РАЗДЕЛ 2. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лабораторная работа №1 Защита документов MS Office

Цель: изучить методы защиты документов MS Office, правила создания сложных паролей

Защита документов в MS Office

Защита информации (ЗИ) - меры для ограничения доступа к информации для каких-либо лиц (категорий лиц), а также для удостоверения подлинности и неизменности информации.

Установка пароля для открытия и изменения документа, книги или презентации MS Office 2007

Предполагаемое действие:

- ✓ Шифрование документа и задание пароля для его открытия
- ✓ Задание пароля для изменения документа
- ✓ Шифрование книги и задание пароля для ее открытия
- ✓ Задание пароля для изменения книги
- ✓ Шифрование презентации и задание пароля для ее открытия
- ✓ Задание пароля для изменения презентации
- ✓ Изменение пароля
- ✓ Удаление пароля

Шифрование документа и задание пароля для его открытия

Чтобы зашифровать файл и задать пароль для его открытия, выполните действия:

1. Нажмите кнопку **MS Office**  , наведите указатель мыши на пункт **Подготовить** и выберите пункт **Зашифровать документ**.
2. В диалоговом окне **Шифрование документа** введите пароль в поле **Пароль** и нажмите кнопку **ОК**.

Можно ввести до 255 знаков. По умолчанию в этой функции применяется усиленное 128-разрядное шифрование. Шифрование – это стандартный метод, используемый для защиты файлов.

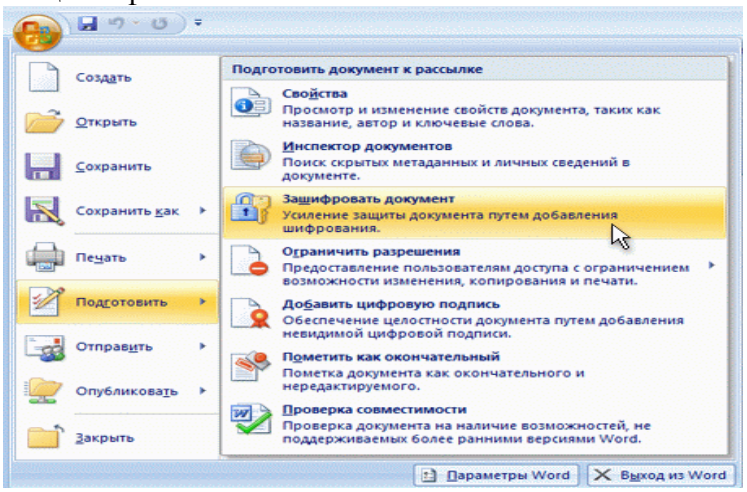


Рис. 1. Меню кнопки MS Office

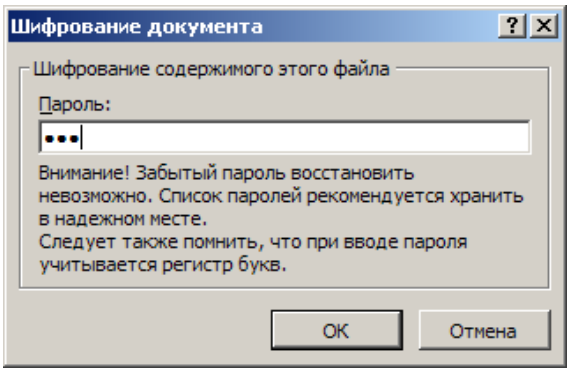


Рис. 2 Диалоговое окно Шифрование документа

3. В диалоговом окне **Подтверждение пароля** введите пароль еще раз в поле **Подтверждение** и нажмите кнопку **ОК**.

Чтобы сохранить пароль, сохраните файл.

Задание пароля для изменения документа

Чтобы обеспечить возможность изменения содержимоготолько авторизованными рецензентами, выполните действия:

1. Нажмите кнопку **MS Office** , а затем выберите команду **Сохранить как**.
2. Щелкните пункт **Сервис**, а затем выберите **Общие параметры**.

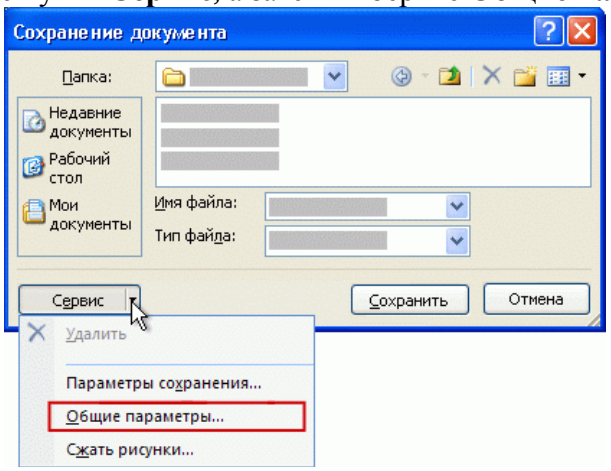


Рис. 3. Окно Сохранение документа

3. Выполните одно или оба следующих действия:

✓ Если нужно, чтобы рецензенты вводили пароль перед просмотром документа, введите пароль в поле **Пароль для открытия**. По умолчанию при этом используется расширенное шифрование, но в отличие от команды **Зашифровать документ**, описанной выше, в этом случае можно ввести только до 15 знаков.

✓ Если нужно, чтобы рецензенты вводили пароль перед сохранением внесенных в документ изменений, введите пароль в поле **Пароль разрешения записи**. При этом шифрование не используется. Эта функция предназначена для сотрудничества с рецензентами, которым вы доверяете, а не для

защиты файлов.

Примечание: можно назначить оба пароля — один для доступа к файлу, а другой — для разрешения определенным рецензентам изменять его содержимое. Убедитесь, что эти пароли различны.

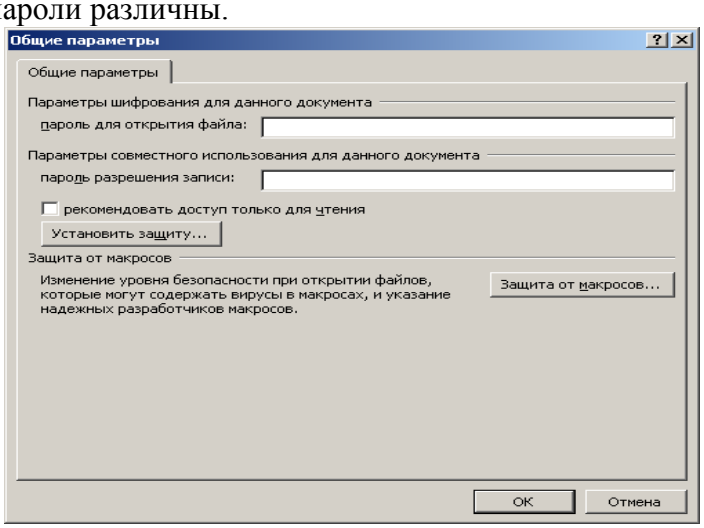


Рис. 4. Диалоговое окно задания пароля

4. Чтобы предотвратить случайное изменение файла рецензентами, установите флажок **рекомендовать доступ только для чтения**. При открытии файла рецензентам будет предложено открыть его в режиме «только для чтения».
5. Нажмите кнопку **ОК**.
6. При запросе подтвердите пароль введите его еще раз, а затем нажмите кнопку **ОК**.

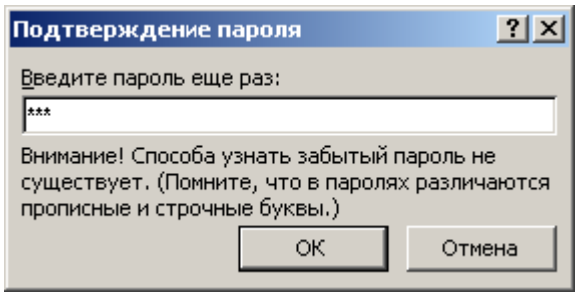


Рис. 5. Окно подтверждения пароля

7. В диалоговом окне **Сохранить как** нажмите кнопку **Сохранить**.
8. Если последует приглашение, нажмите кнопку **Да,** чтобы заменить существующий документ.

Задание 1. Изменение пароля в документах

- ✓ Измените ранее установленные пароли в документах.
- ✓ Выполните конспект в тетради.
- ✓ Удалите пароль в одном из документов.

Создание надёжных паролей

Пароли обычно являются самым слабым звеном в системе безопасности ПК. Надежность паролей играет важную роль, потому что для взлома паролей используются все более изощренные программы и мощные компьютеры.

Надежный пароль должен отвечать следующим требованиям:

- ✓ пароль должен состоять не менее чем из восьми знаков
- ✓ должен содержать знаки, относящиеся к каждой из следующих трех групп:

Группа	**Примеры**
Буквы (прописные и строчные)	A, B, C... (a, b, c...)
Цифры	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Символы (все знаки, не являющиеся буквами или цифрами)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] / : " ; ' < > ? , . /

- ✓ должен содержать не менее одного символа
- ✓ должен значительно отличаться от паролей, использовавшихся ранее
- ✓ не должен содержать фамилии или имени пользователя или быть распространённым словом

Удовлетворяемый этим требованиям пароль подобрать уже не так просто. Часто для этого требуются недели и даже месяцы. Но если злоумышленник располагает неограниченным временем, то он вскроет этот пароль. Поэтому следует изменять его до того, как он это сделает. Рекомендуется делать это **не реже одного раза за три месяца.** Если есть подозрение, что кто-то подобрал пароль — смените его немедленно.

