МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ
РЕСПУБЛИКИ УЗБЕКИСТАН

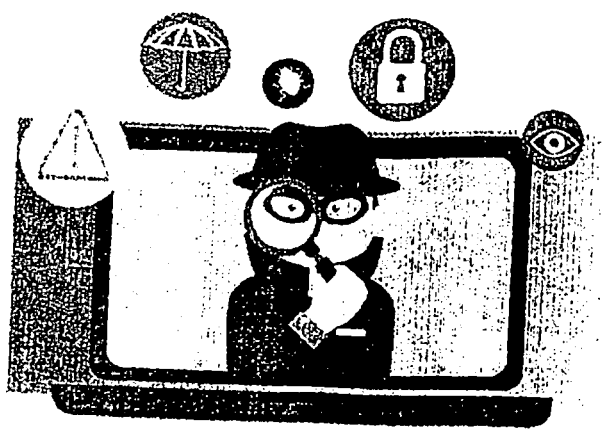
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

ФАКУЛЬТЕТ КИБЕРБЕЗОПАСНОСТИ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

З.И. АЗИЗОВА

МЕТОДИЧЕСКОЕ ПОСОБИЕ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ ПО ПРЕДМЕТУ «ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»



ТАШКЕНТ-2023

Данное методическое пособие содержит теоретические сведения об анализе и оценке рисков информационной безопасности, криптографических методах защиты информации, моделях логического контроля доступа пользователей информационных систем, разведывательных атаках, межсетевом экранировании, в нем также наглядно представлены способы восстановления данных, настройка механизмов аутентификации на основе пароля и настройка межсетевого экрана в ОС Windows, ограничение доступа пользователей системы, процесс восстановления данных со съемных носителей с помощью программного средства TestDisk, процесс установки и настройки антивирусных программ, шифрование данные с помощью программ TrueCrypt/ VeraCrypt, способы сброса паролей, и др.

Каждая практическая работа включает в себя цель работы, краткие теоретические сведения, практическую часть, задания к практической работе, литературу. В целях контроля понимания и усвоения материала каждая тема сопровождается вопросами для самопроверки.

Составители:

Азизова З.И. — старший преподаватель кафедры информационной безопасности ТУИТ им. Мухаммада ал-Хоразмий

Рецензенты:

Керимов К.Ф. — заведующий кафедрой системного и прикладного программирования ТУИТ им. Мухаммада ал-Хоразмий, D.Sc., профессор

Насруллаев Н.Б. — директор Нурафшанского филиала Ташкентского университета информационных технологий им. Мухаммада ал-Хоразмий , PhD, доцент

Практическая работа №1

Тема: Оценка рисков в кибербезопасности

Цель работы: приобретение навыков определения необходимости и детального анализа рисков безопасности для их последующей оценки.

Теоретические сведения:

Анализ диаграммы «галстук-бабочка»: данный метод представляет собой *графическое описание и анализ развития исследуемого нежелательного события от причин до последствий.* Основное внимание в данном методе уделяется контрмерам против исследуемого события и причин, которые к нему приводят.

Выполнение данного метода можно выделить следующие этапы:

1. Определение события для анализа в центре диаграммы.
2. Составление перечня причин, которые могут привести к исследуемому событию.
3. Анализ механизма развития ситуации до исследуемого события
4. Можно описать факторы, которые могут привести к эскалации события и его последствий.
5. Отображение барьеров, которые помешают причинам развиться до события, т.н. предупреждающие меры. Также можно отобразить барьеры для факторов эскалации (см. пункт 4).
6. Составление перечня последствий, к которым может привести исследуемое событие
7. Отображение барьеров, которые помешают изучаемому событию развиться до последствия.

По выполнению анализа «галстук-бабочка» мы получаем простую диаграмму, наглядно демонстрирующую основные пути опасных событий и барьеры, направленные на предотвращение или смягчение нежелательных последствий, или же усиление и ускорение ожидаемых событий (в том случае, если исследуемое событие является положительным).

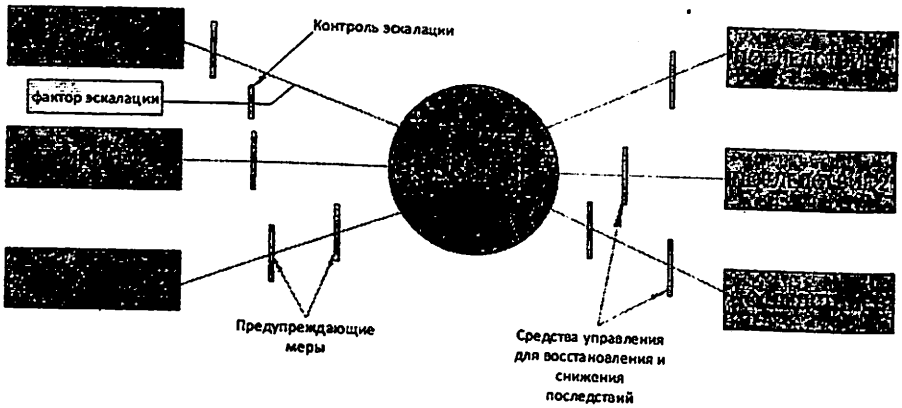


Рис 1.1. Пример диаграммы «галстук-бабочка»

Анализ диаграммы «галстук-бабочка» применяется для отображения риска с указанием ряда возможных причин и последствий. Применяется в случае, когда не требуется детальности анализа «дерева» неисправностей или тогда, когда в большей степени требуется обеспечение наличия барьера или меры управления для каждого способа реализации отказа. Применение данного анализа целесообразно в случае, когда имеются четкие независимые пути развития событий, приводящие к отказу.

Анализ диаграммы «галстук-бабочка» обычно более прост для понимания, чем «дерево» неисправностей и «дерево» событий, и поэтому его применение может быть целесообразно как средство информационного взаимодействия в случаях, когда анализ проводится с применением более сложных методик.

Анализ диаграммы «галстука-бабочки» имеет следующие *преимущества*:

- прост для понимания и позволяет наглядно графически отобразить проблему;
- направлен на рассмотрение мер управления, которые, как предполагается, имеются как в отношении предотвращения, так и уменьшения риска, и их результативности;

- может применяться в отношении благоприятных последствий;
- не требует высокого уровня компетентности для проведения анализа.

Метод имеет следующие *недостатки*:

- не позволяет отображать совокупности причин, возникающих одновременно и вызывающих последствия (случай, когда в «дереве» неисправностей, отражающем левую сторону диаграммы, находится логический элемент «И»);
- может чрезмерно упрощать сложные ситуации, особенно, когда проводится количественное определение.

Анализ «дерева» неисправностей (Анализ дерева отказов, Fault tree analysis, FTA): данный метод используется для идентификации и анализа факторов, которые могут привести к нежелательному событию, так называемому конечному событию. Исследуемые факторы выставляются в последовательность, в которой они могут произойти, и связываются логически. Этими факторами могут быть события, связанные со сбоями или отказами компонентов различного оборудования, например, компьютера, программного обеспечения, ошибками сотрудников или другими событиями, которые могут привести к нежелательному событию.

Для применения данного метода требуется хорошее знание исследуемой системы, как она может выйти из строя, и понимание того, что может привести к нежелательному событию. Может быть очень полезным построение детальной схемы дерева неисправностей. Кроме того, возможно подсчитать вероятность исследуемого нежелательного события. Для этого необходимы сведения о вероятности всех событий, описанных в дереве неисправностей.

