МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ЭКОНОМИКИ СЕРВИСА

“Утверждаю”
Проректор по учебной работе
_____К.Мирзаев
“____”_____20 г

МЕТОДИЧЕСКОЕ УКАЗАНИЕ

по предмету
«Информационные комплексы и технологии в экономике»
для выполнения практических и лабораторных работ

«Компьютерный вирус и их защита. Цель и особенности архивирования информации»

САМАРКАНД

Методическое указание составлена на основе учебного плана, рабочего учебного плана и типовой программы предмета “Информационные комплексы и технологии в экономике” утвержденной приказом Минвуза от «25» август 2018 года № 744, одобрено на заседании кафедры «Информационные технологии» от ___ _____2018г.

Рекомендовано учебно-методическим и научным объединением Самаркандского института экономики и сервиса от ___ _____20 г.

Методическое указание предназначено для студентов всех направлений института, а также магистрантов всех специальностей.

Составители:

Рустамов Ж.Э. – СамИЭС, ассистент кафедры “Высшая математика и информационные технологии”

Рецензенты:

Раджабов Н.А. – СамГАСИ, доцент кафедры “Информационных технологии” , к.ф.-м.н.

Nazarov U.A. – СамГАСИ, доцент кафедры “Информационных технологии” , к.ф.-м.н.

Начальник учебно-методического отдела:

20 _ год “_____”_____ _____ Шодмонов И.Э.

(подпись)

Зав. кафедрой

«Информационные технологии»:

20 _ год “_____”__._____ _____А.Э.Эрназаров

(подпись)

Содержание

1.Цель и задачи работы. 4
2.Теоретические сведения. 4
Алгоритмы шифрования архиваторов 7
Использование антивирусных программ....7
План выполнения практических занятий 9
Основная литература и дополнительная литература а также источник информации 13

ТЕМА: Компьютерный вирус и их защита. Цель и особенности архивирования информации

План:

1. Цель и задачи работы.
2. Теоретические сведения.
3. Алгоритмы шифрования архиваторов
4. Использование антивирусных программ
5. План выполнения практических занятий
6. Технология защиты сетевых компьютеров. Брандмауэр.
7. Теоретические сведения
8. Выполнение работы
9. Лабораторной работы

1.Цель и задачи работы.

Изучить способы защиты документов в пакете MICROSOFT OFFICE и в архивах. Исследовать стойкость данных защит к взлому.

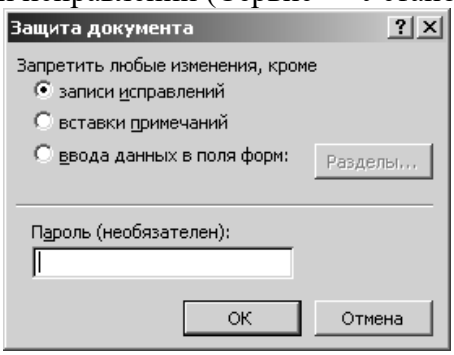
2.Теоретические сведения.

Защита документов Microsoft Office

Программный пакет Microsoft Office является наиболее популярным и часто используемым пакетом при подготовке электронных документов. При работе с приложениями MS Office возникает проблема обеспечения защиты информации, содержащейся в документе, для чего в пакет *Microsoft Office* были введены различные типы защит.

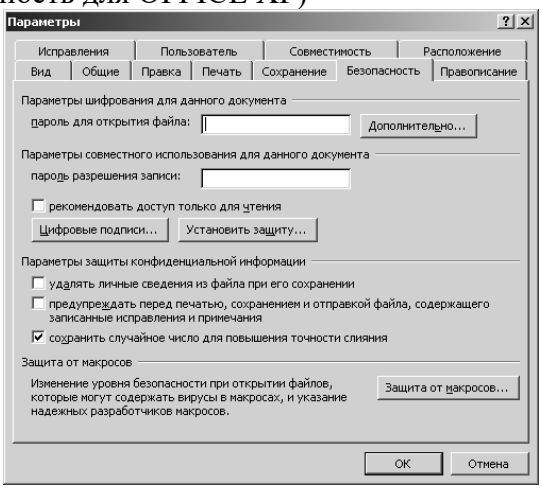
Существует 3 основных типа защит документов в Microsoft Word.

1. Защита документа от записи исправлений (Сервис -> Установить защиту).



2. Защита документа от изменений (доступ по чтению).