Надёжные и сложные пароли можно придумывать самим, а можно воспользоваться генераторами паролей. Их можно найти в Интернете в большом количестве, создав запрос поиска «password generator».

Задание 2. Создание сложных паролей вручную

- ✓ Придумайте несколько (минимум три) сложных паролей. Запишите их.
- ✓ Изучите список 10 сложных паролей, найденных в Интернете:

SwIG6)/^	***/5Ns6I.**	**VKO!*N$k**
0(qDxuX(	**1>/8+DT6**	**hRT..)]R 4WS7Z#iY**
Dm>OoCe=	**>f!#qrX.**	**L!OiEopf**

- ✓ Сравните придуманные вами и сгенерированные пароли. Какие легче запоминаются и лучше удовлетворяют требованиям безопасности? Выводы запишите в тетрадь

Контрольные вопросы:

1. Опишите алгоритм задания пароля на открытие документа в MS Word
2. Опишите алгоритм задания пароля на изменение документа в MS Word
3. Опишите алгоритм задания пароля на открытие книги в MS Excel
4. Как защитить ячейку, лист, скрыть лист?
5. Как отменить пароли в документах MS Word, MS Excel?
6. Как установить пароли (на открытие, на изменение) в документах MS Office 2007 и 2010?
7. Перечислите правила создания паролей

Лабораторная работа №2
Работа с программой вскрытия паролей AZPR

Цель: изучить возможности защиты архива паролем, научиться использовать программу вскрытия паролей Advanced ZIP Password Recovery

Проблема: забытые пароли

Если вы будете честно следовать правилам установки паролей, то вскоре начнёте их путать и забывать. Windows берёт часть работы на себя. Он запомнит, если вы захотите, логины и пароли на веб-сайтах, сохранит ключи шифрования, электронные сертификаты. Единственное, что вам необходимо помнить — это ваши имя пользователя и пароль. Пользователь в Windows сам управляет своими паролями. При утере пароля администратор, конечно, может присвоить новый пароль. Но при этом вы потеряете доступ ко всем вашим зашифрованным данным и сертификатам.

Если требуется восстановить утерянный пароль (либо проверить насколько уязвимым по отношению к атакам является компьютер), можно воспользоваться программами восстановления паролей. Они различаются по методам взлома (атаки со словарём, извлечение хэшей паролей из базы данных SAM или, что ещё лучше, извлечение подобной информации из памяти, грубый перебор всех вариантов) и способом работы (после загрузки с диска, после загрузки в другой операционной системе, с другого компьютера, подключённого к сети, с другого рабочего стола).

Рассмотрим пример программы для восстановления паролей

Advanced Office Password Recovery (AOPR) - программа для восстановления забытых паролей к документам Microsoft Office.

Advanced Office Password Recovery позволяет восстанавливать пароли либо обходить парольную защиту файлов и документов, созданных в продуктах семейства MS Office всех версий. В данный момент поддерживаются версии с

2.0 по 2010 включительно. Программа поддерживает документы, созданные MS Word, Excel, Access, Outlook, Project, Money, PowerPoint, Publisher, а также OneNote. Кроме перечисленного, программа позволяет получить доступ к исходным текстам VBA макросов, защищенных паролем.

Возможности Advanced Office Password Recovery

- ✓ Поддержка всех версий Microsoft Office с 2.0 по 2010
- ✓ Мгновенное восстановление отдельных паролей
- ✓ Изменение пароля на указанный пользователем
- ✓ Мгновенное снятие защиты с документов, для которых когда-либо были подобраны пароли
- ✓ Использование всех обнаруженных уязвимостей продуктов семейства MS Office для восстановления доступа к документам

- ✓ Предварительная атака с набором типичных параметров для восстановления стойких паролей
- ✓ Поддержка атаки по словарю и прямого перебора паролей с использованием шаблонов масок
- ✓ Аппаратное ускорение (подана заявка на патент) уменьшает время перебора паролей в 50 раз
- ✓ Технология аппаратного ускорения с использованием видеокарт NVIDIA или ATI
- ✓ Поддержка одновременно до 32 центральных процессоров или ядер и до 8 графических процессоров
- ✓ Оптимизация кода под современные процессоры позволяет достичь максимальной в данном классе продуктов скорости перебора паролей

Мгновенное восстановление доступа к защищенным документам

Во многих случаях **Advanced Office Password Recovery** позволяет восстановить доступ к защищенным документам в ту же секунду. Например, старые версии MS Office используют очень простую систему шифрования, которая позволяет вычислить пароль. Также в некоторых версиях Office используются алгоритмы с ограничением длины ключа

Помимо указанных приложений, с помощью **Advanced Office Password Recovery** возможно мгновенное восстановление доступа к документам, защищенным другими версиями продуктов семейства MS Office. В частности, поддерживается возможность восстановления сохраненных паролей, используемых для авторизации через MS Passport (LiveID).

Методы восстановления пароля Предварительная атака

Если документ защищен стойким паролем, его расшифровка может занять много времени. Для удобства пользователей в программе предусмотрена предварительная атака, которая автоматически перебирает все типичные пароли и использует атаку по словарю. Также производится поиск среди паролей, которые когда-либо были восстановлены для других документов**.**

Перебор по маске

В случае наличия дополнительной информации о пароле (известна длина пароля в символах или любая часть пароля, либо есть информация об использовании или отсутствии в пароле определенных символов и цифр) скорость восстановления может быть существенно увеличена методом перебора по заданной маске.

Атака по словарю

Согласно статистике, существенная часть паролей, используемых для защиты офисных документов, содержит одно или несколько слов из словаря. Метод подбора паролей по словарю позволяет в десятки раз сократить время, требуемое для восстановления пароля. **Advanced Office Password Recovery** поддерживает атаку по словарю, перебирая пароли, состоящие из слов и их возможных комбинаций в разных регистрах и на нескольких языках. Поддерживается возможность подключения дополнительных словарей.

Прямой перебор

В случае полного отсутствия информации о пароле осуществляется перебор всех возможных вариантов пароля определенной длинны для восстановления доступа к документу. В **Advanced Office Password Recovery** используются новейшие методы низкоуровневой оптимизации кода под современные процессоры, позволяющие достичь высокой производительности перебора по сравнению с конкурирующими продуктами.

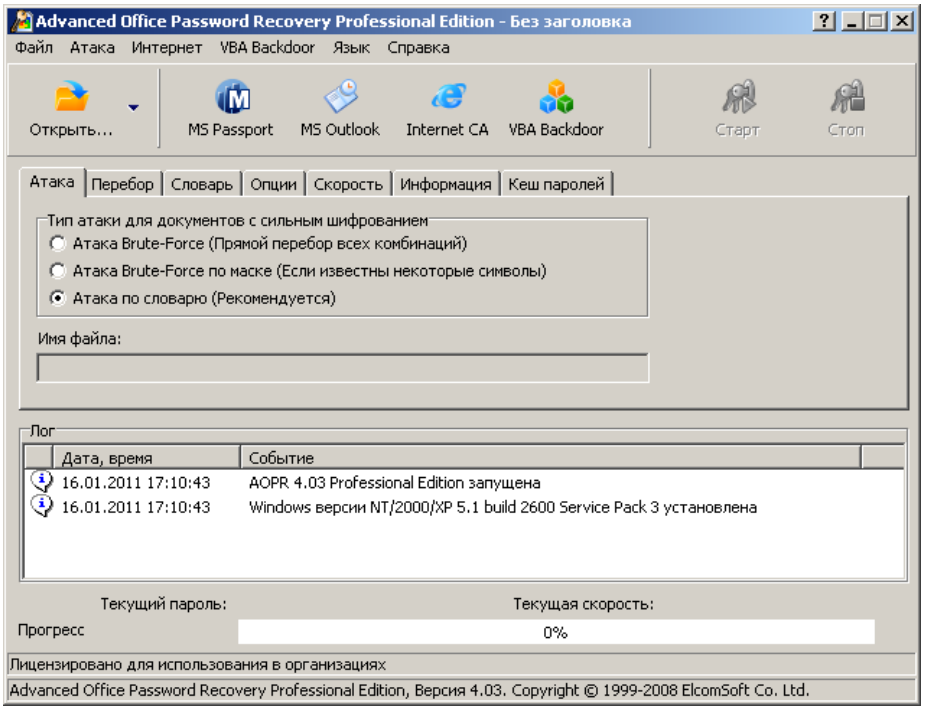


Рис. 3 Интерфейс программы

Выполнить практическое задание:

Задание 1. Восстановление пароля в документах MS Office

Указание: при выполнении задания используйте документы MS Word, MS Excel, MS Access, защищенные паролем

- ✓ Откройте программу **Advanced Office Password Recovery (AOPR)**
- ✓ В панели инструментов окна программы выберите **Открыть**
- ✓ В окне открытия файла выберите защищенный файл MS Word
- ✓ Просмотрите результат: пароль восстановлен?
- ✓ Аналогично выберите документ MS Excel, затем файл базы данных MS Access
- ✓ Изучите возможности программы

Выполнить конспект задания в тетради

Задание 2

1. Выполните поиск в сети Internet специализированных программных средств для создания, а также для восстановления паролей
2. Подготовьте сообщение по данной теме

