Министерство образования и науки Челябинской области

Государственное бюджетное профессиональное образовательное учреждение

**«Южно-Уральский государственный технический колледж»**

**методические рекомендации**

**по практическим работам**

по МДК.03.01

**«Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи»**

для специальности 11.02.15

**«Инфокоммуникационные сети и системы связи»**

2020 г.

|  |  |  |
| --- | --- | --- |
| Методические рекомендации составлены в соответствии с программой | ОДОБРЕНО  Предметной (цикловой)  комиссией  протокол № 3  от «23» октября 2021 г.  Председатель ПЦК  Михайленко Ю.Н. | УТВЕРЖДАЮ  Заместитель директора  по НМР  \_\_\_\_\_\_\_\_Т.Ю.Крашакова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2021 г. |

**Составитель:**

Воителева Т.П., преподаватель Южно-Уральского государственного технического колледжа.

Содержание

Введение…………………………………………………..…………………………2

Практическая работа № 1……………………………………………………...…...4

«Определение надежности пароля»

Практическая работа № 2…………………………………………………….…….7

«Ограничение доступа на вход в систему»

Практическая работа № 3………………………………………………………...15

«Идентификация и аутентификация пользователей»

Практическая работа № 4…………………………………………………….…..19

«Регистрация событий (аудит)»

Практическая работа № 5………………………………………………………...22

«Определение угрозы безопасности компьютерной системы»

Практическая работа № 6 …………………………………………………..……..30

«Обеспечение физической безопасности»

Практическая работа № 7 …………………………………………………..……..33

«Реализация физической безопасности с помощью средств Windows Server»

Практическая работа № 8 …………………………………………………..……..37

«Определение модели управления доступом»

Практическая работа № 9 …………………………………………………..……..47

«Уничтожение остаточной информации»

Практическая работа № 10…………………………………………………….…..53

«Настройка браузера в ОС семейства Windows»

Практическая работа № 11………………………………………………….……..64

«Настройка браузера в ОС Linux.»

Практическая работа № 12………………………………………………….……..66

«Определение трудоемкости взлома симметричного криптоалгоритма»

Практическая работа № 13……………………………………………………..….71

«Определение трудоемкости взлома несимметричного

криптоалгоритма»

Практическая работа № 14………………………………………………….….….76

«Составление схем обнаружения вредоносных программ»

Практическая работа № 15……………………………………………….…….….83

«Схемы работы антивирусных программ»

Практическая работа № 16……………………………………………….…….….88

«Выбор модели межсетевого экрана»

Практическая работа № 17……………………………………………...……….95

«Защита удаленного доступа»

Практическая работа № 18……………………………………………….……….99

«Технологии обнаружения и предотвращения вторжений»

Литература………………………………………………………………..……….103

**Введение**

Для овладения знаниями и их закрепления, приобретения умений и навыков, необходимых в дальнейшей познавательной и трудовой деятельности необходимы практические занятия. Практические работы относятся к основным видам учебных занятий.

Практические работы в курсе изучения дисциплины «Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи» способствуют овладению указанным видом профессиональной деятельности и элементами соответствующих профессиональных компетенций:

* ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности;
* ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
* ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.

Обучающийся в ходе выполнения практических работ должен:

знать:

* принципы построения информационно-коммуникационных сетей;
* международные стандарты информационной безопасности;
* акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
* технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
* классификацию угроз сетевой безопасности;
* методы и способы защиты информации, передаваемой по кабельным направляющим системам;
* правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю;
* средства защиты различных операционных систем и среды передачи информации.

уметь:

* классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
* определять оптимальные способы обеспечения информационной безопасности;
* осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
* выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
* выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
* защищать базы данных при помощи специализированных программных продуктов.

Ведущими целями проведения практических занятий являются:

* обобщение, систематизация, углубление, закрепление полученных теоретических знаний по дисциплине;
* формирование умений применять полученные знания на практике;
* развитие интеллектуальных умений: аналитических, проектировочных, конструкторских;
* выработка таких профессионально значимых качеств, как самостоятельность, ответственность, творческая инициатива, умение работать в коллективе.

Выполнение каждой работы предваряет краткий теоретический материал, необходимый для усвоения данной темы. До начала выполнения студенты должны ознакомиться с целью работы, теорией по данной теме, порядком выполнения работы.

По результатам выполненной практической работы студенты должны оформить отчет, и ответить на контрольные вопросы.

Практическая работа № 1

«Определение надежности пароля»

**Цель работы**. Получение практических навыков определения надежности пароля.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

Одной из самых существенных проблем, связанных с обеспечением безопасности в организации являются пароли к учетным записям важных пользователей. Даже если вы, являясь системным администратором, тщательно спланируете и настроите параметры безопасности групповой политики, включая настройки брандмауэра в режиме повышенной безопасности, развернете антивирусное программное обеспечение и будете поддерживать в обновленном состоянии систему и антивирусное ПО, настроите политики IPSec (сокращение от **IP Security** — набор [протоколов](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) для обеспечения защиты данных, передаваемых по межсетевому протоколу [IP](http://ru.wikipedia.org/wiki/IP), позволяет осуществлять подтверждение подлинности и/или [шифрование](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) IP-пакетов), развернете сервера защиты доступа к сети, а у учетных записей ваших пользователей будут недостаточно сложные пароли, безопасность всей вашей компании может быть под угрозой.

При помощи групповой политики можно (и нужно) задать ограничение по созданию сложных паролей, установить интервал для блокировки учетной записи в случае неправильного ввода пароля, а также настроить политики аудита для анализа неудачных попыток входа в систему. Но даже пароли, которые операционная система будет считать сложными (то есть длина пароля будет превышать определенное количество символов, пароль будет содержать символы верхнего, нижнего регистра, а также цифры), могут на самом деле оказаться уязвимыми и простыми для злоумышленников, которые будут их взламывать. Именно этот этап обеспечения безопасности вашей компании может оказаться для вас наиболее сложным, так как здесь ваше участие играет лишь посредственную роль, а любое халатное отношение со стороны ваших пользователей может летально сказаться на инфраструктуре всей компании.

**Пример продолжительности подбора паролей**

В таблице 1 представлено оценочное время полного перебора паролей в зависимости от их длины. Предполагается, что в пароле могут использоваться 36 различных символов ([латинские](http://ru.wikipedia.org/wiki/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82) буквы одного регистра + цифры), а скорость перебора составляет 100 000 паролей в секунду.

Таблица 1. Пример продолжительности подбора паролей

|  |  |  |  |
| --- | --- | --- | --- |
| **Кол-во знаков** | **Кол-во вариантов** | [**Стойкость**](http://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%8F#.D0.AD.D0.BD.D1.82.D1.80.D0.BE.D0.BF.D0.B8.D1.8F_.D0.BA.D0.B0.D0.BA_.D0.BC.D0.B5.D1.80.D0.B0_.D1.81.D0.BB.D0.BE.D0.B6.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D0.BF.D0.B0.D1.80.D0.BE.D0.BB.D1.8F) | **Время перебора** |
| 1 | 36 | 5 бит | менее секунды |
| 2 | 1296 | 10 бит | менее секунды |
| 3 | 46 656 | 15 бит | менее секунды |
| 4 | 1 679 616 | 21 бит | 17 секунд |
| 5 | 60 466 176 | 26 бит | 10 минут |
| 6 | 2 176 782 336 | 31 бит | 6 часов |
| 7 | 78 364 164 096 | 36 бит | 9 дней |
| 8 | 2,821 109 9x1012 | 41 бит | 11 месяцев |
| 9 | 1,015 599 5x1014 | 46 бит | 32 года |
| 10 | 3,656 158 4x1015 | 52 бита | 1 162 года |
| 11 | 1,316 217 0x1017 | 58 бит | 41 823 года |
| 12 | 4,738 381 3x1018 | 62 бита | 1 505 615 лет |

Таким образом, пароли длиной до 7 символов включительно в общем случае не являются надежными.

**Какие пароли можно считать стойкими?**

Для того, чтобы это определить, необходимо изучить таблицу 2.

Таблица 2. Пример продолжительности подбора паролей. Определение стойкости пароля.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Алгоритм | Длина | Набор символов | Количество вариантов | Время перебора на «обычной системе» Q6600 + HD4770 | Время перебора на системе 4xGTX295 | Время перебора на суперкластере 100x 4xGTX295 |
| RAR 3.x | 4 | Латинские маленькие + большие + цифры + спецсимволы | 96^4 = 84934656 | 7.6 часов | 1.5 часа | 45 сек |
| RAR 3.x | 6 | Латинские маленькие + большие + цифры + спецсимволы | 96^6 = 782757789696 | 8 лет | 1.33 лет | 5 дней |
| WPA | 8 | Латинские маленькие + большие + цифры | 62^8 = 218340105584896 | 495 лет | 82 лет | 300 дней |
| WinZip 9+ | 8 | Латинские маленькие + большие + цифры | 62^8 = 218340105584896 | 51 год | 8.5 лет | 31 день |

Вывод неутешительный для brute-force атаки. При правильно выбранном пароле из 8-ми символов подобрать его в осмысленное время просто невозможно.

Другими словами, невозможно точно рассчитать стойкость пароля, ее можно лишь приблизительно оценить. Для этого пригодятся формулы, описанные ниже.

Время, необходимое для гарантированного нахождения пароля равно: t = n/V где V количество перебираемых комбинаций в секунду, а n количество существующих паролей. В свою очередь n зависит от максимально возможной длины пароля и количества символов, из которых может быть составлен пароль.

**Пример.** Допустим, пароль состоит из 10 цифр. Рассчитаем, сколько же вариантов паролей будет при 10-значном пароле:

10 (количество символов, из которых может состоять пароль - 0 1 2 3 4 5 6 7 8 9) в степени 10 (длина пароля), что равно 10'000'000'000 вариантов.

А теперь рассчитаем, сколько времени займет непрерывный 24/7 брут (прямой перебор) такого пароля.

Предположим, что брут перебирает 100 паролей в секунду, значит перебор займет:

10000000000 / 100 (получим количество секунд) / 60 (получим количество минут) / 60 (получим количество часов) / 24 (получим количество дней) / 365 (получим примерное количество лет), что равно примерно 3 года.

1. Порядок выполнения работы
2. Составить пароль из двух цифр. Вычислить его надежность.
3. Составить пароль из одной цифры и одной буквы алфавита. Определить его надежность.
4. Составить пароль из 8 символов. Определить его надежность.

При расчетах принимать скорость перебора, равной 100 паролей в секунду.

1. Контрольные вопросы.
2. Отчего зависит надежность пароля?
3. Отчего зависит скорость определения пароля методом перебора?
4. Что необходимо применять на предприятии для обеспечения ИБ?
5. Какие меры должны быть применены для обеспечения ИБ на предприятии?
6. Содержание отчета
7. Составленные пароли.
8. Расчет надежности паролей.
9. Вывод.
10. Ответы на контрольные вопросы.

Практическая работа № 2

«Ограничение доступа на вход в систему»

**Цель работы**. Научиться работать с процедурами создания учётных записей пользователей и управления их.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

Учётная запись пользователя – это запись, которая содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации, например, биометрические характеристики). Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде (в целях его безопасности).

Для повышения надёжности могут быть, наряду с паролем, предусмотрены альтернативные средства аутентификации, например, специальный секретный вопрос (или несколько вопросов) такого содержания, что ответ может быть известен только пользователю. Такие вопросы и ответы также хранятся в учётной записи.

Создание учетных записей пользователей

В операционной системе Windows 7 учетные записи можно создавать следующими способами:

Создание учетной записи с помощью Панели управления (средство Управление учетными записями пользователей). Для того чтобы создать учетную запись при помощи средства Учетные записи пользователей, нужно сделать следующее:

Выполните команду Пуск - Панель управления и из списка компонентов панели управления выберите Учетные записи пользователей;

В диалоговом окне Учетные записи пользователей перейдите по ссылке Управление другой учетной записью, а затем нажмите на Создание учетной записи;

Далее нужно ввести имя для учетной записи, выбрать тип учетной записи и нажать на кнопку Создание учетной записи.

Имя пользователя не должно совпадать с любым другим именем пользователя или группы на данном компьютере. Оно может содержать до 20 символов верхнего или нижнего регистров, за исключением следующих: " / \ [ ] : ; | = , + \* ? <> @, а также имя пользователя не может состоять только из точек и пробелов.

В этом окне можно выбрать один из двух типов учетных записей:

Обычный доступ - обычные учетные записи пользователей, которые предназначены для повседневной работы,

Администратор - учетные записи администратора, которые предоставляют полный контроль над компьютером и применяются только в необходимых случаях.

При помощи диалогового окна Управление учетными записями пользователей можно не только создавать учетные записи, но и выполнять с ними простейшие действия:

1. изменение имени;
2. создание пароля;
3. изменение пароля;
4. удаление пароля;
5. изменение рисунка;
6. установка родительского контроля;
7. изменение типа учетной записи;
8. удаление учетной записи;
9. включение и отключение гостевой учетной записи.

Чтобы внести изменения в созданную учетную запись, нужно выбрать ее из списка и открыть окно учетной записи и выбрать соответствующую команду, далее следовать указаниям в диалоговых окнах.

Рассмотрим алгоритм создания пароля для учетной записи Новый пользователь.

Выберите учетную запись, для которой нужно создать пароль (в данном случае Новый пользователь) и перейдите по ссылке Создание пароля. Эта ссылка будет отображаться только в том случае, если у пользователя этой текущей записи нет пароля.

В диалоговом окне Создание пароля введите пароль для данной учетной записи, а затем повторите его в поле Подтверждение пароля и еще можно ввести подсказку в поле Введите подсказку для пароля. Подсказка – это текст, который операционная система отображает на экране приветствия. В связи с тем, что подсказку может увидеть любой пользователь, который попытается войти в вашу систему, она должна быть менее очевидной, но при этом понятной для того, кто ее создал в том случае, если он забудет пароль. После ввода пароля, подтверждения пароля и подсказки для создания пароля учетной записи нажмите на кнопку Создать.

Изменение пароля

Если у учетной записи пользователя уже имеется пароль, но его нужно сменить, необходимо выполнить следующее:

Выполните команду Пуск - Панель управления и из списка компонентов панели управления выберите Учетные записи пользователей;

Выберите свою учетную запись и перейдите по ссылке Изменение пароля.

Находясь в окне Изменение пароля, в поля Новый пароль и Подтверждение пароля введите и подтвердите новый пароль для учетной записи. В поле Введите подсказку для пароля введите подсказку.

Удаление пароля

В том случае, если у пользователя есть пароль и этот пароль для работы за компьютером ему не нужен, выполним следующие действия:

Выполните команду Пуск - Панель управления и из списка компонентов панели управления выберите Учетные записи пользователей;

Выберите свою учетную запись и нажмите на ссылку Удаление пароля;

В диалоговом окне Удаление пароля подтвердите удаление пароля, нажав на кнопку Удалить пароль.

Создание учетной записи при помощи средства «Учетные записи пользователей» (диалоговое окно Выполнить)

Доступный через панель управления диалог Управление учетными записями пользователей имеет очень серьезное ограничение: оно предлагает на выбор только учетные записи типа Обычный доступ или Администратор.

Для того чтобы при создании нового пользователя его можно было поместить в какую-либо определенную группу, нужно сделать следующее:

Выполните команду Пуск – Все программы – Стандартные – Выполнить для открытия диалогового окна Выполнить;

В диалоговом окне Выполнить в поле Открыть введите control userpasswords2 и нажмите ОК;

В диалоговом окне Учетные записи пользователей нажмите на кнопку Добавить для запуска мастера добавления нового пользователя;

В появившемся диалоговом окне Добавление нового пользователя введите имя пользователя. Поля Полное имя и Описание не являются обязательными, то есть их можно заполнять при желании. Нажмите Далее;

В окне Введите и подтвердите пароль этого пользователя введите пароль для данной учетной записи, а затем продублируйте его в поле Подтверждение, после чего нажмите Далее;

На последнем шаге мастера необходимо установить переключатель, определяющий группу безопасности, к которой должна относиться данная учетная запись пользователя. Можно выбрать одну из следующих групп: Обычный доступ, Администратор или Другой. Последний переключатель стоит использовать в том случае, если нужно отнести пользователя к какой-то другой группе, созданной по умолчанию в операционной системе Windows 7.

В следующем списке перечислены 15 встроенных групп операционной системы Windows 7. Эти права назначаются в рамках локальных политик безопасности:

Administrators (Администраторы). Пользователи, входящие в эту группу, имеют полный доступ на управление компьютером и могут при необходимости назначать пользователям права пользователей и разрешения на управление доступом. По умолчанию членом этой группы является учетная запись администратора. Если компьютер подключен к домену, группа «Администраторы домена» автоматически добавляется в группу «Администраторы». Эта группа имеет полный доступ к управлению компьютером, поэтому необходимо проявлять осторожность при добавлении пользователей в данную группу;

Backup Operators (Операторы архива). Пользователи, входящие в эту группу, могут архивировать и восстанавливать файлы на компьютере независимо от любых разрешений, которыми защищены эти файлы. Это обусловлено тем, что право выполнения архивации получает приоритет над всеми разрешениями. Члены этой группы не могут изменять параметры безопасности.

Cryptographic Operators (Операторы криптографии). Членам этой группы разрешено выполнение операций криптографии.

Debugger Users (Группа удаленных помощников). Члены этой группы могут предлагать удаленную помощь пользователям данного компьютера.

Distributed COM Users (Пользователи DCOM). Членам этой группы разрешено запускать, активировать и использовать объекты DCOM на компьютере.

Event Log Readers (Читатели журнала событий). Членам этой группы разрешается запускать журнал событий Windows.

Guests (Гости). Пользователи, входящие в эту группу, получают временный профиль, который создается при входе пользователя в систему и удаляется при выходе из нее. Учетная запись «Гость» (отключенная по умолчанию) также является членом данной встроенной группы.

IIS\_IUSRS. Это встроенная группа, используемая службами IIS.

Network Configuration Operators (Операторы настройки сети). Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP. Эта группа не имеет членов по умолчанию.

Performance Log Users (Пользователи журналов производительности). Пользователи, входящие в эту группу, могут управлять счетчиками производительности, журналами и оповещениями на локальном или удаленном компьютере, не являясь при этом членами группы «Администраторы».

Performance Monitor Users (Пользователи системного монитора). Пользователи, входящие в эту группу, могут наблюдать за счетчиками производительности на локальном или удаленном компьютере, не являясь при этом участниками групп «Администраторы» или «Пользователи журналов производительности».

Power Users (Опытные пользователи). По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учетные записи обычных пользователей. В предыдущих версиях операционной системы Windows эта группа была создана для того, чтобы назначать пользователям особые административные права и разрешения для выполнения распространенных системных задач. В этой версии операционной системы Windows учетные записи обычных пользователей предусматривают возможность выполнения большинства типовых задач настройки, таких как смена часовых поясов. Для старых приложений, требующих тех же прав опытных пользователей, которые имелись в предыдущих версиях операционной системы Windows, администраторы могут применять шаблон безопасности, который позволяет группе «Опытные пользователи» присваивать эти права и разрешения, как это было в предыдущих версиях операционной системы Windows.

Remote Desktop Users (Пользователи удаленного рабочего стола). Пользователи, входящие в эту группу, имеют право удаленного входа на компьютер.

Replicator (Репликатор). Эта группа поддерживает функции репликации. Единственный член этой группы должен иметь учетную запись пользователя домена, которая используется для входа в систему службы репликации контроллера домена. Не добавляйте в эту группу учетные записи реальных пользователей.

Users (Пользователи). Пользователи, входящие в эту группу, могут выполнять типовые задачи, такие как запуск приложений, использование локальных и сетевых принтеров и блокировку компьютера. Члены этой группы не могут предоставлять общий доступ к папкам или создавать локальные принтеры. По умолчанию членами этой группы являются группы «Пользователи домена», «Проверенные пользователи» и «Интерактивные». Таким образом, любая учетная запись пользователя, созданная в домене, становится членом этой группы.

Создание учетной записи при помощи утилиты Локальные пользователи и группы (использование возможно в ОС Windows 7 Максимальная (Ultimate))

Утилита Локальные пользователи и группы расположена в компоненте Управление компьютером, представляющем собой набор средств администрирования, с помощью которых можно управлять одним компьютером, локальным или удаленным. Утилита Локальные пользователи и группы служит для защиты и управления учетными записями пользователей и групп, размещенных локально на компьютере. Можно назначать разрешения и права для учетной записи локального пользователя или группы на определенном компьютере (и только на этом компьютере).

Использование утилиты Локальные пользователи и группы позволяет ограничить возможные действия пользователей и групп путем назначения им прав и разрешений.

Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера.

Разрешение представляет собой правило, связанное с объектом (обычно с файлом, папкой или принтером), которое определяет, каким пользователям и какой доступ к объекту разрешен.

Для того чтобы создать локальную учетную запись пользователя при помощи утилиты Локальные пользователи и группы, нужно сделать следующее:

Откройте утилиту Локальные пользователи и группы одним из следующих способов:

Выполните команду Пуск - Панель управления и из списка компонентов панели управления выберите Администрирование, затем откройте компонент Управление компьютером. В Управлении компьютером откройте Локальные пользователи и группы;

Выполните команду Пуск – Все программы – Стандартные – Выполнить (или комбинация клавиш hello\_html\_maf49875.jpg+R) для открытия диалогового окна Выполнить;

В диалоговом окне Выполнить в поле Открыть введите lusrmgr.msc и нажмите ОК;

Откройте узел Пользователи и либо в меню Действие, либо из контекстного меню выбрать команду Новый пользователь;

В диалоговом окне Новый пользователь введите соответствующие сведения. Помимо указанных данных, можно воспользоваться следующими флажками: Требовать смену пароля при следующем входе в систему, Запретить смену пароля пользователем, Срок действия пароля не ограничен, Отключить учетную запись и нажать на кнопку Создать, а затем Закрыть.

Для того чтобы добавить пользователя в группу, дважды щелкните имя пользователя для получения доступа к странице свойств пользователя.

На вкладке Членство в группах нажмите на кнопку Добавить.

В окне Выбор группы можно выбрать группу для пользователя двумя способами:

В поле Введите имена выбираемых объектов введите имя группы и нажмите на кнопку Проверить имена.

Или в окне Выбор группы нажмите на кнопку Дополнительно, чтобы открыть диалоговое окно Выбор группы. В этом окне нажмите на кнопку Поиск, чтобы отобразить список всех доступных групп, выберите подходящую группу и нажмите два раза ОК.

1. Порядок выполнения работы

Задание 1 Ознакомиться с технологиями создания и управления учетными записями пользователей. Примените к созданной учётной записи настройки, указанные в варианте.

Задание 2 Создайте новую учетную запись пользователя с помощью командной строки.

Задание 3 Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.