Выполнение данного метода можно выделить следующие этапы:

1. *Определение конечного события, которое необходимо проанализировать.* Это может быть отказ или более общие последствия отказа. После того как последствия отказа проанализированы, в дерево неисправностей может быть включена часть, относящаяся к сокращению интенсивности и последствий отказа;

2. *Нахождение возможных причин или видов отказов, приводящих к конечному событию, начиная с конечного события;*
3. *Анализ идентифицированных видов и причин отказа для определения того, что конкретно привело к отказу;*
4. *Последовательная идентификация нежелательного функционирования системы с переходом на более низкие уровни системы*, пока дальнейший анализ не станет нецелесообразным. В технической системе это может быть уровень отказа компонентов. События и факторы на самом низком уровне анализируемой системы называют базисными событиями;
5. *Оценка вероятности начальных событий (если применимо), и последующий расчет вероятности конечного события.* Для обеспечения достоверности количественной оценки следует показать, что полнота и качество входных данных для каждого элемента достаточны для получения выходных данных необходимой достоверности. В противном случае дерево неисправностей недостаточно достоверно для анализа вероятности, но может быть полезным для исследования причинно-следственных связей.

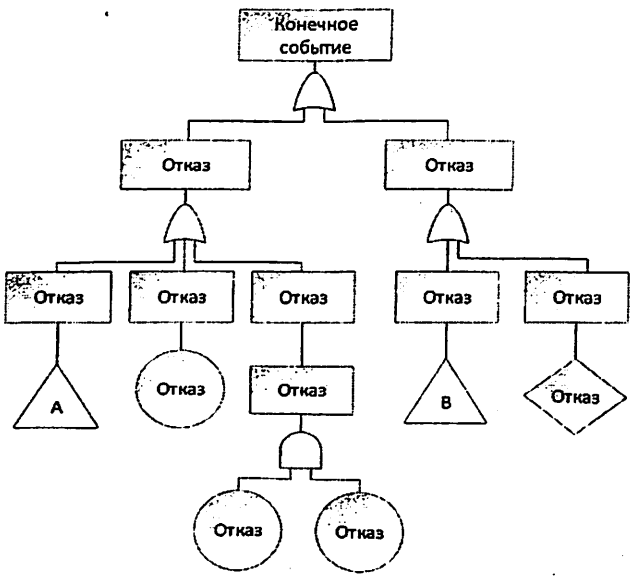


Рис.1.2. Пример диаграммы анализ «дерева» неисправностей

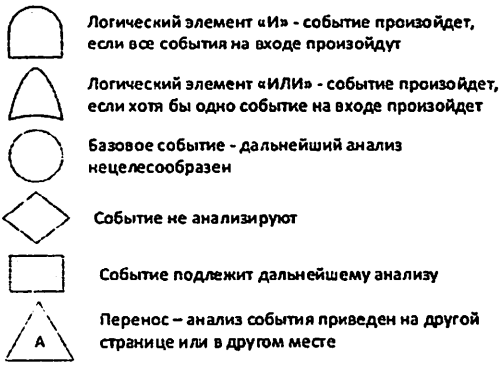


Рис.1.3. Символьные обозначения анализа дерева неисправностей

Анализ дерева неисправностей дает наглядное представление путей возникновения исследуемого конечного события и взаимосвязанных ситуаций, когда может одновременно произойти более одного события. Также можно оценить вероятность конечного события.

Преимущества:

1) Предоставление точного, систематизированного и гибкого подхода позволяет анализировать разнообразные факторы, включая действия персонала и физические явления.
2) Применение подхода "сверху вниз" позволяет рассматривать воздействия тех отказов, которые непосредственно связаны с конечным событием.
3) Применение особенно целесообразно для анализа систем, допускающих подключение большого количества устройств и взаимодействие с ними (систем, имеющих множественные интерфейсы).
4) Графическое представление позволяет упростить понимание функционирования системы и рассматриваемых факторов, но поскольку древовидные схемы зачастую весьма громоздки, их обработка может потребовать применения компьютерных программ, что обеспечивает возможность рассмотрения более сложных логических взаимосвязей (например, с использованием логических операций "*и-не*" и "*не-и*"), но при этом затрудняет верификацию дерева неисправностей.

5) Логический анализ дерева неисправностей и определение набора минимальных сечений полезны при идентификации простых путей отказа в сложных системах, где комбинации событий могут привести к возникновению конечного события.

Недостатки:

1. Неопределенность оценок вероятностей базисных событий влияет на оценку вероятности возникновения конечного события. Это может привести к высокому уровню неопределенности в ситуации, когда вероятность отказа для конечного события точно неизвестна, но достоверность оценок существенно выше для хорошо изученной системы.
2. В некоторых ситуациях начальные события не связаны между собой, и порой трудно установить, учтены ли все важные пути к конечному событию. Например, недостаточное исследование всех источников возгорания может привести к неверной оценке риска возникновения пожара (конечного события). В этой ситуации анализ вероятности с применением метода FTA невозможен.
3. Дерево неисправностей является статичной моделью, в которой фактор временной зависимости не учитывают.
4. Дерево неисправностей может быть применено только к бинарным состояниям (работоспособному/неработоспособному).
5. Несмотря на то что ошибки человека могут быть учтены в схеме дерева неисправностей на качественном уровне, несоответствия степени и качества, часто характеризующие ошибки человека, в дереве неисправностей учесть достаточно сложно.
6. Дерево неисправностей не позволяет легко учесть и исследовать цепные реакции (эффект домино) и условные отказы.

Практическая часть:

Пример выполнения оценки рисков методом анализа «Галстук-бабочка» для нежелательного события «Несанкционированный доступ к информации» приведен на рисунке 1.4.

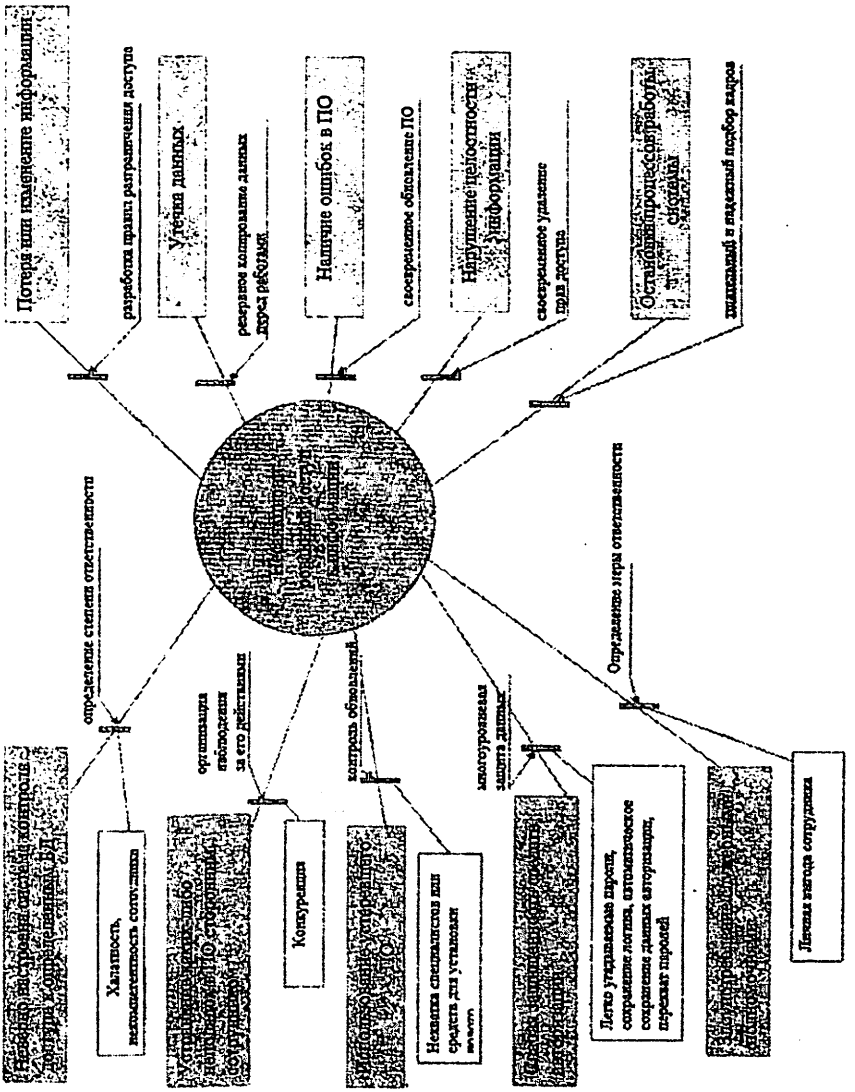


Рис.1.4. Пример заполнения диаграммы анализа «галстук-бабочка» для события «Несанкционированный доступ к информации»