Установка пароля на архив

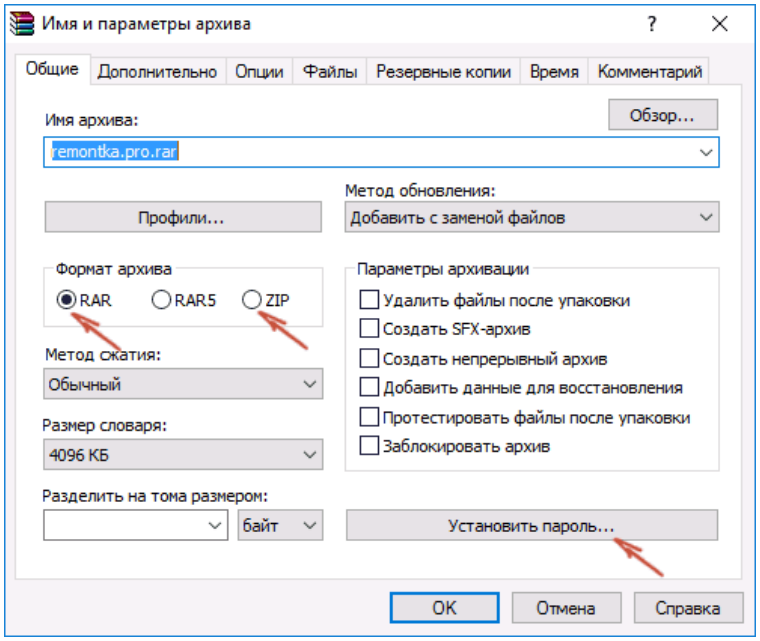
Создание архива с паролем, при условии, что этот пароль достаточно сложен — очень надежный способ защитить свои файлы от просмотра посторонними. Несмотря на обилие разнообразных программ **Password Recovery** для подбора паролей архивов, если он будет достаточно сложным, взломать его не получится.

Установка пароля на архивы ZIP и RAR в программе WinRAR

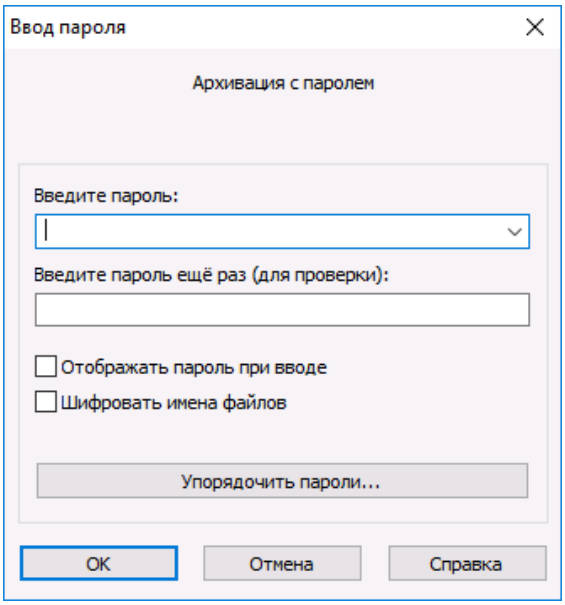
В WinRAR вы можете создавать архивы RAR и ZIP, и устанавливать пароли на оба

типа архива. Однако, шифрование имен файлов доступно только для RAR (соответственно, в ZIP, чтобы извлечь файлы понадобится ввести пароль, однако имена файлов будут видны и без него).

Первый способ создать архив с паролем в WinRAR — выделить все файлы и папки для помещения в архив в папке в Проводнике или на Рабочем столе, кликнуть по ним правой кнопкой мыши и выбрать пункт контекстного меню **Добавить в архив…** с иконкой WinRAR.



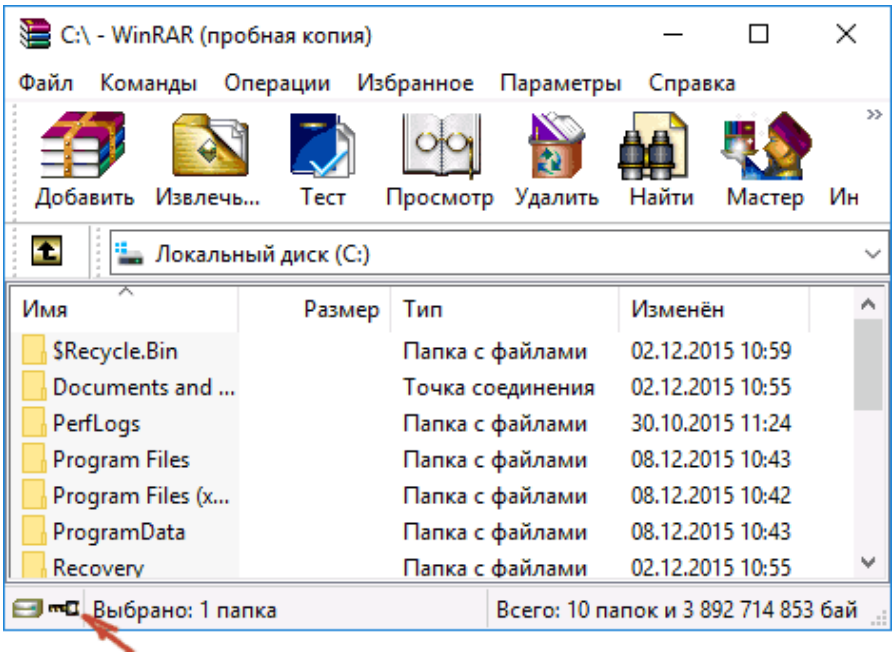
Откроется окно создания архива, в котором, помимо выбора типа архива и места его сохранения, вы можете нажать кнопку **Установить пароль,** после чего дважды ввести его, при необходимости включить шифрование имен файлов (только для RAR). После этого нажмите ОК, и еще раз ОК в окне создания архива — архив будет создан с паролем.



Если в контекстном меню по правому клику нет пункта для добавления в архив WinRAR, то вы можете просто запустить архиватор, выбрать файлы и папки для архивации в нем, нажать кнопку **Добавить** в панели сверху, после чего проделать те же действия по установке пароля на архив.

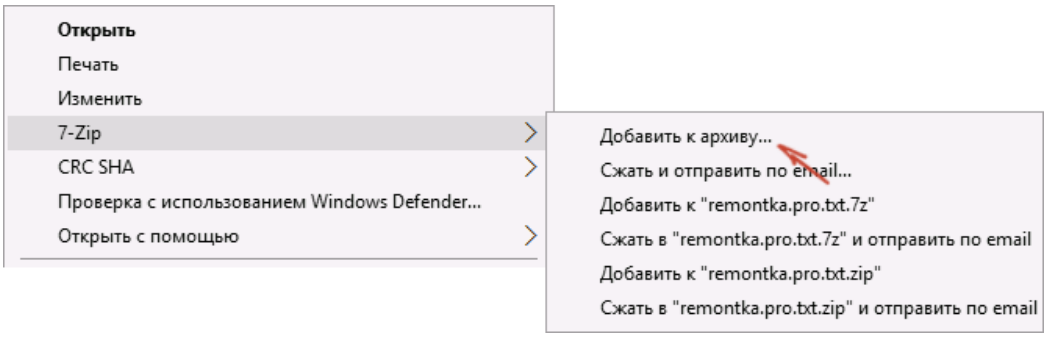
Второй способ поставить пароль на архив или все архивы, в дальнейшем

создаваемые в WinRAR — нажать по изображению ключа слева внизу в строке состояния и задать необходимые параметры шифрования. При необходимости установите отметку **Использовать для всех архивов**.