Задание 4 Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя

Варианты заданий



1. Контрольные вопросы
2. Как создать учётные записи пользователей?
3. Как создать учётные записи пользователей для компьютеров, состоящих в рабочей группе?
4. Как создать учётные записи при помощи оснастки «Локальные пользователи и группы»?
5. Как создать учётные записи при помощи командной строки?
6. Как управлять учётными записями при помощи диалога «Управление учётными записями?
7. Перечислите способы создания учетных записей пользователей на ПК
8. Укажите возможности членов группы Администраторы
9. Укажите возможности членов группы Опытные пользователи
10. Укажите возможности членов группы Пользователи
11. Укажите возможности членов группы Гости
12. Укажите возможности членов группы Операторы архива
13. Укажите возможности членов группы Операторы настройки сети
14. Укажите возможности членов группы Пользователи удаленного рабочего стола
15. Опишите технологию создания учетной записи с помощью панели управления
16. Перечислите действия, которые можно выполнять с созданной учетной записью
17. Опишите технологию создания учетной записи с помощью утилиты Учетные записи пользователей (окно Выполнить)
18. Опишите технологию создания учетной записи с помощью утилиты Локальные пользователи и группы
19. Как установить членство в группе?
20. Укажите команду создания учетной записи с помощью утилиты Net User: краткая форма команды, поясните операторы
21. Укажите команду создания учетной записи с помощью утилиты Net User: развернутая форма команды, поясните операторы
22. Укажите команду удаления учетной записи в режиме командной строки
23. С помощью какой команды можно просмотреть все свойства учетной записи в режиме командной строки?
24. Содержание отчета
25. Снимки экрана с созданной учетной записью.
26. Ответы на контрольные вопросы

Практическая работа № 3.

«Идентификация и аутентификация пользователей»

**Цель работы.** Научиться работать с алгоритмами идентификации и аутентификации пользователей.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. **Общие положения**

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации. Без порядка на проходной не будет порядка и внутри охраняемой территории.

Идентификация позволяет субъекту - пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова "аутентификация" иногда используют сочетание "проверка подлинности". Субъект может подтвердить свою подлинность, если предъявит по крайней мере одну из следующих сущностей:

нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.,

нечто, чем он владеет: личную карточку или иное устройство аналогичного назначения,

нечто, что является частью его самого: голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики,

нечто, ассоциированное с ним, например, координаты.

К сожалению, надежная идентификация и аутентификация затруднена по ряду принципиальных причин. Во-первых, компьютерная система основывается на информации в том виде, в каком она была получена; строго говоря, источник информации остается неизвестным. Например, злоумышленник мог воспроизвести ранее перехваченные данные. Следовательно, необходимо принять меры для безопасного ввода и передачи идентификационной и аутентификационной информации; в сетевой среде это сопряжено с особыми трудностями. Во-вторых, почти все аутентификационные сущности можно узнать, украсть или подделать. В-третьих, имеется противоречие между надежностью аутентификации с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность подглядывания за вводом. В-четвертых, чем надежнее средство защиты, тем оно дороже.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации. Обычно компромисс достигается за счет комбинирования двух первых из перечисленных базовых механизмов проверки подлинности.

Наиболее распространенным средством аутентификации являются пароли. Система сравнивает введенный и ранее заданный для данного пользователя пароль; в случае совпадения подлинность пользователя считается доказанной. Другое средство, постепенно набирающее популярность, - секретные криптографические ключи пользователей.

Обратим внимание на то, что процесс идентификации и аутентификации может идти не только между пользователем и системой - его целесообразно применять и к равноправным партнерам по общению, а также для проверки подлинности источника данных. Когда аутентификации подвергаются процесс или данные, а не человек, выбор допустимых средств сужается. Компьютерные сущности не могут чем-то обладать, у них нет биометрических характеристик. Единственное, что у них есть, это информация; значит, проверка подлинности может основываться только на том, что процесс или данные знают. С другой стороны, память и терпение у компьютерных сущностей не в пример лучше человеческих, они в состоянии помнить или извлекать из соответствующих устройств и многократно применять длинные криптографические ключи, поэтому в распределенных средах методы криптографии выходят на первый план; по существу, им нет альтернативы.

Ввод пароля можно подсмотреть. Пароли нередко сообщают коллегам. Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор. Пароли уязвимы по отношению к электронному перехвату - это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход - использование криптографии для шифрования паролей перед передачей по линиям связи или вообще их не передавать, как это делается в сервере аутентификации Kerberos.

Тем не менее следующие меры позволяют значительно повысить надежность парольной защиты:

1. наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
2. управление сроком действия паролей, их периодическая смена;
3. ограничение доступа к файлу паролей;
4. ограничение числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;
5. обучение и воспитание пользователей (например, тому, что пароли, в отличие от обеда, лучше не разделять с другом);
6. использование программных генераторов паролей [2], которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.
7. **Порядок выполнения работы**

Задание 1 Опишите параметры локальной политики безопасности операционной системы

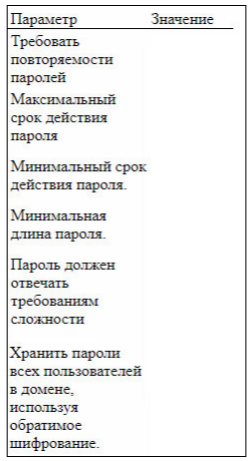
Windows:

– кто имеет доступ к компьютеру;

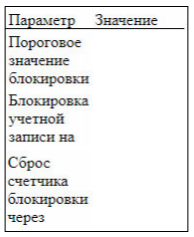
– какие ресурсы могут использовать пользователи на компьютере;

– включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задание 2 Опишите параметры и значения параметров Политики паролей. Заполните таблицу:



Задание 3 Опишите параметры и значения параметров Политики учетной записи. Заполните таблицу:



Задание 4 Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения вашего задания.

Задание 5 После успешного выполнения предыдущего задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

Задание 6 Проведите эксперименты с другими параметрами Политики учетных записей.

1. **Контрольные вопросы**
2. Какие бывают методы идентификации?
3. Как происходит процесс аутентификации?
4. Какие существуют проблемы использования пароля?
5. **Содержание отчета**
6. Определение идентификации.
7. Определение аутентификации.
8. Ответы на контрольные вопросы

**Практическая работа № 4**

**Регистрация событий (аудит)**

**Цель работы.** Научиться работать с механизмами регистрации событий.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. **Общие положения**

Зарегистрированная информация о событиях безопасности предназначена для использования при реализации процессов мониторинга информационной безопасности в информационных (автоматизированных) системах.

При необходимости зарегистрированная информация о событиях безопасности может передаваться в средства автоматизации мониторинга информационно безопасности. Для этого средства, осуществляющие регистрацию событий безопасности, должны обеспечивать предоставление доступа к информации о зарегистрированных событиях безопасности и (или) выгрузку событий безопасности в средства автоматизации мониторинга информационно безопасности.

Применяются следующие определения:

событие безопасности – зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств защиты информации, или ситуацию, которая может быть значимой для безопасности информации;

регистрация события безопасности – процесс (процедура) выполнения автоматизированной или автоматической функции занесения в журнал регистрации событий безопасности (журнал аудита) записи о событии безопасности;

регистрируемая информация (о событии безопасности) – сведения о зарегистрированном событии безопасности, подлежащие регистрации в журнале регистрации событий безопасности (журнале аудита);

регистрационная запись (о событии безопасности) – запись в журнале регистрации событий безопасности (журнале аудита), содержащая регистрируемую информацию о событии безопасности, представленную в установленном формате;

зарегистрированное событие безопасности – событие безопасности, по которому была внесена регистрационная запись в журнал регистрации событий безопасности (журнал аудита);

журнал регистрации событий безопасности (журнал аудита) – объект или совокупность объектов информационной (автоматизированной) системы (объектов файловой системы или объектов базы данных), предназначенный (предназначенная) для хранения регистрационных записей о зарегистрированных событиях безопасности.

События безопасности регистрируются следующими составными частями системы (средствами):

- средствами защиты информации;

- средствами обеспечения безопасности информационных технологий;

- иными программно-техническими средствами и программным обеспечением, применяемыми в информационных (автоматизированных) системах.

Средства защиты информации регистрируют события безопасности, связанные с реализацией функций безопасности.

Средства обеспечения безопасности информационных технологий и иные программно-технические средства и программное обеспечение, применяемые в информационных (автоматизированных) системах, регистрируют события безопасности, связанные с реализацией мер защиты в информационных (автоматизированных) системах.

Другими словами, под регистрацией понимается сбор и накопление информации о событиях, происходящих в информационной системе предприятия. У каждого сервиса свой набор возможных событий, но в любом случае их можно подразделить на внешние - вызванные действиями других сервисов, внутренние - вызванные действиями самого сервиса, и клиентские - вызванные действиями пользователей и администраторов.

Аудит - это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация регистрации и аудита преследует следующие главные цели:

* обеспечение подотчетности пользователей и администраторов;
* обеспечение возможности реконструкции последовательности событий;
* обнаружение попыток нарушений информационной безопасности;
* предоставление информации для выявления и анализа проблем.

1. Порядок выполнения работы

Задание 1 Опишите параметры и значения параметров Политики аудита. Заполните таблицу.

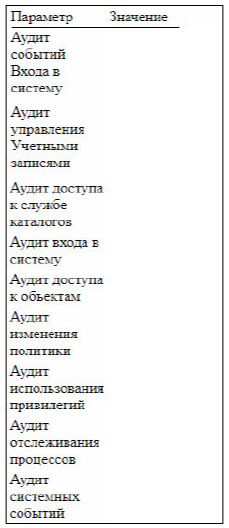
Задание 2 Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале?

Задание 3 Включите аудит успеха и отказа всех параметров.

Задание 4 Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись.

Задание 5 Удалите раннее созданную учетную запись и зафиксируйте все события системного журнала, связанные с этим действием.

Таблица для задания 1.



1. Контрольные вопросы
2. Какие существуют средства регистрации и аудита?
3. Приведите примеры программ регистрации
4. Содержание отчета
5. Определения аудита и регистрации
6. Заполненная таблица.
7. Выполнение заданий.

Практическая работа № 5.

«Определение угрозы безопасности компьютерной системы»

**Цель работы.** Научиться определять угрозу физической безопасности.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. **Общие положения**

**Угрозы информационной безопасности**

При построении системы *защиты персональных данных* (далее СЗПД) ключевым этапом является построение частной модели угроз для конкретной организации. На основании этой модели в дальнейшем подбираются адекватные и достаточные средства защиты.

Под **угрозами безопасности ПД** при их обработке в ИСПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе *случайного, доступа* к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Появление угроз безопасности может быть связано как с преднамеренными действиями злоумышленников, так и с непреднамеренными действиями персонала или пользователей ИСПД.

Угрозы безопасности могут быть реализованы двумя путями:

* через технические каналы утечки;
* путем несанкционированного доступа.

Обобщенная схема реализации канала угроз ПД показана на [рисунке 1](http://www.intuit.ru/department/security/enspdata/4/#image.4.1)

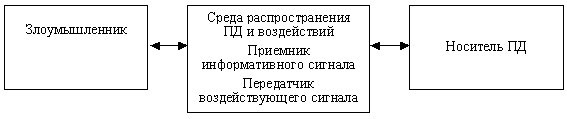


Рисунок 1. Обобщенная схема канала реализации угроз безопасности персональных данных

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. Среда распространения бывает однородной, например, только воздух при распространении электромагнитного излучения, или неоднородной, когда сигнал переходит из одной среды в другую. Носителями ПД могут быть люди, работающие с ИСПД, технические средства, вспомогательные средства и т.д. Главное, что информация при этом отображается в виде полей, сигналов, образов, количественных характеристиках физических величин.

Как правило, выделяют следующие угрозы за счет реализации технических каналов утечки:

* угрозы утечки речевой информации. Фактически злоумышленник перехватывает информацию с помощью специальной аппаратуры в виде акустических, виброакустических волн, а также электромагнитного излучения, модулированного акустическим сигналом. В качестве средств могут использоваться различного рода электронные устройства, подключаемые либо к каналам связи, либо к техническим средствам обработки ПД.
* угрозы утечки видовой информации. В этом случае речь идет о непосредственном просмотре ПД при наличии прямой видимости между средством наблюдения и носителем ПД. В качестве средств наблюдения используются оптические средства и видеозакладки;
* угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Речь идет о перехвате побочных (не связанных с прямым функциональным значением элементов ИСПД) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПД. Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПД. Наводки электромагнитных излучений возникают при излучении элементами технических средств ИСПД информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПД и различных вспомогательных устройств.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПД правила разграничения доступа к информации. Этими субъектами могут быть:

* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

Под **нарушителем** здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПД при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПД, нарушители подразделяются на два типа:

* нарушители, не имеющие доступа к ИСПД, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;
* нарушители, имеющие доступ к ИСПД, включая пользователей ИСПД, реализующие угрозы непосредственно в ИСПД, – внутренние нарушители.

Для ИСПД, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места, *терминальные устройства* ИСПД, подключенные к сетям общего пользования.

Обобщим полученные знания с помощью [рисунка 2](http://www.intuit.ru/department/security/enspdata/4/#image.4.2).

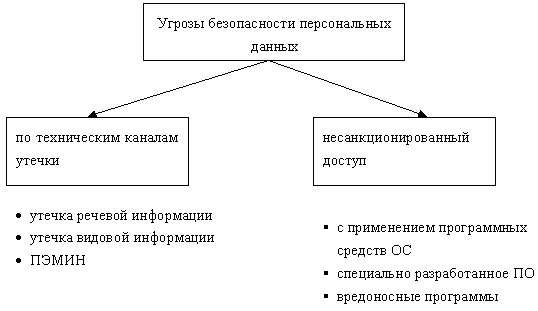


Рисунок 2. Классификация угроз безопасности персональных данных по способу реализации

Угрозы можно классифицировать по различным признакам, например, по виду нарушаемого *свойства информации* (конфиденциальность, целостность, доступность), по типу ИСПД, на которые направлена атака, по типу используемой для атаки уязвимости.

**Общая характеристика уязвимостей информационной системы персональных данных**

Появление потенциальных угроз безопасности связано с наличием слабых мест в ИСПД - уязвимостей. **Уязвимость информационной системы персональных данных** – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении ИСПД, которые могут быть использованы для реализации угрозы безопасности персональных данных.

Причинами возникновения уязвимостей в общем случае являются:

1. ошибки при разработке программного обеспечения;
2. преднамеренные изменения программного обеспечения с целью внесения уязвимостей;
3. неправильные настройки программного обеспечения;
4. несанкционированное внедрение вредоносных программ;
5. неумышленные действия пользователей;
6. сбои в работе программного и аппаратного обеспечения.

Уязвимости, как и угрозы, можно классифицировать по различным признакам:

1. по типу ПО – системное или прикладное.
2. по этапу жизненного цикла ПО, на котором возникла уязвимость – проектирование, эксплуатация и пр.
3. по причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов.
4. по характеру последствий от реализации атак – изменение прав доступа, подбор пароля, вывод из строя системы в целом и пр.

Наиболее часто используемые уязвимости относятся к протоколам сетевого взаимодействия и к операционным системам, в том числе к прикладному программному обеспечению.

Уязвимости операционной системы и прикладного ПО в частном случае могут представлять:

* функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
* фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
* отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
* ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Так, например, протокол прикладного уровня FTP, широко используемый в Интернете, производит аутентификацию на базе открытого текста, тем самым позволяя перехватывать данные учетной записи.

Прежде чем приступать к построению системы защиты информации необходимо провести *анализ уязвимостей* ИСПД и попытаться сократить их количество, то есть использовать метод превентивности. Можно закрыть лишние порты, поставить "заплатки" на программное обеспечение (например, servicepack для Windows), ввести более сильные методы аутентификации и т.п. Эти меры могут существенно сократить материальные, временные и трудовые затраты на построение системы *защиты персональных данных* в дальнейшем.

**Наиболее часто реализуемые угрозы (атаки)**

В связи с повсеместным развитием Интернета наиболее часто атаки производятся с использованием уязвимостей протоколов сетевого взаимодействия. Рассмотрим 7 наиболее распространенных атак.

1. **Анализ сетевого трафика**

Данный вид атаки направлен в первую очередь на получение пароля и идентификатора пользователя путем "прослушивания сети". Реализуется это с помощью *sniffer* – специальная программа-анализатор, которая перехватывает все пакеты, идущие по сети. И если протокол, например, FTP или TELNET, передает аутентификационную информацию в открытом виде, то злоумышленник легко получает доступ к учетной записи пользователя.

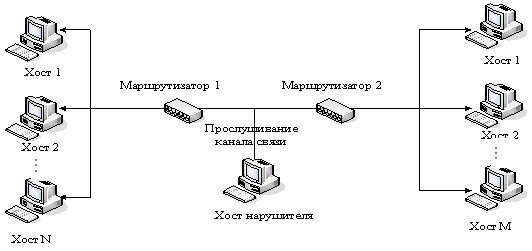


Рисунок 3. Схема реализации угрозы “Анализ сетевого трафика”

1. **Сканирование сети**

Суть данной атаки состоит в сборе информации о топологии сети, об открытых портах, используемых протоколах и т.п. Как правило, реализация данной угрозы предшествует дальнейшим действиям злоумышленника с использованием полученных в результате сканирования данных.

1. **Угроза выявления пароля**

*Целью атаки* является преодоление парольной защиты и получении НСД к чужой информации. Методов для кражи пароля очень много: простой перебор всех возможных значений пароля, перебор с помощью специальных программ (*атака словаря*), перехват пароля с помощью программы-анализатора сетевого трафика.

1. **Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.** Доверенный объект – это элемент сети, легально подключенный к серверу.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав *доверенного субъекта* взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени*доверенного субъекта*. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИСПД– цели угроз.

1. **Навязывание ложного маршрута сети**

Данная атака стала возможной из-за недостатков протоколов маршрутизации (RIP, OSPF, *LSP*) и управления сетью (ICMP, SNMP), таких как слабая аутентификация маршрутизаторов. Суть атаки состоит в том, что злоумышленник, используя уязвимости протоколов, вносит несанкционированные изменения в маршрутно-адресные таблицы.

1. **Внедрение ложного объекта сети**

Когда изначально объекты сети не знают информацию друг о друге, то для построения адресных таблиц и последующего взаимодействия, используется *механизм запрос* (как правило, широковещательный) - ответ с искомой информацией. При этом если нарушитель перехватил такой запрос, то он может выдать ложный ответ, изменить таблицу маршрутизации всей сети, и выдать себя залегального субъекта сети. В дальнейшем все пакеты, направленные к легальному субъекту, будут проходить через злоумышленника.

1. **Отказ в обслуживании**

Этот тип атак является одним из самых распространенных в настоящее время. Целью такой атаки является отказ в обслуживании, то есть нарушение доступности информации для законных субъектов информационного обмена.

Могут быть выделены несколько разновидностей таких угроз:

* скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПД на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросовпо*протоколу ICMP* (Ping *flooding*), шторм запросов на установление TCP-соединений (SYN-*flooding*), шторм запросов к FTP-серверу;
* явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение *очередей запросов* на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения *очередей запросов*, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-*flooding*), шторм сообщений почтовому серверу (*Spam*);
* явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP RedirectHost, DNS-*flooding*) или идентификационной и аутентификационной информации;
* явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "*Nuke*", "UDP-*bomb*") или имеющих длину, превышающую максимально допустимый размер (угроза типа "PingDeath"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПД в ИСПД, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПД, какое максимально может "вместить" трафик (направленный "шторм запросов"), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Мы рассмотрели наиболее часто реализуемые угрозы при сетевом взаимодействии. На практике угроз значительно больше. Частная модель угроз безопасности строится на основе двух документов ФСТЭК – "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" и "Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПД". Если организация большая, и в ней несколько систем ИСПД, наиболее разумным решением будет привлечение квалифицированных специалистов сторонних фирм для построения частной модели угроз и проектирования СЗПД.

1. **Порядок выполнения**
2. Изучить существующие угрозы информационной безопасности
3. Изучить уязвимости систем информационной безопасности.
4. Привести примеры.
5. Оформить отчет.
6. **Контрольные вопросы**
7. Что такое угроза?
8. Что такое уязвимость?
9. Какие угрозы наиболее часто реализуются?
10. **Содержание отчета**
11. Основные определения
12. Перечень наиболее часто реализуемых угроз (атак)
13. Перечень угроз за счет реализации технических каналов утечки:
14. Причины возникновения уязвимостей
15. Примеры угроз и уязвимостей.

Практическая работа № 6.

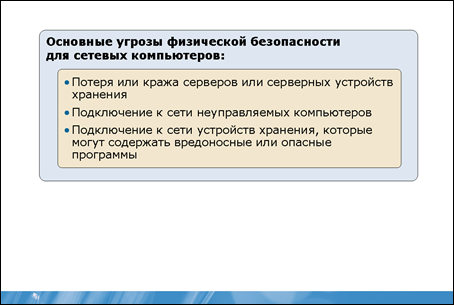
«Обеспечение физической безопасности»

**Цель работы.** Научиться определять и разграничивать обязанности пользователей за ОИБ.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

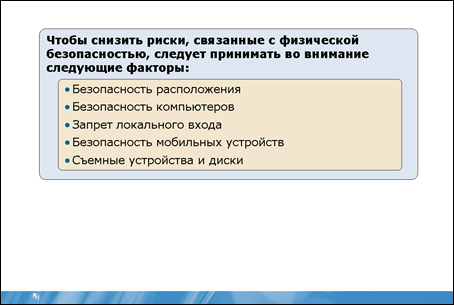
1. Общие положения



Помимо физического повреждения неправильно размещенных серверов и потери данных, существуют следующие основные угрозы физической безопасности компьютеров, подключенных к сети:

* несанкционированный доступ к данным из-за потери или кражи серверов или серверных устройства хранения;
* несанкционированный доступ к данным из-за подключения к вашей сети неуправляемых компьютеров;
* несанкционированный доступ к данным из-за использования в сети устройств хранения, которые могут содержать вредоносные или опасные программы.

**Рекомендации по физической безопасности**



Чтобы снизить риски, связанные с физической безопасностью, следует принимать во внимание следующие факторы:

* безопасность расположения. Если этого по возможности давайте доступ к месту, где физически располагаются компьютеры, только авторизованным лицам. Это сложнее сделать в филиалах и на некоторых коммерческих рынках, например, в розничных магазинах;
* безопасность компьютеров. Убедитесь, что серверы или компьютеры, содержащие важные данные или имеющие доступ к ним, физически находятся в безопасности. Лучше всего размещать серверы и устройства хранения в компьютерных комнатах с физическими механизмами защиты, например, с кодовыми замками. В средах, требующих высокого уровня безопасности, лучше реализовать средства биометрического контроля, чтобы только авторизованные лица могли получить физический доступ к компьютерам;
* запрет локального входа. Возможность в интерактивном режиме войти в систему на компьютере - право, которое обычно есть у всех пользователей для всех компьютеров в лесу, за исключением контроллеров домена. Возможно, стоит дополнительно ограничить право локального входа, если требуется значительный уровень безопасности. Если пользователь не может войти в систему, ему труднее выполнять действия в сети;
* безопасность мобильных устройств. Мобильные устройства, например, ноутбуки и мобильные телефоны, позволяют пользователям получать доступ к корпоративной сети из любого места. Однако это создает опасность при потере или краже таких устройств. Убедитесь, что на мобильных устройствах реализованы средства обеспечения безопасности, чтобы в случае потери устройства данные не оказались раскрыты. На таких мобильных устройствах, как телефоны с Windows Mobile, можно реализовать технологии удаленной очистки. На ноутбуках можно применять шифрованную файловую систему (EFS) и шифрование дисков BitLocker;
* съемные устройства и диски. Внимательно продумайте, стоит ли подвергать систему опасности ради удобства пользователей, которые копируют файлы на съемные устройства хранения. Если принято решение, что можно пользоваться съемными устройства хранения, рассмотрите возможность применения на таких устройствах средства BitLocker-to-Go™. Оно позволяет шифровать данные на устройстве.