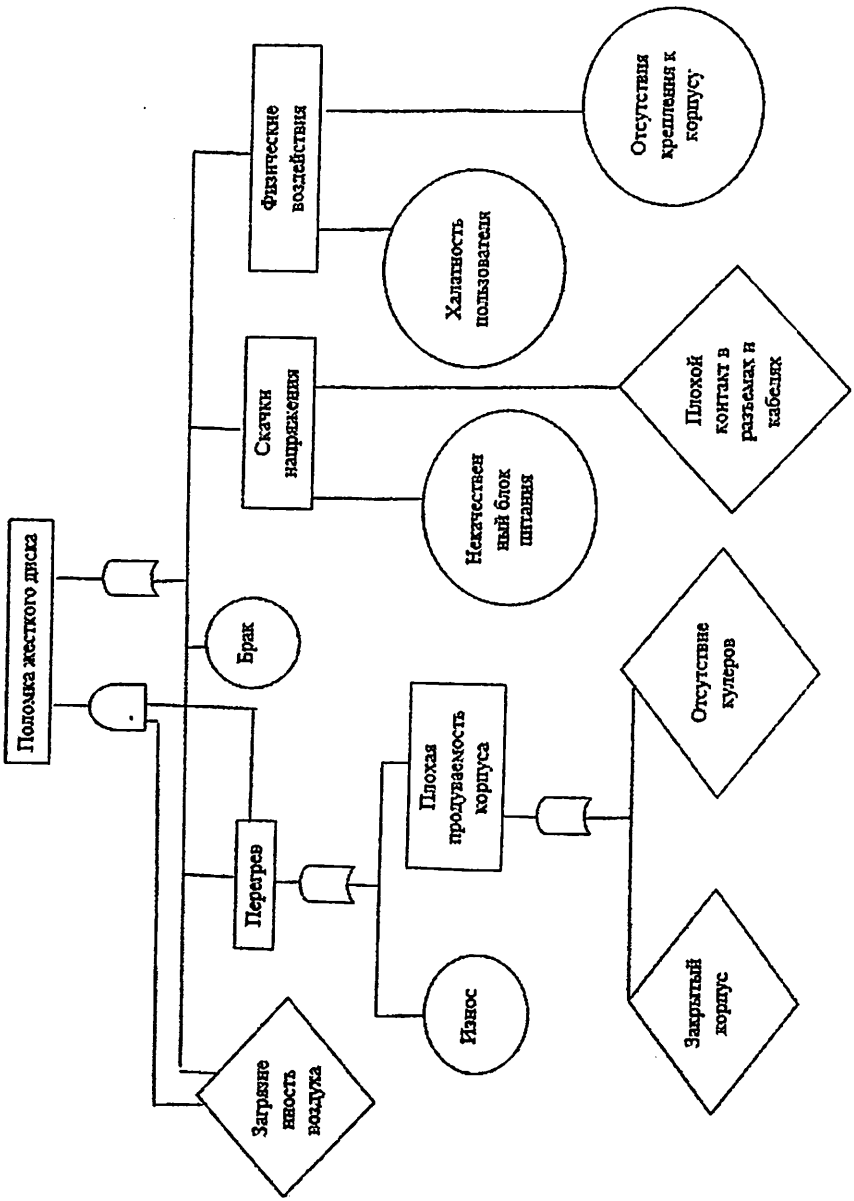


Рис.1.4. Пример заполнения диаграммы анализ «дерева» неисправностей для нежелательного события «Поломка жесткого диска»

Задания к практической работе:

Задание №1. Анализ "галстук-бабочка". Выберите нежелательное событие в области информационных технологий, представляющее собой риск. Используя метод оценки рисков на основе анализа «галстук-бабочка» *проведите анализ выбранного Вами риска, с подробным графическим описанием причин возникновения данного риска* (источника риска), включая факторы эскалации (ухудшающие факторы), контроль эскалации (меры управления ухудшающими факторами), *предотвращающие меры управления*, а также *укажите последствия данного риска и возможные средства управления для восстановления и снижения последствий* (уменьшающие и восстанавливающие меры управления).

В качестве заключения сформулируйте выводы по использованному методу оценки рисков и выполнению данного задания.

Задание №2. Анализ «дерева» неисправностей». Выполните анализ дерева неисправностей одной из причин (источника риска) *возникновения* рассмотренного при анализе «галстук-бабочка» *нежелательного события*, с наглядным представлением путей возникновения конечного события (в вашем случае, рассматриваемой причины наступления нежелательного события) и взаимосвязанных ситуаций, когда может произойти более одного события.

В качестве заключения сформулируйте выводы по использованному методу оценки рисков и выполнению данного задания.

Содержание отчета:

1. Титульный лист;
2. Выполнение задания №1;
3. Выводы по выполнению задания №1;
4. Выполнение задания №2;
5. Выводы по выполнению задания №2;
6. Ответы на контрольные вопросы.

Контрольные вопросы:

1. Дайте определение понятия риск.
2. Для чего необходимо проводить оценку рисков?
3. Какие методы оценки рисков, помимо анализа «галстук-бабочка» и анализа дерева неисправностей, Вы знаете?
4. В чем преимущества и недостатки анализа «галстук-бабочка»?
5. Перечислите преимущества и недостатки метода анализа «дерева» неисправностей.
6. В чем различия рассмотренных методов оценки рисков?

Практическая работа №2

Тема: Принципы работы классических алгоритмов шифрования

Цель работы: приобретение и закрепление практических навыков шифрования и дешифрования сообщений при помощи методов симметричного и асимметричного шифрования, освоение принципов работы алгоритмов RSA и Эль-Гамаля, ЭЦП.

Теоретические сведения:

I. Симметричные криптосистемы

1. Шифрование методом перестановки

Метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока, при этом сами символы не изменяются.

Самая простая перестановка – написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например:

исходный текст: *пусть будет так, как мы хотели*

подготовленный текст: *пусть будет такка кмыхо тели*

зашифрованный текст: *илето хымка ккатт едубь тсуп*

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем зашифровать исходное выражение, следует его дополнить незначащей буквой, например О, до числа, кратного пяти:

пусть будет такка кмыхо телио

Тогда шифрограмма будет выглядеть следующим образом:

оилет охымк аккат тедуб ьтсуп

2. Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций.

Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены. Шифр назван в честь

Контрольные вопросы:

1. Дайте определение понятия риск.
2. Для чего необходимо проводить оценку рисков?
3. Какие методы оценки рисков, помимо анализа «галстук-бабочка» и анализа дерева неисправностей, Вы знаете?
4. В чем преимущества и недостатки анализа «галстук-бабочка»?
5. Перечислите преимущества и недостатки метода анализа «дерева» неисправностей.
6. В чем различия рассмотренных методов оценки рисков?

Практическая работа №2

Тема: Принципы работы классических алгоритмов шифрования

Цель работы: приобретение и закрепление практических навыков шифрования и дешифрования сообщений при помощи методов симметричного и асимметричного шифрования, освоение принципов работы алгоритмов RSA и Эль-Гамаля, ЭЦП.

Теоретические сведения:

I. Симметричные криптосистемы

1. Шифрование методом перестановки

Метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока, при этом сами символы не изменяются.