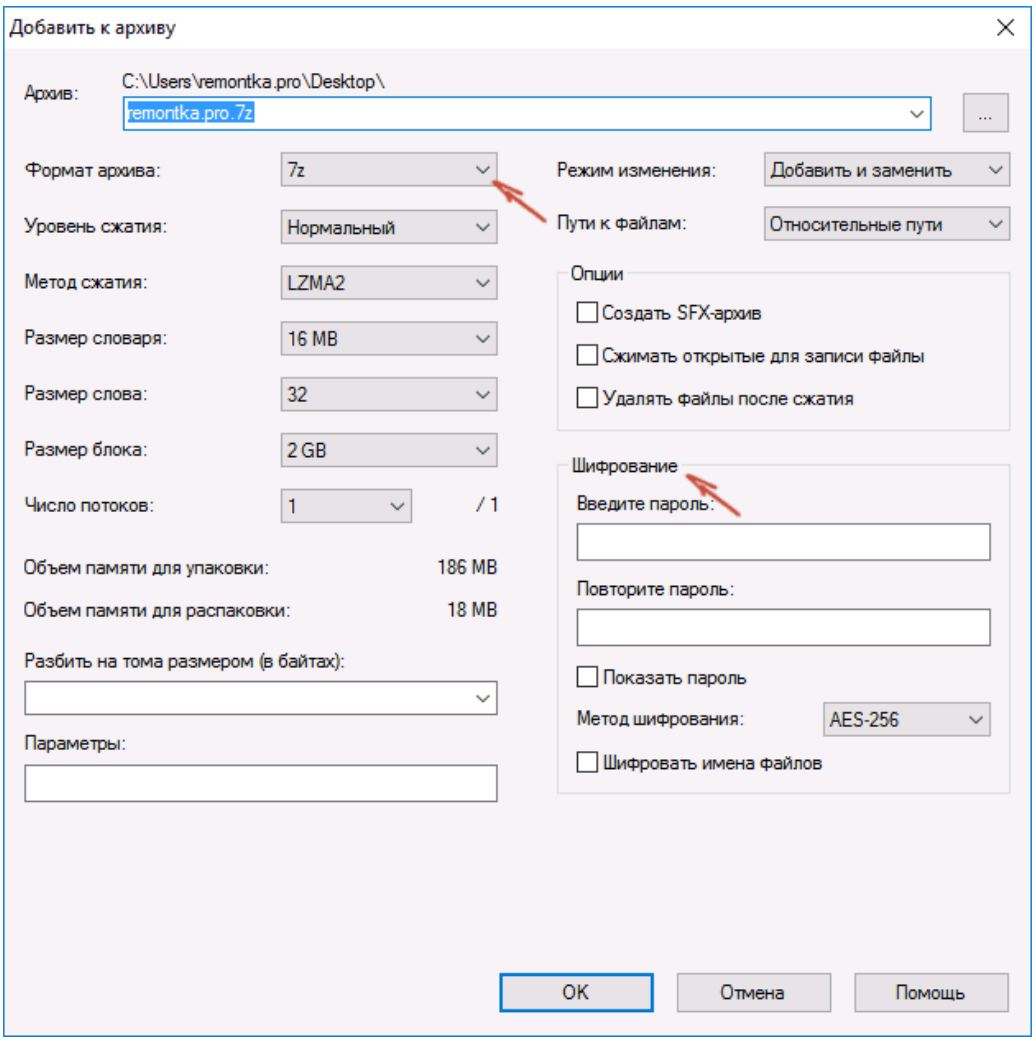


Создание архива с паролем в 7-ZIP

С помощью бесплатного архиватора 7-Zip можно создавать архивы 7z и ZIP, устанавливать на них пароль и выбирать тип шифрования (а распаковывать можно и RAR). Точнее, можно создавать и другие архивы, но установить пароль возможно лишь на два указанных выше типа.



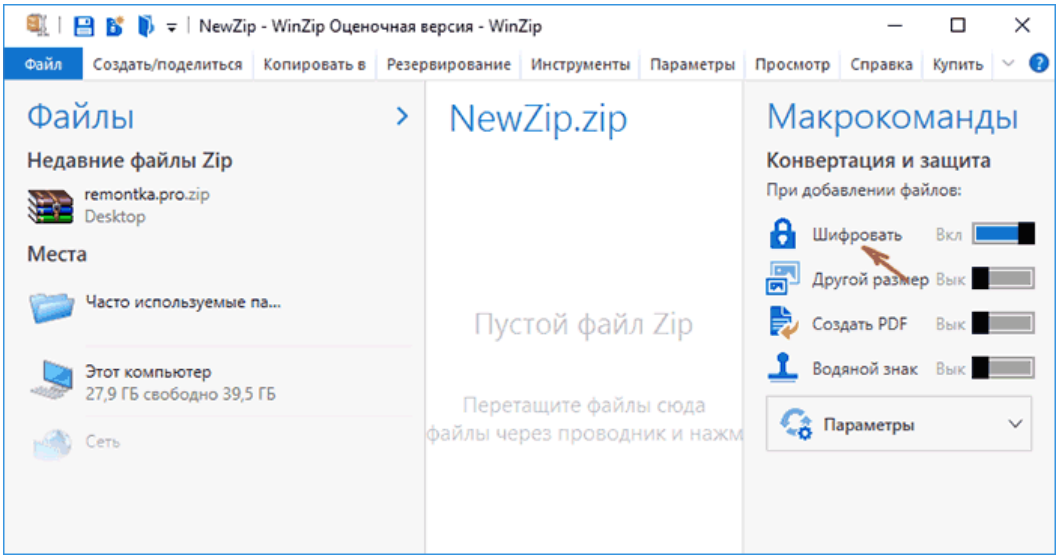
Так же, как и в WinRAR, в 7-ZIP создание архива возможно с помощью пункта контекстного меню **Добавить к архиву** в разделе **7-ZIP** или из главного окна программы с помощью кнопки **Добавить**.



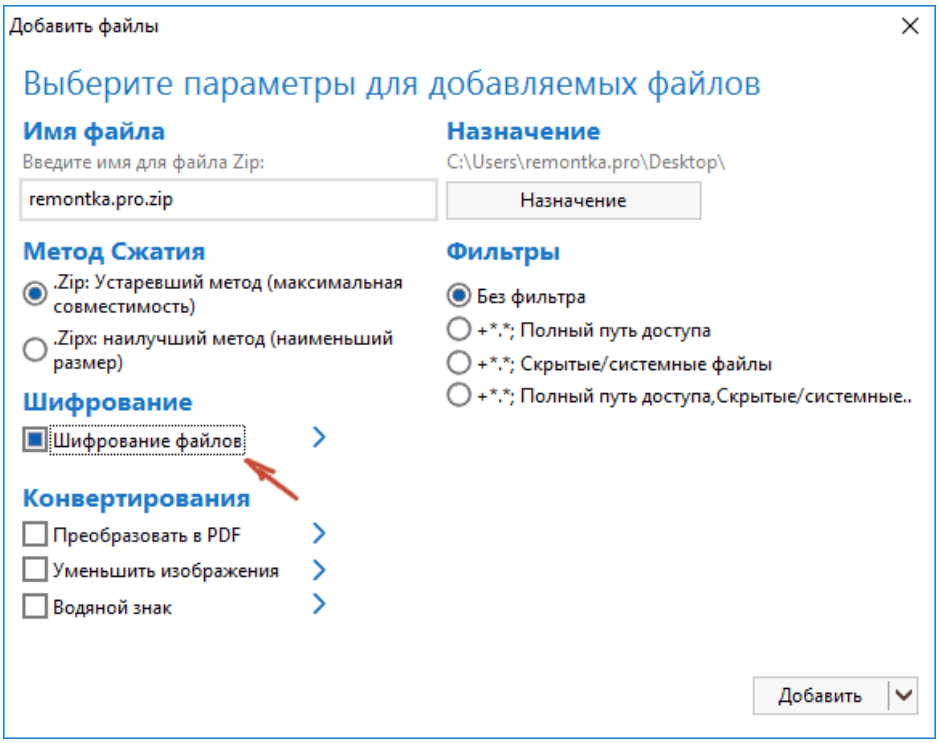
В обоих случаях вы увидите одинаковое окно добавления файлов в архив, в котором, при выборе форматов 7z (по умолчанию) или ZIP будет доступно включение шифрования, при этом для 7z доступно также и шифрование файлов. Просто задайте желаемый пароль, при желании включите скрытие имен файлов и нажмите OK. В качестве метода шифрования рекомендованы AES-256 (для ZIP имеется также ZipCrypto).

В WinZip

С помощью WinZIP можно создать архивы ZIP (или Zipx) с шифрованием AES-256 (по умолчанию), AES-128 и Legacy (тот самый ZipCrypto). Сделать это можно в главном окне программы, включив соответствующий параметр в правой панели, а затем задав параметры шифрования ниже (если вы их не зададите, то при добавлении файлов в архив вас просто попросят указать пароль).



При добавлении файлов в архив с помощью контекстного меню проводника, в окне создания архива просто отметьте пункт **Шифрование файлов**, нажмите кнопку **Добавить** внизу и установите пароль на архив после этого.



Выполнить практическое задание:

Задание 3. Создайте 2 архива, содержащие по 3 файла. Установите пароль на каждый архив

Работа с программами взлома на примере AZPR

Программа AZPR используется для восстановления забытых паролей ZIP- архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (brute force) и атака по словарю (dictionary-based attack).

Панель управления:

- ✓ кнопки **Открыть** и **Сохранить** позволяют работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль. Это позволяет приостанавливать и возобновлять вскрытие.
- ✓ кнопки **Старт** и **Стоп** позволяют соответственно начинать и заканчивать подбор пароля.
- ✓ кнопка **Набор** позволяет задать свое множество символов, если известны символы, из которых состоит пароль.
- ✓ кнопка **Справка** выводит помощь по программе.
- ✓ кнопка **О AZPR** выводит информацию о программе.
- ✓ кнопка **Выход** позволяет выйти из программы

.

Рассмотрим возможности программы:

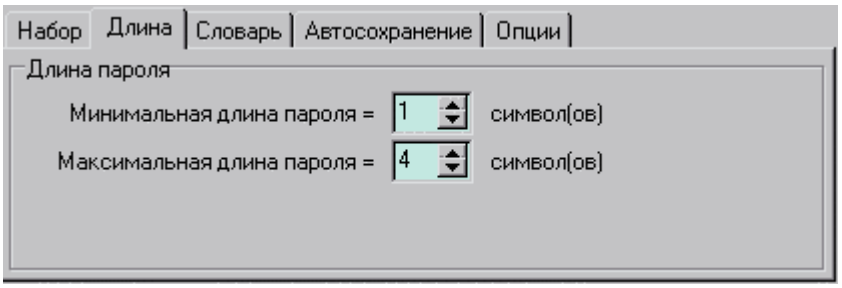
Выбирается архив для вскрытия и тип атаки (см. рис).

Выбираются параметры работы:

✓ Закладка **Набор**

Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки Набор. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле маска. В нем нужно ввести известную часть пароля в виде **P?s?W?r?** , где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.

✓ Закладка **Длина -** позволяет выбрать длину пароля



✓ Закладка **Словарь**

Позволяет выбрать файл-словарь. Выбирайте файл **English.dic**, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

✓ Закладка **Автосохранение**

Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

✓ Закладка **Опции**

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения протокола работы и возможность минимизации программы в **tray** (маленькая иконка рядом с часами).

Выполнить практическое задание:

Задание 4. Вскрытие пароля архива

Используются архивы с паролями из задания 3.

