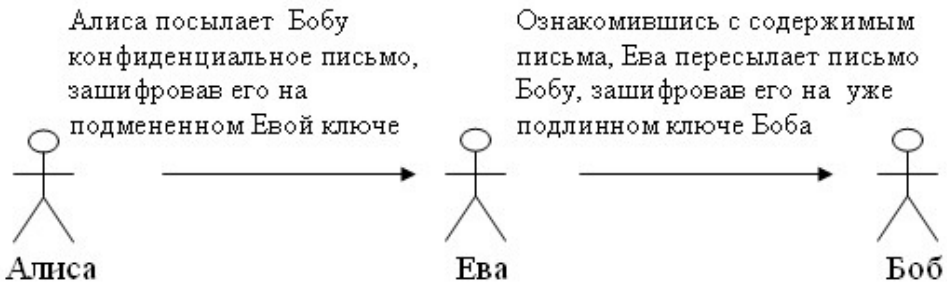

Рис. 1. Атака типа man-in-the-middle

Избежать подобной атаки можно, подтвердив подлинность используемого ключа. Но Алиса и Боб лично никогда не встречались, и передать, например, дискету с ключом из рук в руки не могут. Поэтому, решение задачи подтверждения подлинности берет на себя *третья доверенная сторона* - некий арбитр, которому доверяют оба абонента. Заверяется *ключ* с помощью цифрового сертификата.

На самом деле, подобный способ применяется и вне компьютерных систем. Когда для подтверждения подлинности человека используется паспорт, то в роли третьей доверенной стороны выступает государство (от имени которого действовали в выдавшем паспорт отделе милиции).

Но вернемся к цифровым сертификатам. Для подтверждения подлинности открытых ключей создается *инфраструктура открытых ключей* (англ. *Public* Key *Infrastructure*, сокр. *PKI*). *PKI* представляет собой набор средств, мер и правил, предназначенных для управления ключами, политикой безопасности и обменом защищенными сообщениями. Структура *PKI* представлена на рис. 2.

Для простоты последующего изложения, будем представлять *сеть* в виде совокупности *удостоверяющих центров* (другое название - *центр сертификации*, от англ. *Certification Authority*, сокр. - *CA*) и пользователей. *Центр сертификации* - *абонент*, которому доверено право удостоверять своей подписью сертификаты, связывающие открытые ключи абонентов с их идентификационной информацией. Сами *центры сертификации* тоже получают сертификаты своих ключей у центров более высокого уровня.

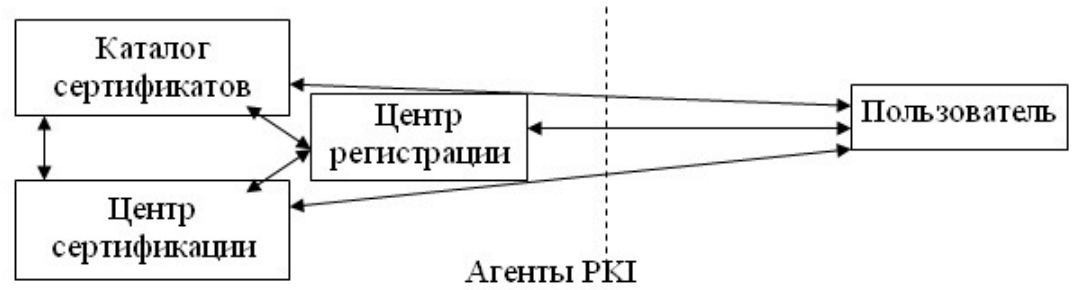

Рис. 2. Структура PKI

Таким образом, *центры сертификации* и пользователи формируют древовидную иерархическую структуру (рис. 3). В вершине этого дерева находится корневой *центр*

сертификации, на рисунке - CA_1. Его особенность заключается в том, что он использует *самоподписанный сертификат*, т.е. сам заверяет свой *ключ*.

В приведенном примере, CA_1 заверяет электронной подписью сертификаты подчиненных центров сертификации CA_2 и CA_3, а те, в свою*очередь*, подписывают *сертификаты пользователей* и центров более низкого уровня.

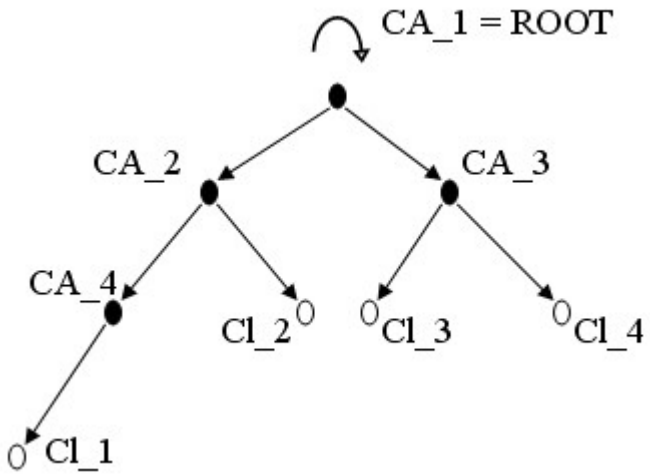

Рис. 3. Иерархия центров сертификации и клиентов

Перейдем к рассмотрению самих сертификатов. Наибольшее распространение получили цифровые сертификаты, формат которых определен стандартом X.509.

На данный момент, принята третья версия стандарта. Формат сертификата изображен на рис. 4.

Номер версии содержит числовое *значение*, соответствующее номеру версии (для сертификата версии 1 равен 0 и т.д.). В первой версии X.509 не было уникальных номеров ("*ID* Изготовителя", "*ID* Субъекта") и *полей расширения*. Во второй версии добавились указанные идентификаторы, в третьей - расширения.

Серийный номер - уникальный номер, присваиваемый каждому сертификату.

Алгоритм подписи - *идентификатор* алгоритма, используемого при подписании сертификата. Должен совпадать с полем **Алгоритм ЭЦП**.

Изготовитель - имя *центра сертификации*, выдавшего сертификат. Записывается в формате *Relative* Distinguished Name - RDN (варианты перевода названия - "относительное отдельное имя", "относительное характерное имя"). Данный формат используется в службах каталога, в частности, в протоколе *LDAP*.

При записи *Relative* Distinguished Name используются специальные ключевые слова:

- CN (Common Name) - общее имя;
- OU (Organization Unit) - организационная единица;
- DC (Domain Component) - составная часть доменного имени.

Например, в сертификате Microsoft *Windows Hardware Compatibility*, который находится в *хранилище сертификатов Windows*XP *значение* данного поля следующее:

- CN = Microsoft Root Authority
- OU = Microsoft Corporation
- OU = Copyright (c) 1997 Microsoft Corp.

Как видно, указывается имя *центра сертификации*, компания, которой он принадлежит и т.д.

Субъект - имя владельца сертификата, представленное в том же формате RDN. Для указанного в предыдущем примере сертификата значения данного поля:

- CN = Microsoft Windows *Hardware Compatibility*
- OU = Microsoft Corporation
- OU = Microsoft Windows *Hardware Compatibility* Intermediate CA
- OU = Copyright (c) 1997 Microsoft Corp.

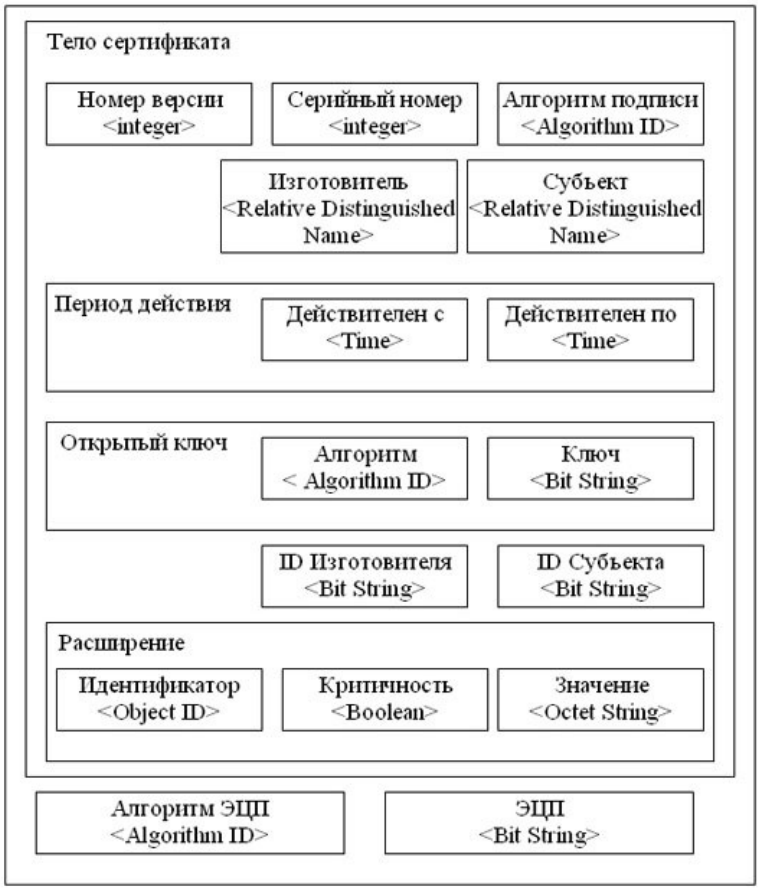

Рис. 4. Сертификат формата X.509 v.3

Период действия - описывает временной *интервал*, в течение которого *центр сертификации* гарантирует отслеживание *статуса сертификата*(сообщит абонентам сети о факте досрочного отзыва сертификата и т.д.). Период задается датами начала и окончания действия.