Самая простая перестановка – написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например:

исходный текст: *пусть будет так, как мы хотели*

подготовленный текст: *пусть будет такка кмыхо тели*

зашифрованный текст: *илето хымка ккатт едубь тсуп*

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем зашифровать исходное выражение, следует его дополнить незначащей буквой, например О, до числа, кратного пяти:

пусть будет такка кмыхо телио

Тогда шифрограмма будет выглядеть следующим образом:

оилет охымк аккат тедуб ьтсуп

2. Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций.

Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены. Шифр назван в честь

римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. Естественным развитием шифра Цезаря стал шифр Виженера. С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

$$y = x + k \,(mod\, n)\,,$$

$$x = y - k \,(mod\, n)\,,$$

где x – символ открытого текста, y – символ шифрованного текста, n - мощность алфавита (кол-во символов), k – ключ.

К *недостаткам* системы Цезаря следует отнести следующие:

- подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста;
- сохраняется алфавитный порядок в последовательности заменяющих букв; при изменении значения k изменяются только начальные позиции такой последовательности;
- число возможных ключей k мало;
- шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте.

Криптоаналитическая атака против системы одноалфавитной замены начинается *с подсчета частот появления символов*: определяется число появлений каждой буквы в шифротексте. Затем полученное распределение частот букв в шифротексте сравнивается с распределением частот букв в алфавите исходных сообщений, например в английском. Буква с наивысшей частотой появления в шифротексте заменяется на букву с наивысшей частотой появления в английском языке и т.д. Вероятность успешного вскрытия системы шифрования повышается с увеличением длины шифротекста.

Концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

3. Одноразовый шифровальный блокнот (метод Вернама)

Одноразовый шифровальный блокнот (one-time pad) – это прекрасная схема шифрования, т.к. при правильной реализации она невзламываема. Она была создана Гилбертом Вернамом в 1917 году и иногда называется шифром Вернама.

Этот алгоритм не использует сдвиг алфавитов, как шифры Цезаря и Виженера, вместо этого он использует блокнот, заполненный случайными значениями. Нам нужно зашифровать некое сообщение и преобразовать его в биты, для этого мы используем наш одноразовый шифровальный блокнот, который заполнен случайными битами. В процессе шифрования используется двоичная математическая функция ***«исключающее ИЛИ»*** **(XOR, ⊕)**.

Схема передачи сообщений с использованием шифрования методом Вернама показана на рис.2.1. Шифрование исходного текста, предварительно преобразованного в последовательность двоичных символов x, осуществлялось путем сложения по модулю 2 символов x с последовательностью двоичных ключей k.

XOR – это операция над двумя битами, она часто используется в двоичной математике и методах шифрования. При выполнении XOR над двумя битами, имеющими одинаковое значение, в результате получается 0 (1 XOR 1 = 0), если значение битов разное, в результате получается 1 (1 XOR 0 =

Например:

Поток сообщения *1 0 0 1 0 1 0 1 1 1*

Ключевой поток *0 0 1 1 1 0 1 0 1 0*

Поток шифротекста *1 0 1 0 1 1 1 1 0 1*

Так, в нашем примере выполняется операция XOR над первым битом сообщения (1) и первым битом в одноразовом блокноте (0), что дает первое значение шифротекста (1). Затем выполняется XOR над следующим битом сообщения (0) и следующим битом в блокноте (0), что дает второе значение шифротекста (0). Этот процесс продолжается пока все сообщение не будет

зашифровано. Полученное в результате зашифрованное сообщение отправляется получателю.

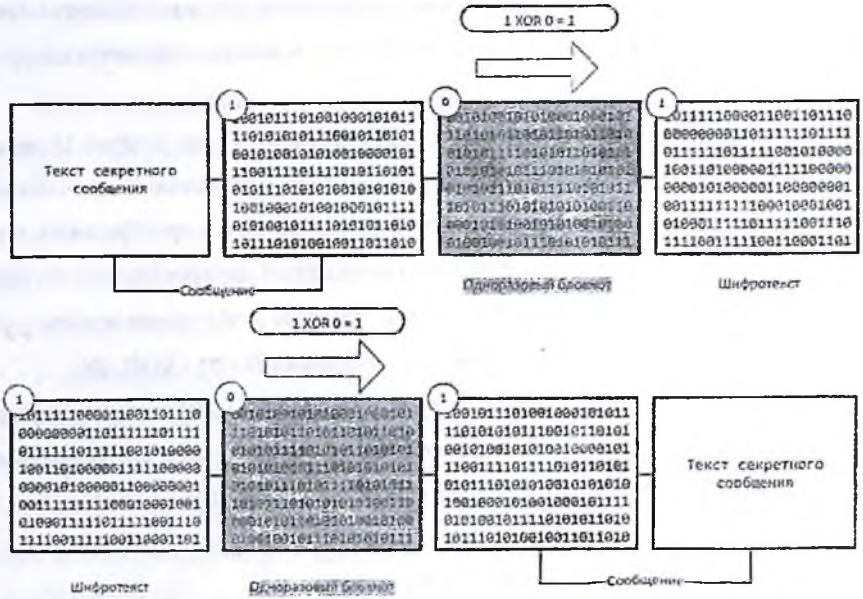


Рис.2.1. Одноразовый шифровальный блокнот

На рисунке 2.1 видно, что получатель должен иметь точно такой же шифровальный блокнот для расшифрования сообщения путем выполнения обратного процесса. Получатель выполняет XOR над первым битом зашифрованного сообщения и первым битом в блокноте. В результате он получает первый бит открытого текста. Получатель продолжает этот процесс, пока не расшифрует все сообщение.

Схема шифрования с использованием одноразового шифровального блокнота считается невзламываемой только в том случае, если в процессе ее реализации выполнены следующие *условия*:

1. *Блокнот должен использоваться только один раз.* Если он используется более одного раза, это может привести к появлению шаблонов (pattern) в процессе шифрования, что поможет злоумышленнику взломать шифр.

2. *Блокнот должен существовать ровно столько же времени, что и само сообщение.* Если он уничтожен раньше, не удастся расшифровать сообщение. А если он используется и в дальнейшем, его многократное применение создает описанную выше проблему с появлением шаблонов.
3. *Блокнот должен распространяться безопасным образом и защищаться получателем.* Это очень сложный и неудобный процесс, поскольку блокноты обычно представляют из себя просто отдельные листы бумаги, которые нужно доставлять с доверенным курьером и надежно охранять в каждом пункте назначения.
4. *Блокнот должен быть заполнен действительно случайными значениями.* Это кажется простой задачей, однако даже современные компьютерные системы не обладают генераторами действительно случайных чисел, на них используются генераторы псевдослучайных чисел.

Схема передачи сообщений с использованием шифрования методом Вернама показана на рис.2.2. Шифрование исходного текста, предварительно преобразованного в последовательность двоичных символов x, осуществлялось путем сложения по модулю 2 символов x с последовательностью двоичных ключей k: $y = x \oplus k$

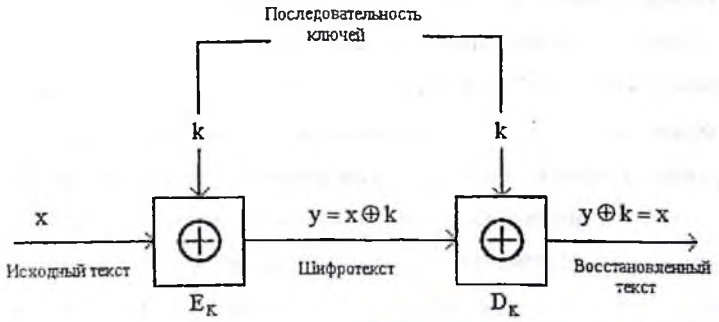


Рис. 2.2. Схема шифрования и расшифрования сообщений по методу Вернама

Практическая часть:

Пример: Сообщение – *VARIANT*, ключ – *TBNCVD*.