Проведение атаки перебором (bruteforce attack)

1. Используя программу для вскрытия паролей произвести атаку на зашифрованные архивный файлы созданный вами (не менее 5 файлов). Используйте при создания паролей разное сочетание допустимых символов алфавита, но не более 4 символов. Зафиксируйте время нахождения пароля в каждом случае. Сделайте выводы, как от сложности пароля зависит время вскрытия пароля.
2. Выполнив пункт 1, сократить область перебора до фактически используемого (например если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

Проведение атаки по словарю (dictionary attack)

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.
2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

Оформить конспект работы в тетради Контрольные вопросы:

1. Какие виды атак на пароль Вы знаете?
2. Что такое плохой пароль?
3. Как можно противостоять атаке полным перебором?
4. Как длина пароля влияет на вероятность раскрытия пароля?
5. Какие рекомендации по составлению паролей Вы можете дать?

Лабораторная работа №3 Исследование и настройка межсетевого экрана

Цель: изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера; практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана Outpost

Теоретические сведения к практической работе

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

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также о всей компании в целом. Кроме того, проблемы компьютерным сетям предприятий создают факты проникновения компьютерных хулиганов, которые, взломав систему сетевой защиты компании, могут завладеть конфиденциальной информацией или нанести физический вред оборудованию, используя специализированное вредоносное ПО.

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

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

работы в качестве рабочей станции, в конфигурации «по-умолчанию» можно встретить и такие сервисы…

Необходимо отметить, что на сегодняшний день работы по проникновению злоумышленников через «дыры» в защите на 90% автоматизированы. Поэтому,

«самостоятельное» появление вредоносного ПО на вашем компьютере, которое встречается сегодня очень часто, связано в большинстве случаев с наличием непреднамеренных лазеек в неиспользуемых, а значит, не обновляющихся, службах.

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

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

- Межсетевые экраны (брандмауэры, FireWall, МСЭ);
- Сканеры (сканеры открытых портов и сервисов).

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

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

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

Системы программной и аппаратной защиты рабочих станций – брандмауэры (FireWalls)

Архитектура firewall

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

Фильтрация пакетов (packet filtering firewalls)

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

Параметры, которые могут проверяться:

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

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

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

пропустить пакет;

- если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

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

- фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;
- этот метод легко реализуем аппаратно;
- одно-единственное правило может стать ключевым при защите всей сети;
- фильтры не требуют специальной конфигурации компьютера;
- метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

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

Firewall цепного уровня (circuit level firewalls)

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю. Поскольку первый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи. Содержание таблицы следующее:

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

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

- firewall цепного уровня быстрее программного, так как производит меньше

проверок;

- firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
- возможно скрытие внутренней топологии сети. Недостатки firewall цепного уровня:
- нет проверки пакетов на программном уровне;
- слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
- нет проверки передаваемых данных;
- трудно проверить разрешение или отрицание передачи пакетов.

Firewall программного уровня

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

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

Недостатки proxy:

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

Динамическая фильтрация пакетов (dynamic packet filter firewalls)

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

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

Уровень kernel proxy

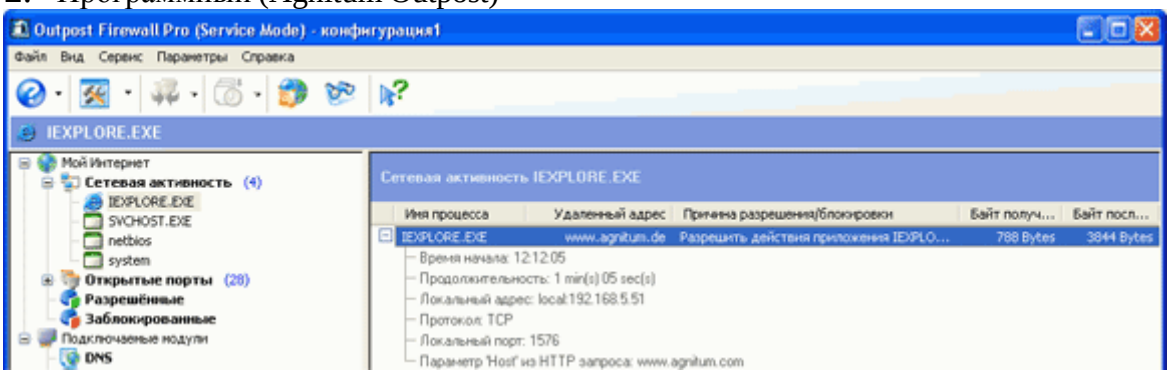
Уровень kernel proxy возник достаточно недавно. Основная его идея — попытка поместить описанный выше алгоритм firewall программного уровня в ядро операционной системы, что избавляет компьютер от лишних затрат времени на передачу данных между ядром и программой proxy. Это повышает производительность и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

Примеры межсетевых экранов

1. Аппаратный (D-Link)

DFL-1100
Межсетевой экран для сетей крупных предприятий

2. Программный (Agnitum Outpost)



Вспомогательные системы обеспечения безопасности компьютерных сетей - сканеры.

Архитектура сканера

Основной принцип функционирования сканера заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки).

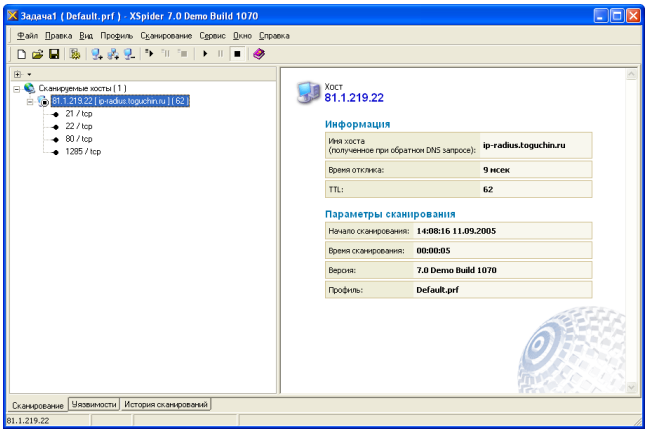
Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP- порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования. Современный сетевой сканер выполняет четыре основные задачи:

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

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

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

Пример сканера XSpider



1. Порядок выполнения работы.

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

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

Практическая работа проводится в двух вариантах:

1. Автономный.

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

2. Совместный.

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

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

Порядок работы

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

Действия, общие для двух этапов:

1. Взять из папки \\m00\fit2005 файлы установки сканера XSpider и МСЭ Agnitum Outpost;
2. На каждом рабочем месте выполнить установку сканера и МСЭ;
3. При установке Outpost соглашаться со всеми вопросами. По окончании установки – перезагрузить машину;
4. Перед началом работы перевести установленный МСЭ в режим разрешения. Открыть Outpost -> меню «Параметры» -> «Политики» -> выбрать режим «Разрешать»;
5. Узнать имя и IP-адрес своего рабочего компьютера: «Пуск» ->«Выполнить» -> “cmd” -> “ipconfig /all”;

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

Группа 1:

1. Запустить пинг компьютера-соседа из группы 2: «Пуск» -> «Выполнить» -> “cmd” -> “ping ip-addr -t”; (утилита ping располагается в C:\windows\system32)

2. Смотреть на ответные пинг-пакеты.
3. Фиксировать моменты, когда ответные пакеты пропадают и появляются.
4. Сравнить данные с моментами изменения конфигурации МСЭ напарником

Группа 2:

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

Поменяться с напарником ролями и повторить вышеуказанные пункты.

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

Группа 1:

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

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не будет без установки в XSpider специальной опции: меню «Профиль» ->

«Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».

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

Группа 2:

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

Поменяться с напарником ролями и повторить вышеуказанные пункты.

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

Контрольные вопросы:

1. Опишите утилиту ping, методы и случаи ее применения.
2. Описать данные, полученные о компьютере напарника с помощью XSpider
3. Какого типа уязвимости были найдены?
4. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
5. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия?

Лабораторная работа№ 4
Обеспечение безопасности локальной сети. Настройка параметров безопасности браузера

Цель: изучить возможности настройки безопасности локальной сети и браузера

Политику безопасности можно сравнить с пограничником, охраняющим границу страны. Рассмотрим два способа улучшения безопасности работы виртуальной сети за два приема.

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем — это уязвимость)

Часто при установке Windows пароль администратора пустой и этим может воспользоваться злоумышленник. Иначе говоря, при установке Windows в автоматическом режиме с настройками по умолчанию мы имеем пользователя **Администратор** с пустым паролем и любой **User** может войти в такой ПК с правами администратора. Чтобы решить проблему выполним команду **Мой компьютер-Панель управления-Администрирование- Управление компьютером-Локальные пользователи-Пользователи** (рис. 1).

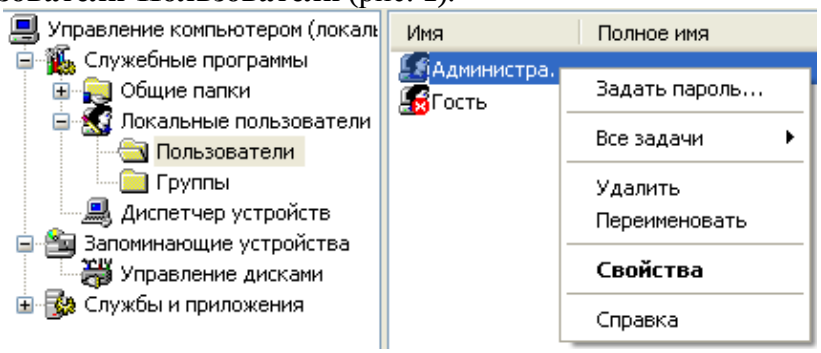


Рис. 1. Диалоговое окно Управление компьютером

Здесь по щелчку правой кнопкой мыши на **Администраторы** зададим администратору пароль, например, 12345. Это плохой пароль, но лучше, чем ничего. Теперь в окне **Администрирование** зайдем в **Локальную политику безопасности**. Далее идем по веткам дерева: **Локальные политики- Параметры безопасности-Учетные записи: Переименование учетной записи Администратор** (рис.2).