1. **Порядок выполнения**
2. Изучить элементы организации физической безопасности информации на стационарных элементах ИС.
3. Изучить элементы организации физической безопасности информации на мобильных элементах ИС.
4. Привести примеры.
5. Оформить отчет.
6. **Контрольные вопросы**
7. Что такое физическая безопасность?
8. Привести примеры организации физической безопасности на предприятии?
9. Как реализуется защита мобильных устройств?
10. **Содержание отчета**
11. Основные определения
12. Перечень угроз физической безопасности информации.
13. Перечень факторов, которые надо знать, чтобы снизить риски, связанные с физической безопасностью
14. Примеры нарушений физической безопасности.

Практическая работа № 7.

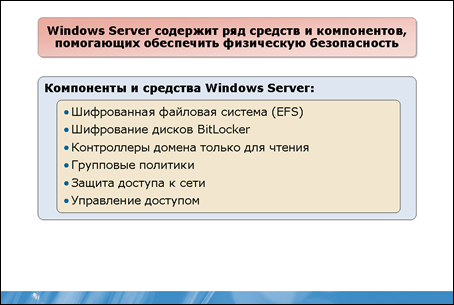
«Реализация физической безопасности с помощью средств Windows Server»

**Цель работы.** Научиться основам реализации физической безопасности.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения



Windows Server содержит ряд средств и компонентов, помогающих обеспечить физическую безопасность.

Шифрованная файловая система (EFS)

EFS - это встроенное средство шифрования файлов для файловых систем Windows. EFS является компонентом файловой системы NTFS; это средство обеспечивает прозрачные шифрование и расшифровку файлов с использованием улучшенных стандартных алгоритмов шифрования. Чтение зашифрованных данных доступно только пользователям и программам, которые обладают соответствующим ключом шифрования. Зашифрованные файлы можно защитить даже от тех лиц, которые имеют физический доступ к компьютеру, на котором эти файлы расположены. Даже лица, которые в других случаях авторизованы для доступа к компьютеру и его файловой системе, не могут просматривать данные.

Шифрование дисков BitLocker

BitLocker защищает операционную систему компьютера и данные, хранящиеся на томе операционной системы, обеспечивая шифрование данных на компьютере, даже если проникновение на компьютер происходит, когда операционная система не работает. BitLocker предоставляет решение, тесно интегрированное с ОС Windows Server 2008 R2 и Windows 7, предназначенное для устранения угроз кражи или раскрытия данных, возникающих в результате потери, кражи или неправильного вывода компьютеров из эксплуатации.

Контроллеры домена только для чтения (RODC)

Контроллер домена только для чтения - это новый тип контроллера домена в Windows Server 2008 R2. С помощью контроллера домена только для чтения можно легко развернуть контроллер домена в местах, где невозможно гарантировать физическую безопасность, например в филиале. В контроллере домена только для чтения размещается реплика базы данных только для чтения в доменных службах Active Directory для данного домена.

Когда контроллер домена только для чтения обслуживает запрос входа в систему пользователя из вашей сети, учетные данные этого пользователя кэшируются на сервере. Таким образом кэшируются только учетные записи пользователей из филиала. Если контроллер домена только для чтения украден, раскрытой оказывается только часть учетных записей домена, поэтому восстановить безопасность учетных записей пользователей будет проще и быстрее.

|  |
| --- |
| **Примечание.** По умолчанию на контроллере домена только для чтения не кэшируются учетные записи пользователей. Этот способ является более безопасным, так как даже в случае кражи контроллера домена только для чтения пароли пользователей не раскрываются. Однако если происходит сбой связи между головным офисом, где находятся контроллеры домена, доступные для записи, и филиалом, то при выключенном кэшировании пользователи филиала не могут войти в систему до восстановления связи. |

Групповые политики

Если пользователям разрешено подключать к соединенным с сетью компьютерам устройства хранения, например USB-накопители или внешние жесткие диски, это может создать дополнительные угрозы безопасности. Windows Server может использовать объекты групповой политики, чтобы устанавливать на соединенных с сетью компьютерах правила, контролирующие или запрещающие подключение устройств хранения.

Защита доступа к сети

Если компьютеры могут подключаться к сети из неуправляемых расположений, например из домов пользователей, или если к сети могут подключаться компьютеры других организаций, возникает угроза безопасности.

Сеть защищена не более, чем самый незащищенный подключенный к ней компьютер. Есть множество программ и средств, помогающих защитить компьютеры, подключенные к сети, например антивирусное или обнаруживающее вредоносные программы программное обеспечение. Однако если программное обеспечение на некоторых компьютерах устарело или, хуже того, выключено или неправильно настроено, эти компьютеры представляют угрозу безопасности.

На компьютерах, постоянно находящихся в офисе и всегда подключенных к одной сети, относительно легко поддерживать конфигурации и обновления. Компьютеры, которые подключаются к различным сетям, особенно к неуправляемым, труднее контролировать. Пример - ноутбуки, которые подключаются к сетям клиентов или открытым точкам беспроводного доступа (Wi-Fi). Дополнительные трудности возникают с неуправляемыми компьютерами, которым требуется удаленное подключение к сети, например домашними компьютерами пользователей.

Защита доступа к сети (NAP) - это платформа установки политик, встроенная в операционные системы Windows 7, Windows Vista®, Windows XP с пакетом обновления 3 (SP3), Windows Server 2008 и Windows Server 2008 R2. Защита доступа к сети позволяет надежнее защищать компоненты сети, обеспечивая соответствие требованиям по работоспособности системы.

Защита доступа к сети обеспечивает необходимые программные компоненты, помогающие сохранить управляемость подключенных или подключающихся к сети компьютеров, чтобы они не создавали угрозы безопасности сети и других подключенных к ней компьютеров. Это позволяет более безопасно разрешать подключение компьютеров к сети.

Управление доступом

После подключения компьютеров к сети у них появляется доступ к данным серверов. Целостность данных можно защитить, настроив соответствующие разрешения доступа к файлам. Убедитесь, что разрешения предоставляются, только когда это нужно, и что это минимальные достаточные разрешения. Это особенно важно, если к сети подключаются пользователи не из данной организации.

Задание

Проблемы безопасности связаны с тем фактом, что многие филиалы невозможно защитить физически. Заполнив запись об инциденте, предложите лучший способ разобраться с описанными в компании «Метель» проблемами физической безопасности.

Необходимо выполнить следующие основные задачи.

1. Прочтите сопроводительную документацию.
2. Заполните запись об инциденте.

**Сопроводительная документация**

**«**Политики безопасности сети «Метель». Ноутбуки**»**

Этот документ определяет корпоративные политики компании «Метель», связанные с ноутбуками и другими портативными вычислительными устройствами.

**Политики**

1. Любое сетевое устройство, которое выносят из офиса «Метель», должно быть настроено так, чтобы потеря устройства не привела к несанкционированному доступу к хранящимся на нем данным.

2. Ноутбуки можно подключать к другим сетям при соблюдении следующих условий.

а. Установлен подходящий брандмауэр.

б. На компьютер установлены последние обновления безопасности.

в. Установлена защита от вирусов и вредоносных программ.

3. На ноутбуках разрешается использовать портативные устройства хранения, если их потеря не может привести к несанкционированному доступу к хранящимся на них данным.

Реально существующее положение дел в компании «Метель».

* Исследователи пользуются ноутбуками и часто уносят их домой.
* В некоторых филиалах нет выделенных помещений для серверов.
* Внешние сотрудники, работающие по контракту, могут подключать свои компьютеры к сети исследовательского отдела.
* Персонал использует личные USB запоминающие устройства на рабочих компьютерах.

|  |
| --- |
|  |
| **Вопросы**  Заполните раздел "Решение" сводкой своих предложений. |

1. **Порядок выполнения**
2. Прочтите документацию и запись об инциденте с целью определить причины проблемы.
3. Прочтите **политики безопасности компании «Метель», раздел "Ноутбуки"**, чтобы определить, должны ли вы обеспечить какие-то изменения в филиале в соответствии с корпоративными политиками.
4. Опишите способы решения проблем.
5. **Контрольные вопросы**
6. Какие политики безопасности применяются к ноутбукам в филиалах в соответствии с разделом "Ноутбуки" документа "Политики безопасности сети Contoso"?
7. Какие проблемы безопасности вы видите в филиалах?
8. Как вы решите проблемы, касающиеся использования ноутбуков?
9. Как вы решите проблему отсутствия достаточного количества выделенных помещений для серверов?
10. Как вы решите проблемы, касающиеся использования компьютеров контрактных сотрудников?
11. Как вы решите проблемы, касающиеся съемных носителей?
12. **Содержание отчета**
13. Перечислите проблемы в организации
14. Перечислите нарушения групповой политики безопасности (раздел «Ноутбуки»)
15. Предложите способы решения данных проблем

Практическая работа № 8.

«Определение модели управления доступом»

**Цель работы**. Получение практических навыков определения модели управления доступом.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

**Основные положения моделей доступа.**

Цель управления доступом – это ограничение операций, которые может проводить легитимный пользователь (зарегистрировавшийся в системе). Управление доступом указывает, что конкретно пользователь имеет право делать в системе, а так же какие операции разрешены для выполнения приложениями, выступающими от имени пользователя.

Таким образом, управление доступом предназначено для предотвращения действий пользователя, которые могут нанести вред системе, например, нарушить безопасность системы.

Используемые термины

|  |  |
| --- | --- |
| Доступ | Доступ субъекта к объекту для определенных операций. |
| Объект | Контейнер информации в системе |
| Субъект | Сущность, определяющая пользователя при работе в системе |
| Пользователь | Человек, выполняющий действия в системе или приложение выступающее от его имени. |

Методы управления доступом

**Общее описание**

Управление доступом – это определение возможности субъекта оперировать над объектом в общем виде описывается следующей диаграммой:

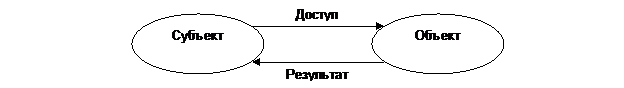


Рисунок 1. Управление доступом

На данный момент существует три различных метода для управления доступом к объектам в системе:

* Дискреционный метод контроля доступа
* Обязательный метод контроля доступа
* Ролевой метод контроля доступа.

Заранее отметим, что эти методы не обязательно применяются отдельно друг от друга, а могут комбинироваться для удовлетворения различных требований к безопасности системы (рисунок 2).

При этом комбинирование различных моделей может быть довольно простым, если они не противоречат друг другу. Т.е. если не существует ситуаций, когда исходя из одной модели, субъект имеет доступ к объекту, а из другой не имеет. Эти конфликты должны разрешаться на уровне администрирования системы.

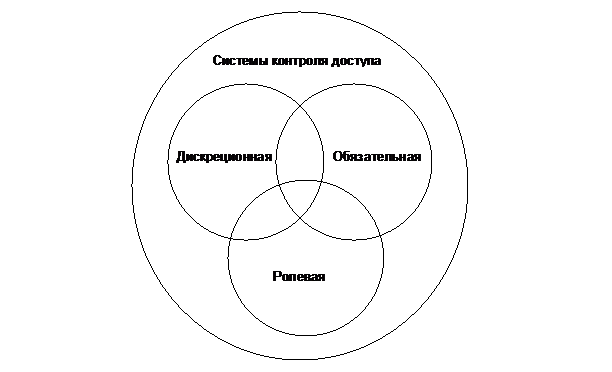


Рисунок 2: Системы контроля доступа

**Модель дискреционного контроля за доступом**

Средства Дискреционного Контроля за Доступом (DiscretionaryAccessControl - DAC) обеспечивают защиту персональных объектов в системе. Контроль является дискреционным в том смысле, что владелец объекта сам определяет тех, кто имеет доступ к объекту, а также вид их доступа.

Дискреционный контроль доступа управляет доступом субъектов к объектам, базируясь на идентификационной информации субъекта и списка доступа объекта, содержащего набор субъектов (или групп субъектов) и ассоциированных с ними типов доступа (например, чтение, запись). При запросе доступа к объекту, система ищет субъекта в списке прав доступа объекта и разрешает доступ, если субъект присутствует в списке и разрешенный тип доступа включает требуемый тип. Иначе доступ не предоставляется.

Гибкость DAC позволяет использовать его в большом количестве систем и приложений. Благодаря этому этот метод очень распространен, особенно в коммерческих приложениях. Очевидным примером использования DAC является система Windows NT/2k/XP (Рисунок 3).

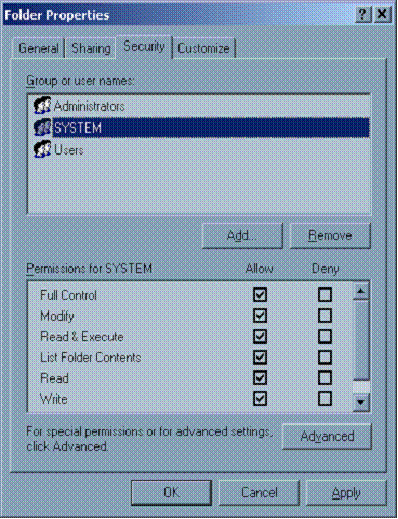


Рисунок 3. Дискреционная модель контроля доступа Windows XP.

Однако DAC имеет существенный недостаток. Он заключается в том, что он не предоставляет полной гарантии того, что информация не станет доступна субъектам, не имеющим к ней доступа. Это проявляется в том, что субъект имеющий право на чтение информации может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта. Система DAC не устанавливает никаких ограничений на распространение информации после того как субъект ее получил.

Еще одной особенностью DAC, которую можно отнести к недостаткам, является то, что все объекты в системе принадлежат субъектам, которые настраивают доступ к ним для других. На практике оказывается, что в большинстве случаев данные в системе принадлежат не отдельным субъектам, а всей системе. Наиболее распространенным примером такой системы является информационная система.

Классическая система дискреционного контроля доступа называется "закрытой" в том смысле, что изначально объект не доступен никому, и в списке прав доступа описывается список разрешений. Также существуют "открытые" системы, в которых по умолчанию все имеют полный доступ к объектам, а в списке доступа описывается список ограничений.

**Модель обязательного контроля за доступом**

Средства Обязательного Контроля за Доступом (MandatoryAccessControl - MAC). Контроль является обязательным в том смысле, что пользователи не могут изменять стратегию MAC в отношении объектов. При создании объекта система автоматически присваивает ему атрибуты MAC, и изменить эти атрибуты может только администратор, имеющий соответствующие полномочия. Средства MAC не позволят пользователю случайно или преднамеренно сделать информацию доступной для лиц, которые не должны обладать ею.

Обязательный контроль доступа управляет доступом на основе классификации объектов и субъектов системы. Каждому субъекту и объекту системы назначается некоторый уровень безопасности (УБ). Уровень безопасности объекта, как правило, описывает важность этого объекта и возможный ущерб, который может быть причинен при разглашении информации содержащейся в объекте. Уровень безопасности субъекта является уровнем доверия к нему. В простейшем случае все уровни безопасности являются членами некоторой иерархии. Например: Совершенно Секретно (СС), Секретно (С), Конфиденциально (К) и Рассекречено (Р), при этом верно следующее: СС > C > K > P, т.е. каждый уровень включает сам себя и все уровни находящиеся ниже в иерархии.

**Обеспечение безопасности информации**

Доступ субъекта к объекту предоставляется, если выполнено некоторое условие отношения (которое зависит от типа доступа) между уровнями безопасности объекта и субъекта. В частности, должны выполняться следующие условия:

* Доступ на чтение дается если УБ субъекта включает в себя УБ объекта.
* Доступ на запись дается если УБ субъекта включается в УБ объекта.

Выполнение этих условий, гарантирует, что данные высокоуровневых объектов (например Совершенно Секретно) не попадут в низкоуровневые объекта (например Рассекреченный) (рисунок 4).

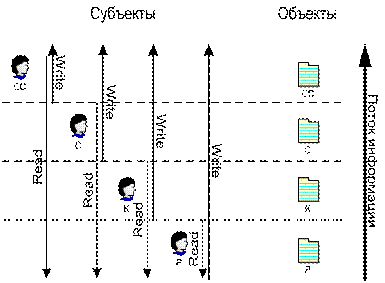


Рисунок 4: Управление потоками информации для обеспечения безопасности данных

В этой модели важно различать понятия пользователь и субъект. Уровни безопасности назначаются субъектам, а пользователи могут выступать от имени субъекта в тот или иной момент. При этом в различных ситуациях один пользователь может выступать от имени различных субъектов. При этом важно, чтобы в каждый конкретный момент, пользователь выступал от имени только одного субъекта. Это обеспечивает невозможность передачи информации от высокого уровня к более низкому.

В описанной выше модели существует два неочевидных момента, которые ставят под вопрос непротиворечивость модели.

1. Пользователь нижнего уровня имеет право записывать в объекты всех верхних уровней. Таким образом, он может переписать существующий объект своим собственным, что равносильно удалению. Этот недостаток может быть устранен путем запрета записи на более верхние уровни. При такой схеме правила будут выглядеть так:

* Доступ на чтение дается если УБ субъекта включает в себя УБ объекта.
* Доступ на запись дается если УБ субъекта равняется УБ объекта.

2. Из диаграммы видно, что пользователи с более высоким уровнем доверия не могут изменять объекты с более низким уровнем безопасности. Эта проблема разрешается тем, что пользователь при доступе к различным документам может выступать от имени субъектов с различными уровнями доверия. Т.е. пользователь с уровнем доверия «С» может выступать от имени субъектов с уровнем доверия «С», «К» и «Р».

**Обеспечение достоверности информации**

Кроме обеспечения безопасности информации, часто требуется обеспечение ее достоверности. Т.е. чем выше уровень доверия объекта, тем выше его достоверность, и чем выше уровень безопасности субъекта, тем более достоверную информацию он может вносить в систему. Для такой модели, описанные выше правила следует видоизменить следующим образом:

* Доступ на запись дается если УБ субъекта включает в себя УБ объекта.
* Доступ на чтение дается если УБ субъекта включается в УБ объекта.

Видно, что критерии правил просто поменялись местами.

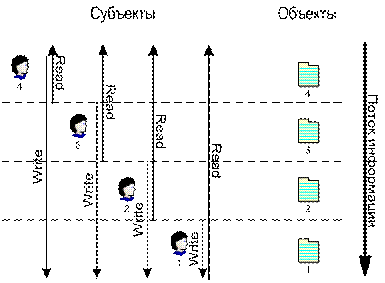


Диаграмма 4: Управление потоками информации для обеспечения надежности данных.

Наряду с использованием уровней безопасности, в модели обязательного контроля за доступом можно использовать категории. В таком случае каждому объекту и субъекту, кроме уровня безопасности можно назначить список категорий, к которым он (субъект или объект) относится. Категории объекта используются для описания областей, где этот объект используется, а категории субъекта описывают в каких областях субъект работает. Такая система позволяет более детально управлять доступом в системе.

**1.2.4 Ролевая модель контроля за доступом**

Основная идея ролевой модели контроля за доступом (Role-BasedAccessControl - RBAC) основана на максимальном приближении логики работы системы к реальному разделению функций персонала в организации.

Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе. Применение данного метода подразумевает определение ролей в системе. Понятие роль можно определить как совокупность действий и обязанностей, связанных с определенным видом деятельности. Таким образом, вместо того, чтобы указывать все типы доступа для каждого пользователя к каждому объекту, достаточно указать тип доступа к объектам для роли. А пользователям, в свою очередь, указать их роли. Пользователь, "выполняющий" роль, имеет доступ определенный для роли.

Пользователь может выполнять различные роли в разных ситуациях. Одна и та же роль может использоваться несколькими различными пользователями, причем иногда даже одновременно. В некоторых системах пользователю разрешается выполнять несколько ролей одновременно, в других есть ограничение на одну или несколько не противоречащих друг другу ролей в каждый момент времени.

Основными достоинствами ролевой модели управления доступом являются:

**Простота администрирования**

В классических моделях разграничения доступа, права на выполнение определенных операций над объектом прописываются для каждого пользователя или группы пользователей. В ролевой модели разделение понятий роль и пользователь позволяет разбить задачу на две части: определение роли пользователя и определение прав доступа к объекту для роли. Такой подход сильно упрощает процесс администрирования, поскольку при изменении области ответственности пользователя, достаточно убрать у него старые роли и назначить другие соответствующие его новым обязанностям. В случае, когда права доступа определяются напрямую между пользователями и объектами, эта же процедура потребует массу усилия по переназначению новых прав пользователя.

**Иерархия ролей**

Систему ролей можно настроить таким образом, чтобы она намного ближе отражала реальные бизнес процессы посредством построения иерархии ролей. Каждая роль наряду со своими собственными привилегиями может наследовать привилегии других ролей. Такой подход также существенно упрощает администрирование системы.

**Принцип наименьшей привилегии**

Ролевая модель позволяет пользователю регистрироваться в системе с наименьшей ролью, позволяющей ему выполнять требуемые задачи. Пользователям, имеющим множество ролей, не всегда требуются все их привилегии для выполнения конкретной задачи

Принцип наименьшей привилегии очень важен для обеспечения достоверности данных в системе. Он требует, чтобы пользователь давали только те из разрешенных ему привилегий, которые ему нужны для выполнения конкретной задачи. Для этого требуется выяснить цели задачи, набор привилегий требуемых для ее выполнения и ограничить привилегии пользователя этим набором. Запрещение привилегий пользователя не требуемых для выполнения текущей задачи позволяет избежать возможности обойти политику безопасности системы.

**Разделение обязанностей**

Еще одним важным принципом в системе управления доступом является разделение обязанностей. Довольно распространены ситуации, в которых ряд определенных действий не может выполняться одним человеком во избежание мошенничеств. Примером этому могут служить операции по созданию платежа и его подтверждению. Очевидно, что эти операции не могут выполняться одним и тем же человеком. Система ролевого управления доступом помогает решить эту задачу с максимальной простотой.

Формально ролевую модель управления доступом можно изобразить следующим образом:

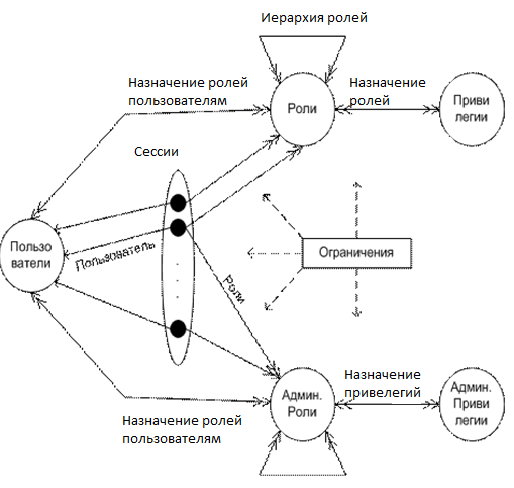


Диаграмма 5: Ролевая модель управления доступом.

Модель состоит из следующих сущностей: пользователи, роли и привилегии. Интуитивно понятно, что пользователь это либо человек, либо программа, работающая от имени пользователя. Роль это вид деятельности пользователя в организации, а привилегия это разрешение на определенный доступ к одному или нескольким объектам системы.