Операция XOR

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Сообщение:

V	A	R	I	A	N	T
21	0	17	8	0	13	19
10101	00000	10001	01000	00000	01101	10011

Ключ

T	B	N	C	V	D
19	1	13	2	21	3
10011	00001	01101	00010	10101	00011

Шифрование

Сообщение		V		A		R		I		A		N		T
Ключ		T		B		N		C		V		D		T
		21		0		17		8		0		13		19
		19		1		13		2		21		3		19
	⊕	*10101*	⊕	*00000*	⊕	*10001*	⊕	*01000*	⊕	*00000*	⊕	*01101*	⊕	*10011*
		10011		*00001*		*01101*		*00010*		*10101*		*00011*		*10011*
		00110		*00001*		*11100*		*01010*		*10101*		*01110*		*00000*
		6		2		28		10		21		14		0
Шифротекст		G		B		$		K		V		O		A

II. Асимметричные криптосистемы

1. Шифрование с открытым ключом. Исследование криптоалгоритма шифрования RSA

Данные, зашифрованные открытым ключом, можно расшифровать только секретным ключом. Следовательно, открытый ключ может распространяться через обычные коммуникационные сети и другие открытые каналы. Таким образом, устраняется главный недостаток стандартных криптографических алгоритмов: необходимость использовать специальные каналы связи для распределения ключей. Разумеется, секретный ключ не может быть вычислен из открытого ключа.

В настоящее время лучшим криптографическим алгоритмом с открытым ключом считается *RSA* (по имени создателей: *Rivest, Shamir, Adelman*). Наиболее важной частью алгоритма RSA, как и других алгоритмов с открытым ключом, является процесс создания пары открытый/секретный ключи. RSA — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

В асимметричных криптосистемах отрытый ключ и криптограмма могут быть отправлены по незащищённым каналам. Концепция таких систем основана на применении однонаправленных функций. В качестве примера однонаправленной функции может служить целочисленное умножение. Прямая задача – вычисление произведения двух больших целых чисел p и q, $n = p * q$.

Обратная задача – факторизация или разложение на множители большого целого числа практически неразрешима при достаточно больших значениях n. Например, если $p \approx q$, а их произведение $n = 2^{664}$, то для разложения этого числа на множители потребуется 2^{23} операций. Другим примером однонаправленной функции является модульная экспонента с фиксированным основанием и модулем.

Например, если $y = a^x$, то можно записать, что $x = log_a(y)$.

Задача дискретного логарифмирования формулируется следующим образом. Для известных целых a, n, y следует найти такое число x, при котором $a^x(mod\, n) = y$. Например, если $a = 2^{664}$ и n^{664} нахождение показателя степени x для известного y потребует около 10^{26} операций, что достаточно много.

В связи с тем, что в настоящее время не удалось доказать, что не существует эффективного алгоритма вычисления дискретного логарифма за приемлемое время, то модульная экспонента также условно отнесена к однонаправленным функциям. Другим важным классом функций, используемых при построении криптосистем с открытым ключом являются, так называемые, *однонаправленные функции с секретом*. Функция относится

к данному классу при условии, что она является однонаправленной и, кроме того, возможно эффективное вычисление обратной функции, если известен секрет. В данной практической работе рассаматривается криптосистема *RSA, использующая модульную экспоненту с фиксированным модулем и показателем степени* (т.е. однонаправленную функцию с секретом).

Определение открытого «e» и секретного «d» ключей:

1. Выбор двух взаимно простых больших чисел p и q.
2. Определение их произведения: $n = p * q$.
3. Определение функции Эйлера: $\phi(n) = (p-1)(q-1)$.
4. Выбор открытого ключа e с учётом условий:

$$1 < e \leq \phi(n), \text{НОД}(e, \phi(n)) = 1.$$

5. Определение секретного ключа d, удовлетворяющего условию

$$e * d \equiv 1 \ (mod\ \phi(n)), \text{ где } d < n \quad = e^{-1} \ (mod\ \phi(n)).$$

Алгоритм шифрования сообщения (действия отправителя):

1. Разбивает исходный текст сообщения на блоки $M_1, M_2, \ldots, M_n$

$$M_i = 0, 1, 2, \ldots, n.$$

2. Шифрует текст сообщения в виде последовательности блоков:

$$C_i = M_i^e (mod\ n).$$

3. Отправляет получателю криптограмму: $C_1, C_2, \ldots, C_n$.
4. Получатель расшифровывает криптограмму с помощью секретного ключа d по формуле: $M_i = C_i^d (mod\ n)$.

Таким образом, открытым ключом является $\{e, n\}$, а личным закрытым ключом $\{d, n\}$.

Практическая часть:

Пример: рассмотрим процедуру шифрования данных на следующем примере (для простоты и удобства расчётов в данном примере использованы числа малой разрядности):

1) Выбираем два простых числа p и q, $p = 3$, $q = 11$.
2) Определяем их произведение (модуль) $n = p * q = 3 * 11 = 33$.

3) Вычисляем значение функции Эйлера $\phi(n) = (p-1)(q-1)$:
$\phi(n) = (3-1)(11-1) = 2 * 10 = 20$.
4) Выбираем случайным образом открытый ключ с учётом выполнения условий $1 < e \leq \phi(n)$ и НОД$(e, \phi(n)) = 1, e = 7$.
5) Вычисляем значение секретного ключа d, удовлетворяющего условию:
$$e * d \equiv 1(mod\ \phi(n)), 7 * d \equiv 1(mod\ 20); d = 3.$$
6) Отправляем получателю пару чисел $(n = 33, e = 7)$. Представляем шифруемое сообщение M как последовательность целых чисел 312.
7) Разбиваем исходное сообщение на блоки $M_1 = 3, M_2 = 1, M_3 = 2$.
8) Шифруем текст сообщения, представленный в виде последовательности блоков: $C_i = M_i^e (mod\ n)$. Тогда:
$C_1 = 3^7 (mod\ 33) = 2187\ (mod\ 33) = 9$,
$C_2 = 1^7 (mod\ 33) = 1\ (mod\ 33) = 1$,
$C_3 = 2^7 (mod\ 33) = 128\ (mod\ 33) = 29$.
9) Отправляем криптограмму $C_1 = 9, C_2 = 1, C_3 = 9$.
10) Получатель расшифровывает криптограмму с помощью секретного ключа d по формуле: $M_i = C_i^d (mod\ n)$. Тогда:
$M_1 = 9^3 (mod\ 33) = 729\ (mod\ 33) = 3$,
$M_2 = 1^3 (mod\ 33) = 1\ (mod\ 33) = 1$,
$M_3 = 29^3 (mod\ 33) = 24389\ (mod\ 33) = 2$.

Полученная последовательность чисел 312 представляет собой исходное сообщение M.

2. Исследование электронной цифровой подписи (ЭЦП) RSA

В алгоритмах ЭЦП как и в асимметричных системах шифрования используются однонаправленные функции. ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. ЭЦП представляет собой относительно небольшой объём дополнительной цифровой информации, передаваемой вместе с подписанным текстом. Концепция формирования ЭЦП основана на обратимости асимметричных

шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности подписи, которая реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Система ЭЦП включает две процедуры: - формирование цифровой подписи; - проверку цифровой подписи. В процедуре *формирования подписи* используется *секретный ключ отправителя сообщения*, в процедуре *проверки подписи – открытый ключ отправителя.*

Безопасность системы RSA определяется вычислительной трудностью разложения на множители больших целых чисел. Недостатком алгоритма цифровой подписи RSA является уязвимость её к мультипликативной атаке. Другими словами, алгоритм ЭЦП RSA позволяет хакеру без знания секретного ключа сформировать подписи под теми документами, в которых результат хэширования можно вычислить как произведение результата хэширования уже подписанных документов.

Обобщённая схема формирования и проверки электронной цифровой подписи приведена на рис.2.3.