Открытый ключ - составное *поле*, содержащее *идентификатор* алгоритма, для которого предназначается данный открытый *ключ*, и собственно сам открытый *ключ* в виде набора битов.

ID Изготовителя и ID Субъекта содержат уникальные идентификаторы *центра сертификации* и пользователя (на случай совпадения имен различных *CA* или пользователей).

Расширения - дополнительный *атрибут*, связанный с субъектом, изготовителем или открытым ключом, и предназначенный для управления процессами сертификации. Более подробно он описан ниже.

Алгоритм электронной цифровой подписи (ЭЦП) - *идентификатор* алгоритма, используемый для подписи сертификата. Должен совпадать со значением поля **Алгоритм подписи**.

ЭЦП - само *значение* электронно-цифровой подписи для данного сертификата.

Расширения могут определять следующие дополнительные параметры:

- идентификатор пары открытый/секретный ключ *центра сертификации* (изготовителя), если центр имеет несколько различных ключей для подписи сертификатов;
- идентификатор конкретного ключа пользователя (субъекта), если пользователь имеет несколько сертификатов;
- назначение ключа, например, ключ для шифрования данных, *проверки ЭЦП* данных, для проверки *ЭЦП* сертификатов и т.д.;
- уточнение периода использования - можно сократить время действия сертификата, указанное в поле *Период действия* (т.е. период, в течение которого статус сертификата отслеживается, станет больше, чем разрешенное время использования сертификата);
- *политики использования* сертификата;
- выбор соответствия *политик использования* сертификата для *центра сертификации* и пользователя, если имеются различные варианты;
- *альтернативное имя* пользователя и *центра сертификации*;
- указания, является ли пользователь сам *центром сертификации* и насколько глубоко разрешается разворачивать *сертификационный путь*.

Предположим, что ключевые пары сгенерированы, открытые ключи заверены сертификатами и размещены в каталоге, реализованном с помощью *web-сервера*, ftp-сервера, службы каталога или другой технологии. Теперь, если *абонент* А желает проверить подпись абонента В под полученным сообщением (или зашифровать для В сообщение с помощью его открытого ключа и т.д.), он выполняет следующие действия:

1. запрашивает в сетевом справочнике сертификат C_B открытого ключа подписи (шифрования,...) абонента В;
2. проверяет достоверность сертификата C_B (см. ниже);
3. в случае успеха проверяет подпись под сообщением (зашифровывает сообщение,...) с помощью открытого ключа, извлеченного из C_B.

Процедура проверки достоверности сертификата C_B состоит в следующем:

1. проверяется срок действия сертификата C_B, если он закончился, сертификат считается недостоверным;
2. из C_B извлекается имя ЦС, подписавшего этот сертификат, обозначим его D ;
3. если D=B, то сертификат самоподписанный, он считается достоверным только, если D=ROOT (хотя, возможно, в некоторых сетях право выдавать самоподписанные сертификаты имеет не один ROOT, это - политика сети);
4. если же $D \neq B$, то из справочника запрашивается сертификат C_D открытого ключа подписи абонента D, проверяется на достоверность сертификат C_D;
5. в случае отрицательного ответа принимается решение о недостоверности сертификата C_B, иначе из C_D извлекается открытый ключ K_D;
6. с помощью K_D проверяется подпись под сертификатом C_B, по результатам проверки этой подписи судят о достоверности C_B.

Если ключи шифрования досрочно вышли из обращения (причины могут быть различны - *пользователь* увольняется из компании, *секретный ключ* скомпрометирован и т.д.), *центр сертификации* извещает об этом остальных пользователей сети путем выпуска списка отозванных сертификатов (англ. *Certificate* Revocation *List*, сокр. *CRL*). Структура *CRL* представлена на рис. 5.

Поля списка содержат следующую информацию:

- **Номер версии** определяет номер версии формата *CRL*. Текущая используемая версия - вторая.

- **Алгоритм подписи** - идентификатор алгоритма, с помощью которого подписан *CRL*. Должен совпадать по значению с полем **Алгоритм ЭЦП**.
- **Изготовитель** - имя *центра сертификации* в формате RDN.
- **Выпущен** - дата выпуска *CRL*.
- **Следующий** - дата, до которой будет выпущен следующий *CRL*.
- **Расширения** - описывают *центр сертификации*, точку для поиска *CRL* данного центра, номер данного списка и т.д.
- **Отозванный сертификат** - таких полей будет столько, сколько сертификатов отзывается - содержит номер отзываемого сертификата, дату, с которой сертификат отозван, описание причины отзыва.
- **Алгоритм ЭЦП** - идентификатор алгоритма *ЭЦП*, используемого для подписи списка.
- **ЭЦП** - сама *электронная цифровая подпись*.

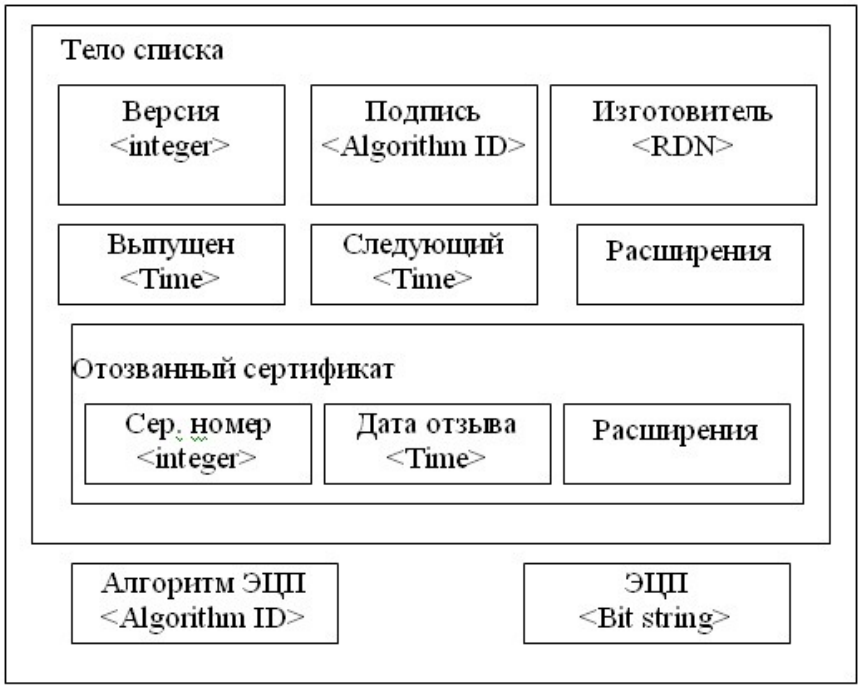

Рис. 5. Структура списка отозванных сертификатов

Проблемы с *CRL* заключаются в том, что может возникнуть ситуация, когда *ключ* уже отозван, но *CRL* еще не выпущен, т.е. пользователи не могут получить информацию о компрометации ключа. Кроме того, распространение *CRL* идет *по* запросу клиента и нарушитель может препятствовать их получению.

Другая проблема *PKI* - *самоподписанные сертификаты*. Сертификат *ROOT* должен раздаваться всем абонентам сети в начале работы и сохраняться в защищенном от подделки хранилище. Иначе нарушитель может попробовать навязать свой сертификат в качестве сертификата корневого центра.

Мы рассмотрели случай реализации **иерархической модели** *PKI*, при которой *центры сертификации* организованы в древовидную структуру с корневым *центром сертификации* на верху иерархии. На практике также встречаются другие варианты организации:

- **одиночный центр сертификации**, который выдает себе *самоподписанный сертификат* - данная модель часто реализуется в небольших организациях, но она имеет отмеченный выше недостаток, связанный с *самоподписанными сертификатами*;

- **одноранговая модель**, при которой независимые *центры сертификации* взаимно сертифицируют друг друга.

Надо отметить, что сфера применения цифровых сертификатов сейчас достаточно широка. В частности, они используются для распределения открытых ключей в протоколах защиты электронной почты *S/MIME* или *PGP*, с помощью цифровых сертификатов проверяется подлинность участников соединения *по* протоколу *SSL* и т.д.