Из диаграммы видно, что связи "Назначение ролей пользователям" и "Назначение привилегий" принадлежат типу много-в-много. Пользователь может иметь несколько ролей и несколько пользователей могут принадлежать одной роли. Аналогично несколько привилегий могут принадлежать одной роли и несколько ролей могут иметь одну и ту же привилегию. Также в этой модели присутствует частично упорядоченное множество - иерархия ролей. На этом множестве задано отношение принадлежности где для ролей x и y, x > y означает что роль x наследует привилегии роли y. Это отношение транзитивно.

Сессия относит пользователя к множеству ролей. Интуитивно понятно, что пользователь активизирует сессию для выполнения некоторой задачи. В этот момент система может определить те роли и привилегии, которые требуются пользователю для выполнения задачи и запретить остальные.

1. 3 Анализ существующих моделей

**Области применения**

Сразу оговоримся, что нельзя сказать какая из существующих моделей лучше или хуже. Каждая из описанных моделей служит для выполнения определенных задач и выбор одной или нескольких моделей обуславливается спецификой области применения.

Различные организации имеют свои специфичные требования к политике безопасности. Система дискреционного управления доступом подразумевает, что все ресурсы системы принадлежат пользователям системы, а значит следить за доступом к ресурсу должен его владелец, т.е. пользователь. Такие системы в основном рассчитаны на небольшое количество пользователей. При росте числа пользователей, количество работ по администрированию системы возрастает многократно.

Для организаций, в которых требуется четкая централизованная система управления доступа, при которой каждый пользователь имеет ровно столько информации, сколько ему требуется, и безопасность или надежность данных является основным приоритетом, уместно использовать систему обязательного контроля за доступом. Обычно это большие организации, где функции всех ее членов строго регламентированы. К ним в основном относятся военные институты.

Также довольно часто требуется совместить гибкость настройки с централизованным управлением. Тогда использование комбинации обязательного и дискреционного контроля за доступом представляется вполне целесообразным. Такая комбинация позволяет централизованно ограничить доступ к наиболее критичным ресурсам на самом верхнем уровне, и в то же время позволить пользователям управлять доступом к менее важным данным.

Системы с ролевым управлением доступом целесообразно использовать в больших организациях, со сложной иерархией и большим количеством разделяемых операций. В такой системе данные обычно принадлежат не пользователю а системе. И управление доступом к ресурсам основывается не на принадлежности ресурса, а на функциях пользователя в организации. Вообще говоря, ролевой метод управления доступом является модификацией модели обязательного, но он не основан на многоуровневой системе требований к безопасности. Также важно понимать, что RBAC больше связан с управлением доступом к операциям над объектами, а не к самим объектам.

**Фундаментальное различие**

Модель дискреционного контроля за доступом и модель обязательного контроля за доступом имеют одно фундаментальное отличие от ролевой модели. Оно заключается в том, что первые две модели заранее определяют политику безопасности системы и позволяют ее настраивать для каждой конкретной ситуации. В тоже время ролевая модель ни в коей мере не предопределяет политику безопасности, а позволяет ее настроить в том виде в каком это требуется организации. Таким образом, настройка системы безопасности системы на основе ролевой модели контроля за доступом производится в две стадии.

1. Настройка политики безопасности системы.

2. Определение прав доступа для субъектов и объектов в системе.

В то время как для первых двух моделей политика безопасности системы уже предопределена.

Такое различие позволяет создавать дискреционную модель и модель обязательного контроля на основе ролевой модели. Далее мы приведем метод настройки ролевой модели под модели обязательного и дискреционного контроля за доступом.

1. Порядок выполнения работы

Задание 1 Выполните задания.

Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).

Установите для этой папки разрешения полного доступа для одного из пользователейгруппы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.

Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.

Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

Составьте отчет о проведенных экспериментах.

Задание 2 Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

1. Контрольные вопросы
2. Где можно использовать ролевую модель управления доступом?
3. Где можно использовать дискреционную модель управления доступом?
4. Где можно использовать обязательную модель управления доступом?
5. Какая модель применяется в колледже?
6. Можно ли использовать модели вместе?
7. Что такое список управления доступом ACL?
8. Как реализуется дискреционная модель доступа в ОС Windows?
9. Содержание отчета
10. Модели управления доступом.
11. Основные термины.
12. Области применения моделей.
13. Алгоритмы работы моделей управления доступом.
14. Модель управления доступом в колледже.
15. Выполнение заданий

**Практическая работа № 9**

**Уничтожение остаточной информации**

**Цель работы.** Научиться работать с механизмами уничтожения остаточной информации.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.
  1. **Общие положения**

Остаточная информация – информация на запоминающем устройстве, оставшаяся от формально удалённых операционной системой данных. Информация может остаться из-за формального удаления файла или из-за физических свойств запоминающих устройств. Остаточная информация может привести к непреднамеренному распространению конфиденциальной информации, если хранилище данных окажется вне зоны контроля (например, будет выкинуто с мусором или передано третьей стороне).

В настоящее время во избежание появления остаточной информации применяется множество методов. В зависимости от эффективности и назначения они подразделяются на очистку и уничтожение. Конкретные методики используют перезаписывание, размагничивание, шифрование и физическое уничтожение.

**Причины появления**

Многие ОС, файловые менеджеры и другое ПО предоставляют возможность не удалять файл немедленно, а перемещать файл в корзину, чтобы позволить пользователю легко исправить свою ошибку.

Но даже если возможность обратимого удаления явно не реализована или пользователь не применяет её, большинство операционных систем, удаляя файл, не удаляют содержимое файла непосредственно, просто потому, что это требует меньше операций и, чаще всего, быстрее. Вместо этого они просто удаляют запись о файле из директории файловой системы. Содержимое файла — реальные данные — остается на запоминающем устройстве. Данные существуют до тех пор, пока ОС не использует заново это пространство для новых данных. Во множестве систем, остается достаточно системных метаданных для несложного восстановления при помощи широко доступных утилит. Даже если восстановление невозможно, данные, если не были перезаписаны, могут быть прочитаны ПО, читающим сектора диска напрямую. Программно-техническая экспертиза часто применяет подобное ПО.

Также, при форматировании, переразбиении на разделы или восстановлении образа системой не гарантируется запись по всей поверхности, хотя диск и выглядит пустым или, в случае восстановлении образа, на нем видны только файлы, сохранённые в образе.

Наконец, даже если запоминающее устройство перезаписывается, физические особенности устройств делают возможным восстановление информации при помощи лабораторного оборудования благодаря, например, явлению остаточной намагниченности.

**Контрмеры**

Очистка — удаление конфиденциальной информации с записывающих устройств таким образом, что гарантируется, что данные не могут быть восстановлены с помощью обычных системных функций или утилит для восстановления файлов. Данные могут оставаться доступными для восстановления, но не без специальных лабораторных методов.

Очистка, обычно, административная защита от непреднамеренного распространения данных внутри организации. Например, перед повторным использованием дискеты внутри организации, ее содержимое может быть очищено для предотвращения непреднамеренного распространения информации следующему пользователю.

Уничтожение

Уничтожение — удаление конфиденциальной информации с записывающего устройства так, чтобы данные не могли быть восстановлены никаким известным способом. Удаление, в зависимости от конфиденциальности данных, обычно совершается перед выходом устройства из-под надзора, как например, перед списанием оборудования или перемещением его на компьютер с другими требованиями по безопасности данных.

**Методики**

Перезаписывание

Распространенная методика для предотвращения остаточной информации — перезаписывание устройства новыми данными. Из-за того, что такие методики могут быть реализованы целиком на программной стороне и могут быть использованы на отдельной части запоминающего устройства, это популярная и недорогая опция для многих приложений. Перезаписывание вполне подходящий метод очистки, если устройство доступно на запись и не повреждено.

Простейшая реализация записывает повсюду одни и те же последовательности: чаще всего — серии нулей. Как минимум, так предотвращается получение данных с устройства посредством обычных системных функций.

Для противостояния более сложным методам восстановления, часто предустановлены конкретные шаблоны перезаписи. Это могут быть и обобщённые шаблоны, предназначенные устранения отслеживаемых следов. Например, повторяющаяся запись перемежающихся шаблонов из единиц и нулей может быть более эффективной, чем запись одних нулей. Часто задаются сочетания шаблонов.

Проблема с перезаписыванием в том, что некоторые части диска могут быть недоступны из-за износа оборудования или других проблем. Программная перезапись также может быть проблематичной в высокозащищённых средах, со строгим контролем за смешиванием данных, обеспечиваемым программным обеспечением. Использование сложных технологий хранения также может сделать перезапись файлов неэффективной.

**Осуществимость восстановления перезаписанных данных**

Питер Гутманн изучал в середине 1990-х восстановление данных с формально перезаписанных устройств. Он предположил, что магнитный микроскоп способен извлечь данные и разработал особые последовательности для конкретных видов дисков, предназначенных для предотвращения этого. Эти последовательности известны как метод Гутмана.

Дэниел Финберг, экономист частной организации National Bureau of Economic Research, заявил, что любая возможность восстановить перезаписанные данные с современного жёсткого диска является «городской легендой».

В ноябре 2007, Министерство Обороны США признала перезапись подходящей для очистки магнитных устройств, но не подходящей для уничтожения данных. Только размагничивание или физическое уничтожение считается подходящим.

С другой стороны, согласно «Special Publication 800-88» (2006 г.) Национального института стандартов и технологий (США) (p. 7): «Исследования показали, что большинство современных устройств может быть очищено за одну перезапись» и «для жестких дисков ATA произведённых после 2001 г. (свыше 15 GB) термины очистка и уничтожение совпадают».

**Размагничивание**

Размагничивание — удаление или ослабление магнитного поля. Применённое к магнитному носителю, размагничивание может уничтожить все данные быстро и эффективно. Используется прибор, называемый размагничиватель, предназначенный для уничтожения данных.

Размагничивание обычно выводит жёсткий диск из строя, так как уничтожает низкуровневое форматирование, производимое во время изготовления. Размагниченные дискеты, обычно, могут быть переформатированы и использованы заново.

В высокозащищённых средах исполнитель может быть обязан использовать сертифицированный размагничиватель. Например, в правительстве и оборонных ведомствах США может быть предписано использовать размагничиватель из списка «Списка допущенных приборов» Агентства национальной безопасности .

Шифрование

Шифрование данных перед записью может ослабить угрозу остаточной информации. Если шифровальный ключ надёжен и правильно контролируется (то есть, сам не является объектом остаточной информации), то все данные на устройстве могут оказаться неизвлекаемыми. Даже если ключ хранится на жёстком диске, перезаписывание только ключа может оказаться проще и быстрее, чем всего диска.

Шифрование может производиться пофайлово или сразу всего диска. Тем не менее, если ключ хранится, даже временно, на той же системе, что и данные, он может быть объектом остаточной информации и может быть прочитан злоумышленником. См. атака через холодную перезагрузку.

Физическое уничтожение

Физическое уничтожение хранилища данных считается самым надежным способом предотвращения появления остаточной информации, хотя и за самую высокую цену. Не только сам процесс занимает время и обременителен, он также делает оборудование неработоспособным. Более того, при современных высоких плотностях записи, даже небольшой фрагмент устройства может содержать большой объем данных.

Отдельные методики физического уничтожения включают:

Физическое разрушение устройства на части путём размалывания, измельчения и т. д.

Сожжение

Фазовый переход (то есть растворение или возгонка целого диска)

Применение коррозийных реагентов, таких как кислоты, к записывающим поверхностям

Для магнитных устройств, нагрев выше точки Кюри

**Проблемы**

Недоступные области устройств

В запоминающих устройствах могут быть области, ставшие недоступными для обычных средств. Например, магнитные диски могут разметить новые «bad»-сектора, после того как данные были записаны, а кассеты требуют промежутков между записями. Современные жёсткие диски часто производят автоматические перемещения незначительных секторов записей, о которых может даже не знать ОС. Попытки предотвратить остаточную информацию посредством перезаписывания могут провалиться, так как остатки данных могут присутствовать в формально недоступных областях.

Сложные системы хранения

Запоминающие устройства, применяющие различные изощрённые методы, могут привести к неэффективности перезаписывания, особенно для применения к отдельным файлам.

Журналируемые файловые системы увеличивают связность данных, выполняя запись, дублируя информацию, и применяют семантику транзакций. В таких системах остатки данных могут находиться вне обычного «местонахождения» файла.

Некоторые файловые системы применяют копирование при записи или содержат встроенную систему управления версиями, предназначенные для того, чтобы никогда не перезаписывать данные при записи в файл.

Такие технологии как RAID и меры предотвращения фрагментации приводят к тому, что данные файла записываются сразу в несколько мест: либо намеренно (для устойчивости к отказам), либо как остатки данных.

Оптические носители

Оптические носители не магнитны и к ним не применимо размагничивание. Неперезаписываемые оптические носители (CD-R, DVD-R и т. д.) также не могут быть очищены путём перезаписывания. Перезаписываемые оптические носители, такие как CD-RW и DVD-RW, могут подвергаться перезаписыванию. Методики надёжного уничтожения оптических дисков включают: отслоение хранящего информацию слоя, измельчение, разрушение электрической дугой (как при помещении в микроволновую печь) и помещение в растворитель поликарбоната (например, ацетон).

Данные в RAM

Остаточная информация может наблюдаться в SRAM, которая обычно считается непостоянной (то есть содержимое стирается при выключении питания). В исследованиях, появление остаточной информации иногда наблюдается даже при комнатной температуре.

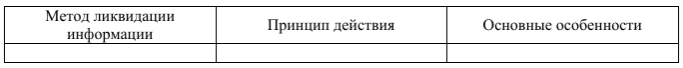
В другом исследовании обнаружена остаточная информация в DRAM, вновь со временем затухания от секунд до минут при комнатной температуре и «целая неделя без питания при охлаждении жидким азотом». Авторы исследования смогли использовать атаку через холодную перезагрузку для получения ключа шифрования для нескольких систем шифрования всего диска. Несмотря на некоторое угасание памяти, они смогли использовать избыточности в форме хранения, возникающие после преобразования ключей для эффективного использования, такие как в последовательности ключей. Авторы рекомендуют, покидая компьютер, выключать его, а не оставлять в «спящем режиме». И, если используются системы вроде Bitlocker, устанавливать PIN-код на загрузку.

* 1. **Порядок выполнения работы**

Задание 1 Опишите причины возникновения остаточной информации.

Задание 2 Приведите примеры устройств уничтожения информации с магнитных носителей.

Задание 3 Изучите особенности современных методов ликвидации информации на магнитных носителях. Заполните таблицу.



Задание 4 Изучите основные особенности современных устройств ликвидации магнитных записей. Заполните таблицу.



Задание 5 Перечислите основные требования к современным устройствам уничтожения информации с магнитных и других носителей.

Задание 6 Охарактеризуйте программные методы уничтожения информации.

1. Контрольные вопросы.
2. Перечислите основные причины появления остаточной информации.
3. Каковы способы распознавания остаточной информации?
4. Перечислите основные проблемы при уничтожении остаточной информации?
5. Перечислите основные методики уничтожения остаточной информации?
6. Содержание отчета
7. Заполнить таблицы.
8. Выполнить задания.
9. Ответить на вопросы

Практическая работа № 10

«Настройка браузера в ОС семейства Windows»

**Цель работы**. Научиться настраивать стандартный браузер в Windows

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.
  + 1. **Общие положения**

Прежде чем говорить о настройках безопасности и конфиденциальности в InternetExplorer, следует напомнить некоторые базовые понятия, использующиеся в настройках браузера, и прежде всего рассказать о цифровых сертификатах, цифровой подписи и подписных программных компонентах.

Как работают цифровые сертификаты

Обеспечение безопасной коммуникации сводится, прежде всего, к решению трех задач:

1. сохранению тайны передаваемой информации (запрет доступа к документу неавторизованных пользователей);
2. аутентификации корреспондента (предотвращения отказа от совершаемых действий);
3. идентификации корреспондента (подтверждение, что данные действительно получены от определенного лица).

Очевидно, что шифрование позволяет решить первую задачу — обеспечить тайну передаваемой информации, однако на основе шифрования можно решить все три задачи. Наибольшее распространение получил метод шифрования с помощью ключа, согласно которому открытый текст комбинируется с цепочкой чисел (ключом) по правилам определенного (криптографического) алгоритма.

Различают схемы шифрования с помощью симметричного ключа и шифрования с публичным ключом. Первая схема предполагает, что секретный одинаковый (симметричный) ключ должен быть установлен на компьютеры и отправителя, и получателя. То есть заранее необходимо знать, какие компьютеры будут «разговаривать» между собой. Несимметричное шифрование (шифрование с публичным ключом) основано на использовании пары ключей: открытого (публичного) и закрытого (частного).

Схема шифрования с публичным ключом

Послание можно зашифровать и частным, и публичным ключами, а расшифровать — только вторым ключом из пары. Таким образом, послание, зашифрованное частным ключом, можно расшифровать только публичным ключом, и наоборот. Частный ключ известен только владельцу, и его нельзя никому передавать, в то время как публичный ключ распространяется открыто для всех корреспондентов. Пару ключей — частный и публичный — можно использовать для решения задач как аутентификации ([рис. 1](http://www.compress.ru/article.aspx?id=10136&part=11ext1)), так и секретности ([рис. 2](http://www.compress.ru/article.aspx?id=10136&part=21ext1)).

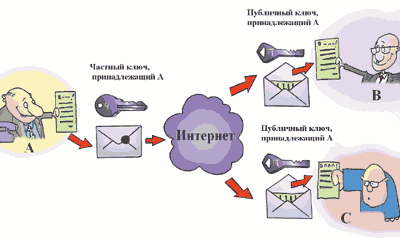


Рис. 1. Сообщение мог послать только А (лишь он обладает частным ключом), то есть проблема аутентификации обеспечена. Но B, например, не уверен, что письмо не прочитал также С. Таким образом, проблема конфиденциальности не обеспечена

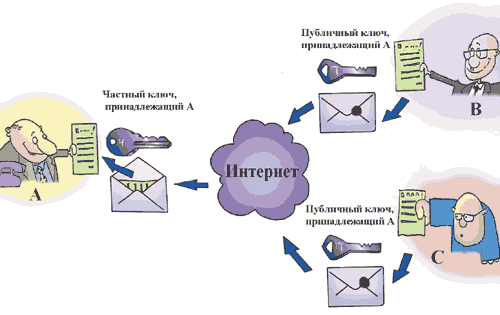


Рис. 2. Сообщение может прочесть только А, так как лишь он обладает частным ключом, раскрывающим сообщение, то есть проблема конфиденциальности решена. Но А не может быть уверен, что сообщение не прислал B, выдающий себя за С. Таким образом, проблема аутентификации не решена

Схема для первого случая представлена на [рис. 1](http://www.compress.ru/article.aspx?id=10136&part=11ext1): пользователь А заранее отсылает публичный ключ своим корреспондентам В и С, а затем отправляет им сообщение, зашифрованное его частным ключом. Схема показывает, как решается задача аутентификации.

Схема, обеспечивающая секретность или конфиденциальность, представлена на [рис. 2](http://www.compress.ru/article.aspx?id=10136&part=21ext1).

На [рис. 1](http://www.compress.ru/article.aspx?id=10136&part=11ext1) и [2](http://www.compress.ru/article.aspx?id=10136&part=21ext1) показан процесс обмена посланиями между людьми, однако в Сети мы общаемся также с различными сервисными службами. Например, когда мы собираемся скачать с какого-нибудь сервера программу, нам тоже важно знать, что он принадлежит именно фирме-разработчику ПО, а не фирме-пирату, которая незаконно распространяет программу. В принципе, когда кто-то получает от вас сообщение, зашифрованное вашим частным ключом, то он уверен в аутентичности послания. Таким образом, в данном случае шифрование эквивалентно поставленной подписи. Однако шифрование на основе алгоритмов с открытым ключом — это достаточно длительный вычислительный процесс, который не подходит для широкого использования в качестве цифровой подписи.

Цифровая подпись

Для того чтобы объяснить, как функционирует цифровая подпись, необходимо ввести понятие односторонней хеш-функции, то есть функции, преобразующей исходное послание любой длины в строку символов ограниченной длины (так называемый дайджест послания). При использовании 16-байтной хеш-функции вы на выходе получите запись длиной 16 байт. Хеширование — это одностороннее, то есть необратимое, в отличие от шифрования, преобразование. По дайджесту послания нельзя восстановить исходное сообщение, но можно его однозначно идентифицировать.

Рассмотрим конкретный пример ([рис. 3](http://www.compress.ru/article.aspx?id=10136&part=31ext1)). Пусть А, применив хеш-функцию, получил дайджест в виде некоего кода, который обозначен как код 1. Затем, используя свой личный ключ, А зашифровывает дайджест, который и становится аналогом подписи данного документа. Далее А отправляет открытый текст послания и цифровую подпись В. Абонент В расшифровывает подпись публичным ключом, который он получил от А, и убеждается, что письмо действительно от А. Таким образом, аутентификация состоялась.

Затем необходимо удостовериться, что послание не было изменено в процессе доставки.

В результате расшифровки В получает дайджест послания — код 1. Затем В, используя ту же хеш-функцию, что и А, хеширует текст послания и получает дайджест в виде некоторого кода 2. Если код 1 и код 2 совпадают, то В может сделать вывод о том, что текст послания не был изменен на этапе доставки.

Таким образом, цифровая подпись, или электронная подпись, — это метод аутентификации отправителя или автора подписи, подтверждающий, что содержание документа не было изменено. Цифровая подпись может быть поставлена как в зашифрованном, так и в открытом послании.

Цифровые сертификаты

При использовании схемы шифрования с открытым ключом вы можете сгенерировать открытый (публичный) и закрытый (частный) ключи и распространить открытый ключ вашим корреспондентам или выложить его в Сети на открытом сервере. Однако злоумышленник может назваться вашим именем и разослать открытый ключ от вашего лица или выложить его на открытом сервере. Как определить, кто является истинным владельцем публичного ключа, а кто мошенником? Для этого нужна третья сторона, которой доверяют все корреспонденты. С этой задачей справляются центры сертификации CA (CertificationAuthority). Они выдают сертификаты — цифровые данные, подписанные цифровой подписью поручителя, подтверждающие соответствие открытого ключа и информации, идентифицирующей его владельца. Сертификат содержит серийный номер, информацию о владельце ключа, название сертификационного центра, публичный ключ, время, в течение которого сертификат действителен, и т.д. Каждая копия сертификата имеет цифровую подпись организации, которая выдала сертификат, так что каждый, кто получит сертификат, может удостовериться в его подлинности.

Сертификат является неким аналогом удостоверения личности. Общеизвестно, что даже при личной встрече проблема идентификации не снимается, именно поэтому существуют паспорта, водительские удостоверения и т.д. В Сети мы обычно общаемся с партнером, которого не видим, поэтому удостоверения личности в Сети еще более необходимы.

Классы сертификатов

В InternetExplorer используется два вида сертификатов: личные сертификаты и сертификаты Web-узла. Личный сертификат используется для подтверждения личности пользователя, обратившегося на Web-узел, требующий сертификата. Сертификат Web-узла подтверждает подлинность Web-узла тем клиентам, которые обращаются к нему за сервисом.

Личные сертификаты относятся к разным уровням. Для получения сертификата низшего уровня требуется минимальная проверка владельца публичного ключа.

При выдаче сертификата высшего уровня проверяются не только личные данные владельца, но и его кредитоспособность. В этом случае сертификат может выступать аналогом кредитной карты, подтверждающим кредитоспособность при сделках в Web.

Для получения личного сертификата пользователь обязан внести плату, которая тем больше, чем выше уровень сертификата.