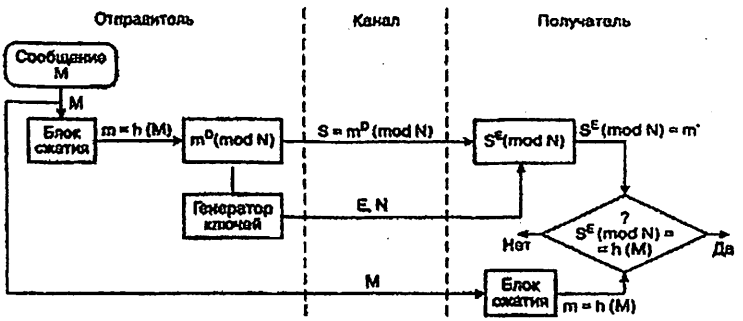


Рис.2.3. Схема электронной цифровой подписи RSA

Алгоритм электронной цифровой подписи (ЭЦП) RSA

Определение открытого «e» и секретного «d» ключей (действия отправителя)

1) Выбор двух взаимно простых больших чисел p и q.
2) Определение их произведения $n = p \cdot q$.
3) Определение функции Эйлера: $\phi(n) = (p-1)(q-1)$.
4) Выбор секретного ключа d с учетом условий: $1 < d \leq \phi(n)$, НОД$(d, \phi(n)) = 1$.
5) Определение значения открытого ключа e: $e < n$,

$$e \cdot d \equiv 1 (mod\ \phi(n)).$$

Формирование ЭЦП

1) Вычисление хэш-значения сообщения M: $m = h(M)$.
2) Для получения ЭЦП шифруем хэш-значение m с помощью секретного ключа d и отправляем получателю цифровую подпись $S = m^d\ (mod\ n)$ и открытый текст сообщения M.

Аутентификация сообщения - проверка подлинности подписи

1) Расшифровка цифровой подписи S с помощью открытого ключа e и вычисление её хэш-значения $m' = S^e\ (mod\ n)$.
2) Вычисление хэш-значения принятого открытого текста M

3) $m = h(M)$.

4) Сравнение хэш-значений m и m', если $m = m'$, то цифровая подпись S – достоверна.

Практическая часть:

Пример: рассмотрим процедуру формирования ЭЦП сообщения M:

Вычисление хэш-значения сообщения M: $m = h(M)$.

Хешируемое сообщение M представим как последовательность целых чисел 312. В соответствии с приведённым выше алгоритмом формирования ЭЦП RSA выбираем два взаимно простых числа $p = 3$, $q = 11$, вычисляем значение $n = p * q = 3 * 11 = 33$, выбираем значение секретного ключа $d = 7$ и вычисляем значение открытого ключа $e = 3$. Вектор инициализации H_0 выбираем равным 6 (выбирается случайным образом). Хэш-код сообщения $M = 312$ формируется следующим образом:

$H_1 = (M_1 + H_0)^2 \ (mod\ n) = (3+6)^2 (mod\ 33) = 81\ (mod\ 33) = 15$;

$H_2 = (M_2 + H_1)^2 \ (mod\ n) = (1+15)^2 (mod\ 33) = 256\ (mod\ 33) = 25$;

$H_1 = (M_1 + H_0)^2 \ (mod\ n) = (3+6)^2 (mod\ 33) = 81 (mod\ 33) = 15$.

Для получения ЭЦП шифруем хэш-значение m с помощью секретного ключа d и отправляем получателю цифровую подпись $S = m^d \ (mod\ n)$ и открытый текст сообщения M:

$$S = 3^7 \ (mod\ 33) = 2187\ (mod\ 33) = 9\ .$$

Проверка подлинности ЭЦП:

Расшифровка S (т.е. вычисление её хэш-значения m') производится с помощью открытого ключа e:

$$m' = S^e \ (mod\ n) = 9^3\ (mod\ 33) = 729\ (mod\ 33) = 3\ .$$

Если сравнение хэш-значений m' и m показывает их равенство, т.е. $m = m'$, то подпись достоверна.

3. Исследование криптоалгоритма шифрования Эль-Гамаля

Схема шифрования Эль-Гамаля может быть использована как для формирования цифровых подписей, так и шифрования данных. Безопасность схемы Эль-Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

В настоящее время наиболее перспективными системами криптографической защиты являются системы с открытым ключом. В таких системах для шифрования сообщения используется закрытый ключ, а для расшифрования – открытый.

Открытый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифровывание данных с помощью открытого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует секретный ключ, который не может быть определён из открытого ключа.

При использовании алгоритма шифрования Эль Гамаля длина шифротекста вдвое больше длины исходного открытого текста М. В реальных

схемах шифрования необходимо использовать в качестве модуля n большое простое число, имеющее в двоичном представлении длину 512 ... 1024 бит.

Следует отметить, что формирование каждой подписи по данному методу требует нового значения k, причём это значение должно выбираться случайным образом. Если нарушитель раскроет значение k, повторно используемое отправителем, то может раскрыть и секретный ключ x отправителя.

Порядок выполнения работы соответствует приведённой ниже криптосистеме шифрования данных по схеме Эль-Гамаля.

Определение открытого «e» и секретного «d» ключей (действия отправителя)

1. Выбор двух взаимно простых больших чисел p и q, $q < p$;
2. Выбор значения секретного ключа x, $x < p$;
3. Определение значения открытого ключа y из выражения: $y = q^x (mod\ p)$;

Алгоритм шифрования сообщения M

1. Выбор случайного числа k, удовлетворяющего условию: $0 \leq k < p - 1$ и НОД $(k, p-1) = 1$;
2. Определение значения a из выражения: $a = q^k (mod\ p)$;
3. Определение значения b из выражения: $b = y^k M\ (mod\ p)$;
4. Криптограмма C, состоящая из a и b, отправляется получателю;
5. Получатель расшифровывает криптограмму с помощью выражения: $M\ a^x = b\ (mod\ p)$;

Практическая часть:

Процедуру шифрования данных рассмотрим на следующем примере.

Пример: (для удобства расчётов в данном примере использованы числа малой разрядности).

1) Выбираем два взаимно простых числа $p = 11$ и $q = 2$;
2) Выбираем значение секретного ключа x, $(x < p)$, $x = 8$;

3) Вычисляем значение открытого ключа y из выражения: $y = q^x \, (mod\ p) = 2^8 \, (mod\ 11) = 256 \, (mod\ 11) = 3$;

4) Выбираем значение открытого сообщения $M = 5$;

5) Выбираем случайное число $k = 9$; НОД $(9, 10) = 1$;

6) Определяем значение a из выражения: $a = q^k (mod\ p) = 2^9 \, (mod\ 11) = 512 \, (mod\ 11) = 6$;

7) Определяем значение b из выражения: $b = y^k \, M \, (mod\ p) = 3^9 * 5 \, (mod\ 11) = 98415 \, (mod\ 11) = 9$.

Таким образом, получаем зашифрованное сообщение как $(a, b) = (6, 9)$ и отправляем получателю.

8) Получатель расшифровывает данный шифротек ст, используя секретный ключ x и решая следующее сравнение: $M * a^x \equiv b \, (mod\ p) = 5 * 6^8 \equiv 9 \, (mod\ 11) = 8398080 \equiv 9 \, (mod\ 11)$

Вычисленное значение сообщения $M = 5$ представляет собой заданное исходное сообщение.