Начиная с *Windows 2000 Server* в состав *серверных ОС* Microsoft входит *программное обеспечение* для создания центров сертификации. Создание корпоративного ЦС может понадобиться, если принято решение использовать защиту электронной почты с помощью *S/MIME*, *шифрование данных* при хранении средствами *EFS* (*EFS* - Encrypted File *System* - реализует *шифрование данных* на дисках с файловой системой *NTFS*), *шифрование* сетевого трафика с помощью протокола IPSec.

Различные практические аспекты использования цифровых сертификатов рассматриваются в лабораторных работах № 6 и 7. Первая из них посвящена работе с сертификатами с точки зрения конечного пользователя (в том числе, получение сертификата для защиты электронной почты с помощью *S/MIME*), а вторая - созданию и администрированию *центра сертификации*. Вопросы использования *EFS* рассматриваются в работе № 8.

Вопросы:

7. Инфраструктура открытых ключей (*Public* Key *Infrastructure*, сокр. *PKI*).
8. Центры распределения ключей.
9. Инфраструктура открытых ключей.
10. Цифровые сертификаты.
11. Криптографический протокол.
12. Атака типа "человек посередине" (man in the middle).
13. Структура Key Infrastructure.
14. Иерархия центров сертификации и клиентов.
15. Сертификат формата X.509 v.3.
16. Структура списка отозванных сертификатов.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 7.
Использование цифровых сертификатов.

Цель: получение и совершенствование практических навыков использования цифровых сертификатов.

Знать: использование протоколов *SSL*/TSL; центр сертификации VeriSign; параметры сертификата; защищенное хранилище ключей и сертификатов в операционной системе Windows.

Уметь: производить подключение к системам Интернет-банкинга; выбор сертификата для защиты почты с помощью S/MIME в Outlook.

Актуальность темы заключается в получении и совершенствовании практических навыков использования цифровых сертификатов.

Теоретическая часть

В ходе данной практической работы мы познакомимся с некоторыми вопросами использования цифровых сертификатов.

Начнем с их использования протоколом *SSL*/TSL (на самом деле это два разных протокола, но т.к. TSL разработан на базе *SSL*, принцип использования сертификатов один и тот же). Этот протокол широко применяется в сети *Интернет* для защиты данных передаваемых между web-серверами и браузером клиента. Для аутентификации сервера в нем используется сертификат X.509.

Для примера обратимся на *сайт* Ситибанка (http://www.citibank.ru), в раздел **"Мой банк"**, предназначенный для ведения банковских операций через *Интернет* (рис. 1).

Префикс https в строке адреса и изображение закрытого замка справа от строки указывают, что установлено защищенное соединение. Если щелкнуть мышью *по* изображению замка, то увидим представленное на рис. 8.1 сообщение о том, что подлинность узла с помощью сертификата подтверждает *центр сертификации* VeriSign. Значит, мы на самом деле обратились на *сайт* Ситибанка (а не подделанный нарушителями *сайт*) и можем безопасно вводить логин и *пароль*.

Выбрав **"Просмотр сертификата"** можно узнать подробности о получателе и издателе, другие параметры сертификата (рис. 2).

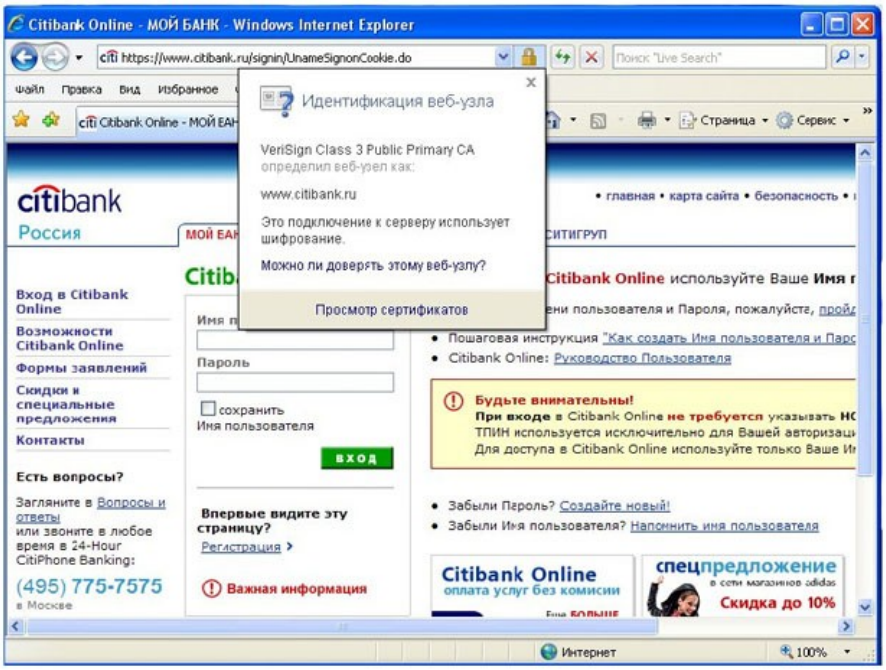

Рис. 1- Защищенное соединение

Теперь рассмотрим другой вариант - мы подключаемся *по SSL* к web-серверу, а *браузер* не может проверить его подлинность. Подобная ситуация произошла при подключении в раздел *Интернет*-обслуживания Санкт-Петербургского филиала оператора мобильной связи Tele2 -https://www.selfcare.tele2.ru/work.html (на рис. 3).

Если нажать ссылку **"Продолжить открытие этого web-узла",** то можно будет просмотреть сертификат.

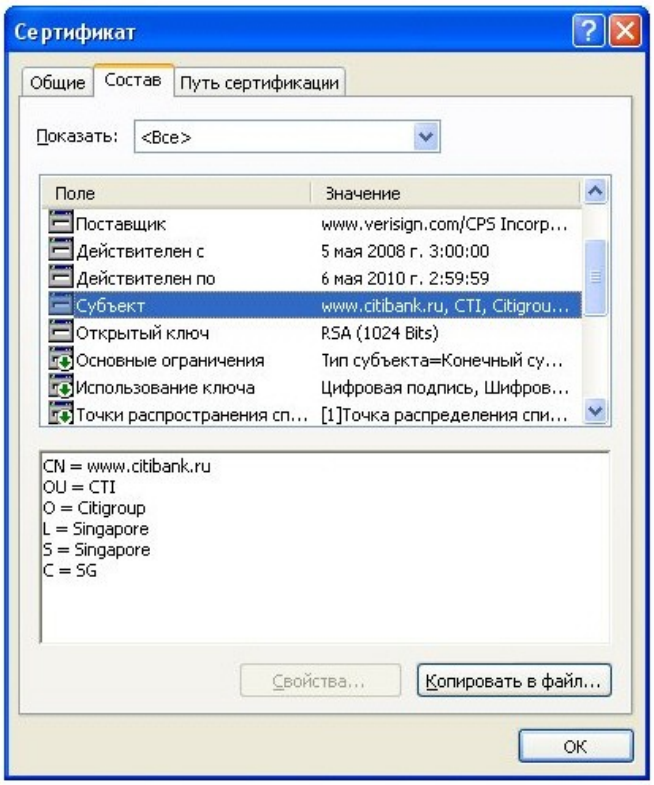

Рис.2- Параметры сертификата

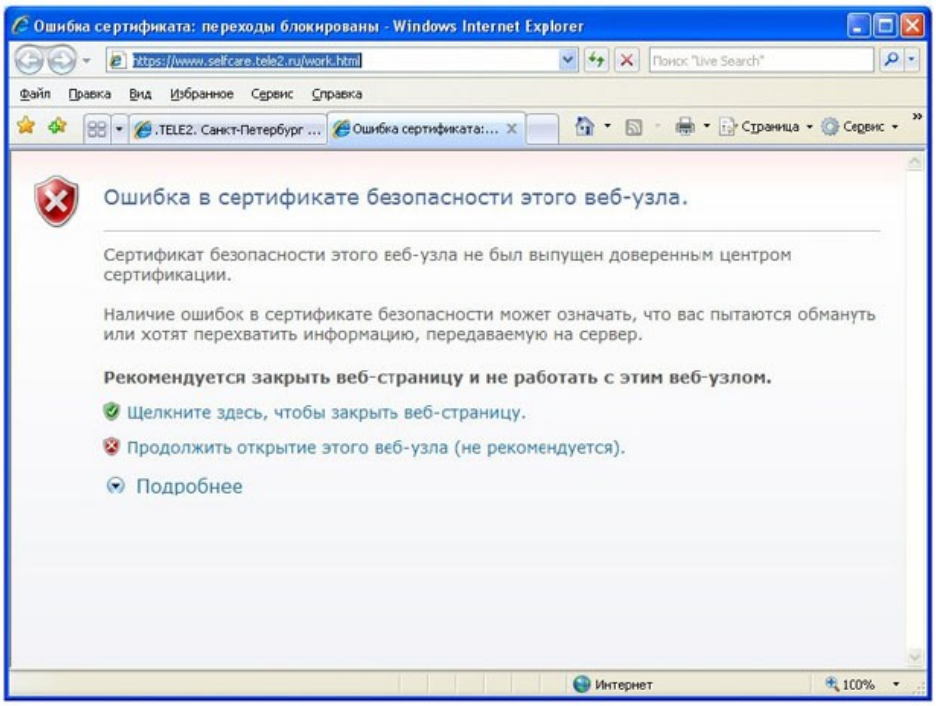

Рис.3- Браузер сообщает о проблеме с сертификатом

Рассмотрим, как хранятся сертификаты.

Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку *консоль* управления *MMC* **"Сертификаты"**.

Из *меню* **Выполнить** запустите *консоль* командой mmc. В *меню* **Консоль** выберите **Добавить или удалить оснастку**, а в списке оснасток выберите **Сертификаты**. Если будет предложен выбор (а это произойдет, если Вы работаете с правами администратора), выберите *пункт* **"Моей учетной записи"**.

Таким образом, мы можем просматривать сертификаты текущего пользователя. Если ранее сертификаты не запрашивались, то в разделе **"Личные сертификаты"** элементов не будет.

В разделе **"Доверенные корневые центры сертификации"** представлен достаточно обширный *список* центров, чьи сертификаты поставляются вместе с операционной системой.

Найдите в нем сертификат VeriSign *Class* 3 *Public* Primary *CA*. Благодаря тому, что сертификат VeriSign *Class* 3 *Public* Primary *CA*, уже был установлен, в рассмотренном в начале работы примере с подключением к системам *Интернет*-банкинга, *браузер* мог подтвердить подлинность узла.

Теперь перейдем к разделу **"Сертификаты, к которым нет доверия"**. Там находятся отозванные сертификаты. Как *минимум*, там будут находиться два сертификата, которые *по* ошибке или злому умыслу кто-то получил от имени корпорации Microsoft в центре сертификации VeriSing в 2001 году. Когда это выяснилось, сертификаты отозвали (рис. 4).

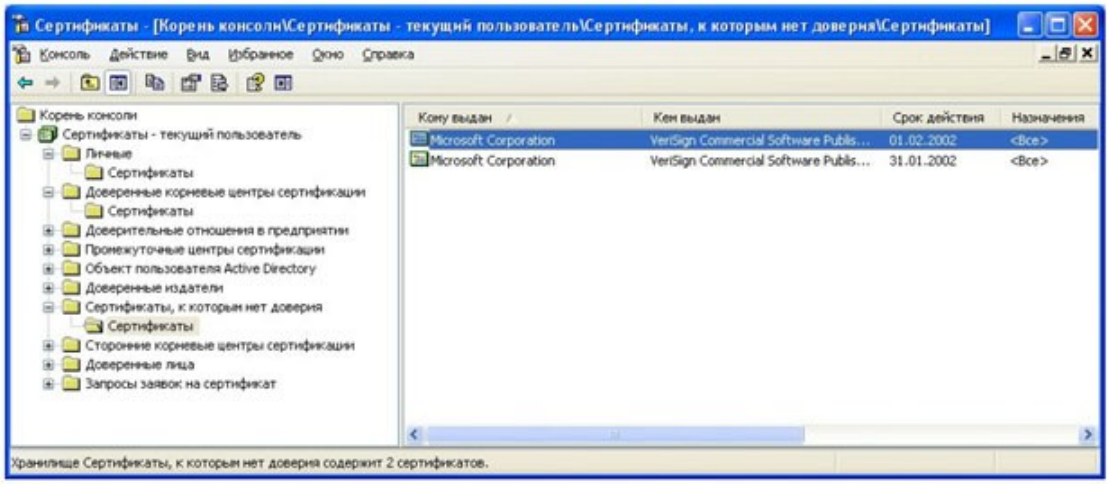

Рис. 4- Отозванные сертификаты

Теперь рассмотрим процесс запроса сертификата. На сайте *центра сертификации* Thawte http://www.thawte.com можно бесплатно получить сертификат для электронной почты. Для этого в *меню* сайта **Products** выберите **Free Personal E-Mail Certificates**.

После этого надо заполнить небольшую анкету, указав имя, фамилию, страну, предпочитаемую кодировку, *адрес* электронной почты (должен быть обязательно действующим), дальше - *пароль* и контрольные вопросы для восстановления. Когда все заполнено, на указанный *адрес* почты будет отправлено *письмо* со ссылкой для выполнения дельнейших шагов *генерации ключей* и двумя проверочными значениями, которые нужно ввести, перейдя *по* ссылке. Таким образом, подлинность и принадлежность адреса будет подтверждена.

Далее система предложит ввести *адрес* почты (в качестве *имя пользователя*) и выбранный ранее *пароль*. После чего можно запросить сертификат X.509. Понадобится указать тип браузера и почтового клиента (например, *Internet Explorer* и *Outlook*). После этого потребуется ответить на запросы системы, касающиеся *генерации ключей* (разрешить выполнение ActiveX элемента, выбрать *криптопровайдер*, разрешить генерацию).

После завершения этого этапа на почтовый *адрес* будут выслано второе *письмо*, подтверждающее *запрос* сертификата. А спустя некоторое время - третье, со ссылкой для получения сертификата.

Пройдя *по* ссылке, надо будет снова ввести имя и *пароль* и на странице нажать кнопку **"Install Your Cert"** и согласиться с добавлением сертификата.

В результате в оснастке **Сертификаты** появится личный сертификат выпущенный издателем Thawte *Personal* Freemail *Issuing CA* для субъекта Thawte Freemail *Member* с указанным вами адресом почты (рис. 5).

Если использовать сертификат для защиты почты, дальнейшая настройка зависит от почтового клиента. Если это Microsoft *Outlook*, можно использовать встроенную в него поддержку протокола *S/MIME*. В *Outlook* 2003 для выбора сертификата надо войти в *меню* **Сервис Параметры**, там выбрать вкладку **Безопасность** и там в параметрах шифрованной электронной почты выбрать используемый сертификат и алгоритмы (рис. 6).

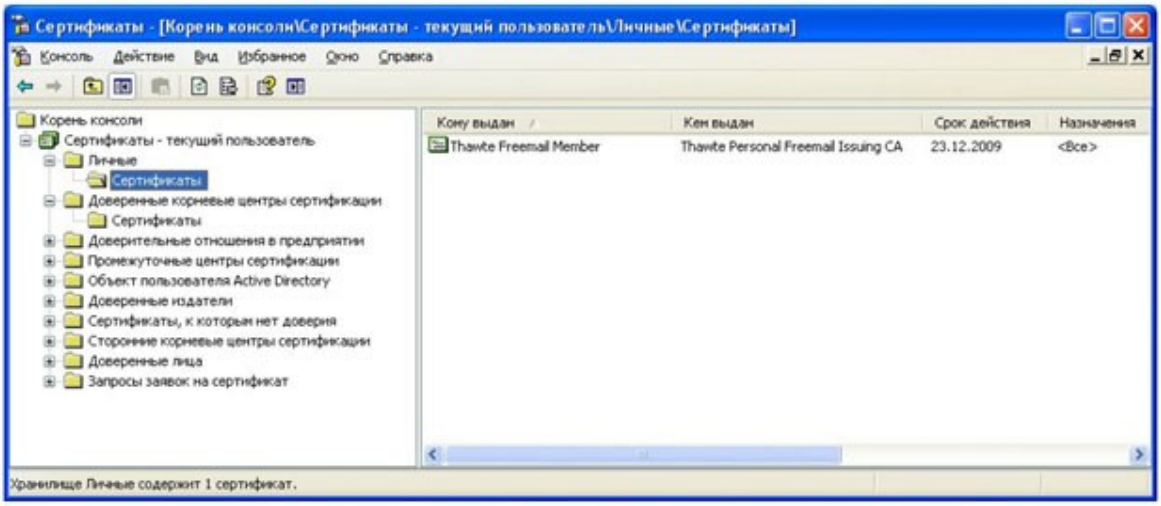

Рис. 5- Полученный сертификат

Запросите сертификат в Thawte и настройте *почтовый клиент* для использования *S/MIME*.

Проблема была в том, что сертификат "самоподписанный": он был выдан *центром сертификации* http://www.selfcare.tele2.ru самому себе. *Браузер* сообщает о невозможности удостовериться в подлинности узла из-за того, что данный *центр сертификации* отсутствует в списке доверенных, а проверить его подлинность с помощью "вышестоящего" по иерархии центра не представляется возможным (т.к. вышестоящего центра нет). Доверять или нет такому сертификату – каждый решает самостоятельно.