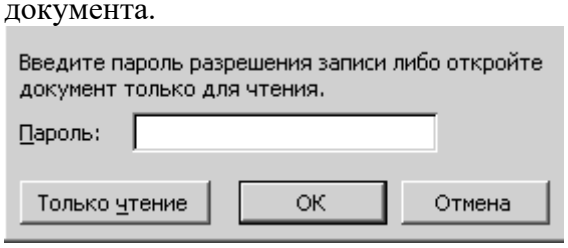
3. Защита на открытие документа (Сервис->Параметры->Сохранение для OFFICE 2000 или Сервис->Параметры->Безопасность для OFFICE XP)



Первые 2 типа защит обладают нулевой криптостойкостью (стойкостью ко взлому).

Защита от записи (доступ только по чтению)

В случае установки данного типа защиты, при открытии документа от пользователя будет запрошен пароль, разрешающий запись документа. Если пароль не будет введен, то будет дано разрешение только на чтение документа.



Этот метод защиты является самым слабым. Пароль защиты записи хранится в документе в открытом виде. Его можно найти любым редактором кода. Этот пароль даже не хэшируется. Защищать документ этим типом защиты крайне не рекомендуется, его криптостойкость равна нулю. Совет – если пользоваться этим методом защиты, то пароль лучше задавать на русском языке, в этом случае его несколько труднее обнаружить.

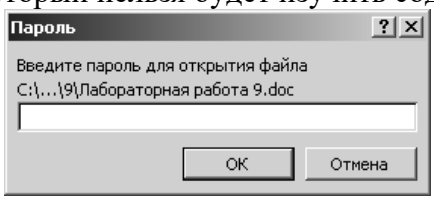
Защита от изменений

В случае установки данного типа защиты, вплоть до ее снятия, все изменения, вносимые пользователем в документ, будут подчеркиваться и отмечаться красным цветом.

Криптостойкость данной защиты не намного отличается от предыдущего типа. Пароль также хранится в документе, отличие только в том, что он хэшируется. Длина хэша – 32 бита. Для снятия защиты можно либо заменить хэш на заранее известный, либо вычислить первый подходящий под хэш пароль. Для такой длины хэша подходящих паролей может быть несколько. Существует возможность заменить хэш на хэш-образ, соответствующий пустому паролю.

Защита на открытие документа

В случае установки данного типа защиты, при открытии документа от пользователя будет запрашиваться пароль, не введя который нельзя будет изучить содержимое документа.



Из всех рассмотренных способов защиты в Word, данный метод является самым стойким. При установке пароля, документ шифруется по симметричному алгоритму RC4. В документе хранится зашифрованный хэш-образ пароля, используемый при проверке. Хэш имеет длину 128 бит и формируется по алгоритму MD5. Единственный способ нахождения пароля – полный перебор. Если длина пароля большая, и пароль выбран в соответствие с требованиями, то взломать данный тип защиты за приемлемое время довольно сложно.

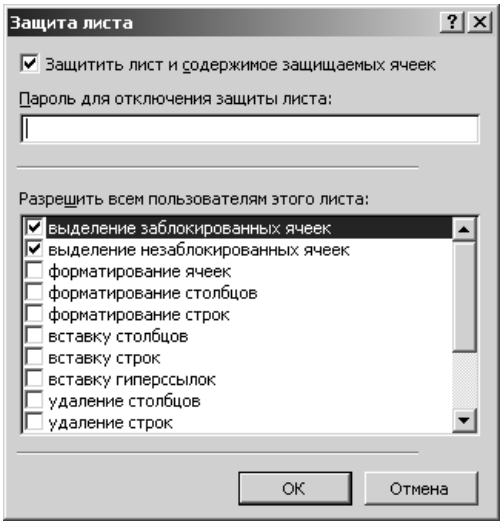
Защита документов Microsoft Excel

При защите документов Excel, отличие заключается только во введении паролей на ячейки/листы/книги.

Защита листа

Защита листа позволяет защитить его элементы, например, ячейки с формулами, запретив доступ к ним всем пользователям, или предоставить доступ отдельным пользователям к определенным диапазонам ячеек. Можно запретить вставку, удаление и форматирование строк и столбцов, изменение содержимого заблокированных ячеек или перемещение курсора на заблокированные или разблокированные ячейки и т.д.

Защита листа реализуется через функцию Сервис->Защита->Защитить лист.