Подлинность сертификата подтверждается подписью сертификационного центра, выдавшего сертификат.

Корневой сертификат — это так называемый самоподписной сертификат некоторого центра сертификации. Он называется корневым, поскольку выше него нет инстанции, которая могла бы удостоверить его подлинность. В браузере (например, в InternetExplorer) уже предустановлены корневые сертификаты известных центров сертификации, например такого, как Verisign. Корневой сертификат содержит публичный ключ и информацию о его владельце. Когда вы получаете личный сертификат вашего корреспондента, заверенный подписью Verisign, вы можете убедиться в его подлинности и сохранить его на своем компьютере. Во вновь полученном сертификате находится публичный ключ данного корреспондента, поэтому когда вы получите письмо (или файл, содержащий программу), подписанное этим корреспондентом, то, используя его публичный ключ, вы сможете убедиться в подлинности его подписи. Система сделает это сама и выдаст вам сообщение, что данному корреспонденту (Web-узлу) можно доверять.

Система сертификации обычно имеет многоуровневый характер ([рис. 4](http://www.compress.ru/article.aspx?id=10136&part=41ext1)).

При обращении на защищенный Web-узел пользователь InternetExplorer получит уведомление о том, что соединение является безопасным и передаваемые пользователем данные не будут доступны третьим лицам ([рис. 5](http://www.compress.ru/article.aspx?id=10136&part=51ext1)).

Система информирует пользователя, что Web-узел имеет действительный сертификат и предоставляемая пользователем информация (например, номер кредитной карты) зашифрована и не может быть прочитана третьими лицами. При входе на защищенный Web-узел InternetExplorer в строке состояния отображает значок закрытого замка.

Чтобы самому посылать зашифрованные или подписанные цифровой подписью сообщения, пользователь должен получить личный сертификат и настроить InternetExplorer на работу с ним.

Процедура получения личного сертификата

Существует несколько категорий надежности сертификатов, которые выдаются независимыми центрами сертификации. Сертификаты выдаются теми же издателями сертификатов. Чтобы получить сертификат, необходимо зарегистрироваться у выбранного издателя сертификатов. Для получения личного сертификата нужно обратиться на Web-сервер издателя сертификатов, сообщить о себе данные, необходимые для получения конкретного сертификата, и выбрать длину закрытого ключа. Перед отправкой формы ваш браузер сгенерирует пару ключей — публичный (открытый) и частный (закрытый) — и внесет их в защищенную паролем базу данных. Закрытый ключ не должен быть известен никому, в том числе и сертификационному центру. Открытый ключ, напротив, отсылается вместе с другими данными в сертификационный центр для включения его в сертификат. После получения оплаты сертификационный центр выпускает сертификат и указывает URL, откуда его можно скачать. После получения сертификата браузер пользователя автоматически запускает процедуру установки.

Система подписанных приложений

Приобретая коробочное ПО, вы обычно не сомневаетесь, что программный продукт, находящийся внутри, принадлежит производителю. Однако, скачивая продукт из Сети, вы не можете быть уверены, что поставщик данного ПО является именно тем, за кого он себя выдает, а скачиваемое ПО не содержит вирусов.

Данная проблема решается путем внедрения в распространяемый продукт кода аутентификации (Authenticode), позволяющего разработчикам ПОпосредством использования цифровой подписи включать информацию о разработчике в распространяемые программы.

Скачивая ПО, подписанное кодом аутентификации и заверенное центром сертификации, пользователи могут быть уверены, что данное ПО не было изменено после подписания.

Согласно компонентной модели, такие элементы, как ActiveX- или Java-аплеты, могут загружаться на ваш компьютер во время обращения на Web-ресурс, например, для воспроизведения анимации. Для того чтобы исключить загрузку небезопасного кода, применяется система подписанных приложений. На основе данной технологии пользователи могут безбоязненно получать подписанные ActiveXcontrols, Java-аплеты и другие приложения. Если пользователь InternetExplorer встретит компонент, распространяемый без подписи, программа (в зависимости от внутренних настроек безопасности браузера) либо откажется загрузить такой код, либо выдаст предупреждение о небезопасном компоненте. Если же пользователь столкнется с подписаннымаплетом, клиентская программа подтвердит безопасность компонента ([рис. 6](http://www.compress.ru/article.aspx?id=10136&part=61ext1)).

Установка и удаление сертификатов в InternetExplorer

Для просмотра предустановленных сертификатов выберите пункт Сертификаты на панели Свойства обозревателя ([рис. 7](http://www.compress.ru/article.aspx?id=10136&part=71ext1)), что приведет к появлению панели Сертификаты ([рис. 8](http://www.compress.ru/article.aspx?id=10136&part=81ext1)). В ней доступны следующие вкладки: Личные, Другие пользователи, Промежуточные центры сертификации, Доверенные корневые центры сертификации и т.д.

Сертификаты в категории Личные имеют соответствующие частные ключи. Информация, подписанная посредством персональных сертификатов, идентифицируется частным ключом пользователя. По умолчанию, InternetExplorer размещает все сертификаты, идентифицирующие пользователя (посредством частного ключа), в категорию Личные. Во вкладке Доверенные корневые центры сертификации обычно уже предустановлены корневые сертификаты, которые можно просмотреть и получить всю информацию о них: кем они выданы, срок их действия и т.д ([рис. 9](http://www.compress.ru/article.aspx?id=10136&part=91ext1)).

Щелкнув мышью по каждому из сертификатов, можно получить о нем дополнительные сведения, включая состав и путь сертификации ([рис. 10](http://www.compress.ru/article.aspx?id=10136&part=101ext1)).

Для импорта и экспорта сертификатов в InternetExplorer имеется менеджер импорта и экспорта сертификатов — InternetExplorerCertificateManager ([рис. 11](http://www.compress.ru/article.aspx?id=10136&part=111ext1)).

Для того чтобы вызвать мастера импорта сертификатов, выполните команду Сервис а Свойства обозревателя а Содержание а Сертификаты а Импорт.

Менеджер сертификатов позволяет вам инсталлировать и удалять сертификаты клиентские и сертификаты Центров Сертификации.

Средства сохранения конфиденциальности в InternetExplorer

Средства сохранения конфиденциальности InternetExplorer связаны с параметрами режима обработки файлов cookiеs. Прежде чем рассказать о настройках конфиденциальности браузера, кратко напомним, что представляют собой cookiеs.

Cookies

Cookies — небольшие текстовые записи, которые сохраняются браузером на компьютере пользователя по запросу сервера. Эта текстовая информация хранится на компьютере пользователя в примитивной базе данных до тех пор, пока не будет удалена. Сookies, в которых хранится история обращений пользователя к конкретному Wеb-серверу, посылают многие Web-серверы. Технология cookies позволяет разработчикам сайтов четче отслеживать характер обращений на их сайт и предоставлять пользователям дополнительные сервисы.

Например, владельцам сайта важно знать, сколько человек просмотрело их сайт, желательно получить информацию, кто пришел на сайт впервые, а кто — повторно.

Данная задача легко может быть решена с помощью технологии cookies. Программное обеспечение Web-сайта может сгенерировать уникальный ID-номер каждого посетителя сайта, отослать его пользователю, и он будет храниться на пользовательском компьютере. При повторном посещении эти данные считываются, и Web-сайт узнает своего посетителя. В дальнейшем по мере посещения данной странички информация в вашем cookie может изменяться. При этом следует отметить, что сервер может ассоциировать разные cookies с различными частями Web-сайта.

Как известно, протокол HTTP (в отличие от протоколов FTP, Telnet) не обеспечивает постоянного соединения между клиентом и сервером. За время одного запроса Web-сервер посылает только один файл, и после завершения передачи соединение разрывается по инициативе сервера. Таким образом, сервер не помнит о предыдущих обращениях пользователя и введенных им настройках. Использование технологии cookies позволяет запоминать пользователя, считывая из файлов cookies его имя, персональные настройки и т.д.

Различают постоянные и временные файлы cookies. Временные файлы cookies хранятся на компьютере пользователя только в течение текущего сеанса браузера, а постоянные сохраняются на компьютере пользователя и считываются Web-узлом при повторном посещении.

С помощью технологии cookies владелец сайта может проследить за перемещениями пользователя по сайту, получить сведения о его предпочтениях и использовать их в рекламных целях, основываясь на полученных данных. Некоторые пользователи усматривают в этом нарушение конфиденциальности.

В cookies могут храниться такие сведения о пользователе, как определенные индивидуальные настройки, выбранные им при посещении узла, а также личные идентификационные данные, которые были внесены пользователем в соответствующие регистрационные формы. Следует отметить, что cookies, полученные с сервера, могут содержать только те персональные данные, которые пользователь сам послал данному серверу. Для хранения cookies браузер должен вести определенную базу данных на компьютере пользователя. Если вы пользуетесь MicrosoftInternetExplorer, то на вашем компьютере эта база данных представлена папкой с файлами, имена которых состоят из имен пользователя и сервера, и может иметь, например, следующий вид: прохоров@spylog[2].txt.

Просмотрев подобный файл, нетрудно убедиться, что это простые текстовые файлы. Например, файл прохоров@spylog[2].txt имеет вид:

VISIDSVWDOBAOFOTIYBYDIPspylog.com/1024136250380829567102216316196829530892\*

В данной текстовой строке содержится имя сайта spylog.com, который я посетил, и служебная информация. Обычно браузер имеет ограничения на максимальный размер cookies (не более 4 Кбайт), общее количество cookies (не более 500) и максимальное количество cookies, хранимых для одного сервера (около 20).

Cookies имеют небольшой размер и не могут содержать много данных. Обычно информация о том, какие сайты посещал тот или иной пользователь, хранится на Web-сервере, а cookies используются для поиска сведений о том, какие страницы посещались данным пользователем, какая реклама ему уже показывалась, а какая нет, списка заказанных им товаров и т.п.

Технология cookies позволяет делать персонализованные страницы. Например, если вы задали свои координаты при регистрации на некотором сайте, показывающем погоду, то он сможет сообщать вам погоду специально для вашего региона.

Сайты электронной коммерции могут использовать cookies для создания покупательской корзины. Информация обо всех вещах, которые вы добавляете в вашу корзину, хранится в базе данных Web-сервера вместе в вашим ID. Если вы хотите получить счет, то, поскольку серверу известны все заказанные вами товары, ему несложно будет получить из базы данных информацию об их стоимости и выставить вам счет. Негативное отношение к cookies объясняется тем, что в них хранится информация о посещаемых вами ресурсах. Например, если вашим компьютером, кроме вас, пользуется кто-то еще, то он может узнать, какие ресурсы вы посещали, а иногда и ваши личные данные.

При посещении Web-сайтов с чужого компьютера следует помнить, что они могут внести на него нежелательные cookies. В этом случае можно запретить размещение cookies или удалить их по окончании работы.

Удаление cookies безопасно в плане работоспособности вашего компьютера. Однако следует иметь в виду, что если вы удалите cookies, принадлежащие сайту, который вы часто посещаете, то вместе с этими сookies будут потеряны ваши индивидуальные настройки.

Контроль над cookies в Internet Explorer

Учитывая неоднозначное отношение к cookies, современные браузеры позволяют осуществлять контроль за помещением cookies на ваш компьютер. Если вы пользуетесь браузером InternetExplorer 6.0, то можете определить различную политику использования cookies при доступе к разным сайтам. Так, на одной группе сайтов cookies будут блокироваться, а на другой — нет. При этом следует отметить, что если запретить сохранение всех файлов cookies для некоторых Web-узлов, то на них нельзя будет реализовать определенные средства настройки. Если, например, вы хотите получать на некотором сайте сведения о погоде в конкретном регионе, то без разрешения на применение технологии cookie вы не сможете реализовать эту настройку.

Говоря о настройке конфиденциальности в InternetExplorer, следует упомянуть о стандарте P3P (PlatformforPrivacyPreferencesProject), который поддерживается в InternetExplorer 6.0. Спецификация P3P разрабатывается консорциумом W3C и регламентирует, каким образом Интернет-ресурс обрабатывает информацию о пользователях. P3P помогает пользователям осуществлять контроль над конфиденциальной информацией при посещении Web-сайтов. К категории конфиденциальной информации, защищаемой P3P, относятся персональные данные пользователя (имя, e-mail, адрес проживания, место работы и т.д.), а также сведения об активности пользователя в Интернете, регистрируемые в файлах cookies.

Спецификация (P3P) позволяет Web-узлам преобразовывать политики обеспечения конфиденциальности в стандартизированные машиночитаемые форматы, которые могут быть автоматически возвращены и легко обработаны браузером пользователя. Серверы, собирающие информацию о посетителях (в первую очередь Интернет-магазины) и игнорирующие этот формат, могут оказаться заблокированными. Многие рейтинговые системы (SpyLog, Mail.ru и др.) уже осуществили совместимость с P3P.

Для обеспечения совместимости с протоколом P3P Web-ресурс должен описать свою политику конфиденциальности, то есть определить, какие сведения о пользователях он фиксирует, как их хранит и какие файлы cookies создает. Данное описание формализуется в соответствии со спецификацией P3P и размещается в корневой директории сайта. InternetExplorer считывает данный файл и получает необходимую информацию.

Средства сохранения конфиденциальности InternetExplorer представляют: возможности просмотра политики конфиденциальности P3P Web-узла и настройки различных параметров режима обработки файлов cookies и включают систему оповещения о том, что открываемый Web-узел не соответствует выбранным параметрам конфиденциальности.

Основными каналами утечки конфиденциальной информации являются третьи, или сторонние, сайты, то есть сайты, к которым адресуется пользователь параллельно с просматриваемым узлом. Сторонним называется любой Web-узел, не отображаемый в окне обозревателя. На просматриваемомWeb-узле могут быть размещены материалы со сторонних Web-узлов, которые, в свою очередь, могут использовать файлы cookies.

В IE 6.0 по умолчанию установлен уровень защиты, предполагающий блокировку cookies сторонних сайтов, которые:

несовместимы с P3P, то есть не декларировали свою политику конфиденциальности;

запрашивают личную информацию без явного согласия пользователя;

запрашивают личную информацию без неявного согласия пользователя.

Чтобы изменить параметры конфиденциальности, во вкладке Конфиденциальность переместите ползунок вверх, чтобы установить более высокий уровень защиты, и вниз, чтобы понизить его ([рис. 12](http://www.compress.ru/article.aspx?id=10136&part=121ext1)).

На панели можно настроить шесть уровней безопасности. Первый уровень Блокировать все cookies предусматривает блокировку файлов cookies для всех Web-узлов, при этом cookies, уже имеющиеся на компьютере, не будут доступны для Web-узлов. Следующий уровень Высокий подразумевает более мягкие условия — блокировку файлов cookies для узлов, не имеющих компактной политики (формализованных условий конфиденциальности), и узлов, использующих личные идентификационные данные пользователя без его явного согласия. Существуют также Средний (показан на [рис.12](http://www.compress.ru/article.aspx?id=10136&part=121ext1)), Низкий уровни и, наконец, режим Принимать все cookies, позволяющий сохранять на компьютере все файлы cookies.

Нажав на кнопку Дополнительно на панели ([рис. 12](http://www.compress.ru/article.aspx?id=10136&part=121ext1)), вы перейдете в панель, где можно определить дополнительные параметры конфиденциальности, то есть перекрыть автоматическую обработку файлов cookies и определить режим приема основных и сторонних cookies.

InternetExplorer делит Интернет на зоны разного уровня безопасности, что позволяет назначить требуемый уровень защиты каждому Web-узлу. Это Зона Интернета, Местная интрасеть, Надежные узлы и Ограниченные узлы ([рис. 13](http://www.compress.ru/article.aspx?id=10136&part=131ext1)).

Зона Интернета

К этой зоне относятся все Web-узлы, которые не имеют отношения к вашему компьютеру или к иной зоне. По умолчанию для этой зоны назначен средний уровень защиты, который подходит для большей части узлов Интернета.

Безопасный и одновременно функциональный, он подразумевает, что неподписанные управляющие элементы ActiveX не загружаются, а перед загрузкой небезопасного содержимого появляется предупреждение.

Местная интрасеть (местная зона)

Обычно в этой зоне содержатся все адреса, для доступа к которым не требуется прокси-сервер. Для этой зоны по умолчанию устанавливается средний уровень безопасности. Таким образом, InternetExplorer будет позволять сохранение на компьютере объектов cookies с Web-узлов в этой зоне и их чтение Web-узлами, на которых они были созданы.

Надежные узлы

По умолчанию для этой зоны устанавливается низкий уровень безопасности. InternetExplorer будет позволять сохранение на компьютере объектов cookies с Web-узлов в этой зоне и их чтение Web-узлами, на которых они были созданы.

Узлы ограниченной надежности

Для этой зоны по умолчанию устанавливается высокий уровень безопасности. InternetExplorer будет блокировать все объекты cookies с Web-узлов в этой зоне.

Для того чтобы получить отчет о конфиденциальности по тому или иному ресурсу, выполните команду Вид а Отчет о конфиденциальности, что приведет к появлению одноименной панели ([рис. 14](http://www.compress.ru/article.aspx?id=10136&part=141ext1)), на которой вы сможете увидеть, какие cookies были заблокированы на основе ваших параметров конфиденциальности.

Настройка ограничений доступа к нежелательным ресурсам

Если вы пользуетесь компьютером дома и опасаетесь, что ваши дети будут просматривать страницы, доступ к которым нежелателен, вы можете прибегнуть к настройкам, расположенным на вкладке Ограничение доступа ([рис. 15](http://www.compress.ru/article.aspx?id=10136&part=151ext1)).

Можно запретить доступ к тематическим группам сайтов или к конкретным сайтам.

В принципе, оградить ребенка от посещения сайтов определенной тематики достаточно сложно, но если вы знаете конкретные сайты, доступ к которым вы хотите закрыть, то сделать это значительно проще. В частности, во вкладке Разрешенные узлы вы можете указать список сайтов, запрещенных к просмотру ([рис. 15](http://www.compress.ru/article.aspx?id=10136&part=151ext1)).

Настройка персональных данных и контроль за ними

Просматривая различные ресурсы Интернета, пользователи часто подписываются на разные службы и вынуждены при этом сообщать данные о себе. InternetExplorer позволяет создать профиль, в котором будут храниться ваши личные данные ([рис. 16](http://www.compress.ru/article.aspx?id=10136&part=161ext1)).

Однако если вы не хотите, чтобы вам приходило огромное количество спама, то личные данные и прежде всего e-mail не следует раздавать всем подряд. Проверьте, какой режим установлен в вашем браузере. Выполните команду Сервис-Свойства обозревателя-вкладка Дополнительно-раздел Безопасность. Если у вас установлен флажок «Задействовать профиль» ([рис. 17](http://www.compress.ru/article.aspx?id=10136&part=171ext1)), то по первому запросу сервера браузер будет сообщать ваши персональные данные, поэтому следует отключить эту опцию.

Обратите также внимание на другие пункты и установите флажки в следующих разделах: Предупреждать о недействительных сертификатах узлов, Предупреждать о переключении режима безопасности, Проверять аннулирование сертификатов издателей, Проверять аннулирование сертификатов серверов ([рис. 17](http://www.compress.ru/article.aspx?id=10136&part=171ext1)).

1. Порядок выполнения работы
2. Составить алгоритм работы цифрового сертификата.
3. Составить алгоритм работы cookies.
4. Составить алгоритм работы со схемой шифрования с публичным ключом.
5. Составить алгоритм установки и удаления сертификатов в InternetExplorer..
6. Контрольные вопросы.
7. Перечислите основополагающие принципы теории информации.
8. Недостатки использования cookies?
9. Для чего применяют цифровую подпись? Сертификат?
10. Что относится к организации безопасной передачи и обмена информацией с помощью браузера?
11. Содержание отчета
12. Алгоритм работы цифрового сертификата.
13. Алгоритм работы cookies.
14. Алгоритм работы со схемой шифрования с публичным ключом.
15. Алгоритм установки и удаления сертификатов в InternetExplorer..

Практическая работа № 11

«Настройка браузера в ОС семейства Linux»

**Цель работы**. Научиться настраивать браузер в Linux

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.
  + 1. **Общие положения**

В составе всех дистрибутивов Linux присутствует lptables (брандмауэр linux), который является частью ядра и позволяющий фильтровать сетевые пакеты. Ручная настройка lptables под силу не каждому. Но существуют и более удобные для обычного пользователя браузеры. Например, графический интерфейс Firestarter для брандмауэра Linux Firestarter упрощает процесс настройки брандмауэра linux. Из него можно закрывать и открывать порты, а также просматривать сетевой трафик данного компьютера.

Установим Брандмауер в Linux. Большинство дистрибутивов содержит этот пакет в своих репозиториях. После установки, во время первого запуска Firestarter (брандмауэра linux), вызовется программа-мастер, которая предложит выбрать сетевой интерфейс, на котором он будет активен.

Настройка брандмауэра linux довольна проста. Если есть такое приложение, которое требует открыть определенные порты, то с помощью frestarter возможно открыть данный доступ. Разрешите входящие соединения на вкладке Policy. Щелкните правой кнопкой мыши под опцией Allow Service и выберите опцию Add Rule. Из открывшегося окна выберите сервис и исходящий IP-адрес.

Обычно я открывал порты для torrent-ов, в transmission можно всегда проверить, открыт или закрыт определенный порт.frestarter- графическая программа для настройки брандмауэра Linux.

Также можно ограничивать сетевой трафик на вкладке Outbount TraffcPolicy. После чего можно выбрать опцию Permissive (Разрешить), здесь необходимо добавить хосты в черный список, которые нужно блокировать. Или Resrictive (ограничивать), которая работает противоположно, то есть разрешит порты только из белого списка.

Через основной интерфейс Firestarter можно мониторить активные соединения с брандмауером Linux, статус, список входящих и исходящих соединений, объем данных, список источников, пункт назначения сетевого трафика, порт и программу, которая руководит трафиком.

В таких дистрибутивах Linux как Fedora, Mandriva присутствуют уже свои предустановленные графические приложения для настройки брандмауэра. Хоть даже и самые простые, но лучше, чем ничего. Gufw самый простой графический интерфейс для настройки брандмауэра, разработанный специально для Ubuntu.

1. Порядок выполнения работы
2. Составить алгоритм настройки брэндмауэра в Linux.
3. Найти, какие еще браузеры используются в Linux, описать алгоритм их работы.
4. Контрольные вопросы.
5. Перечислите основополагающие принципы безопасной работы в интернете.?
6. Что означает «дружественный» интерфейс?
7. Что такое «порт»? Когда необходимо, чтобы он был открыт?
8. Содержание отчета
9. Алгоритм настройки брэндмауэра в Linux.
10. Алгоритм настройки еще одного любого браузера в Linux

Практическая работа № 12.

«Определение трудоемкости взлома симметричного криптоалгоритма»

**Цель работы.** Приобретение теоретических навыков трудоемкости взлома симметричных криптоалгоритмов.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.
  1. **Общие положения**

Алгоритмы шифрования и дешифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами. Главным принципом в них является условие, что *передатчик и приемник заранее знают алгоритм шифрования*, а также ключ к сообщению, без которых информация представляет собой всего лишь набор символов, не имеющих смысла.

**Симметри́чные криптосисте́мы** (также **симметричное шифрование**, **симметричные шифры**) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Классическим примером таких алгоритмов являются **симметричные криптографические алгоритмы**, перечисленные ниже:

* Простая перестановка
* Одиночная перестановка по ключу
* Двойная перестановка
* Перестановка "Магический квадрат"

(Определить достоинства и недостатки данных симметричных криптографических алгоритмов)

**Простая перестановка**

Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи несмыслового текста.