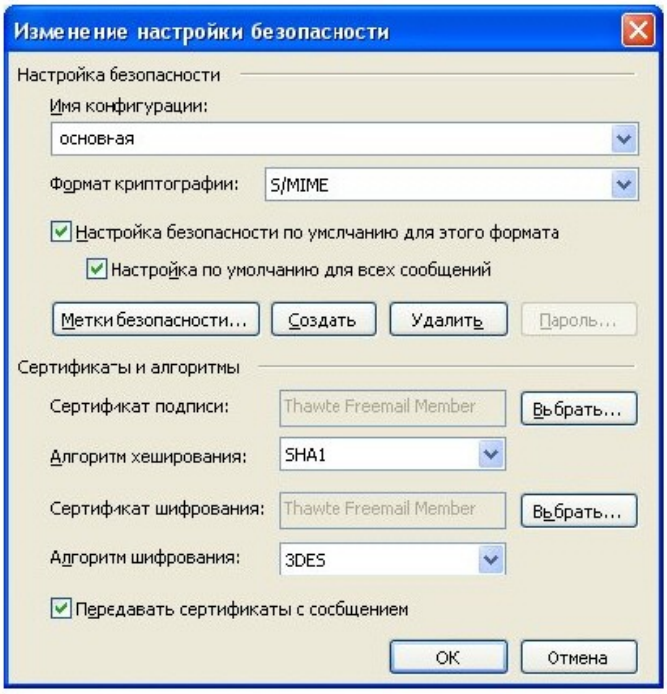

Рис. 6- Выбор сертификата для защиты почты с помощью S/MIME в Outlook

Вопросы:

1. Использование протоколов *SSL*/TSL.
2. Центр сертификации VeriSign.
3. Защищенное хранилище ключей и сертификатов в операционной системе Windows.

4. Подключение к системам Интернет-банкинга.
5. Отозванные сертификаты к которым нет доверия.
6. Выбор сертификата для защиты почты с помощью S/MIME в Outlook.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»

Практическая работа 8.
Резервное копирование в Windows Server 2008.

Цель: познакомиться со средствами организации резервного копирования в операционной системе Microsoft *Windows Server* 2008.

Знать: утилиты администрирования; полное резервное копирование и копирование отдельных дисков; выбор дисков для резервного копирования.

Уметь: применять доступные резервные копии для выбранного сервера; производить выбор типа и параметров восстановления; выбор типа резервного копирования для диска.

Актуальность темы познакомиться со средствами организации резервного копирования в операционной системе Microsoft *Windows Server* 2008.

Теоретическая часть

С точки зрения управления рисками, важность процедуры резервного копирования очень высока. В тех случаях, когда реализация угрозы приводит к изменению или удалению данных, повреждению программных *компонент* системы, *резервное*

копирование позволяет снизить причиненный *ущерб* и значительно ускорить восстановление системы. При разработке политики резервного копирования нужно определить, как *минимум*, следующие параметры:

- частоту выполнения резервных копий;
- порядок восстановления данных из резервных копий;
- объем носителей информации, выделяемых для хранения резервных копий;
- количество хранимых копий;
- вопросы обеспечения безопасности носителей резервных копий.

Утилиты резервного копирования *Windows Server* 2008 существенно отличаются от того, что было в *Windows Server* 2003 (где эти задачи решались с помощью утилиты ntbackup). Чтобы их использовать, для начала требуется их установить (*по* умолчанию, они не устанавливаются). Делается это с помощью оснастки **Server Manager**, где надо выбрать *пункт* **Add Feature** в разделе **Features** (рис. 1) и в появившемся списке выбрать *пункт* **Windows Server Backup Features** (рис. 2).

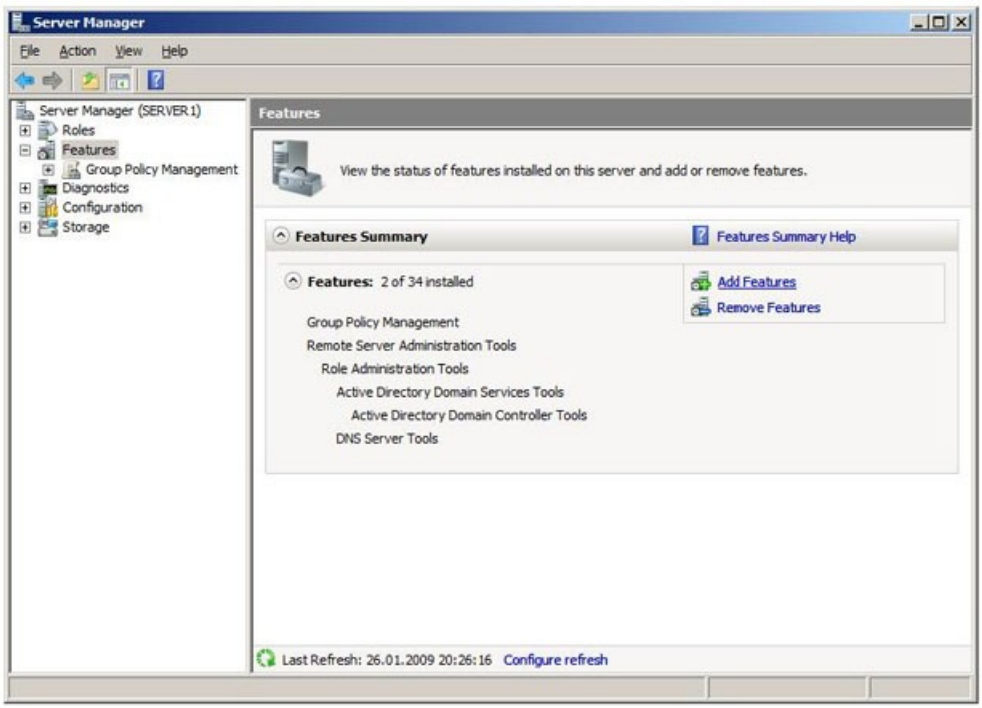

Рис. 1- Оснастка Server Manager позволяет добавить компоненты

Как видно на рис. 2, предлагается выбрать следующие опции:

- Windows Server Backup;
- Command-line tools (*утилиты командной строки*).

Установка последних, позволяет управлять резервным копированием с помощью сценариев и требует установки *Windows* PowerShell. Но для выполнения лабораторной будет достаточно установить только *Windows Server Backup*.

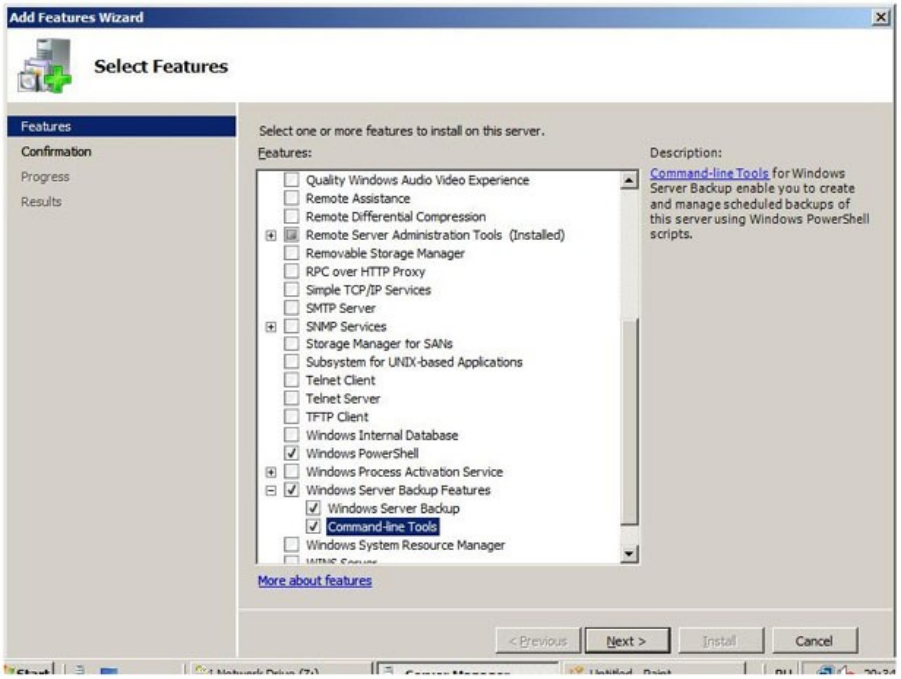

Рис.2- Добавляем утилиты администрирования

После установки, в *меню* **Administrative Tools** становится доступной оснастка **Windows Server Backup**. С ее помощью можно проводить *резервное копирование* данных на локальном или удаленном компьютере (если это разрешено настройками).

Рассмотрим, как это происходит. Запустим утилиту. *Резервное копирование* может проводить *пользователь*, состоящий в группе **Administrators** (Администраторы) или **Backup Operators** (*Операторы* архива). При этом, у членов группы **Backup Operators** при запуске оснастки **Windows Server Backup** будет дополнительно запрашиваться *пароль* (в окне **User Account Control**), т.к. эти *операции* относятся к разряду потенциально опасных.

В окне оснастки в списке доступных действий (**Actions**), расположенном в правой части экрана, выберем опцию **Backup Once …** (т.е. однократная *архивация*). Запустившийся мастер резервного копирования предложит выбор между настройками для уже запланированного копирования (**The same options that you used in the Backup Schedule Wizard for scheduled backups**) и новыми (**Different options**). Нужно выбрать второй вариант (если, как в нашем примере, *утилита* ранее не использовалась, то первый *пункт* списка будет неактивен).