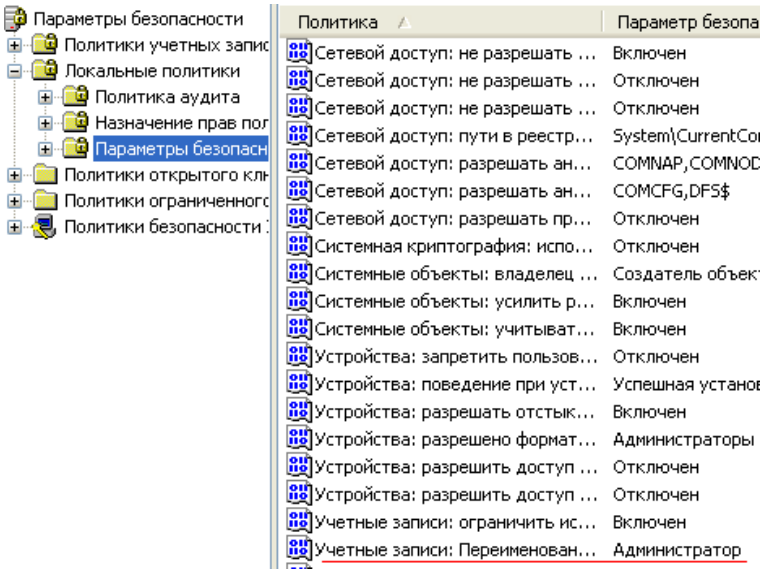


Рис. 2. Находим в системном реестре запись Переименование учетной записи Администратор

Здесь пользователя **Администратор** заменим на **Admin** (рис. 3).

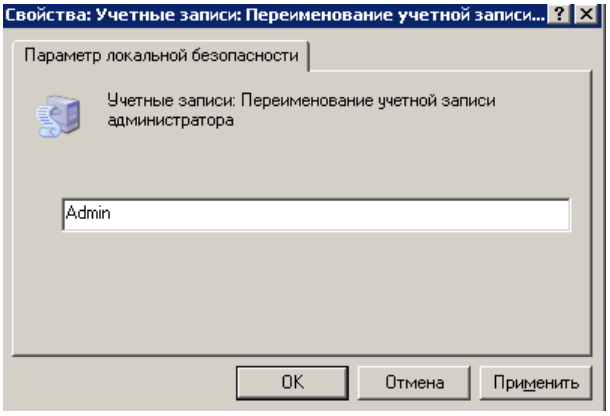


Рис. 3. Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий у нас получилась учетная запись Admin с паролем 12345 и правами администратора.

Теперь мы имеем пользователя **Администратор** с паролем, одна из уязвимостей системы устранена.

Примечание

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, использовав окно **Учетные записи пользователей**, что гораздо проще

Примечание

Учетная запись Гость позволяет входить в ПК и работать на нем (например, в Интернет) без использования специально созданной учетной записи. Запись Гость не требует ввода пароля и по умолчанию блокирована. Гость не может устанавливать или удалять программы. Эту учетную запись можно отключить, но нельзя удалить.

Шаг 2. Делаем окно приветствия пустым (убираем уязвимость 2)

У нас окно входа в систему содержит подсказку Admin, давайте ее уберем, сделав окно пустым. Для начала в окне **Учетные записи пользователей** жмем на кнопку **Изменение входа пользователей в систему** и уберем флажок **Использовать страницу приветствия.**

Теперь повысим безопасность сети еще на одну условную ступень, сделав оба поля окна приветствия пустыми (рис. 4).

Рис. 4. Обе строки данного окна сделаем пустыми

Выполним команду **Панель управления-Администрирование – Локальные политики безопасности- Локальные политики-Параметры безопасности—Интерактивный вход: не отображать последнего имени пользователя**. Эту запись необходимо включить (рис. 5).

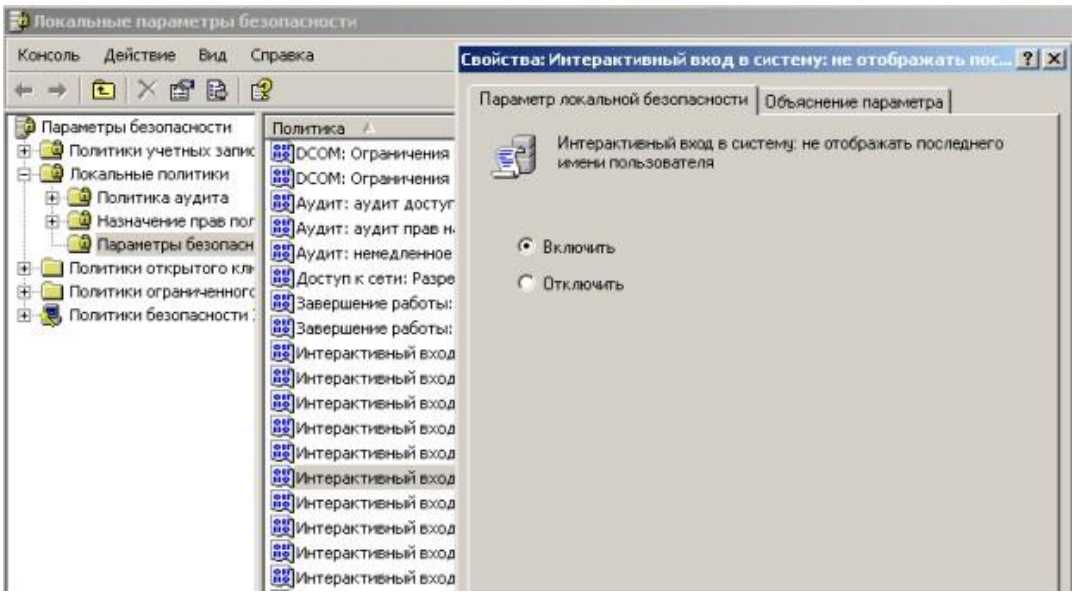


Рис. 5. Активируем переключатель Включить

Теперь после завершения сеанса пользователь должен угадать не только пароль, но и имя пользователя (рис. 6).

Рис. 6. Обе строки окна приветствия пусты

Выявление сетевых уязвимостей сканированием портов ПК

Злоумышленники используют сканирование портов ПК для того, чтобы воспользоваться ресурсами чужого ПК в Сети. При этом необходимо указать **IP** адрес ПК и открытый **port,** к примеру, **195.34.34.30:23**. После этого происходит соединение с удаленным ПК с некоторой вероятностью входа в этот ПК.

- ✓ TCP/IP port — это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт — потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP (отправка почты) — 25 порт, WWW — 80 порт, FTP —21 порт.
- ✓ Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютер.

Одна из функций администратора сети (сисадмина) — выявить недостатки в функционировании сети и устранить их. Для этого нужно просканировать сеть и закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы TCP/IP, которые можно отключить:

- ✓ finger — получение информации о пользователях
- ✓ talk— возможность обмена данными по сети между пользователями
- ✓ bootp — предоставление клиентам информации о сети
- ✓ systat — получение информации о системе
- ✓ netstat — получение информации о сети, такой как текущие соединения
- ✓ rusersd — получение информации о пользователях, зарегистрированных в данный момент

Просмотр активных подключений утилитой Netstat

Команда **netstat** обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии. С ее помощью можно получить список серверных приложений, работающих на данном компьютере. Большинство серверов находится в режиме **LISTEN**— ожидание запроса на соединение. Состояние **CLOSE_WAIT** означает, что соединение разорвано. **TIME_WAIT** — соединение ожидает разрыва. Если соединение находится в состоянии **SYN_SENT**, то это означает наличие процесса, который пытается, установить соединение с сервером. **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются).

Итак, команда **netstat** показывает содержимое различных структур данных, связанных с сетью, в различных форматах в зависимости от указанных опций. Для сокетов (программных интерфейсов) TCP допустимы следующие значения состояния:

- ✓ CLOSED — Закрыт. Сокет не используется.
- ✓ LISTEN — Ожидает входящих соединений.