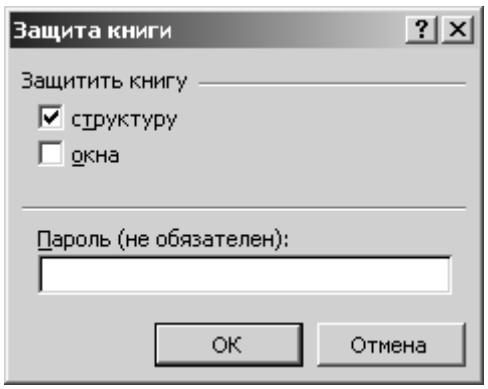
После открытия данного окна, пользователь может разрешить выполнение над элементами листа необходимые действия. Остальные действия по умолчанию запрещены. Для блокирования и разблокирования определенных ячеек необходимо использовать функцию ФОРМАТ ЯЧЕЕК->ЗАЩИТА.

Используя функцию ЗАЩИТА->РАЗРЕШИТЬ ИЗМЕНЕНИЕ ДИАПАЗОНОВ, можно разрешить определенным группам пользователей выполнять операции над ячейками без ввода пароля. Другие пользователи будут получать запрос на ввод пароля и после его ввода смогут редактировать диапазон.

Для реализации данного типа защиты используется хэширование паролей (16 бит). Существует множество паролей, которые подходят под известный хэш-образ. Можно попытаться, например, защитить лист паролем «test» и попытаться открыть его при помощи пароля «zzyw».

Защита книги

Защитить книгу можно используя функцию СЕРВИС-> ЗАЩИТА->ЗАЩИТИТЬ КНИГУ.



С помощью данной функции, можно запретить добавление и удаление листов, или отображение скрытых листов. Кроме этого, можно запретить изменение размеров или положения окна, настроенного для отображения книги. Действие такой защиты распространяется на всю книгу.

Защита информации в архивах

Парольная защита архивов является одним из наиболее часто используемых защит при передаче конфиденциальных документов по открытому каналу. Большинство современных архиваторов позволяют защитить свое содержание от несанкционированной распаковки. Однако, используемые в различных архиваторах методы различаются по степени защищенности используемых в них алгоритмов шифрования.

Известны различные методы атаки на архивные пароли. Одни методы атакуют собственно алгоритм шифрования, используемый в архиве, другие – человеческий фактор.

1. Атака полным перебором – самый трудоемкий метод, но позволяет вскрыть все архивы. Атака осуществляется на основании заданной длины пароля и набора символов, которые пере-

бираются. Скорость атаки зависит от алгоритма проверки пароля, а также от количества символов в наборе и длины.

2. Атака по словарю – атака на человеческий фактор. Алгоритм нахождения пароля, основанный на предположении, что пароль представляет собой некоторое осмысленное слово, либо выражение, введенное на каком-либо языке. По сравнению с методом прямого перебора, скорость взлома значительно возрастает, поскольку любой язык мира содержит меньше слов, чем все возможное множество символов. Для применения этой атаки необходим словарь.

3. Атака посредством изменения одного байта в программе – самый простейший метод взлома. Может использоваться в случаях отсутствия продуманной защиты архивного шифрования.

4. Атака, основанная на правилах. В данном случае осуществляется полный перебор паролей, но состоящих из заданного набора символов. Эти наборы символов указываются экспертом.

5. Атака по открытому тексту. Данный метод позволяет легко вскрыть пароль архива, если известна часть кода открытого текста архива. Например, если архивируется программа, написанная на языке С++, то однозначно в ней присутствует такой открытый текст, как # include.

Метод атаки по открытому тексту может применять к следующим архиваторам: **ARJ** (необходимо знать открытую последовательность символов длиной не менее длины пароля), **ZIP** (надо знать по крайней мере 13 символов открытого текста), **RAR 1.5** (надо знать 3-4 байта открытого текста).

Для защиты от взлома, пользователь должен выбирать архиватор со стойким к взлому алгоритмом шифрования, а также использовать длинные пароли (не менее 6 символов).

Алгоритмы шифрования архиваторов

Архиватор ARJ использует очень слабый алгоритм шифрования - систему Вернама. В архивированном тексте присутствует некоторая неслучайная информация - например, таблица Хаффмана и некоторая другая служебная информация. Поэтому, точно зная или предсказав с некоторой вероятностью значение этих служебных переменных, можно с той же вероятностью определить и соответствующие символы пароля. Использование слабых алгоритмов часто приводит к успеху атаки по открытому тексту. В случае архиватора ARJ, если злоумышленнику известен хотя бы один файл из зашифрованного архива, или известен непрерывный участок открытого текста длиной большей либо равной длине пароля, он с легкостью определит пароль архива и извлечет оттуда все остальные файлы. Дешифрование по методу Вернама позволяет достичь скорости перебора в 300000 паролей/сек. на машине класса Pentium/120.