Задания к практической работе:

Задание 1. Зашифруйте с помощью шифра Цезаря открытый текст, заданным согласно варианту ключом (см. в таблице), используя следующий алфавит: *«abcdefghijklmnopqrstuvwxyz»*

Вариант	Открытый текст	Ключ
1	LAWERATTORNEY	11
2	MOUSEKEYBOARD	12
3	NETWORKFIREWALL	13
4	ATTACKDETECTION	14
5	WRONGDIRECTION	15
6	NEWSCALLBACK	16
7	DIRECTDIVISION	17
8	SPEEDBACKBONE	18
9	TRANSPORTLAYER	19
10	NETWORKPROTOCOL	20
11	USERDATAGRAM	21
12	INTERNETLAYER	22
13	NETWORKADAPTER	23
14	COMPUTERSCIENCE	24
15	COMPLEXSOLUTION	25

16	INFORMATIONSECURITY	6
17	SCRIPTINJECTION	7
18	DESIGNSTRUCTURE	8
19	ENGLISHLANGUAGE	9
20	WEBAPPLICATION	10
21	ANOTHERHELLOWORLD	11
22	NETCOMPLICATED	12
23	NEWFRUSTRATIONS	13
24	THEETHERNALSUN	14
25	ANDSQLINJECTION	15

Задание 1.1. Составить блок-схему и программную реализацию шифра Цезаря. Листинг программы шифрования сообщения M с использованием шифра Цезаря отобразить в отчете к практической работе.

Задание 1.2. Расшифруйте следующий шифротекст взломав шифр Цезаря.

а)

iwxh xh djg raphhgddb. xi xh axvwi, ratpc pcs apgvt. iwt gddb xh cxrt. xih rtxaxcv pcs lpaah pgt lwxit, xih uaddg xh qgdlc. iwtgt xh dct sddg pcs iwgtt lxcsdlh xc xi. lwtc xi xh lpgb, iwtn pgt detc. lwtc xi xh rdas, iwtn pgt hwji. iwt sddg xh palpnh hwji lwtc lt wpkt djg athhdch.
iwtgt xh p qaprzqdpgs dc iwt lpaa. lt lgxit dc xi. dc iwt qaprzqdpgs iwtgt pgt hdbt ldgsh. iwtn pgt tcvaxhw ldgsh. lt gtps iwtb: "lt lpci id zcdl tcvaxhw."
lt hxi dc rwpxgh xc ugdci du sthzh. iwt sthzh pgt cxrt pcs vgttc.
iwt itprwtg'h sthz xc ctpg iwt qaprzqdpgs. iwtgt pgt cdi bpcn ejexah xc djg raphh. iwtgt pgt dcan htktcittc xc xi. idspn uxuittc ejexah pgt egthtci, ild pgt pqhtci.
lt atpgc bpcn hjqytrih pi hrwdda. iwtn pgt: gjhhxpc, tcvaxhw, wxhidgn, axitgpijgt, bpiwtbpixrh, ewnhxrh, rwtbxhign, qxdadvn, vtdvgpewn pcs ewnhxrpa igpxcxcv (dg ei).

б)

gur ovt pybpx ba gur gbjre bs gur cnynpr bs jrfgzvafgre va ybaqba vf bsgra pnyyrq ovt ora. ohg ovt ora vf ernyyl gur oryy bs gur pybpx. vg vf gur ovttrfg pybpx oryy va oevgnva. vg jrvtuf 13.5 gbaf.
gur pybpx gbjre vf 318 srrg uvtu. lbh unir gb tb hc 374 fgrcf gb ernpu gur gbc. fb gur pybpx ybbxf fznyy sebz gur cnirzrag orybj gur gbjre.
ohg vgf snpr vf 23 srrg jvqr. vg jbhyq bayl whfg svg vagb fbzr pynffebbzf.
gur zvahgr-unaq vf 14 srrg ybat. vgf jrvtug vf rdhny gb gung bs gjb ontf bs pbny. gur ubhe-unaq vf 9 srrg ybat.
gur pybpx oryy vf pnyyrq ovt ora nsgre fve orawnzva unyy. ur unq gur wbo gb frr gung gur oryy jnf chg hc.

fve orawnzva jnf n ovt zna. bar qnl ur fnvq va cneyvnzrag, "funyy jr pnyy gur oryy fg. fgrcura'f?" fg. fgrcura'f vf gur anzr bs gur gbjre.
ohg fbzrbar fnvq sbe n wbxr, "jul abg pnyy vg ovt ora?" abj gur oryy vf xabja nyy bire gur jbeyq ol gung anzr.

Задание 2. По заданному алфавиту зашифровать сообщение методом Вернама, после чего расшифровать шифротекст и получить исходное сообщение. № варианта выбрать согласно порядковому номеру по списку в журнале.

Алфавит		№ варианта	Сообщение	Ключ
0	A	1	ATTORNEY	GHTR
1	B	2	KEYBOARD	UITEP
2	C	3	FIREWALL	RTYAN
3	D	4	DETECTION	DFCN
4	E	5	DIRECTION	AEDSQ
5	F	6	CALLBACK	NCXZ
6	G	7	DIVISION	FHRTE
7	H	8	BACKBONE	KLSAE
8	I	9	TRANSPORT	IUYTR
9	J	10	PROTOCOL	EWQSD
10	K	11	DATAGRAM	MNCBX
11	L	12	INTERNET	PLMNF
12	M	13	NETWORK	SCVBO
13	N	14	COMPUTER	JKSDA
14	O	15	COMPLEX	XAZJE
15	P	16	SECURITY	JNJERT
16	Q	17	INJECTION	OMFLD
17	R	18	STRUCTURE	IOWER
18	S	19	LANGUAGE	BNDKX
19	T	20	APPLICATION	YTR
20	U	21	ENDOFLIST	ENVM
21	V	22	LOSTDATA	UFGT
22	W	23	SYSTEMFAIL	WERT
23	X	24	ATTERYLOW	QOPD
24	Y	25	HIGHVOLT	YUID
25	Z	26	SQUIDPROXY	GMBH
26	@			
27	#			
28	$			
29	%			
30	&			
31	?			

Задание 2.1. Составить блок-схему и программную реализацию шифра Цезаря. Листинг программы шифрования методом Вернама сообщения M отобразить в отчете к практической работе.

Задание 3. Зашифровать заданное сообщение, используя p и q своего варианта (указано в таблице). Дополнительные параметры рассчитать самостоятельно, например, e = 5, 7, 11, 13, 17, 23 и т.д. Для расчета возведения в степень использовать калькулятор Windows. Выполните проверку правильности дешифрования полученных зашифрованных данных при помощи закрытого ключа $\{d, n\}$.

№	p	q	Сообщение M
1	13	11	15
2	17	13	17
3	19	17	22
4	17	11	12
5	19	13	6
6	23	11	4
7	23	13	8
8	23	17	2
9	23	19	3
10	29	11	7
11	29	13	12
12	29	17	6
13	29	19	4
14	29	23	8
15	31	11	2
16	31	13	3
17	31	17	7
18	31	19	10
19	31	23	5
20	37	11	3
21	37	13	2

Задание 3.1. Составить блок-схему и программы алгоритма шифрования RSA и формирования ЭЦП RSA. Листинг программ шифрования заданного сообщения M с использованием алгоритма RSA отобразить в отчете к практической работе.

Содержание отчета:

1. Титульный лист;
2. Выполнение заданий №1, №1.1, №1.2, выводы по выполнению заданий;

fve orawnzva jnf n ovt zna. bar qnl ur fnvq va cneyvnzrag, "funyy jr pnyy gur oryy fg. fgrcura'f?" fg. fgrcura'f vf gur anzr bs gur gbjre.
ohg fbzrbar fnvq sbe n wbxr, "jul abg pnyy vg ovt ora?" abj gur oryy vf xabja nyy bire gur jbeyq ol gung anzr.

Задание 2. По заданному алфавиту зашифровать сообщение методом Вернама, после чего расшифровать шифротекст и получить исходное сообщение. № варианта выбрать согласно порядковому номеру по списку в журнале.