**Одиночная перестановка по ключу**

Более практический метод шифрования, называемый одиночной перестановкой по ключу очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

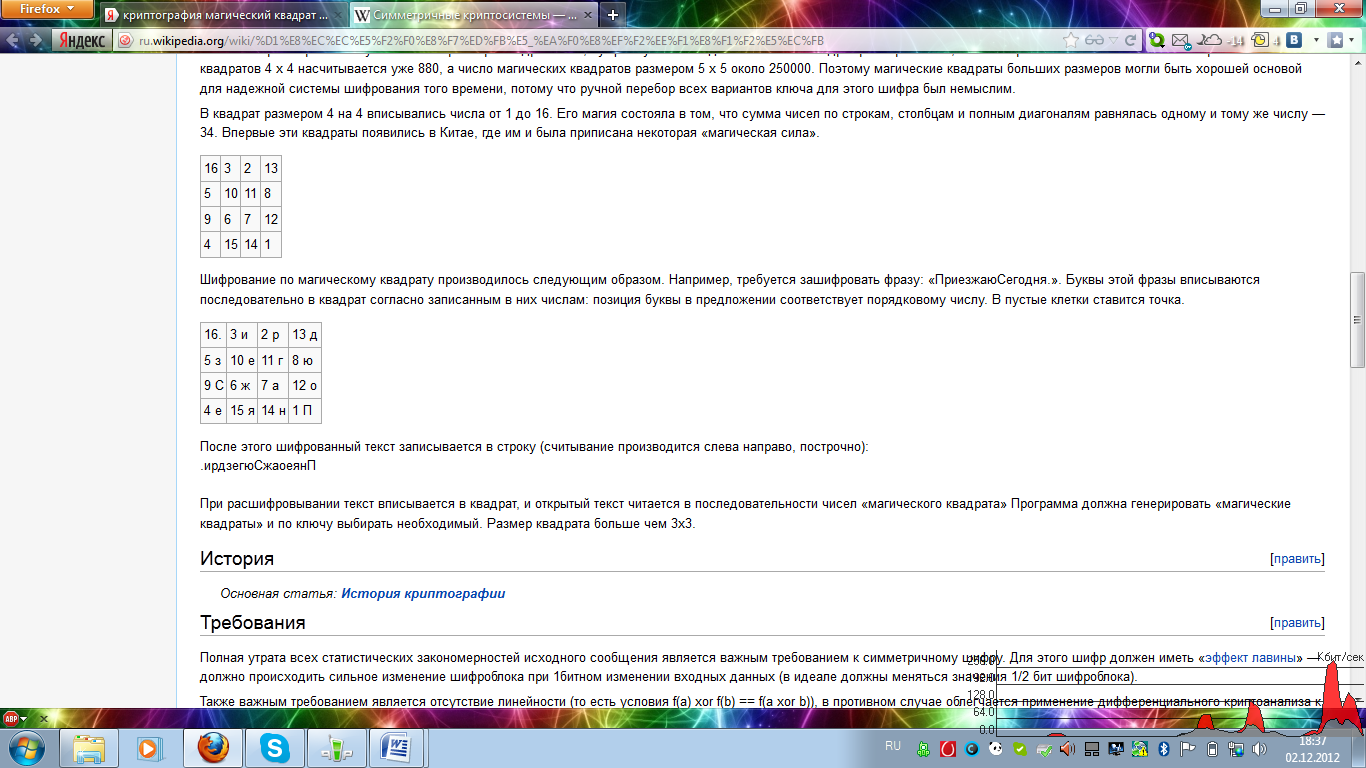
**Двойная перестановка**

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

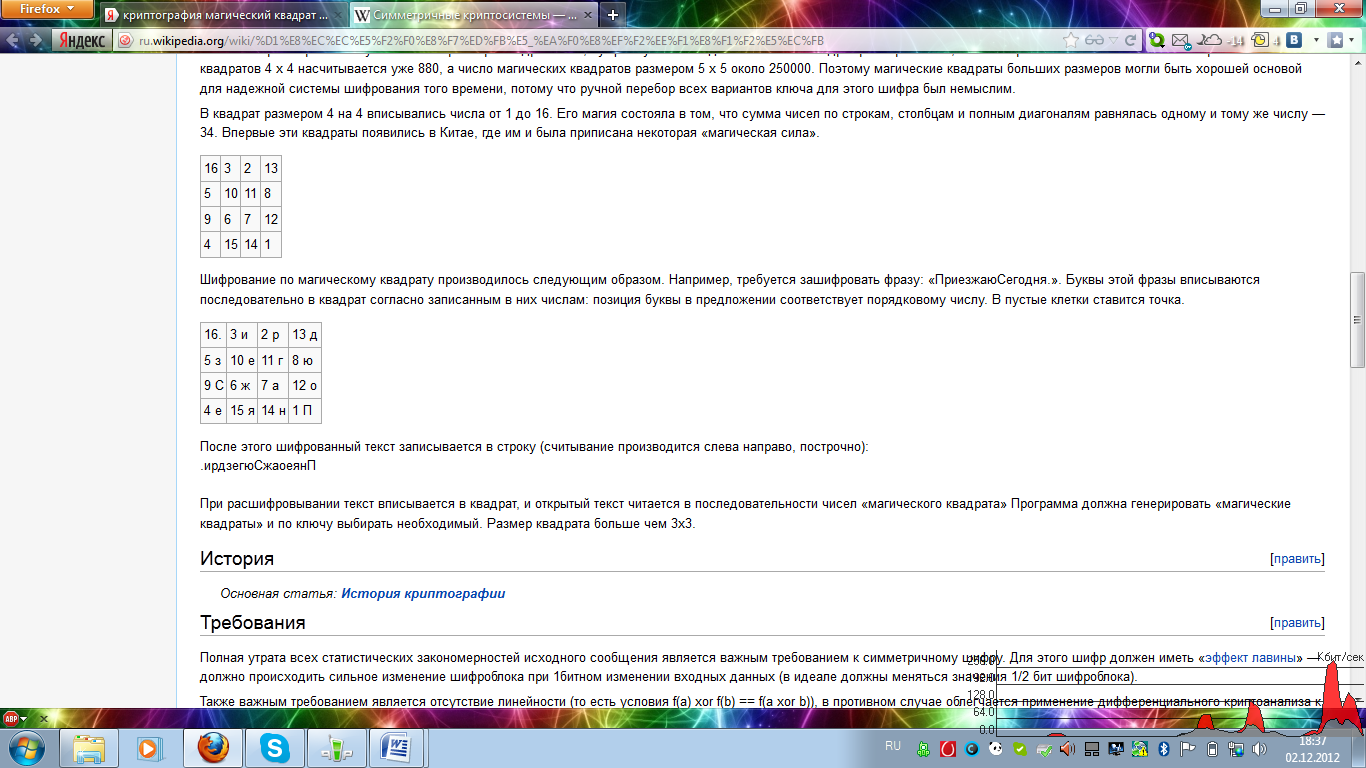
**Перестановка «Магический квадрат»**

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 х 3, если не принимать во внимание его повороты. Магических квадратов 4 х 4 насчитывается уже 880, а число магических квадратов размером 5 х 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

В квадрат размером 4 на 4 вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу — 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».



Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «ПриезжаюCегодня.». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка.



После этого шифрованный текст записывается в строку (считывание производится слева направо,построчно):.ирдзегюСжаоеянП

При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел «магического квадрата» Программа должна генерировать «магические квадраты» и по ключу выбирать необходимый. Размер квадрата больше чем 3х3.

Большинство симметричных шифров используют сложную комбинацию большого количества подстановок и перестановок. Многие такие шифры исполняются в несколько (иногда до 80) проходов (раундов), используя на каждом проходе «ключ прохода». Множество «ключей прохода» для всех проходов называется «расписанием ключей» (key schedule). Как правило, оно создается из ключа выполнением над ним неких операций, в том числе перестановок и подстановок.

Существует множество (не менее двух десятков) алгоритмов симметричных шифров, существенными параметрами которых являются:

* стойкость
* длина ключа
* число [раундов](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_%28%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8%29)
* длина обрабатываемого блока
* сложность аппаратной/программной реализации
* сложность преобразования

**Распространенные алгоритмы**

* [AES](http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Advanced Encryption Standard*) - американский стандарт шифрования
* [ГОСТ 28147-89](http://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89) — отечественный стандарт шифрования данных
* [DES](http://ru.wikipedia.org/wiki/DES) ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Data Encryption Standard*) - стандарт шифрования данных в США до AES
* [3DES](http://ru.wikipedia.org/wiki/3DES) (Triple-DES, тройной DES)
* [RC6](http://ru.wikipedia.org/wiki/RC6) (Шифр [Ривеста](http://ru.wikipedia.org/wiki/%D0%A0%D0%B8%D0%B2%D0%B5%D1%81%D1%82,_%D0%A0%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%B4_%D0%9B%D0%B8%D0%BD%D0%BD) )
* [Twofish](http://ru.wikipedia.org/wiki/Twofish)
* [IDEA](http://ru.wikipedia.org/wiki/IDEA) ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *International Data Encryption Algorithm*)
* [SEED](http://ru.wikipedia.org/wiki/SEED) - корейский стандарт шифрования данных
* [Camellia](http://ru.wikipedia.org/wiki/Camellia_%28%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%29) - сертифицированный для использовании в Японии шифр
* [CAST](http://ru.wikipedia.org/wiki/CAST_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%29) (по инициалам разработчиков Carlisle Adams и Stafford Tavares)
* [XTEA](http://ru.wikipedia.org/wiki/XTEA) - наиболее простой в реализации алгоритм

**Сравнение с асимметричными криптосистемами**

**Достоинства**

* скорость (по данным Applied Cryptography — на 3 порядка выше)
* простота реализации (за счёт более простых операций)
* меньшая требуемая длина ключа для сопоставимой стойкости
* изученность (за счёт большего возраста)

**Недостатки**

* сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 — 499500 и т. д.
* сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.
* Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передаётся сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования.
* Важным свойством симметричных шифров является **невозможность** их использования для подтверждения авторства, так как ключ известен каждой стороне.

1. Порядок выполнения работы
2. Выполнить анализ систем шифрования
3. Зашифровать выражение из 16 символов при помощи «Магического квадрата» и написать получившиеся символы.
4. Контрольные вопросы.
5. Для чего необходимы системы шифрования?
6. Что означает «симметричный криптоалгоритм»?
7. В чем особенности симметричного криптоалгоритма?
8. Каковы параметры симметричного криптоалгоритма?
9. Какие симметричные криптоалгоритмы существуют?

**Содержание отчета:**

* 1. Название и цель работы
  2. Определение симметричного криптоалгоритма
  3. Классические 4 системы симметричного шифрования, достоинства недостатки
  4. Параметры алгоритмов
  5. Зашифровать выражение из 16 символов при помощи «Магического квадрата» и написать получившиеся символы

Практическая работа № 13.

«Определение трудоемкости взлома несимметричного криптоалгоритма»

**Цель работы.** Приобретение теоретических навыков трудоемкости взлома несимметричных криптоалгоритмов.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

**Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр)** - система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME.

**Идея криптосистемы с открытым ключом**

Идея криптографии с открытым ключом очень тесно связана с идеей односторонних функций, то есть таких функций , что по известному довольно просто найти значение , тогда как определение из невозможно за разумный срок.

Но сама односторонняя функция бесполезна в применении: ею можно зашифровать сообщение, но расшифровать нельзя. Поэтому криптография с открытым ключом использует односторонние функции с лазейкой. Лазейка — это некий секрет, который помогает расшифровать. То есть существует такой , что зная и , можно вычислить . К примеру, если разобрать часы на множество составных частей, то очень сложно собрать вновь работающие часы. Но если есть инструкция по сборке (лазейка), то можно легко решить эту проблему.

Понять идеи и методы криптографии с открытым ключом помогает следующий пример — хранение паролей в компьютере. Каждый пользователь в сети имеет свой пароль. При входе он указывает имя и вводит секретный пароль. Но если хранить пароль на диске компьютера, то кто-нибудь его может считать (особенно легко это сделать администратору этого компьютера) и получить доступ к секретной информации. Для решения задачи используется односторонняя функция. При создании секретного пароля в компьютере сохраняется не сам пароль, а результат вычисления функции от этого пароля и имени пользователя.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | A | B | C | D | E |
| 2 | F | G | H | I/J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ё | Ж | З | И | Й | К |
| 3 | Л | М | Н | О | П | П |
| 4 | С | Т | У | Ф | Х | Ц |
| 5 | Ч | Ш | Щ | Ъ | Ы | Ь |
| 6 | Э | Ю | Я | - | - | - |

Метод №1.

Зашифруем слово «SOMETEXT»:

Для шифрования на квадрате находили букву текста и вставляли в шифровку нижнюю от неё в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца.

Таблица координат

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква текста: | S | O | M | E | T | E | X | T |
| Буква шифротекста: | X | T | R | K | Y | K | C | Y |

Таким образом после шифрования получаем:

|  |  |
| --- | --- |
| До шифрования: | SOMETEXT |
| После шифрования: | XTRKYKCY |

Метод№2

Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально:

Таблица координат

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква: | S | O | M | E | T | E | X | T |
| Координата горизонтальная: | 3 | 4 | 2 | 5 | 4 | 5 | 3 | 4 |
| Координата вертикальная: | 4 | 3 | 3 | 1 | 4 | 1 | 5 | 4 |

Затем координаты считывают по строкам:

|  |
| --- |
| 34 25 45 34 43 31 41 54 |

Далее координаты преобразуются в буквы по этому же квадрату:

Таблица координат

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Координата горизонтальная: | 3 | 2 | 4 | 3 | 4 | 3 | 4 | 5 |
| Координата вертикальная: | 4 | 5 | 5 | 4 | 3 | 1 | 1 | 4 |
| Буква: | S | W | Y | S | O | C | D | U |

Таким образом после шифрования получаем:

Результат

|  |  |
| --- | --- |
| До шифрования: | SOMETEXT |
| После шифрования: | SWYSOCDU |

Метод №3

3425453443314154

Полученная последовательность цифр сдвигается циклически влево на один шаг(нечетное количество шагов):

4254534433141543

Эта последовательность вновь разбивается в группы по два:

42 54 53 44 33 14 15 43

и по таблице заменяется на окончательный шифротекст:

Таблица координат

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Координата горизонтальная: | 4 | 5 | 5 | 4 | 3 | 1 | 1 | 4 |
| Координата вертикальная: | 2 | 4 | 3 | 4 | 3 | 4 | 5 | 3 |
| Буква: | I | U | P | T | N | Q | V | O |

Таким образом после шифрования получаем:

Результат

|  |  |
| --- | --- |
| До шифрования: | SOMETEXT |
| После шифрования: | IUPTNQVO |

Преимущества асимметричных шифров перед симметричными:

Не нужно предварительно передавать секретный ключ по надёжному каналу. Только одной стороне известен ключ шифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обеим сторонам и должен держаться в секрете обеими). Пару можно не менять значительное время (при симметричном шифровании необходимо обновлять ключ после каждого факта передачи). В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки

Недостатки алгоритма несимметричного шифрования в сравнении с симметричным: В алгоритм сложнее внести изменения. Хотя сообщения надежно шифруются, но получатель и отправитель самим фактом пересылки шифрованного сообщения «засвечиваются».

Более длинные ключи. Ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью:

|  |  |
| --- | --- |
| **Длина симметричного ключа, бит** | **Длина ключа RSA, бит** |
| 56 | 384 |
| 64 | 512 |
| 80 | 768 |
| 112 | 1792 |
| 128 | 2304 |

Шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом. Требуются существенно бо́льшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами:

Для ЭЦП сообщение предварительно подвергается хешированию, а с помощью асимметричного ключа подписывается лишь относительно небольшой результат хеш-функции. Для шифрования они используются в форме гибридных криптосистем, где большие объёмы данных шифруются симметричным шифром на сеансовом ключе, а с помощью асимметриичного шифра передаётся только сам сеансовый ключ.

**Виды асимметричных шифров**

RSA (Rivest-Shamir-Adleman)

DSA (Digital Signature Algorithm)

Elgamal (Шифросистема Эль-Гамаля)

Diffie-Hellman (Обмен ключами Диффи — Хелмана)

ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи.

ГОСТ Р 34.10-2001

Rabin

Luc

McEliece

Williams System (Криптосистема Уильямса)

1. Порядок выполнения работы
2. Зашифровать слово всеми способами.
3. Ответить на вопросы.
4. Контрольные вопросы.
5. Для чего необходимы системы шифрования?
6. Что означает «асимметричный криптоалгоритм»?
7. В чем особенности асимметричного криптоалгоритма?
8. Чем отличаются способы шифрования асимметричного криптоалгоритма?

1. Содержание отчета:
2. Определение асимметричного криптоалгоритма
3. Достоинства недостатки
4. Параметры алгоритмов с открытым ключом
5. Зашифровать сообщение (одно слово), используя все три метода

Практическая работа № 14

«Составление схем обнаружения вредоносных программ»

**Цель работы.** Изучить признаки зараженного компьютера, закрепить навыки обнаружения вредоносных программ.

1. Оснащение занятия:

* методические рекомендации;
* персональный компьютер

1. Общие положения:

Несанкционированный доступ к данным является возможным в большинстве случаев посредством вредоносных программ.

Определение «Вредоносная программа» (на жаргоне антивирусных служб «зловред», англ. malware, malicious software — «злонамеренное программное обеспечение») – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации.

Существует множество различных вредоносных программ, порой антивирусные базы сигнатур не успевают получить требуемое обновление для определения вредоносности программы. Но все же разработчики стремятся успеть и дать возможность антивирусу поместить файл хотя бы в карантин.

Рассмотрим несколько признаков зараженного ПК:

**1. Компьютер «разговаривает»:** появляется множество всплывающих окон и сообщений о том, что компьютер заражён, находится в опасности и нуждается в защите. Это верный признак того, что компьютер заражён, возможно, даже лже-антивирусом (иногда его называют «rogueware»).

**2. Компьютер работает слишком медленно:** это может быть признаком многих проблем, включая инфицирование компьютера вирусом. Если система заражена вирусом (например, трояном), то компьютер автоматически запускает много лишних программ. Из-за этого система работает значительно медленнее, чем обычно.

**3. Приложения не загружаются**, т.е. после нескольких попыток запустить приложения из меню или с рабочего стола, ничего не происходит. А может, вместо нужной открывалась совершенно другая программа? Как и в предыдущем случае, это еще не значит, что компьютер точно заражен. Возможно, причина в другом. Но, в любом случае, это сигнал, что что-то не так.

**4. Невозможно подключиться к интернет**у или он работает слишком медленно. Отсутствие подключения к интернету — еще один частый признак заражения компьютера (хотя, возможно, это просто перебои в работе провайдера). Также бывает, что интернет работает, но значительно медленнее, чем обычно. Если компьютер заражён, вирус может автоматически подключаться к интернету, снижая пропускную способность, или может сделать подключение к сети невозможным.

**5. При подключении к интернету открываются различные окна**, или браузер отображает страницы, которые пользователь не открывал. Это верный признак заражения. Многие вирусы перенаправляют трафик на определённые сайты против воли. Также они могут подделывать веб-страницы, тогда пользователь думает, что просматривает надёжный сайт, а на самом деле — его опасную имитацию.

**6. Куда делись файлы?** Хотелось бы, чтобы никто никогда не задал такой вопрос, хотя до сих пор существуют вирусы, которые удаляют, шифруют данные или переносят их из одного места в другое… Если такое произошло, есть повод для беспокойства.

**7. Антивирус исчез**, а брандмауэр заблокирован… Другой распространённый признак угрозы — блокировка системы защиты (антивируса, брандмауэра, и т.д.), которые установлены на компьютере. Однако нужно иметь в виду: если внезапно перестало работать только что-то одно, то, возможно, это — специфическая ошибка данного ПО. А если перестали работать все компоненты системы безопасности, то, скорей всего, компьютер заражен вирусом.

**8. Компьютер использует непонятный язык**. Если язык некоторых приложений поменялся, экран некорректно отображает файлы, компьютер точно заражён.

**9. Сохранённые файлы иг**р, программ и др. пропали из компьютера. Это опять же может быть признаком инфицирования вирусом. Хотя, возможно, причина заключается в неполной или неправильной установке программ.

**10. Компьютер буквально сошёл с ума!** Если компьютер действует сам по себе, система отправляет письма без ведома пользователя, разные сайты открываются самостоятельно, то компьютер инфицирован.

Итак, если ваш компьютер оказался все-таки зараженным следует сделать ряд последовательных шагов для предотвращения максимальной потери важных для вас данных.

1. Отключите компьютер от интернета.
2. Отключите компьютер от локальной сети, если он к ней был подключен.
3. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер.
4. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флэш-карту и пр.).
5. Установите Антивирус Касперского, Доктор Веб или НОД32 если вы этого еще не сделали. *(Все эти антивирусы можно устанавливать даже на зараженный компьютер).*
6. Обновите антивирусные базы. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы (*этот вариант предусматривает скачивание* ***кумулятивного*** *обновления (****одним файлом****)*). Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета.
7. Запустите полную проверку компьютера (кто-то не делает это со дня покупки антивируса), а еще лучше выполните "сканирование при загрузке" (такая опция есть в антивирусе AWAST).
8. Создайте еще одну учетную запись, но с ограниченными правами (не **"Администратор"**) и назовите ее, скажем, **"Интернет"**. Подавляющее число блокировщиков Windows или блокировщиков Рабочего стола не могут захватить контроль над компьютером если Вы работаете из ограниченной учетной записи
9. Установите рекомендуемый уровень настроек антивирусной программы.
10. Запустите полную проверку компьютера.

Данная схема проста, не следует поддаваться панике, нужно четко выполнить последовательные шаги.

**Обнаружение, основанное на сигнатурах** — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий:

Удалить инфицированный файл.

Отправить файл в «карантин» (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).

Попытаться восстановить файл, удалив сам вирус из тела файла.

Для достижения достаточно продолжительного успеха, при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями (в основном в онлайновом режиме).

Антивирусные программы, созданные на основе метода соответствия определению вирусов в словаре, обычно просматривают файлы тогда, когда компьютерная система создаёт, открывает, закрывает или посылает файлы по электронной почте. Таким образом, вирусы можно обнаружить сразу же после занесения их в компьютер и до того, как они смогут причинить какой-либо вред. Надо отметить, что системный администратор может составить график для антивирусной программы, согласно которому могут просматриваться (сканироваться) все файлы на жёстком диске.

## Недостатки и достоинства синтаксических сигнатур

* Позволяют определять конкретную атаку с высокой точностью и малой долей ложных вызовов
* Неспособны выявить какие-либо новые атаки
* Беззащитны перед полиморфными вирусами и изменёнными версиями того же вируса
* Требуют регулярного и крайне оперативного обновления
* Требуют кропотливого ручного анализа вирусов
* Метод эвристического сканирования призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные вирусы в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100%.
* Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний.