Система шифрования RAR-архивов (версии 1.5х) хотя и является лучшей, чем у ARJ, все же позволяет вести перебор с достаточно высокой скоростью. Криптостойкость при атаке с использованием открытого текста оценивается в 2^40 итераций, причем из открытого текста необходимо иметь только первые три байта.

Система шифрования RAR-архивов версии выше 2.0 является пока лучшей из всех архиваторов. Криптостойкость при отсутствии открытого текста равняется 255^128, что невообразимо велико. Знание открытого текста никак не поможет злоумышленнику при вскрытии пароля (данные архивы не атакуются по открытому тексту). Скорость перебора паролей архиваторов RAR последних версий чрезвычайно мала. Перечисленные свойства делают архиваторы RAR последних версий наиболее предпочтительными для формирования закрытых архивов.

Использование антивирусных программ

Цель занятия: Целью работы является практическое работа с антивирусными программами и проверка дисков на наличие вирусов.

Дидактические материалы и технические средства к данной теме: Компьютер наиболее распространенным средством нейтрализации вирусов являются **программные антивирусы.**

Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято *делить на следующие группы*: **детекторы; фаги; вакцины; прививки; ревизоры; мониторы.**

Детекторы обеспечивают выявление вирусов посредством просмотра исполняемых файлов и поиска так называемых сигнатур — устойчивых последовательностей байтов, имеющихся в телах известных вирусов. Наличие сигнатуры в каком-либо файле свидетельствует о его заражении соответствующим вирусом. Антивирус, обеспечивающий возможность поиска различных сигнатур, называют **полидетектором.**

Фаги выполняют функции, свойственные детекторам, но кроме того, «излечивают» инфицированные программы посредством «выкусывания» («пожирания») вирусовиз их тел. По аналогии с полидетекторами, фаги, ориентированные на нейтрализацию различных вирусов, именуют **полифагами.**

Вакцины, в отличие от детекторов и фагов, по своему принципу действия напоминают сами вирусы. Вакцина имплантируется в защищаемую программу и запоминает ряд количественных и структурных характеристик последней. Характеристиками, используемыми вакцинами, могут быть длина программы, ее контрольная сумма и т. п.

Прививки - принцип действия основан на учете того обстоятельства, что любой вирус, как правило, помечает инфицируемые программы каким-либо признаком с тем, чтобы не выполнять их повторное заражение.. Прививка, не вносит никаких других изменений в текст защищаемой программы, помечает ее те же признаком, что и вирус, который, таким образом, после активизации и проверки наличия указанного признака считает ее инфицированной и «оставляет в покое».

Ревизоры обеспечивают слежение за состоянием файловой системы, используя для этого подход, аналогичный реализованному в вакцинах. Программа-ревизор в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра файлов. Другое отличие ревизоров от вакцин состоит в том, что каждый просмотр исполняемых файлов ревизором требует его повторного запуска.

Монитор представляет собой резидентную программу, обеспечивающую перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающую у пользователей подтверждение на выполнение операций, следующих за прерыванием. В случае запрета или отсутствия подтверждения монитор блокирует выполнение пользовательской программы.

Особенно много неприятностей доставляют в последнее время различные модификации компьютерных вирусов, поэтому весьма актуальной является информация о возможных последствиях их вторжения и методах защиты от них. В настоящее время известно уже свыше трех тысяч компьютерных вирусов.

Антивирусные программы.

На рынке в настоящее время присутствуют программные средства обнаружения и обезвреживания компьютерных вирусов, представленные в таблице.

Таблица. Современные антивирусные программные средства

Средства защиты	Назначение	Наименование	Принцип действия
Детекторы	Обнаружение зараженных вирусом файлов	ViruScan, NetScan, Aidstest	Поиск участка кода, принадлежащего известному вирусу
фильтры	Перехват «подозрительных» обращений к ОС и сообщение о них пользова-	FluShotPlus, Anti4Us, Flosemm, Disk Monitor,	Контроль действий, характерных для поведения вируса
Доктора (фаги)	Лечение зараженных программ или дисков	Clean-Up, M-Disk, Aidstest, DrWeb	Уничтожение тела вируса

Ревизоры	Постоянная ревизия целостности (неизменности) файлов	Validate	Запоминание сведений о состоянии программ и системных областей дисков, сравне-
Доктора-ревизоры	Обнаружение и лечение зараженных файлов	DrWeb, KAV и др.	Обнаружение изменений в файлах и дисках и возврат их в

Анализ современных антивирусных программ показывает, что в последнее время наметилась явно выраженная тенденция к интеграции различных видов программ в единое программное средство с функциями детектора-ревизора-доктора, что делает это средство удобным для пользователя. К примеру:Антивирус Касперского (KAV), Доктор Web (DrWeb), Нортон Антивирус (NA) и тд.