Следующее окно мастера позволяет выбрать, производить ли полное *резервное копирование* или *копирование* отдельных разделов (рис. 3). Здесь проявляется первое отличие новых инструментов - *резервное копирование* отдельных папок и файлов производить нельзя, только *логический диск* целиком.

Хотелось бы также обратить внимание на надпись в нижней части экрана, там дается *ссылка* на раздел справки, описывающий выполнение с помощью *утилиты командной строки* резервного копирования только состояния системы (**System State**).

Выберем вариант **Custom**.

Тогда на следующем экране появится *список* дисков (рис. 4). Устанавливая или снимая отметки, можно указать, данные с каких дисков помещаются в резервную копию. *Опция* **Enable System Recovery** включает в *архив разделы*, где находятся

компоненты операционной системы и файлы необходимые для загрузки (т.е. отметку напротив этих разделов будет не снять).

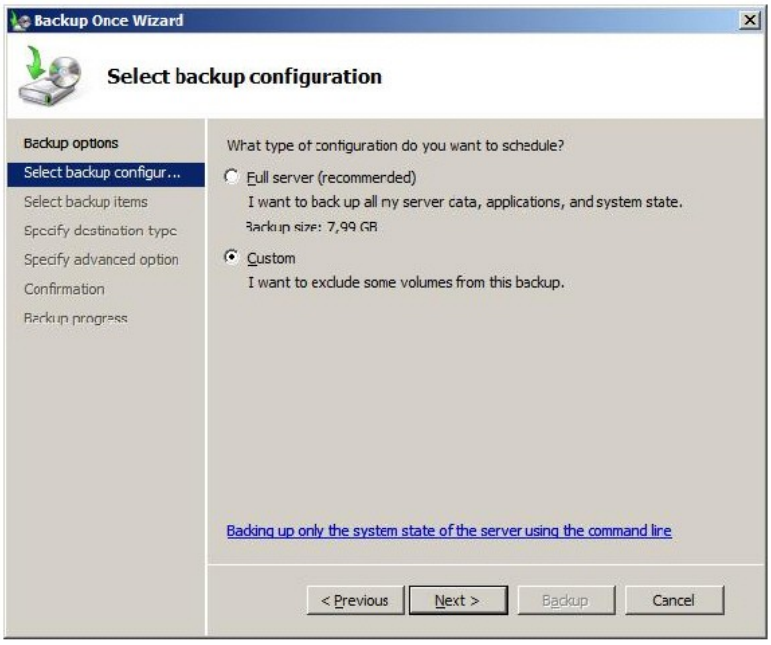

Рис. 3- Выбор между полным резервным копированием и копированием отдельных дисков

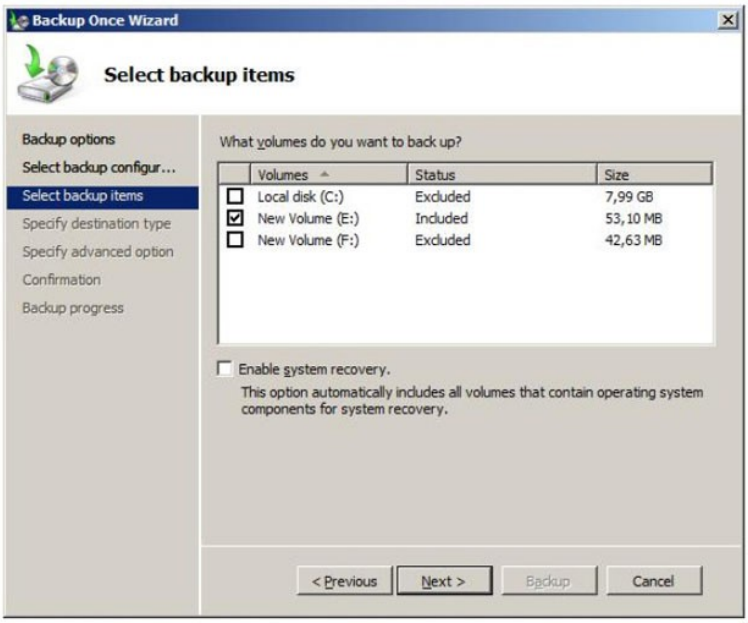

Рис. 4- Выбор дисков для резервного копирования

Предположим, нам нужно сделать резервную копию диска E:, на котором находятся пользовательские данные. Тогда отметки устанавливаем так, как это сделано на рис. 4 и переходим к следующей стадии, на которой нужно определить, куда будет производиться *копирование*. Это может быть локальный *диск* (жесткий *диск*, пишущий DVD-привод и т.д.) или сетевая *папка*. Надо учитывать, что архивная копия не может сохраняться на *диск*, входящий в перечень архивируемых. Также нельзя сохранить *архив* на *диск*, где хранятся файлы операционной системы.

Учитывая все вышеизложенное, в рассматриваемом примере можно сделать резервную копию диска E: на *диск* F:, в сетевую папку или на DVD-*диск*. Выберем первый

вариант, что и укажем в следующем окне мастера. После чего будет предложено выбрать тип резервного копирования (рис. 5).

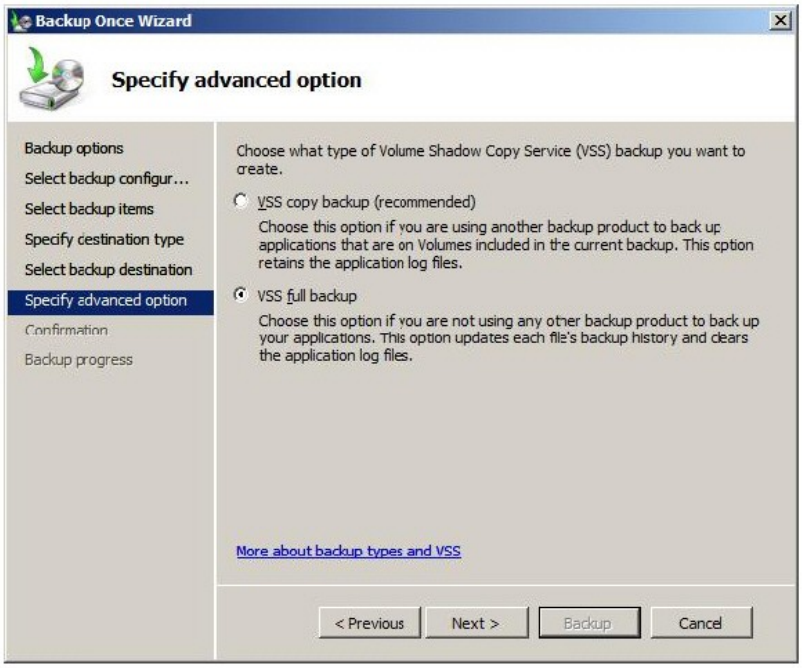

Рис. 5- Выбор типа копирования

Служба *Volume* Shadow *Copy Service* (*VSS*) может при резервном копировании отмечать файлы, как помещенные в *архив*, или не делать это. Если кроме средств *Windows Server* 2008 используются и другие продукты для резервного копирования, рекомендуется выбрать вариант **VSS copy backup**. Если такого нет, можно смело выбирать вариант **VSS full backup**.

В следующем окне мастера будет запрошено подтверждение и, если оно получено, запустится *резервное копирование*.

В результате, в нашем примере на диске F: появится каталог **WindowsImageBackup**, в нем будет создан *подкаталог*, названный *по* имени архивируемого сервера, куда и попадет копия.

Рассмотрим порядок восстановления данных из резервной копии.

В первой части лабораторной работы была сделана резервная копия раздела E:. Пусть понадобилось восстановить содержимое одной из папок из этого раздела. При этом требуется сравнить текущее содержимое папки с архивной копией, т.е. восстанавливать нужно в другую папку.

Запускаем оснастку **Windows Server Backup** и в списке **Actions** выбираем **Recover** (восстановление). Мастер восстановления уточняет, какой *сервер* будет восстанавливаться, после чего представит перечень имеющихся резервных копий (рис.6).