**Проактивные технологии** – совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе.

История развития проактивных технологий антивирусной защиты

Проактивные технологии начали развиваться практически одновременно с классическими (сигнатурными) технологиями. Однако, первые реализации проактивных технологий антивирусной защиты требовали высокий уровень квалификации пользователя, т.е. не были рассчитаны на массовое использование простыми пользователями персональных компьютеров. Спустя десятилетие антивирусной индустрии стало очевидно, что сигнатурные методы обнаружения уже не могут обеспечить эффективную защиту пользователей. Этот факт и подтолкнул к возрождению проактивных технологий.

**Технологии проактивной защиты**

**Эвристический анализ**

Технология эвристического анализа позволяет на основе анализа кода выполняемого приложения, скрипта или макроса обнаружить участки кода, отвечающие за вредоносную активность.  
Эффективность данной технологии не является высокой, что обусловлено большим количеством ложных срабатываний при повышении чувствительности анализатора, а также большим набором техник, используемых авторами вредоносного ПО для обхода эвристического компонента антивирусного ПО.

**Эмуляция кода**

Технология эмуляции позволяет запускать приложение в среде эмуляции, эмулируя поведение ОС или центрального процессора. При выполнении приложения в режиме эмуляции приложение не сможет нанести вреда системе пользователя, а вредоносное действие будет детектировано эмулятором.  
Несмотря на кажущуюся эффективность данного подхода, он также не лишен недостатков – эмуляция занимает слишком много времени и ресурсов компьютера пользователя, что негативно сказывается на быстродействии при выполнении повседневных операций, также, современные вредоносные программы способны обнаруживать выполнение в эмулированной среде и прекращать свое выполнение в ней.

**Анализ поведения**

Технология анализа поведения основывается на перехвате всех важных системных функций или установке т.н. мини-фильтров, что позволяет отслеживать всю активность в системе пользователя. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также, поведенческий анализ является технологической основой для целого класса программ – поведенческих блокираторов ([HIPS – Host-based Intrusion Systems](http://ru.wikipedia.org/wiki/HIPS)).

**Sandboxing (Песочница) – ограничение привилегий выполнения**

Технология Песочницы работает по принципу ограничения активности потенциально вредоносных приложений таким образом, чтобы они не могли нанести вреда системе пользователя.  
Ограничение активности достигается за счет выполнения неизвестных приложений в ограниченной среде – собственно песочнице, откуда приложение не имеет прав доступа к критическим системным файлам, веткам реестра и другой важной информации. Технология ограничения привилегий выполнения является эффективной технологией противодействия современным угрозам, но, следует понимать, что пользователь должен обладать знаниями, необходимыми для правильной оценки неизвестного приложения.

**Виртуализация рабочего окружения**

Технология виртуализации рабочего окружения работает с помощью системного драйвера, который перехватывает все запросы на запись на жесткий диск и вместо выполнения записи на реальный жесткий диск выполняет запись в специальную дисковую область – буфер. Таким образом, даже в том случае, если пользователь запустит вредоносное программное обеспечение, оно проживет не далее чем до очистки буфера, которая по умолчанию выполняется при выключении компьютера. Однако, следует понимать, что технология виртуализации рабочего окружения не сможет защитить от вредоносных программ, основной целью которых является кража конфиденциальной информации, т.к. доступ на чтение к жесткому диску не запрещен.

Применение проактивных технологий в настоящее время

В настоящее время проактивные технологии являются важным и неотъемлемым компонентом антивирусного программного обеспечения. Более того, как правило, в антивирусных продуктах используется сочетание сразу нескольких технологий проактивной защиты, например эвристический анализ и эмуляция кода успешно сочетаются с поведенческим анализом, что позволяет многократно повысить эффективность современных антивирусных продуктов против новых, все более и более изощренных вредоносных программ.

**Эвристический анализ (эвристическое сканирование)** — это совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ, но в то же время этот же термин обозначает один из конкретных способов.

|  |
| --- |
| Практически все современные антивирусные средства применяют технологию **эвристического анализа** программного кода. Эвристический анализ нередко используется совместно с сигнатурным сканированием для поиска сложных шифрующихся и полиморфныхвирусов. Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ |

**Технология эвристического анализа**

Методы эвристического сканирования не обеспечивают какой-либо гарантированной защиты от новых, отсутствующих в сигнатурном наборе компьютерных вирусов, что обусловлено использованием в качестве объекта анализа сигнатур ранее известных вирусов, а в качестве правил эвристической верификации — знаний о механизме полиморфизма сигнатур. В то же время, поскольку этот метод поиска базируется на эмпирических предположениях, полностью исключить ложные срабатывания нельзя.

В ряде случаев эвристические методы оказываются чрезвычайно успешными, к примеру, в случае очень коротких программных частей в загрузочном секторе: если программа производит запись в сектор 1, дорожку 0, сторону 0, то это приводит к изменению раздела накопителя. Но кроме вспомогательной программы [Fdisk](http://ru.wikipedia.org/wiki/Fdisk) эта команда больше нигде не используется, и потому в случае её неожиданного появления речь идёт о загрузочном вирусе.

В процессе эвристического анализа производится проверка эмулируемой программы анализатором кода. К примеру, программа инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика. Эмулятор кода считывает инструкции в буфер антивируса, разбирает их на инструкции и производит их исполнение по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет её с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала — программа определена.

**Недостатки эвристического сканирования**

Чрезмерная подозрительность эвристического анализатора может вызывать ложные срабатывания при наличии в программе фрагментов кода, выполняющего действия и/или последовательности, в том числе и свойственные некоторым вирусам. В частности, распаковщик в файлах, запакованных PE-упаковщиком (Win)Upack вызывает ложные срабатывания целого ряда антивирусных средств, не признающих такой проблемы.

Наличие простых методик обмана эвристического анализатора. Как правило, прежде чем распространять вредоносную программу (вирус), её разработчики исследуют существующие распространенные антивирусные продукты, различными методами избегая её детектирование при эвристическом сканировании. К примеру, видоизменяя код, используя элементы, выполнение которых не поддерживается эмулятором кода данных антивирусов, используя шифрование части кода и др.

Несмотря на заявления и рекламные проспекты разработчиков антивирусных средств относительно совершенствования эвристических механизмов, эффективность эвристического сканирования на данный момент далека от ожидаемой. Независимые тесты компонентов эвристического анализа показывают, что уровень обнаружения новых вредоносных программ составляет не более чем 40-50 % от их числа.[

Даже при успешном определении, лечение неизвестного вируса практически всегда является невозможным. Как исключение, некоторыми продуктами возможно лечение однотипных и ряда полиморфных, шифрующихся вирусов, не имеющих постоянного вирусного тела, но использующих единую методику внедрения. В таком случае, для лечения десятков и сотен вирусов может существовать одна запись в вирусной базе, как это реализовано, к примеру, в антивирусе И. Данилова.

1. Порядок выполнения работы
2. Составить алгоритмы обнаружения вредоносного ПО.
3. Составить алгоритм определения зараженного ПК.
4. Контрольные вопросы.
5. Перечислите алгоритмы обнаружения вредоносного ПО.
6. Как определить, что ПК заражен?
7. Как не допустить заражения ПК?
8. Сравните алгоритмы обнаружения вредоносного ПО. Сделайте вывод.
9. Содержание отчета
   1. Признаки зараженного ПК
   2. Алгоритмы поиска вредоносных программ
   3. Достоинства, недостатки каждой схемы

**Практическая работа № 15**

**«Схемы работы антивирусных программ»**

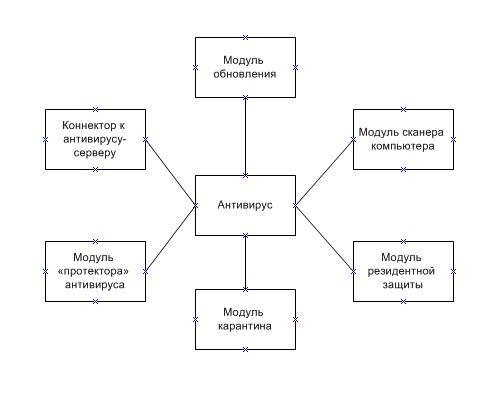
**Цель работы**. Получение практических навыков составления схем и изучение методов работы антивирусных программ.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

Современный *антивирус* является сложным программным средством, которое должно обеспечить надежную защиту компьютерного устройства ( компьютера, карманного компьютера или нетбука) от различных вирусов (зловредных программ). Общая схема *антивируса* представлена на рисунке 1



**Рисунок 1.** Схема антивируса

Как видно из схемы, *антивирус* состоит из следующих частей:

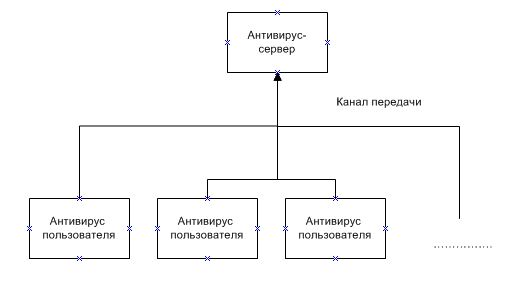
1. Модуль резидентной защиты
2. Модуль карантина
3. Модуль "протектора" *антивируса*
4. *Коннектор* к *антивирусу*-серверу
5. Модуль обновления
6. Модуль сканера компьютера

Модуль резидентной защиты является основным компонентом *антивируса*, находящийся в оперативной памяти компьютера и сканирующий в режиме реального времени все файлы, с которыми осуществляется взаимодействие пользователя, операционной системы или других программ. Слово "резидентный" означает "невидимый", "фоновый". Резидентная защита проявляет себя только при нахождении вируса. Именно на резидентной защите основывается главный принцип антивирусного ПО — предотвратить заражение компьютера. В ее состав входят такие компоненты, как активная защита (сравнение антивирусных сигнатур со сканируемым файлом и выявление известного вируса) и проактивная защита (совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе).

Модуль карантина является модулем, который отвечает за помещение подозрительных файлов в специальное место, именуемое карантином. Файлы, перемещенные в карантин, не имеют возможности выполнять какие-либо действия (они заблокированы) и находятся под наблюдением *антивируса*. *Антивирус* принимает решение поместить файл на карантин при обнаружении в файле признака вирусной деятельности (при этом сам файл с точки зрения *антивируса* вирусом в этом случае не является, просто файл является потенциальной угрозой), либо если файл действительно заражен вирусом, но его необходимо излечить, а не удалять целиком (например, важный документ пользователя, в который попал вирус). В последнем случае файл будет помещен в карантин для последующего излечения от вируса (если же *антивирус* не сможет вылечить файл, его придется удалить, либо оставить, в надежде на то, что с новым обновлением *антивирус* сможет вылечить этот файл). Обычно карантин создается в особой папке антивирусной программы, которая изолирована от каких-либо действий, кроме действий со стороны *антивируса*.

Модуль протектора *антивируса* является модулем, который защищает *антивирус* от стороннего вмешательства со стороны различных программных средств. Этот модуль является защитником *антивируса*. Часто вирусы хотят стереть *антивирус* или предотвратить его работу путем блокировки *антивируса*. Модуль протектора *антивируса* не даст это сделать. Впрочем, не все современные антивирусы снабжены качественными протекторами. Некоторые из них ничего не могут сделать против современных вирусов, а вирусы в свою очередь могут спокойно и беспрепятственно полностью стереть *антивирус*. Также появились вирусы, которые имитируют удаление *антивируса* со стороны пользователя, то есть протектор *антивируса* считает, что сам пользователь по каким-либо причинам хочет удалить *антивирус*, и поэтому не препятствует этому, хотя на самом деле это деятельность вируса. В настоящее время антивирусные компании стали более серьезно подходить к выпуску протекторов, и становится очевидно, что если *антивирус* не будет иметь хороший протектор, его эффективность в борьбе с вирусами будет очень мала.

*Коннектор* к *антивирусу*-серверу является важной частью *антивируса*. *Коннектор* служит для соединения *антивируса* к серверу, с которого *антивирус* может скачать актуальные базы с описанием новых вирусов. При этом соединение должно проходить по специальному защищенному Интернет-каналу. Это очень важный момент, так как злоумышленник может подложить неверные антивирусные базы с лживым описанием вирусов, если *антивирус* будет соединяться с сервером по незащищенному Интернет-каналу. Также в современных антивирусах *коннектор* служит еще и для соединения к специальному серверу, который управляет антивирусом. Подобное соединение изображено на рисунке ниже:



**Рисунок.2.** Схема присоединения к серверу

Как видно из рисунка, *коннектор* позволяет соединять множество антивирусов пользователей с единым антивирусом-сервером, с которого антивирусы пользователя могут скачивать обновления, а также если на стороне *антивируса* пользователя возникли какие-либо неразрешимые проблемы, то *антивирус*-сервер будет удаленно их решать (например, у *антивируса* пользователя стал неисправен какой-либо из модулей и *антивирус*-сервер предоставит этот модуль отдельно для скачивания). В этом случае также очень важную роль играет защищенность канала передачи (канала связи) информации. Со стороны злоумышленников стала применяться интересная практика, в результате которой захватывается контроль над самим каналом передачи информации, и фактически злоумышленник становится управляющим для антивирусов пользователя (для всех или частично, в зависимости от того, какой именно участок канала передачи будет перехвачен злоумышленником). В свою очередь, создатели антивирусов стали зашифровывать данные на канале информации, чтобы злоумышленник не мог получить к ним доступ и как-либо завладеть ими.

Модуль обновления отвечает за то, чтобы обновление *антивируса*, его отдельных частей, а также его антивирусных баз прошло правильно. В современной практике создания антивирусов стала применяться следующая идея: модуль обновления также должен определять подлинные или нет антивирусные базы скачивает сам модуль. Подлинность при этом может проверяться различными методами - от проверок контрольной суммы файла с базами до поиска внутри файла с базами специальной метки, которая говорит о том, что этот файл является подлинным. Подобные действия стали вводиться после того, как участились случаи подмены антивирусных баз со стороны злоумышленников.

Модуль сканера компьютера является, пожалуй, самым старым модулем в современных антивирусах, так как раньше антивирусы состояли только из этого модуля. Этот модуль отвечает за то, чтобы сканировать компьютер на наличие вирусов, если этого будет требовать пользователь компьютера. Сам модуль при сканировании компьютера использует антивирусные базы, которые были добыты с помощью модуля обновления *антивируса*. Если сканер найдет, но не справится с вирусом сразу же, то он поместит файл с вирусом в карантин. Потом, впоследствии, модуль сканера компьютера может связаться через *коннектор* с антивирусом-сервером и получить инструкции по обезвреживанию зараженного файла. Следует отметить, что модуль сканера компьютера предназначен для профилактики компьютера от вирусов, так как основную защиту представляет модуль резидентной защиты. В модуле сканера компьютера используются только антивирусные базы, в которых четко описаны вирусы. Различные элементы проактивной защиты (например, *эвристика*) не используются в модуле сканера компьютера. Обычно создатели вирусов не строят специальную защиту для своих вирусов от модулей сканера компьютера, так как знают, что пользователь не часто проверяет компьютер сканером, и этого промежуточного времени от проверки до проверки хватит, чтобы украсть *персональные данные* пользователя.

**Классификация антивирусных программ**

Классифицируются антивирусные программы на чистые антивирусы и антивирусы двойного назначения (рис. 2).

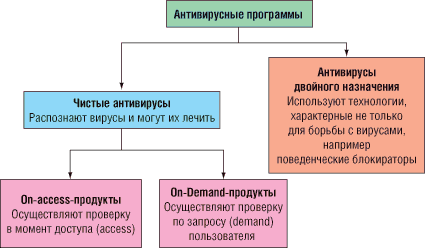


Рисунок 3. Схема классификации антивирусных программ

Чистые антивирусы отличаются наличием антивирусного ядра, которое выполняет функцию сканирования по образцам. Принципиальным в этом случае является то, что возможно лечение, если известен вирус. Чистые антивирусы, в свою очередь, по типу доступа к файлам подразделяются на две категории: осуществляющие контроль по доступу (onaccess) или по требованию пользователя (ondemand). Обычно onaccess-продукты называют мониторами, а ondemand-продукты — сканерами.

Оndemand-продукт работает по следующей схеме: пользователь хочет что-либо проверить и выдает запрос (demand), после чего осуществляется проверка. Onaccess-продукт — это резидентная программа, которая отслеживает доступ и в момент доступа осуществляет проверку.

Кроме того, антивирусные программы, так же как и вирусы, можно разделить в зависимости от платформы, внутри которой данный антивирус работает. В этом смысле наряду с Windows или Linux к платформам могут быть отнесены MicrosoftExchangeServer, MicrosoftOffice, LotusNotes.

Программы двойного назначения — это программы, используемые как в антивирусах, так и в ПО, которое антивирусом не является. Например, CRC-checker — ревизор изменений на основе контрольных сумм — может использоваться не только для ловли вирусов. Разновидностью программ двойного назначения являются поведенческие блокираторы, которые анализируют поведение других программ и при обнаружении подозрительных действий блокируют их. От классического антивируса с антивирусным ядром, распознающего и лечащего от вирусов, которые анализировались в лаборатории и которым был прописан алгоритм лечения, поведенческие блокираторы отличаются тем, что лечить от вирусов они не умеют, поскольку ничего о них не знают. Данное свойство блокираторов позволяет им работать с любыми вирусами, в том числе и с неизвестными. Это сегодня приобретает особую актуальность, поскольку распространители вирусов и антивирусов используют одни и те же каналы передачи данных, то есть Интернет. При этом антивирусной компании всегда нужно время на то, чтобы получить сам вирус, проанализировать его и написать соответствующие лечебные модули. Программы из группы двойного назначения как раз и позволяют блокировать распространение вируса до того момента, пока компания не напишет лечебный модуль.

1. Порядок выполнения работы
2. Составить схемы работы антивирусных программ.
3. Определить сложность работы антивирусных программ, объяснить с чем это связано.
4. Контрольные вопросы
5. Цель антивирусной программы?
6. Виды антивирусных программ?
7. Существуют ли другие методы защиты от вирусов?
8. Содержание отчета
9. Схемы работы антивирусных программ.
10. Анализ схем работы.
11. Вывод.

Практическая работа №16

«Выбор модели межсетевого экрана»

**Цель работы**: приобретение навыков выбора модели межсетевого экрана и схемы его подключения.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

Ряд задач по отражению наиболее вероятных угроз в том или ином объеме способны решать межсетевые экраны (firewalls). В российской литературе данный термин иногда переводится как брандмауэр, фаерволл, реже - межсетевой фильтр.

Межсетевой экран - это автоматизированная система или комплекс систем, позволяющая разделить сеть на две или более частей и обеспечивающая защитные механизмы от НСД на уровне пакетов обмена информацией сетевого, транспортного и прикладного уровней сетевых протоколов семиуровневой модели OSI.

На мировом рынке присутствуют около 50 различных межсетевых экранов, отличающихся платформами функционирования, производительностью и функциональными возможностями. Можно установить следующую **классификацию функциональных требований к межсетевым экранам**.

Функциональные требования к МЭ включают в себя:

* требования к фильтрации на сетевом уровне;
* требования к фильтрации на прикладном уровне;
* требования по ведению журналов и учету;
* требования по администрированию и настройке правил фильтрации;
* требования к средствам сетевой аутентификации.

Фильтрация на сетевом уровне

При фильтрации на сетевом уровне межсетевой экран принимает решение о пропуске пакета в/из защищаемой локальной сети из/в глобальной незащищенной сети. Данное решение МЭ принимает просматривая заголовок этого пакета и анализируя его содержимое. Решение о пропускании или запрещении прохождении пакета может зависеть от сетевых адресов источника и назначения пакета, номеров TCP-портов, времени и даты прохождения пакета и любых полей заголовка пакета.

Достоинствами данного вида фильтрации являются:

* небольшая задержка при прохождении пакетов,
* относительно невысокая стоимость МЭ.

К недостаткам данного вида фильтрации можно отнести:

* возможность просмотра структуры локальной сети из глобальной сети,
* возможность обхода системы защиты при использовании IP-спуфинга (IP-spoofing) - способ атаки, при котором атакующей стороной производится подстановка IP-адреса "разрешенного" сетевого узла в заголовок IP-пакета.

Фильтрация на прикладном уровне

При фильтрации на прикладном уровне решение о пропускании или запрещении прохождении пакета принимается после обработки запроса от клиента на программе-сервере конкретного сервера (WWW, Telnet, FTP, SMTP, Gopher и т.п.). Данный сервер носит название proxy-server (уполномоченный или доверенный сервер). Название "доверенный" - из-за того, что сервер, к которому производится обращение, доверяет proxy-серверу установить связь с клиентом, идентифицировать его и провести аутентификацию. Proxy-сервер пропускает через себя весь трафик, относящийся к данному сервису.

При принятии решения о пропускании и запрещении прохождения пакета proxy-сервер может использовать следующие параметры:

* имя пользователя;
* название сервиса;
* сетевое имя компьютера клиента;
* способ аутентификации;
* время и дата запроса.

Достоинствами данного способа фильтрации являются:

* невидимость структуры локальной сети из глобальной сети;
* возможность организации большого числа проверок, что повышает защищенность локальной сети;
* организация аутентификации на пользовательском уровне.

Основными недостатками данного способа маршрутизации являются низкая производительность обработки и высокая стоимость. Кроме того, при реализации данного способа фильтрации появляется сложность использования протоколов UDP и RPC.

*Ведение журналов и учет*

Ведение журналов, сбор статистики и ее учет является весьма важным компонентом межсетевого экрана. При помощи этих функциональных возможностей администратор может гибко определять политику реагирования на нарушения.

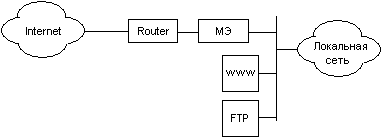
Существует большое количество **схем подключения межсетевых экранов**: - сколько администраторов безопасности - столько мнений. При этом все схемы подразделяются на:

1.стандартные схемы защиты отдельной локальной сети;

2.схемы включения в составе средств коллективной защиты.

Стандартные схемы защиты отдельной локальной сети

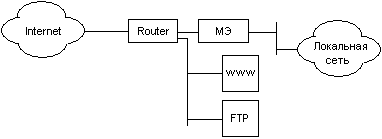
Наиболее простым является решение, при котором межсетевой экран просто экранирует локальную сеть от глобальной. При этом WWW-сервер, FTP-сервер, почтовый сервер и другие сервера, оказываются также защищены межсетевым экраном (см. Рис.1.). При этом требуется уделить много внимания на предотвращение проникновения на защищаемые станции локальной сети при помощи средств легкодоступных WWW-серверов.



*Рисунок 1. Простое включение МЭ*

Для предотвращения доступа в локальную сеть, используя ресурсы WWW-сервера, рекомендуется общедоступные серверы подключать перед межсетевым экраном, так как показано на рисунке 2. Данный способ обладает более высокой защищенностью локальной сети, но низким уровнем защищенности WWW- и FTP-серверов.

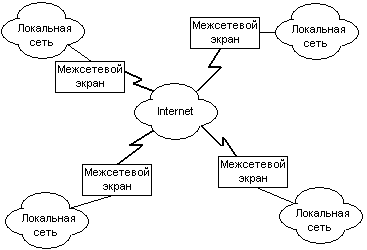
Оба вышеприведенных случая показаны для межсетевых экранов, имеющих два сетевых интерфейса. Межсетевые экраны с одним сетевым интерфейсом существуют, но их настройка, а также настройка маршрутизаторов для работы с таким межсетевым экраном, представляет собой сложную задачу, с ценой решения превышающей стоимость замены МЭ с одним интерфейсом на МЭ с двумя сетевыми интерфейсами. Поэтому, схемы подключения межсетевых экранов с одним сетевым интерфейсом в данной статье не рассматриваются.