Однако приходится констатировать, что в настоящее время абсолютной защиты от неизвестных вирусов не существует, поэтому антивирусные программы постоянно обновляются, как правило, не реже одного раза в месяц. Надежно защитить компьютер от вирусов может только сам пользователь. В первую очередь необходимо правильно организовать работу и избегать бесконтрольной переписи программ с других компьютеров. Во-вторых, особую бдительность необходимо проявлять при работе с выходом в компьютерную сеть, где вероятность внедрения компьютерных вирусов резко возрастает. Учитывая то, что в основе большинства вредоносных программ присутствуют программные вирусы, такие программы всегда должны быть в поле зрения пользователя.

План выполнения практических занятий

1. Включить компьютер
2. Используя команду Пуск определить программу антивирус
3. В панели задач , в среде индикаторов определить наличие антивирусной программы
4. Открыть окно антивируса
5. Сканировать диск
6. Получить результаты
7. Охарактеризовать результаты
8. Сканировать съемный диск
9. Закончить работу

Технология защиты сетевых компьютеров. Брандмауэр.

Цель: научиться защищать сетевой компьютер и настраивать брандмауэр.

Средства для выполнения работы:

- аппаратные: компьютер, подключенный к ЛВС;
- программные: ОС Windows XP; приложение ВМ: VirtualBox; виртуальная машина: VM-1.

Теоретические сведения

Особенности защиты информации в компьютерных сетях обусловлены тем, что сети, обладая несомненными преимуществами обработки информации, по сравнению с локальными компьютерами, усложняют организацию защиты, образуя следующие основные проблемные направления:

1. Разделение совместно используемых ресурсов.
2. Расширение зоны контроля.
3. Комбинация различных программно-аппаратных средств.
4. Неизвестный периметр.
5. Множество точек атаки.
6. Сложность управления и контроля доступа к системе.

Сообществом Интернета под эгидой ***Тематической группы по технологии Интернета (Internet Engineering Task Force, IETF)*** разработано много рекомендаций по отдельным аспектам сетевой безопасности, тем не менее, целостной концепции или архитектуры безопасности пока не предложено.

Основная идея состоит в том, чтобы средствами оконечных систем обеспечивать сквозную безопасность.

Экранирование - единственный сервис безопасности, для которого Гостехкомиссия России одной из первых в мире разработала и ввела в действие**Руководящий документ**, основные идеи которого получили международное признание и фигурируют в профилях защиты, имеющих официальный статус в таких странах, как США. Политика безопасности межсетевого экрана базируется на принципе «все, что не разрешено, запрещено»

Межсетевой экран или *Брандмауэр* — это «полупроницаемая мембрана», которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети интранет и контролирует все информационные потоки во внутренний сегмент и из него. *Контроль трафика* состоит в его фильтрации, то есть выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске было отказано. Фильтрация осуществляется на основании набора условий, предварительно загруженных в брандмауэр и отражающих концепцию информационной безопасности корпорации. Брандмауэры могут быть выполнены как в виде аппаратного, так и программного комплекса, записанного в коммутирующее устройство или сервер доступа (сервер-шлюз, прокси-сервер, хост-компьютер и т. д.). Работа брандмауэра заключается в анализе структуры и содержимого информационных пакетов, поступающих из внешней сети, и в зависимости от результатов анализа пропуска пакетов во внутреннюю сеть (сегмент сети) или полное их отфильтровывание. Эффективность работы межсетевого экрана обусловлена тем, что он полностью переписывает реализуемый стек протоколов TCP/IP, и поэтому нарушить его работу с помощью искажения протоколов внешней сети (что часто делается хакерами) невозможно.

Межсетевые экраны обычно выполняют следующие функции:

- физическое отделение рабочих станций и серверов внутреннего сегмента сети (внутренней подсети) от внешних каналов связи;
- многоэтапная идентификация запросов, поступающих в сеть (идентификация серверов, узлов связи и прочих компонентов внешней сети);
- проверка полномочий и прав доступа пользователей к внутренним ресурсам сети;
- регистрация всех запросов к компонентам внутренней подсети извне;
- контроль целостности программного обеспечения и данных;
- экономия адресного пространства сети (во внутренней подсети может использоваться локальная система адресации серверов);
- сокрытие IP-адресов внутренних серверов с целью защиты от хакеров.