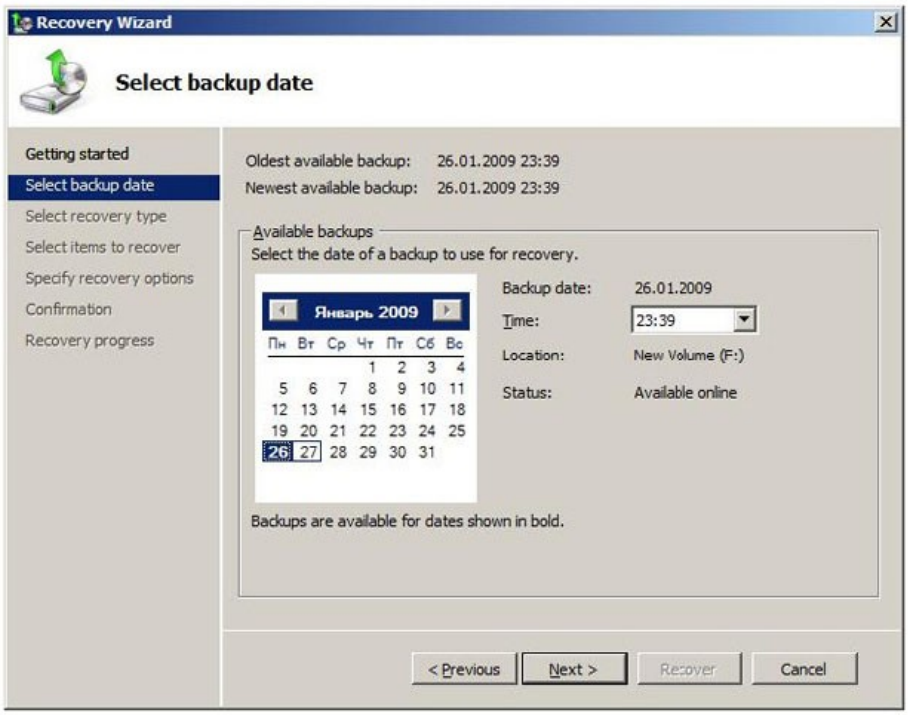

Рис. 6- Перечень доступных резервных копий для выбранного сервера

В следующем окне запрашивается, что именно восстанавливается. Нас интересует отдельная *папка*, потому выбираем вариант **Files and folders** (рис. 7). Другие варианты - восстановление зарегистрированных приложений и восстановление *раздела диска* целиком.

В следующем окне мастера в выпадающем списке нужно найти и выделить выбранную для восстановления папку. Если восстановить нужно несколько объектов, их выделяют совместно, удерживая клавишу **Ctrl** (или **Shift** для выделения диапазона). После этого выбирается *путь* для восстановления и задаются параметры. В нашем примере, мы хотим восстановить выбранную папку с файлами во вновь созданную папку **restored** (рис. 8).

Кроме пути (исходный или альтернативный), выбирается вариант действий при совпадении имен файлов и папок. Это особенно актуально, если восстанавливать файлы в исходную папку. Вариантов три - создавать копии, перезаписывать имеющиеся объекты восстанавливаемыми, оставить имеющиеся объекты.

Последний из выбираемых в этом окне параметров указывает на то, восстанавливать ли настройки безопасности (т.е. списки доступа к файлам).

После выбора всех параметров будет запрошено подтверждение и начнется восстановление.

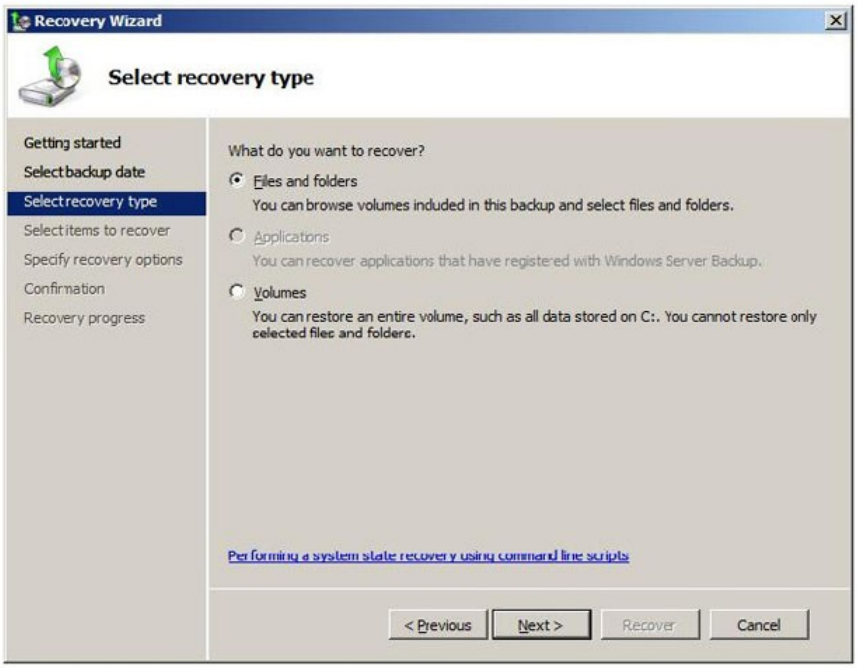

Рис. 7- Выбор типа восстановления

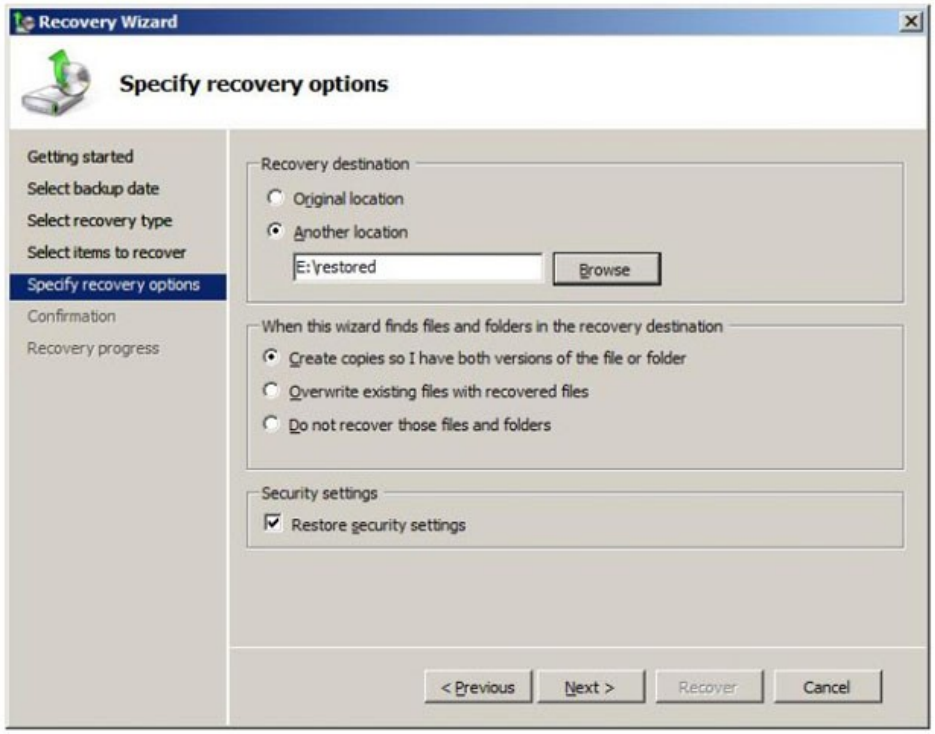

Рис. 8- Параметры восстановления

Теперь рассмотрим организацию резервного копирования *по* расписанию. Для этого в **Windows Server Backup** выберем опцию **Backup Schedule**. Первое окно запустившегося мастера информирует, что прежде чем устанавливать *резервное копирование по* расписанию, нужно определить:

- что будет копироваться (полное резервное копирование сервера или отдельные диски);
- как часто надо проводить копирование;

- где размещать копии.

При этом надо учитывать:

1. даже при выборе резервного копирования отдельных разделов, в их список обязательно должен быть внесен раздел (-ы) с операционной системой;
2. копирование может выполняться один или несколько раз в день;
3. для хранения результатов резервного копирования должен выделяться отдельный диск, внутренний или внешний (например, подключаемый по USB). Перед началом использования, он будет отформатирован мастером архивации. Рекомендуется, чтобы он был не менее, чем в 1,5 раза больше по объему, чем архивируемые диски.

Пусть требуется ежедневно делать *резервное копирование* диска раздела с операционной системой. В окне мастера аналогичном рис. 3, выбираем вариант *Custom*, в окне аналогичном рис. 4 - *диск* C (на котором расположена *операционная система*). Указываем расписание (рис. 9).