*Рисунок 2. Подключение МЭ с вынесением общедоступных серверов*

Применение в составе средств коллективной защиты

Некоторые межсетевые экраны позволяют организовывать виртуальные корпоративные сети (Virtual Private Network). При этом несколько локальных сетей, подключенных к глобальной сети, объединяются в одну виртуальную корпоративную сеть. Передача данных между этими локальными сетями производится прозрачно для пользователей локальных сетей. При этом обеспечивается конфиденциальность и целостность передаваемой информации при помощи различных средств: шифрования, использования цифровых подписей и т.п. При передаче может шифроваться не только содержимое пакета, но и его заголовок, включая все, входящие в него поля. Возможная схема использования межсетевых экранов в составе виртуальных корпоративных сетей приведена на рисунке 3.



*Рисунок 3. Построение виртуальной корпоративной сети*

Основные способы развертывания межсетевых экранов в корпоративных сетях

При подключении корпоративной или локальной сети к глобальным сетям администратор сетевой безопасности должен решать следующие задачи:

• защита корпоративной или локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;

• скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;

• разграничение доступа в защищаемую сеть из глобальной и из защищаемой сети в глобальную.

Необходимость работы с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети. При этом в организации часто возникает потребность иметь в составе корпоративной сети несколько сегментов с разными уровнями защищенности:

• свободно доступные сегменты;

• сегменты с ограниченным доступом;

• закрытые сегменты.

Для защиты корпоративной или локальной сети применяются следующие **основные схемы организации межсетевых экранов**:

1. Межсетевой экран, представленный как фильтрующий маршрутизатор.

2. Межсетевой экран на основе двухпортового шлюза.

3. Межсетевой экран на основе экранированного шлюза.

4. Межсетевой экран с экранированной подсетью.

МЕЖСЕТЕВОЙ ЭКРАН, ПРЕДСТАВЛЕННЫЙ КАК ФИЛЬТРУЮЩИЙ МАРШРУТИЗАТОР

Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации, представляя собой фильтрующий маршрутизатор, расположенный между защищаемой сетью и Интернетом.

Фильтрующий маршрутизатор сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов.

Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в Интернет, в то время как большая часть доступа к ним из Интернета блокируется. В принципе, фильтрующий маршрутизатор может реализовать любую из политик безопасности, описанных ранее. Однако если маршрутизатор не фильтрует пакеты по порту источника и номеру входного и выходного порта, то реализация политики «запрещено все, что не разрешено» в явной форме может быть затруднена.

Межсетевые экраны, основанные на фильтрации пакетов, имеют те же недостатки, что и фильтрующие маршрутизаторы.

МЕЖСЕТЕВОЙ ЭКРАН НА ОСНОВЕ ДВУХПОРТОВОГО ШЛЮЗА

Межсетевой экран на базе двухпортового прикладного шлюза представляет собой хост с двумя сетевыми интерфейсами. При передаче информации между этими интерфейсами и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между прикладным шлюзом и Интернетом размещают фильтрующий маршрутизатор. В результате между прикладным шлюзом и маршрутизатором образуется внутренняя экранированная подсеть. Ее можно использовать для размещения доступного извне информационного сервера. Размещение информационного сервера увеличивает безопасность сети, поскольку даже при проникновении на него злоумышленник не сможет получить доступ к системам сети через шлюз с двумя интерфейсами.

В отличие от схемы межсетевого экрана с фильтрующим маршрутизатором, прикладной шлюз полностью блокирует трафик IP между Интернетом и защищаемой сетью. Только уполномоченные приложения, расположенные на прикладном шлюзе, могут предоставлять услуги и доступ пользователям.

Данный вариант межсетевого экрана реализует политику безопасности, основанную на принципе «запрещено все, что не разрешено в явной форме»; при этом пользователю доступны только те службы, для которых определены соответствующие полномочия. Такой подход обеспечивает высокий уровень безопасности, поскольку маршруты к защищенной подсети известны лишь межсетевому экрану и скрыты от внешних систем.

Рассматриваемая схема организации межсетевого экрана относительно проста и достаточно эффективна. Поскольку межсетевой экран использует хост, то на нем могут быть установлены программы для усиленной аутентификации пользователей. Межсетевой экран может также протоколировать доступ, попытки зондирования и атак системы, что позволяет выявить действия злоумышленников.

МЕЖСЕТЕВОЙ ЭКРАН НА ОСНОВЕ ЭКРАНИРОВАННОГО ШЛЮЗА

Межсетевой экран на основе экранированного шлюза обладает большей гибкостью по сравнению с межсетевым экраном, построенным на основе шлюза с двумя интерфейсами, однако эта гибкость достигается ценой некоторого уменьшения безопасности. Межсетевой экран состоит из фильтрующего маршрутизатора и прикладного шлюза, размещаемого со стороны внутренней сети. Прикладной шлюз реализуется на хосте и имеет только один сетевой интерфейс.

В данной схеме первичная безопасность обеспечивается фильтрующим маршрутизатором, который фильтрует или блокирует потенциально опасные протоколы, чтобы они не достигли прикладного шлюза и внутренних систем. Пакетная фильтрация в фильтрующем маршрутизаторе может быть реализована одним из следующих способов:

• внутренним хостам позволяется открывать соединения с хостами в сети Интернет для определенных сервисов (доступ к ним разрешается среде пакетной фильтрации);

• запрещаются все соединения от внутренних хостов (им надлежит использовать уполномоченные приложения на прикладном шлюзе).

В подобной конфигурации межсетевой экран может использовать комбинацию двух политик, соотношение между которыми зависит от конкретной политики безопасности, принятой во внутренней сети. В частности, пакетная фильтрация на фильтрующем маршрутизаторе может быть организована таким образом, чтобы прикладной шлюз, используя свои уполномоченные приложения, обеспечивал для систем защищаемой сети сервисы типа Telnet, FTP, SMTP.

Основной недостаток схемы межсетевого экрана с экранированным шлюзом заключается в том, что если атакующий нарушитель сумеет проникнуть в хост, перед ним окажутся незащищенными системы внутренней сети. Другой недостаток связан с возможной компрометацией маршрутизатора. Если маршрутизатор окажется скомпрометированным, внутренняя сеть станет доступна атакующему нарушителю.

МЕЖСЕТЕВОЙ ЭКРАН С ЭКРАНИРОВАННОЙ ПОДСЕТЬЮ

Межсетевой экран, состоящий из экранированной подсети, представляет собой развитие схемы межсетевого экрана на основе экранированного шлюза. Для создания экранированной подсети используются два экранирующих маршрутизатора. Внешний маршрутизатор располагается между Интернетом и экранируемой подсетью, а внутренний — между экранируемой подсетью и защищаемой внутренней сетью. В экранируемую подсеть входит прикладной шлюз, а также могут включаться информационные серверы и другие системы, требующие контролируемого доступа. Эта схема межсетевого экрана обеспечивает высокий уровень безопасности благодаря организации экранированной подсети, которая еще лучше изолирует внутреннюю защищаемую сеть от Интернета.

Внешний маршрутизатор защищает от вторжений из Интернета как экранированную подсеть, так и внутреннюю сеть. Внешний маршрутизатор запрещает доступ из Глобальной сети к системам внутренней сети и блокирует весь трафик к Интернету, идущий от систем, которые не должны являться инициаторами соединений.

Этот маршрутизатор может быть использован также для блокирования других уязвимых протоколов, которые не должны передаваться к хост-компьютерам внутренней сети или от них.

Внутренний маршрутизатор защищает внутреннюю сеть от несанкционированного доступа как из Интернета, так и внутри экранированной подсети. Кроме того, он осуществляет большую часть пакетной фильтрации, а также управляет трафиком к системам внутренней сети и от них.

Межсетевой экран с экранированной подсетью хорошо подходит для защиты сетей с большими объемами трафика или с высокими скоростями обмена.

К его недостаткам можно отнести то, что пара фильтрующих маршрутизаторов нуждается в большом внимании для обеспечения необходимого уровня безопасности, поскольку из-за ошибок в их конфигурировании могут возникнуть провалы в системе безопасности всей сети. Кроме того, существует принципиальная возможность доступа в обход прикладного шлюза.

1. Порядок выполнения работы
2. Выполнить анализ работы МЭ.
3. Составить алгоритмы работы МЭ.
4. Контрольные вопросы.
5. Какие бывают схемы включения МЭ?
6. Какая схема включения чаще всего используется в домашней сети?
7. Какая схема может использоваться в сети колледжа?
8. Содержание отчета
9. Наименование и цель работы.
10. Оснащение занятия.
11. Классификацию функциональных требований.
12. Схемы подключения МЭ.
13. Виды межсетевых экранов.
14. Алгоритмы работы МЭ

Практическая работа № 17.

«Защита удаленного доступа»

**Цель работы:** изучить параметры удаленного доступа и меры по его защите.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

**Удаленный доступ** - технология взаимодействия абонентских систем с локальными сетями через территориальные коммуникационные сети. Удаленный доступ осуществляется посредством сервера удаленного доступа. При удаленном доступе используются модели "дистанционного управления" и "удаленной системы".

Предоставление удаленного доступа к локальной сети является обычной практикой для многих организаций. Преимущества такого подхода очевидны – возможность работы с корпоративной почтой, данными и приложениями во время отпуска, командировки, презентации или на переговорах увеличивает производительность труда сотрудников и повышает эффективность бизнес-процессов. Временное подключение к ресурсам организации может потребоваться клиентам, деловым партнерам или проектному/сезонному персоналу. В тоже время сама возможность удаленных подключений оказывает значительное влияние на уровень информационной безопасности организации – неправильная конфигурация системы доступа или разглашение учетных данных пользователей могут привести к утечке конфиденциальной информации и нарушению работоспособности критичных приложений. Кроме того, подключаемые устройства в большинстве случаев являются "недоверенными" и не контролируются службой безопасности, поэтому вирусы, трояны и другое вредоносное программное обеспечение могут легко проникнуть в корпоративную инфраструктуру в обход средств защиты периметра сети.

Стандартные средства удаленного доступа, встроенные в операционные системы или межсетевые экраны, не обеспечивают мобильность подключений, гибкое разграничение прав доступа и проверку состояния защищенности устройств, а также не позволяют получить детальную статистику и отчетность по установленным соединениям.

Для решения указанных проблем и обеспечения эффективной защиты удаленного доступа применяются отдельные устройства, основанные на технологии построения виртуальных сетей (VPN) поверх протокола SSL.

Специализированные SSL VPN шлюзы обладают следующими возможностями:

* безопасное подключение к корпоративной сети с любого места и любого устройства;
* поддержка работы как через стандартный браузер, так и через клиентский модуль;
* управление политиками доступа по пользователям, группам, устройствам и ресурсам;
* контроль состояния защищенности подключаемых устройств;
* отказоустойчивость и распределение нагрузки;
* надежная аутентификация и подробная отчетность.

Применение устройств, обеспечивающих многофакторную аутентификацию (например, смарт-карты или USB/OTP токены), совместно с SSL VPN решениями значительно снижает риск неавторизованного доступа к корпоративной сети и обеспечивает необходимый уровень информационной безопасности организации.

Технологию SSL VPN можно использовать не только для классического удаленного доступа, но и в других ситуациях, требующих защищенного подключения к Web приложениям. Например, применение решений на основе SSL VPN в инфраструктуре терминальных серверов позволяет:

* подключаться к терминальным серверам по протоколу HTTPS;
* аутентифицировать пользователей посредством одноразовых паролей;
* определять допустимое время и продолжительность терминальных сессий;
* проводить аудит трафика «тонких» клиентов;
* проверять наличие актуального антивируса и критических обновлений на подключаемых устройствах.

Cовременные SSL VPN устройства являются наиболее эффективным и безопасным способом подключения удаленных/мобильных пользователей, бизнес партнеров или клиентов к корпоративным ресурсам организации.

Объекты логической идентификации и аутентификации:

* человек (пользователь, оператор, должностное лицо;
* техническое средство (компьютер, терминал);
* документы;
* машинные носители информации;
* информация на дисплее (табло).

Взаимная проверка подлинности полномочий:

* пользователь - администратор;
* пользователь - ресурс;
* пользователь - аппаратная среда;
* пользователь - программа.

Способы передачи пароля по сети:

* в открытом виде (TELNET, FTP);
* в зашифрованном виде;
* в виде свертки (хэш-функция);
* в виде "доказательства с нулевым разглашением" .

Способы обмана при передаче сообщения:

* отказ отправителя от посланного сообщения (ренегатство или отступничество);
* подмена сообщения в пункте приема с выдачей его за подлинное;
* имитация принятия сообщения в пункте приема при его фактическом отсутствии;
* повтор нарушителем ранее перехваченного сообщения.

Задача комплексной идентификации состоит в том, чтобы установить:

* имеет ли пользователь необходимые права доступа к компьютерной информации;
* попадет ли информация, вводимая полномочным пользователем, по своему адресу и будет ли обработана доверенным устройством;
* принадлежит ли электронные документы владельцу, не производилось ли их намеренное или случайное искажение;
* не содержит ли компьютерная программа вредоносных фрагментов.

Способы идентификации данных:

* кодирование с обнаружением ошибок (контрольные суммы);
* кодирование с устранением одиночных и групповых ошибок;
* электронная цифровая подпись (ЭЦП).

Способы проверки аппаратуры и каналов связи:

* использование протокола приема-передачи с квитированием ;
* идентификация аппаратных узлов удаленной информационной системы на программном уровне ;
* контроль за маршрутом сообщений ОТКС;
* использование виртуальных защищенных каналов.;
* процедуры "рукопожатий" и др.

Способы аутентификации личности:

* парольные системы;
* биометрические признаки;
* физические носители аутентифицирующей информации.

1. Порядок выполнения работы
2. Составить алгоритм работы удаленного доступа.
3. Проанализировать возможности протоколов.
4. Контрольные вопросы.
5. Для чего применяют удаленный доступ?
6. Что такое SSL VPN шлюзы?
7. Что позволяет применение решений на основе SSL VPN в инфраструктуре терминальных сереверов?
8. Что такое «тонкий клиент»?
9. Что такое аутентификация, идентификация?
10. Перечислите способы обмана при передаче сообщения.
11. В чем состоит задача комплексной идентификации?
12. Для чего необходимо ведение журналов?
13. Содержание отчета:
14. Определение удаленного доступа.
15. Алгоритм работы удаленного доступа.
16. Возможности SSL VPN шлюзов.
17. Объекты логической идентификации и аутентификации.
18. Способы передачи пароля по сети.

Практическая работа № 18

«Технологии обнаружения и предотвращения вторжений»

**Цель работы**. Получение навыков обнаружения вторжений и изучение методов их предотвращения.

1. Оснащение занятия

* методические рекомендации;
* персональный компьютер.

1. Общие положения

Продукты по обнаружению атак используются в качестве дополнения к существующей системе защиты информации, позволяя обнаруживать злоумышленные действия, направленные против ИС. Что дает возможность администраторам своевременно реагировать на вновь возникающие угрозы. Поэтому основным критерием для выбора метода обнаружения атак является его способность обнаруживать вновь возникающие атаки или типы атак, т.е. его адаптивность.

Выделяют следующие методы обнаружения атак на ИС:

* анализ систем состояний;
* графы сценариев атак;
* экспертные системы;
* методы, основанные на спецификациях;
* сигнатурные методы;
* нейронные сети;
* иммунные сети;
* статистический анализ;
* кластерный анализ;
* поведенческая биометрия.

**Анализ систем состояний.** В данной группе методов функционирование защищаемой системы представляется через множество состояний и множество переходов между ними, т.е. в виде ориентированного графа (как правило, бесконечного). Суть метода обнаружения атак заключается в том, что часть путей в таком графе помечаются как недопустимые; конечное состояние каждого такого пути считается опасным для защищаемой системы. Процесс обнаружения атаки представляет собой построение части графа состояний системы и наблюдаемых переходов между ними, и поиск в полученном графе известных недопустимых путей. Обнаружение последовательности переходов, приводящей в опасное состояние, означает успешное обнаружение атаки. Существуют определенные трудности построения подобной системы.

**Графы сценариев атак.** Метод заключается в обнаружении атак на основе использования методов формальной спецификации на моделях. На вход системе верификации подаётся конечная модель защищаемой системы и некоторое формальное свойство корректности, которое выполняется только для разрешённого поведения системы. Данное свойство корректности делит всё множество поведений на два класса: допустимое поведение, для которого свойство выполняется, и недопустимое, для которого оно не выполняется.

Отличие данного метода от обычных систем верификации заключается в том, что их задача, обычно, найти один контрпример из множества недопустимого поведения, а в предложенном методе строится полный набор таких примеров для конкретной защищаемой системы, что даёт на выходе описание возможных путей атаки. Из-за высокой вычислительной сложности (NP) данный метод может быть использован для поиска уязвимостей проектирования систем и других сложных для обнаружения уязвимостей, но для задачи обнаружения атак в реальном времени он неприменим.

**Экспертные системы.** Использование экспертных систем для обнаружения атак основано на описании функционирования системы в виде множества фактов и правил вывода, в том числе для атак. На вход экспертная система получает данные о наблюдаемых событиях в системе в виде фактов. На основании фактов и правил вывода система делает вывод о наличии или отсутствии атаки. Данная группа методов в общем случае имеет очень большую вычислительную сложность, так как для нее может наблюдаться полный перебор большого числа альтернатив.

**Методы, основанные на спецификациях.** В основе данного метода лежит описание ограничений на запрещенное поведение объектов в защищаемой системе в виде спецификаций атак. В спецификацию может входить: ограничения на загрузку ресурсов, на список запрещенных операций и их последовательностей, на время суток, в течение которого применимы те или иные ограничения. Соответствие поведения спецификации считается атакой. Основным недостатком является сложность разработки спецификаций.

**Сигнатурные методы.** Наиболее часто используемая группа методов, суть которых заключается в составлении некоторого алфавита из наблюдаемых в системе событий и описании множества сигнатур атак в виде регулярных выражений (в общем случае) в построенном алфавите. Как правило, сигнатурные методы работают на самом низком уровне абстракции и анализируют непосредственно передаваемые по сети данные, параметры системных вызовов и записи файлов журналов. В наиболее развитом виде представляет собой реализацию регулярных выражений над различными трассами (сетевой трафик, системные вызовы, записи журналов приложений и т.п.). Сигнатурные методы примечательны тем, что для них хорошо применимы аппаратные ускорители. [10]

Кроме отмеченных недостатков все вышеперечисленные методы не являются адаптивными, а значит не подходят для обнаружения новых атак и новых видов уже существующих атак.

Однако существуют и адаптивные методы обнаружения атак.

**Нейронные сети.** Так как задачу обнаружения атак можно рассматривать как задачу распознавания образов (или задачу классификации), то для её решения также применяются нейронные сети. Для этого функционирование защищаемой системы и взаимодействующих с ней внешних объектов представляется в виде траекторий в некотором числовом пространстве признаков. В качестве метода обнаружения злоупотреблений, нейронные сети обучаются на примерах атак каждого класса и, в дальнейшем, используются для распознавания принадлежности наблюдаемого поведения одному из классов атак. Основная сложность в использовании нейросетей заключается в корректном построении такого пространства признаков, которое позволило бы разделить классы атак между собой и отделить их от нормального поведения.

Нейронные сети для обнаружения аномалий обучаются в течение некоторого периода времени, когда всё наблюдаемое поведение считается нормальным. После обучения нейронная сеть запускается в режиме распознавания. В ситуации, когда во входном потоке не удается распознать нормальное поведение, фиксируется факт атаки. В случае использования репрезентативной обучающей выборки нейронные сети дают хорошую устойчивость в пределах заданной системы; но составление подобной выборки является серьёзной и сложной задачей.

**Иммунные сети.** Также как и нейронные сети, иммунные сети являются механизмом классификации и строятся по аналогии с иммунной системой живого организма. Основное достоинство иммунных сетей заключатся в возможности получения «антител» к неизвестным атакам. В работе [12] предложена модель формального пептида, для которой заявлена возможность использования в системах обнаружения атак. Однако позже было показано, что использование данного метода требует решения системы дифференциальных уравнений в режиме обнаружения, что даёт вычислительную сложность порядка O(n3) при использовании метода Рунге-Кутта. Данный метод имеет большую вычислительную сложность. [13]

**Статистический анализ.** Данная группа методов основана на построении статистического профиля поведения системы в течение некоторого периода «обучения», при котором поведение системы считается нормальным. Для каждого параметра функционирования системы строится интервал допустимых значений, с использованием некоторого известного закона распределения. Далее, в режиме обнаружения, система оценивает отклонения наблюдаемых значений от значений, полученных во время обучения. Если отклонения превышают некоторые заданные значения, то фиксируется факт аномалии (атаки). Для статистического анализа характерен высокий уровень ложных срабатываний при использовании в локальных сетях, где поведение объектов не имеет гладкого, усреднённого характера.

**Кластерный анализ.** Суть данной группы методов состоит в разбиении множества наблюдаемых векторов-свойств системы на кластеры, среди которых выделяют кластеры нормального поведения. В каждом конкретном методе кластерного анализа используется своя метрика, которая позволяет оценивать принадлежность наблюдаемого вектора свойств системы одному из кластеров или выход за границы известных кластеров. Сходен по своей сути со статистическим анализом.

**Поведенческая биометрия.** Включает в себя методы, не требующие специального оборудования (сканеров сетчатки, отпечатков пальцев), т.е. методы обнаружения атак, основанные на наблюдения клавиатурного почерка и использования мыши. В основе методов лежит гипотеза о различии «почерка» работы с интерфейсами ввода-вывода для различных пользователей. На базе построенного профиля нормального поведения для данного пользователя обнаруживаются отклонения от этого профиля, вызванные попытками других лиц работать с клавиатурой или другими физическими устройствами ввода.

Все перечисленные методы второй группы (нейронные сети, иммунные сети, статистический анализ, кластерный анализ, поведенческая биометрия) являются адаптивными и обладают примерно одинаковой вычислительной сложностью. Самым перспективным и развивающимся является метод с использованием нейронных сетей. Существуют различные программные продукты, позволяющие обучить и в последствии использовать полученные нейронные сети. Поэтому данный метод выбирается для задачи адаптивного обнаружения атак.

1. Порядок выполнения работы
2. Составить схемы вторжений.
3. Определить методы обнаружения.
4. Контрольные вопросы
5. Что такое «вторжение»?
6. Какие существуют схемы вторжений?
7. Какие существуют методы обнаружения?

Содержание отчета

1. Схемы видов вторжений.
2. Анализ схем работы.
3. Способы обнаружения.
4. Привести пример.

**Информационное обеспечение обучения**

Основные источники:

1. Мельников В.П. Информационная безопасность: учебник / В.П. Мельников, А.И. Куприянов; под ред. В.П. Мельникова. - 2-е изд., перераб. и дпо. - Москва: КНОРУС, 2018. - 268 с. - (Среднее профессиональное образование)
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Москва : Питер, 2020. – 992 с. : ил. – (Учебник для вузов. Стандарт третьего поколения).

Дополнительные источники:

1. Олифер, В.Г. Основы сетей передачи данных [Электронный ресурс] : учебное пособие / В.Г. Олифер, Н.А. Олифер. — Электрон. дан. — Москва : , 2016. — 219 с. — Режим доступа: https://e.lanbook.com/book/100346.