Брандмауэры могут работать на разных уровнях протоколов модели **OSI**. *На сетевом уровне* выполняется фильтрация поступающих пакетов, основанная на IP-адресах (например, не пропускать пакеты из Интернета, направленные на те серверы, доступ к которым извне не должен осуществляться; не пропускать пакеты с фальшивыми обратными адресами или с IP-адресами, занесенными в «черный список» и т. д.).
На транспортном уровне фильтрация возможна еще и по номерам портов TCP и флагов, содержащихся в пакетах (например, запросов на установление соединения).
На прикладном уровне может выполняться анализ прикладных протоколов (FTP, HTTP, SMTP и т. д.) и контроль за содержанием потоков данных (запрет внутренним абонентам на получение каких-либо типов файлов: рекламной информации или исполняемых программных модулей, например).

В брандмауэре возможно наличие экспертной системы, которая, анализируя трафик, диагностирует события, потенциально представляющие угрозу безопасности внутренней сети, извещает об этом администратора сети, а в случае опасности она может автоматически ужесточать условия фильтрации и т. д.

Основные компоненты брандмауэра:

- политика сетевого доступа;
- механизмы усиленной аутентификации;

- фильтрация пакетов;
- прикладные шлюзы.

В качестве популярных эффективных брандмауэров называются: ***Netscreen 100, CyberGuard Firewall, Kerio Winroute Firewall, Zone Alarm, Agnitum Autpost Firewall, Jetico Personal Firewall, Internet Connection Firewall.*** Еще одним способом сетевой защиты может быть установленное на сервере специальное программное обеспечение, которое позволяет остальным компьютерам сети эмулировать выход в Интернет, оставаясь при этом «невидимым» со стороны глобальной сети. Такой компьютер называют *прокси-сервером (proxy - доверенный)*. Например, ***Microsoft Proxy Server 2.0.*** который, являясь кэширующим сервером (повышает эффективность работы сети – сокращает сетевой трафик), выполняет функции брандмауэра и обеспечивает безопасный доступ в Интернет и имеет два сетевых адаптера – один соединяет его с сетью, другой – с Интернет. Так как локальная сеть «не видна» из Интернет, то легальный IP-адрес имеет только внешний сетевой интерфейс, а IP-адреса внутри сети могут быть выданы из пула, зарезервированного для изолированных сетей. В ОС **Windows XP** с установленным **SP2** (*Service Pack 2* – пакет обновлений 2) входит брандмауэр. Основные возможности: блокировка доступа компьютерным вирусам и червям, запрос пользователя о выборе действия, ведение журнала безопасности.

Выполнение работы

1. Задание 1. Подготовьте компьютер для выполнения

Лабораторной работы:

1. Запустите виртуальную машину **VM-1.**
2. Перейдите в полноэкранный режим работы ***Выполняйте остальные задания лабораторной работы в виртуальной машине.***

Задание 2. Создайте новую политику IP-безопасности на локальном компьютере:

1. Откройте оснастку **Управление политикой безопасности IP**:
   - откройте диалоговое окно **Запуск программ (*Пуск/Выполнить*)**;
   - введите команду **mmc** и нажмите клавишу ***ENTER***;
   - выполните команду меню ***Консоль/Добавить или удалить оснастку***;
   - откройте окно с доступными оснастками с помощью кнопки ***Добавить***;
   - выберите в списке элемент *Управление политикой безопасности IP* и добавьте его с помощью кнопки ***Добавить***;
   - завершите добавление оснастки кнопкой ***Готово***;
   - закройте диалоговое окно **Добавить изолированную оснастку**;
   - закройте диалоговое окно **Добавить/Удалить оснастку** с помощью кнопки ***OK***.
2. Активизируйте оснастку **Политика безопасности IP на «Локальный компьютер»**. *Справа отобразятся установленные по умолчанию политики.*
3. Запустите мастер создания политик безопасности:
   - вызовите контекстное меню оснастки **Политика безопасности IP на «Локальный компьютер»**
   - выполните команду **Создать политику безопасности IP…**.
4. Ознакомьтесь с информацией мастера и щелкните по кнопке ***Далее***.
5. Установите *Имя политики безопасности IP*:
   - введите в поле **Имя** – *My_politic*.
   - введите в поле **Описание** – *Это политика IP безопасности локального компьютера* и щелкните по кнопке ***Далее***.
6. Настройте *политику безопасного соединения*. Для этого установите флажок *Использовать правило по умолчанию* и щелкните по кнопке ***Далее***.
7. Установите *Способ проверки подлинности правила отклика по умолчанию*:
   - активизируйте **Использовать данную строку для защиты обмена ключами**;
   - введите в нижнее поле *123456789*;
   - закройте окно кнопкой ***Далее***.