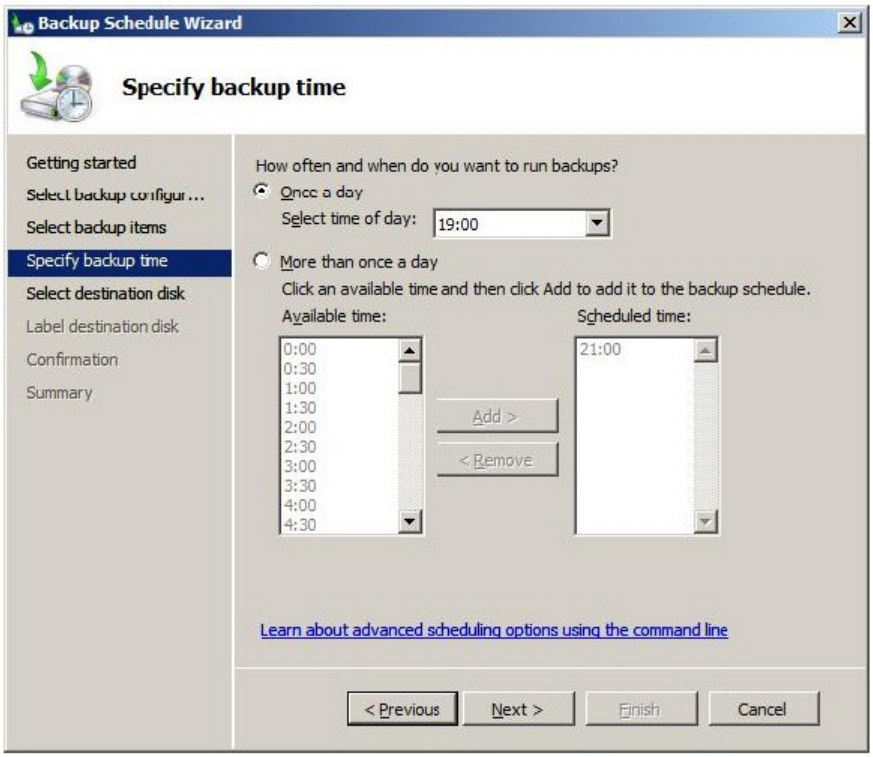

Рис. 9- Расписание резервного копирования

Дальше определяется *диск* (рис. 10), он может быть не отформатирован. Диску будет назначена *метка* с названием сервера и датой определения резервного копирования, после чего будет проведено *форматирование*. Диску не назначается буква и он не будет доступен пользователям как обычный *диск*.

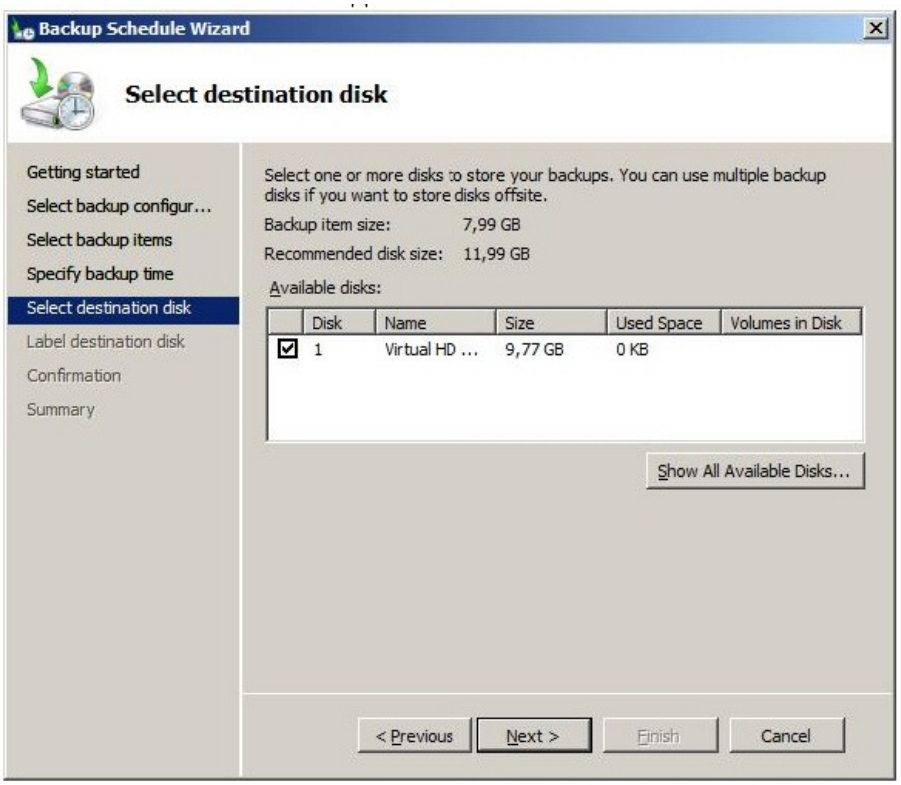

Рис. 10- Диск для хранения резервных копий

Когда работа *по* настройке автоматической архивации завершена, можно сделать дополнительные настройки, повышающие *быстродействие* для отдельных дисков. Для этого в списке **Actions** в оснастке **Windows Server Backup** выберите *пункт* **Configure Performance Settings**. В открывшемся окне (рис. 11) можно установить, какой тип резервного копирования производить для диска – полное (**full**) или добавочное (**Incremental**). *По* умолчанию используется полное. Добавочное помещает в *архив* только измененные с момента последнего архивирования файлы, это позволяет провести *резервное копирование* быстрее, но более существенно снижает *производительность* сервера в период копирования (т.к. надо проводить проверку).

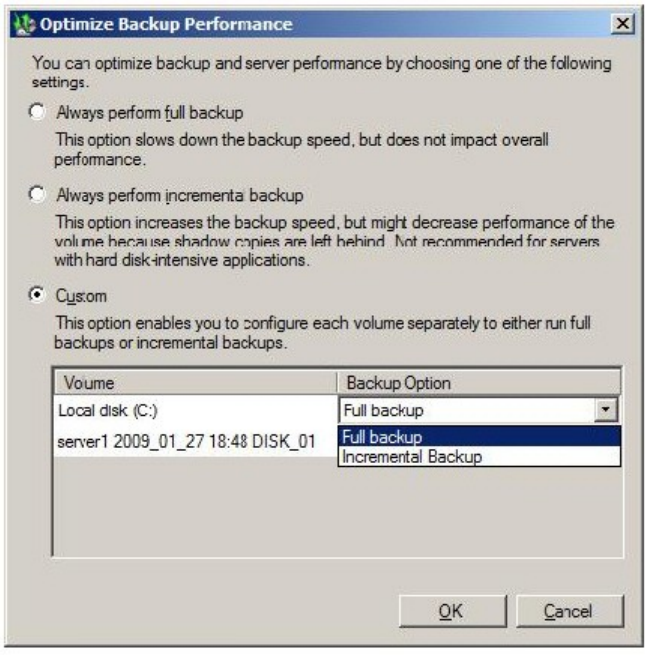

Рис. 11- Выбор типа резервного копирования для диска

Порядок восстановления такой же, как и при однократном копировании. Кстати, посмотреть параметры запланированного резервного копирования можно с помощью оснастки **Task Scheduler** (рис. 12).

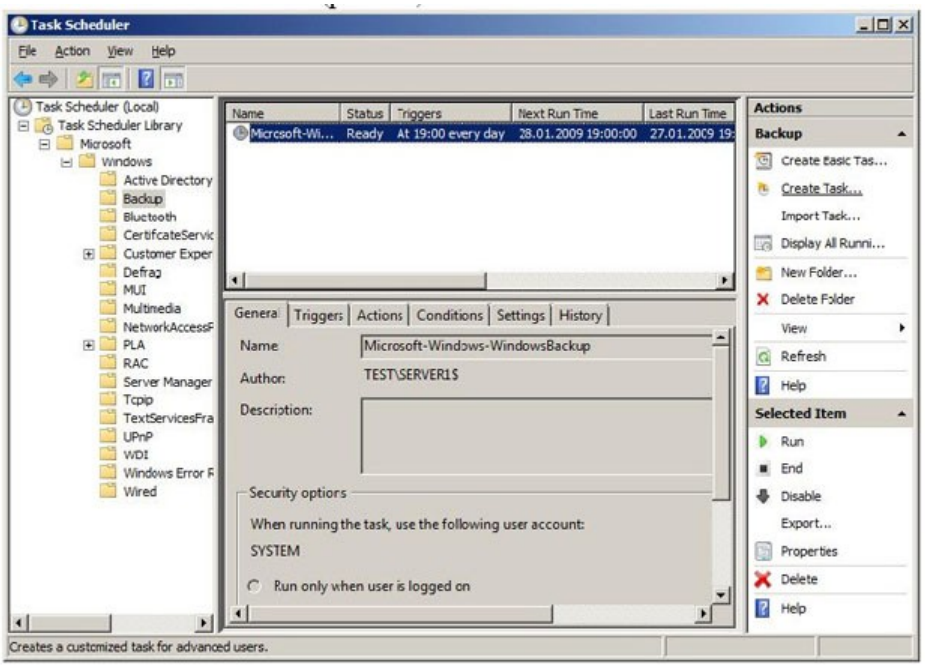

Рис. 12- Параметры созданного задания

Вопросы:

1. Утилиты администрирования.
2. Полное резервное копирование и копирование отдельных дисков.
3. Выбор дисков для резервного копирования.
4. Доступные резервные копии для выбранного сервера.
5. Выбор типа и параметров восстановления.
6. Диск для хранения резервных копий.
7. Выбор типа резервного копирования для диска.

Список литературы

Основная литература

1. Царев, Р.Ю. Программные и аппаратные средства информатики : учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в

кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Перечень Интернет - ресурсов

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»