- ✓ SYN_SENT — Активно пытается установить соединение.
- ✓ SYN_RECEIVED — Идет начальная синхронизация соединения.
- ✓ ESTABLISHED — Соединение установлено.
- ✓ CLOSE_WAIT — Удаленная сторона отключилась; ожидание закрытия сокета.
- ✓ FIN_WAIT_1 — Сокет закрыт; отключение соединения.
- ✓ CLOSING — Сокет закрыт, затем удаленная сторона отключилась; ожидание подтверждения.
- ✓ LAST_ACK — Удаленная сторона отключилась, затем сокет закрыт; ожидание подтверждения.
- ✓ FIN_WAIT_2 — Сокет закрыт; ожидание отключения удаленной стороны.
- ✓ TIME_WAIT — Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки

Примечание

Что такое «сокет» поясняет рис. 7. Пример сокета – 194.86.6..54:21

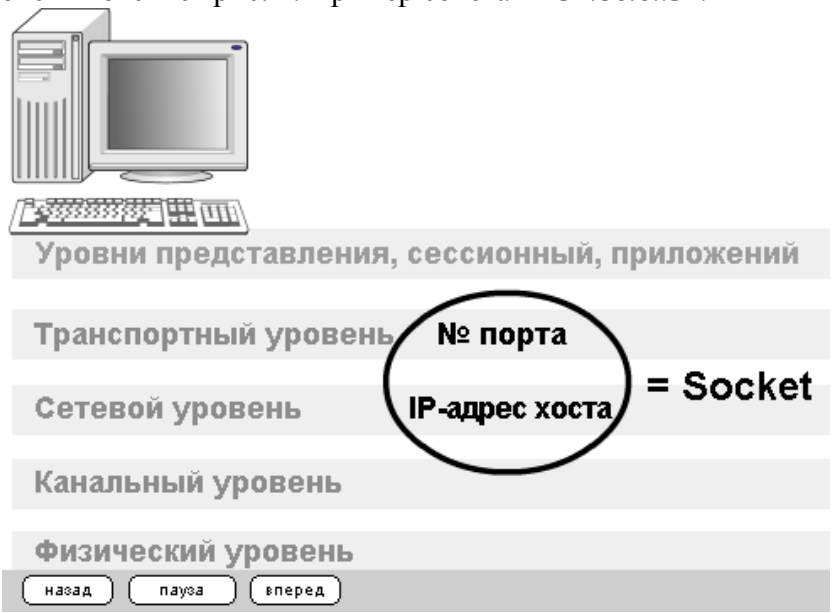


Рис. 7. Сокет это № порта + IP адрес хоста

Выполните практическое задание:

Задание 1. Обнаружение открытых на ПК портов утилитой Netstat

Для выполнения практического задания на компьютере необходимо выполнить команду **Пуск-Выполнить**. Откроется окно **Запуск программы**, в нем введите команду **cmd** (рис. 8).

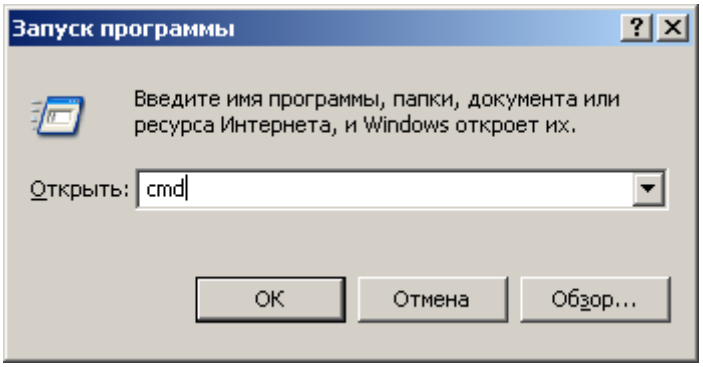


Рис. 8. Окно Запуск программы

Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты TCP/ UDP введите команду **netstat** (рис. 13). Мы видим Локального адреса (это ваш ПК) прослушиваются 6 портов. Они нужны для поддержки сети. На двух портах мы видим режим **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются). Четыре порта используются в режиме **TIME_WAIT** — соединение ожидает разрыва.

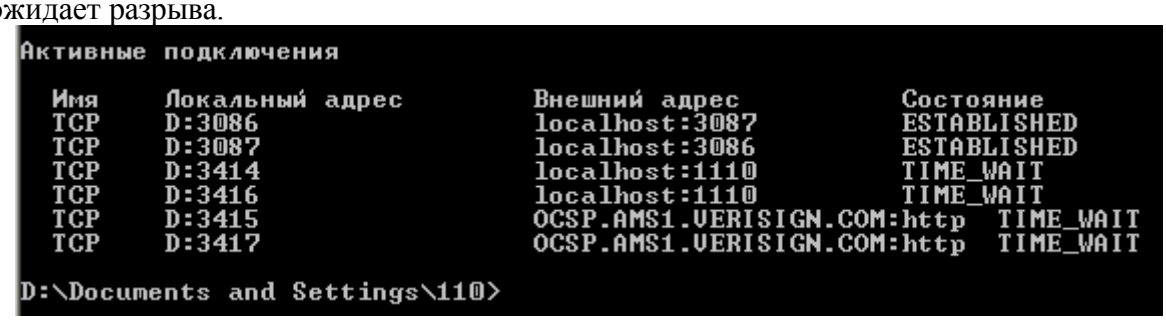


Рис. 9. Список активных подключений на тестируемом ПК

Запустите на вашем ПК Интернет и зайдите, например на **www.yandex.ru**. Снова выполните команду **netstat** Как видим, добавилось несколько новых активных портов с их различными состояниями.

Команда **netstat** имеет следующие опции – табл. 1.

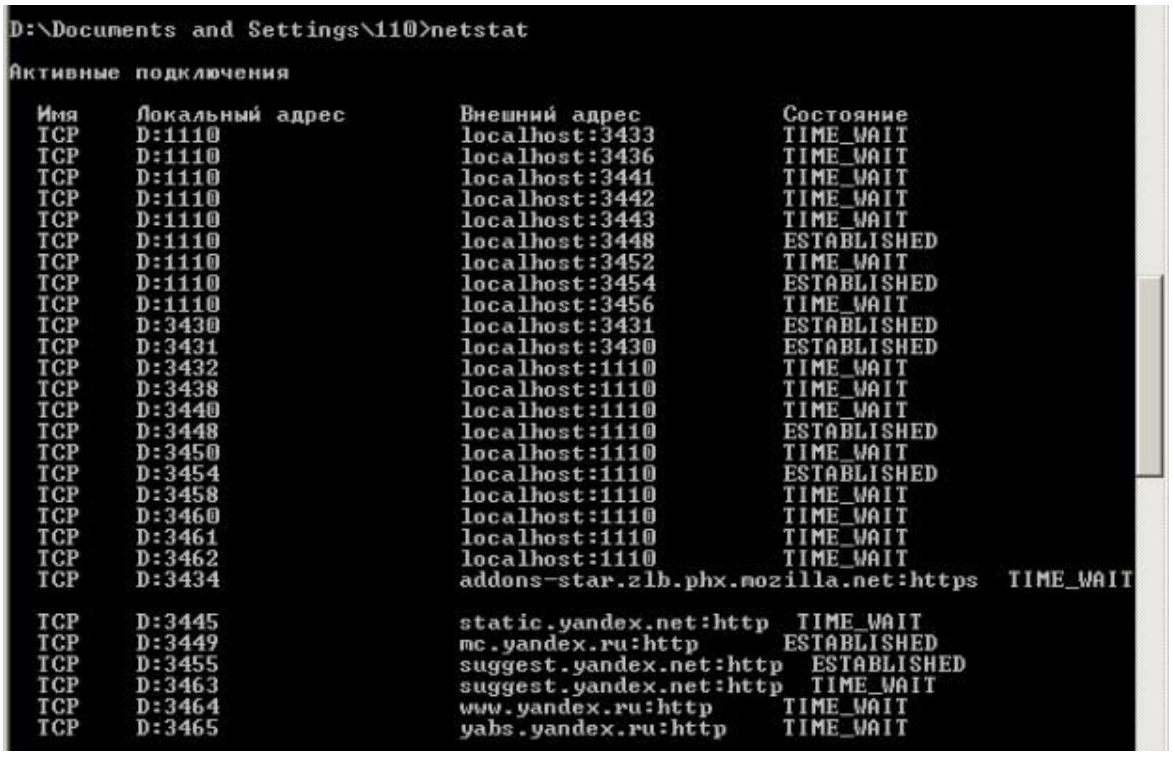


Рис. 10. Активные подключения при работе ПК в Интернет

Программа NetStat Agent

Представьте ситуацию: ваше Интернет-соединение стало работать медленно, компьютер постоянно что-то качает из Сети. Вам поможет программа NetStat Agent. С ее помощью вы сможете найти причину проблемы и заблокировать ее. Иначе говоря, **NetStat Agent** — полезный набор инструментов для мониторинга Интернет соединений и

диагностики сети. Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд **Ping** и**TraceRoute** (рис. 11).

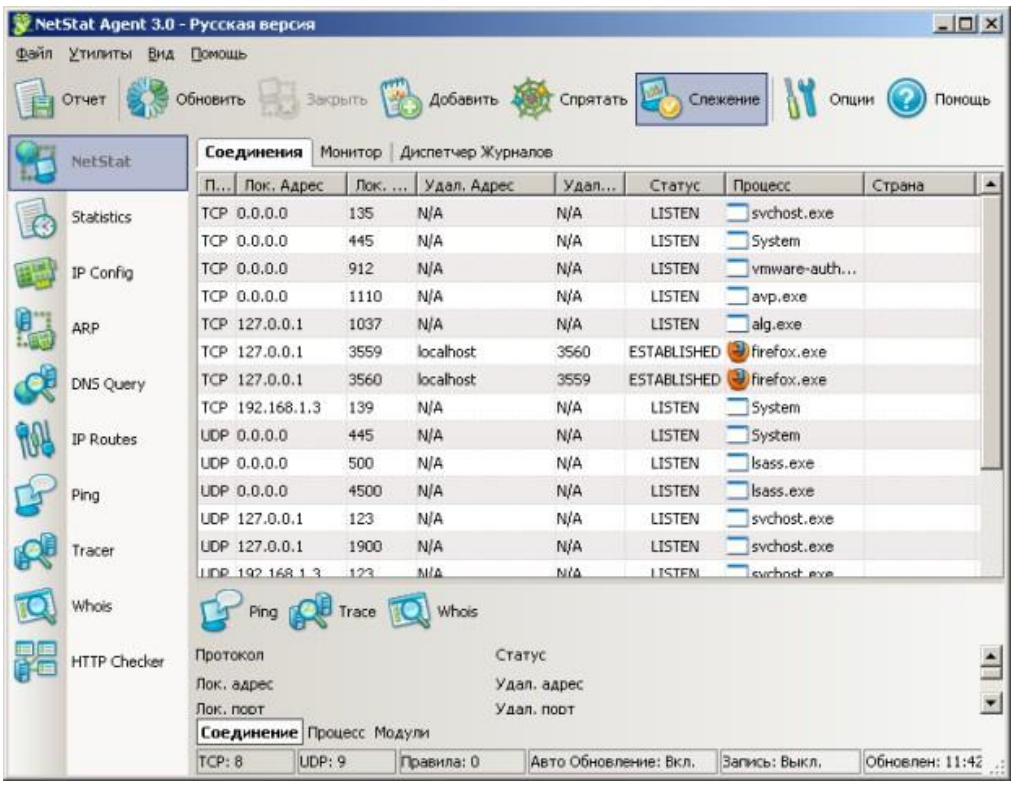


Рис. 11. Главное окно программы NetStat Agent В состав программы NetStat Agent вошли следующие утилиты:

- ✓ **NetStat** — отслеживает TCP и UDP соединения ПК (при этом отображается географическое местоположение удаленного сервера и имя хоста).
- ✓ **IPConfig** — отображает свойства сетевых адаптеров и конфигурацию сети.
- ✓ **Ping** — позволяет проверить доступность хоста в сети.
- ✓ **TraceRoute** — определяет маршрут между вашим компьютером и конечным хостом, сообщая все IP-адреса маршрутизаторов.
- ✓ **DNS Query** — подключается к DNS серверу и находит всю информацию о домене (IP адрес сервера, MX-записи (Mail Exchange) и др.).
- ✓ **Route** — отображает и позволяет изменять IP маршруты на ПК.
- ✓ **ARP** — отслеживает ARP изменения в локальной таблице.
- ✓ **Whois** — позволяет получить всю доступную информацию об IP-адресе или домене.
- ✓ **HTTP Checker** — помогает проверить, доступны ли Ваши веб-сайты.
- ✓ **Statistics** — показывает статистику сетевых интерфейсов и TCP/IP протоколов.

Сканер портов Nmap (Zenmap)

Nmap — популярный сканер портов, который обследует сеть и проводит аудит защиты. Использовался в фильме «Матрица: Перезагрузка» при взломе компьютера. Наша задача не взломать, а защитить ПК, поскольку одно и то же оружие можно использовать как для защиты, так и для нападения. Иначе говоря, сканером портов **nmap** можно определить открытые порты компьютера, а для безопасности сети пользователям

рекомендуется закрыть доступ к этим портам с помощью брандмауэра (рис. 12).

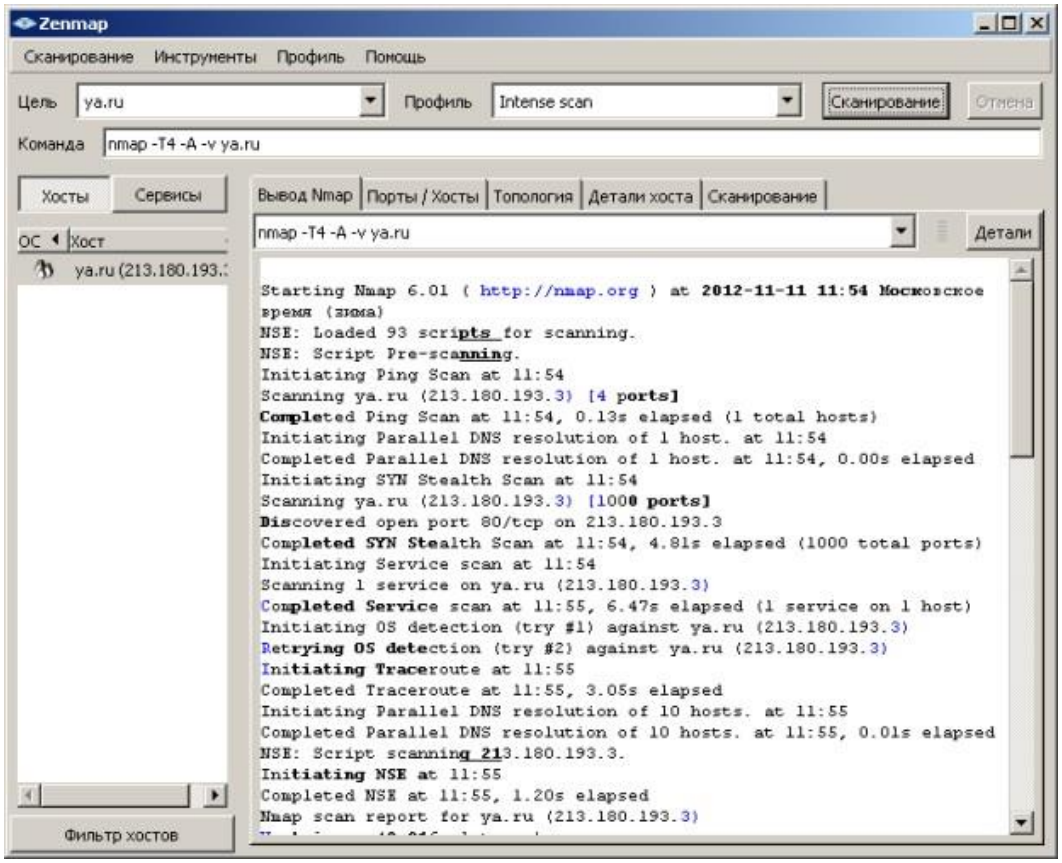


Рис. 12. Интерфейс программы Nmap

Обычно для того, чтобы просканировать все порты какого-либо компьютера в сети вводится команда **nmap –p1-65535 IP-адрес**_компьютера или **nmap –sV IP-адрес компьютера,** а для сканирования сайта — команда **nmap –sS –sV –O -P0 адрес сайта.**

Монитор портов TCPView

TCPView — показывает все процессы, использующие Интернет- соединения. Запустив **TCPView**, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение – рис. 13.

Просмотрите активные сетевые подключения локального ПК с помощью монитора портов tpiview. Определите потенциально возможные угрозы (какие порты открыты, и какие приложения их используют). При необходимости можно закрыть установленное приложением TCP-соединение или процесс правой кнопкой мыши.

Оформить конспект работы в тетради Контрольные вопросы:

1. Какие уязвимости ОС Windows были устранены в данной практической работе и какими путями?
2. Для чего используется утилита Netstat?
3. Перечислите, какие утилиты вошли в состав программы NetStat Agent? Для чего используется каждая из утилит?
4. Для чего используется программа Nmap? TCPView?

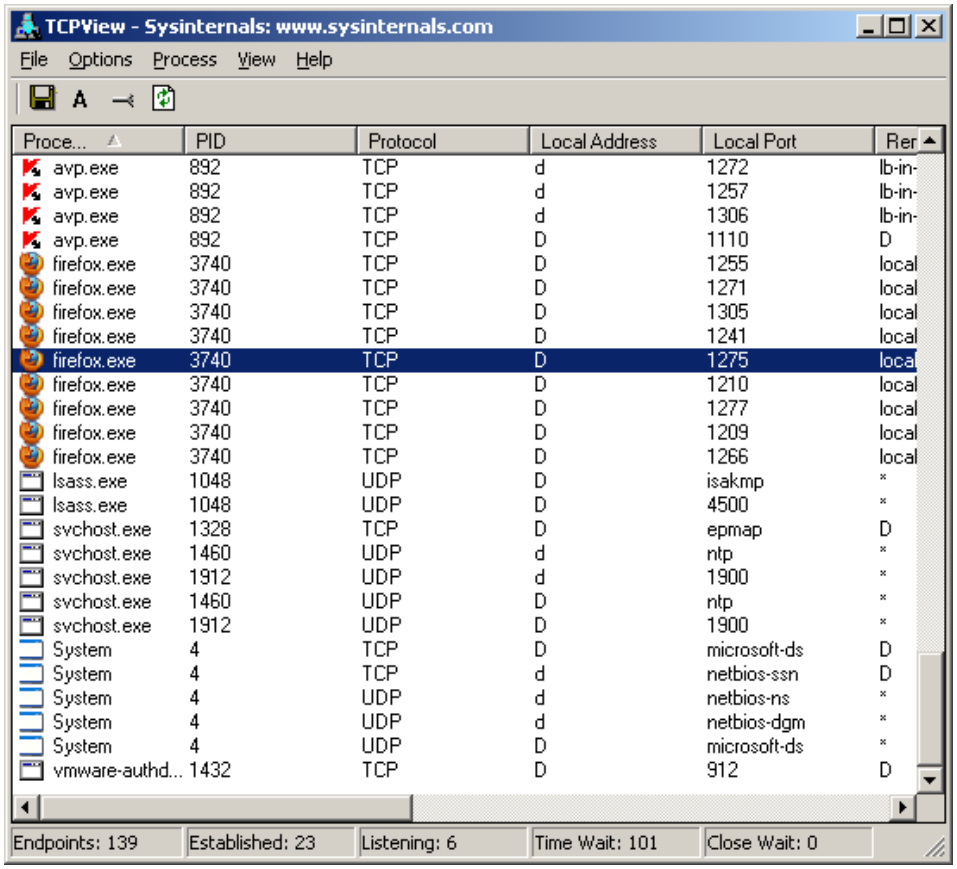


Рис. 13. Главное окно программы TCPView