8. Закройте мастера создания политики безопасности кнопкой ***Готово***. *Откроется диалоговое окно* ***Свойства: My_politic***.
9.
10. Запустите **Мастер правил безопасности** и настройте правила безопасности:
    - запустите мастер кнопкой ***Добавить***;
    - ознакомьтесь с описанием мастера и - ***Далее***;
    - выберите *Это правило не определяет туннель* и щелкните ***Далее***;
    - выберите *Локальные сетевые подключения* и щелкните ***Далее***;
    - выберите *Использовать сертификат данного центра сертификации (ЦС)*;
    - щелкните **Обзор** и выберите любой сертификат, кнопка ***Далее***;
    - в списке фильтров IP выберите *Полный IP трафик* и щелкните ***Далее***;
    - добавьте *новое действие фильтра*:
        - щелкните по кнопке ***Добавить***;
        - ознакомьтесь с описанием запустившегося мастера и - ***Далее***;
        - введите в поле **Имя** – *My_filter* и щелкните по кнопке ***Далее***;
        - выберите *Разрешить* и щелкните по кнопке ***Далее***;
        - завершите добавление нового действия кнопкой ***Готово***.
    - активизируйте созданное вами действие и измените его параметры:
        - щелкните по кнопке ***Изменить***;
        - выберите *Согласовать безопасность*;
        - щелкните по кнопке ***Добавить*** и выберите *Шифрование и обеспечение целостности*;
        - установите флажок *Принимать небезопасную связь, но отвечать с помощью IPSEC* и щелкните по кнопке ***Далее***;
    - завершите работу мастер кнопкой ***Готово***.
11. Добавьте в политику фильтр для блокировки всех входящих подключений:
    - отключите использование мастера (флажок *Использовать мастер*);
    - откройте диалоговое окно **Созданий новых правил** кнопкой ***Добавить***;
    - откройте диалоговое окно **Добавление фильтра** кнопкой ***Добавить***;
    - добавьте новый фильтр:
        - сбросьте флажок *Использовать мастер*;
        - откройте диалоговое окно **Свойства: Фильтр** кнопкой ***Добавить***;
        - в поле **Адрес источника пакетов** выберите *Любой адрес IP*;
        - в поле **Адрес назначения пакетов** выберите *Мой IP адрес*;
        - установите флажок *Отраженный для блокировки приходящих пакетов*;
        - установите *протокол TCP* для фильтрации (***вкладка Протокол\раскрывающийся список Выберите протокол***);
        - завершите настройку нового фильтра кнопкой ***ОК***;
    - закройте диалоговое окно **Список фильтров** кнопкой ***ОК***.
    - завершите добавление нового правила кнопкой ***ОК***.
12. Закройте диалоговое окно **Свойства: My_politic**.
13. Активизируйте выбранную политику (***контекстное меню созданной политики/Назначить***).
14. Проверьте работу политики, воспользовавшись утилитой **ping** на другом компьютере. *Если политика настроена верно, то утилита* **ping** *выдаст сведения о том что данный компьютер недоступен.*

Задание 3.Настройте фильтрацию IP -трафика.

1. Откройте диалоговое окно свойств **Подключения по локальной сети (*Пуск/Панель управления/Сетевые подключения*)**.
2. Откройте диалоговое окно **Свойства: Протокол Интернета (TCP/IP)** и щелкните по кнопке ***Дополнительно***.
3. Перейдите на вкладку **Параметры**.

4. Откройте окно **Фильтрация TCP/IP** с помощью кнопки ***Свойства***.
5. Установите TCP-порты, которые можно использовать:
    - выберите в разделе **TCP-порты** переключатель *Только* и щелкните по кнопке ***Добавить***;
    - введите **номер порта для протокола HTTPS** – *443*;
    - аналогично добавьте порты
        - для **протокола отправки почты SMTP** – *25*;
        - для **протокола получения почты POP3** – *110*;
        - **протокол FTP** – *21*;
        - **протокол Telnet** - *23*.
    - Щелкните ***ОК*** для применения параметров.
6. Запретите использование протокола **Telnet**.
7. Закройте окно **Дополнительные параметры TCP/IP** кнопкой ***ОК***.
8. Закройте окно **Свойства: Протокол Интернета (TCP/IP)** кнопкой ***ОК***.
9. Проверьте настроенную фильтрацию. Для этого подключитесь по протоколу **Telnet** с другого компьютера (*программа **Telnet** входит в состав ОС **Windows**и используется для работы на удаленном компьютере в командной строке*).

Задание 4. Настройте брандмауэр Windows:

1. Откройте **настройки брандмауэра (*Пуск/Панель управления/Центр обеспечения безопасности/Брандмауэр Windows*)**.
2. Разрешите доступ браузеру **Internet Explorer** к Интернету:
    - перейдите на вкладку **Исключения** и щелкните по кнопке ***Добавить программу***.
    - выберите в списке **Internet Explorer** и щелкните по кнопке ***ОК***.
3. Включите ведение журнала безопасности:
    - перейдите на вкладку **Дополнительно**;
    - щелкните по кнопке ***Параметры*** в разделе **Ведение журнала безопасности**;
    - включите запись пропущенных и успешных пакетов;
    - сохраните сделанные изменения кнопкой ***ОК***.
4. Завершите конфигурирование брандмауэра кнопкой ***ОК***.
5. Подключитесь к сети Интернет с помощью браузера **Internet Explorer** *Если все настроено правильно, то вы сможете выйти в Интернет, в противном случае брандмауэр выдаст сообщение о том, что какая-то программа пытается получить доступ в Интернет*

Основная литература и дополнительная литература а также источник информации

Основная литература

1. Kenneth C.Loudon, Jane P.Loudon. Management Information Systems. New York, 2016. Page 669.
2. A.T.Kenjabayev, M.M.Ikramov, A.A.Allanazarov. Axborot-kommunikatsiya texnologiyalari. O‘quv-qo‘llanma.T.-“O‘zbekitson faylasuflari milliy jamiyati nashriyoti”. 2017.- 408 bet
3. S.S.Gulomov, B.A.Begalov. Informatika va axborot texnologiyalari. Darslik.-T.: “Fan”. 2010.- 628 bet.
4. Информационные технологии в экономике и управлении: учебник /под ред. проф. В.В. Трофимова. 2-е изд., перераб. и доп.- М.: Юрайт, 2016.- 482 с.
5. Автоматизированные информационные технологии в экономике: учебник / Под ред. проф. Г.А. Титоренко. 2-е изд. Перераб. и доп. - М.: Юнити, 2015. -399 с
6. Kenjabayev A.T., Jumaniyazova M.Yu., Tillyashayxova M.A. Informatika va axborot texnologiyalari. O‘quv qo‘llanma. “MOLIYA-IQTISOD”. 2013, 160 bet.
7. Джуманиязова М.Ю., Икромов М.М., Тилляшайхова М.А., Информационные технологии в экономике, Учебное пособие для экономических вузов. “MOLIYA-IQTISOD”. 2010, 237 стр.

Дополнительная литература

8. “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha harakatlar strategiyasi to‘g‘risida”gi O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi PF-4947-sonli Farmoni.
9. Mirziyoyev Sh.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – Toshkent: “O‘zbekiston” NMIU, 2017. – 488 b.
10. Mirziyoyev Sh.M.Tanqidiy tahlil, qat’iy tartib-intizom va shaxsiy javobgarlik – har bir rahbar faoliyatining kundalik qoidasi bo‘lishi kerak. – Toshkent: “O‘zbekiston” NMIU, 2017. – 104 b.
11. Mirziyoyev Sh.M. Erkin va farovon, demokratik O‘zbekiston davlatini birgalikda barpo etamiz. – Toshkent: “O‘zbekiston” NMIU, 2017. – 56 b.
12. Mirziyoyev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta’minlash – yurt taraqqiyoti va xalq farovonligining garovi. – Toshkent: “O‘zbekiston” NMIU, 2017. – 48 b.

Интернет ресурсы

13. www.gov.uz - O‘zbekiston Respublikasi xukumat portali
14. www.my.gov.uz – Davlat interaktiv xizmatlari portali
15. www.lex.uz - O‘zbekiston Respublikasi Qonun hujjatlar ma’lumotlari milliy bazasi
16. www.udemy.com – ochiq kodli ommaviy on-line kursi
17. www.khanAcademiya.com - ochiq kodli ommaviy on-line kursi
18. www.http://el.tfi.uz - Toshkent moliya instituti elektron kutubxonasi
19. www.http://el.tfi.uz/pdf/akt.uzl.pdf - Toshkent moliya instituti elektron kutubxonasi;
20. www.catback.ru – научные статьи и учебные материалы по экономике