Алфавит		№ варианта	Сообщение	Ключ
0	A	1	ATTORNEY	GHTR
1	B	2	KEYBOARD	UITEP
2	C	3	FIREWALL	RTYAN
3	D	4	DETECTION	DFCN
4	E	5	DIRECTION	AEDSQ
5	F	6	CALLBACK	NCXZ
6	G	7	DIVISION	FHRTE
7	H	8	BACKBONE	KLSAE
8	I	9	TRANSPORT	IUYTR
9	J	10	PROTOCOL	EWQSD
10	K	11	DATAGRAM	MNCBX
11	L	12	INTERNET	PLMNF
12	M	13	NETWORK	SCVBO
13	N	14	COMPUTER	JKSDA
14	O	15	COMPLEX	XAZJE
15	P	16	SECURITY	JNJERT
16	Q	17	INJECTION	OMFLD
17	R	18	STRUCTURE	IOWER
18	S	19	LANGUAGE	BNDKX
19	T	20	APPLICATION	YTR
20	U	21	ENDOFLIST	ENVM
21	V	22	LOSTDATA	UFGT
22	W	23	SYSTEMFAIL	WERT
23	X	24	ATTERYLOW	QOPD
24	Y	25	HIGHVOLT	YUID
25	Z	26	SQUIDPROXY	GMBH
26	@			
27	#			
28	$			
29	%			
30	&			
31	?			

Задание 2.1. Составить блок-схему и программную реализацию шифра Цезаря. Листинг программы шифрования методом Вернама сообщения M отобразить в отчете к практической работе.

Задание 3. Зашифровать заданное сообщение, используя p и q своего варианта (указано в таблице). Дополнительные параметры рассчитать самостоятельно, например, e = 5, 7, 11, 13, 17, 23 и т.д. Для расчета возведения в степень использовать калькулятор Windows. Выполните проверку правильности дешифрования полученных зашифрованных данных при помощи закрытого ключа $\{d, n\}$.

№	p	q	Сообщение M
1	13	11	15
2	17	13	17
3	19	17	22
4	17	11	12
5	19	13	6
6	23	11	4
7	23	13	8
8	23	17	2
9	23	19	3
10	29	11	7
11	29	13	12
12	29	17	6
13	29	19	4
14	29	23	8
15	31	11	2
16	31	13	3
17	31	17	7
18	31	19	10
19	31	23	5
20	37	11	3
21	37	13	2

Задание 3.1. Составить блок-схему и программы алгоритма шифрования RSA и формирования ЭЦП RSA. Листинг программ шифрования заданного сообщения M с использованием алгоритма RSA отобразить в отчете к практической работе.

Содержание отчета:

1. Титульный лист;
2. Выполнение заданий №1, №1.1, №1.2, выводы по выполнению заданий;

3. Выполнение задания №2 и №2.1, выводы по выполнению заданий;
4. Выполнение задания №3 и №3.1, выводы по выполнению заданий;
5. Ответы на контрольные вопросы.

Контрольные вопросы:

1. Что такое шифрование?
2. В чем различие шифрования от кодирования?
3. Чем отличаются шифры перестановки от шифров замены?
4. Дайте определение и объясните суть симметричного шифрования. Объясните сущность симметричного шифрования.
5. Какие алгоритмы асимметричного шифрования Вы знаете?
6. Преимущества и недостатки алгоритма шифрования RSA.
7. Где может быть использована схема шифрования Эль-Гамаля?

Практическая работа №3

Тема: Шифрование данные с помощью программ TrueCrypt/ VeraCrypt

Цель работы: приобретение навыков работы с программами TrueCrypt/ VeraCrypt, совершенствование знаний по реализации дискового шифрования данных.

Теоретические сведения:

TrueCrypt — компьютерная программа для шифрования для 32- и 64-разрядных операционных систем семейств Microsoft Windows NT5 и новее (GUI-интерфейс), Linux и Mac OS X. Позволяет создавать зашифрованный логический (виртуальный) диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью зашифровать раздел жёсткого диска или иной носитель информации, например USB-флеш-накопитель. Все сохранённые данные в томе TrueCrypt полностью шифруются, включая имена файлов и каталогов. Смонтированный том TrueCrypt подобен обычному логическому диску, поэтому с ним можно работать с помощью обычных утилит проверки и дефрагментации файловой системы.

VeraCrypt — программное обеспечение, используемое для шифрования. VeraCrypt — бесплатный и открытый проект, начатый 22 июня 2013 года в качестве форка TrueCrypt. Запущен и по настоящее время поддерживается Mounir Idrassi, основателем компании IDRIX, после того как 28 мая 2014 года было объявлено о прекращении поддержки программы TrueCrypt.

Практическая часть:

ЧАСТЬ 1. Создание криптоконтейнера TrueCrypt / VeraCrypt

Начнем с создания криптоконтейнера. Запускаем *VeraCrypt / TrueCrypt* и в главном окне жмем на кнопку *Create Volume*.

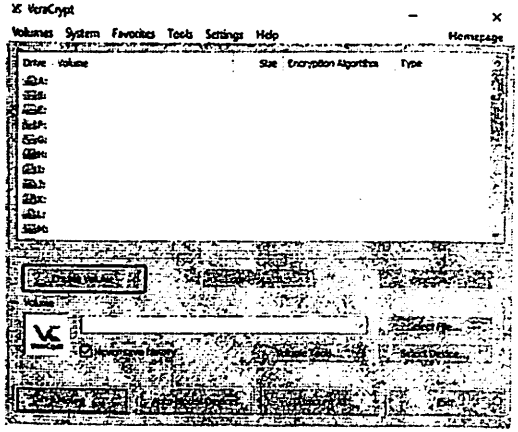


Рис.3.1. Главное окно программы VeraCrypt

Программа спросит, что необходимо зашифровать, и предложит три варианта:

- *Create an encrypted file container* – создать обычный криптоконтейнер, (нам нужен именно он).

- *Encrypt a non-system partition/drive* – зашифровать существующий несистемный раздел на жестком диске, USB-флешке или SD-карте.

- *Encrypt the system partition or entire system drive* – зашифровать диск с уже установленной ОС или же создать дополнительный системный диск. При выборе данной опции необходимо будет вводить пароль каждый раз при загрузке операционной системы.

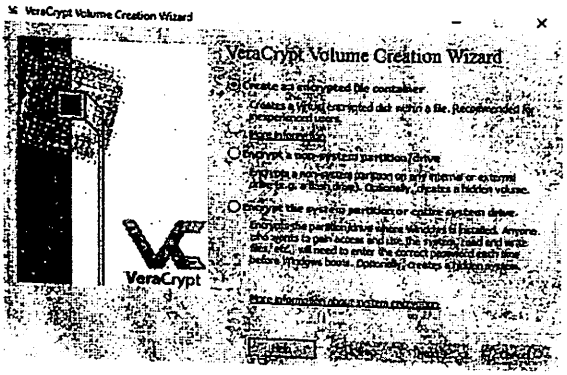


Рис.3.2. Диалоговое окно выбора варианта шифрования

На следующем шаге программа уточнит, какой тип криптоконтейнера необходимо создать: *стандартный* или *скрытый*. В этом работе показано создание стандартного криптоконтейнера - *Standard VeraCrypt volume.*

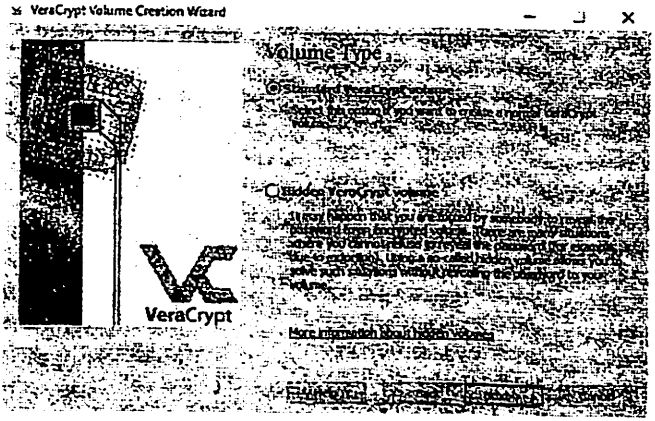


Рис.3.3. Диалоговое окно выбора типа криптоконтейнера

Перейдите к окну выбора имени криптоконтейнера и его расположения. Нажмите *Select File…*

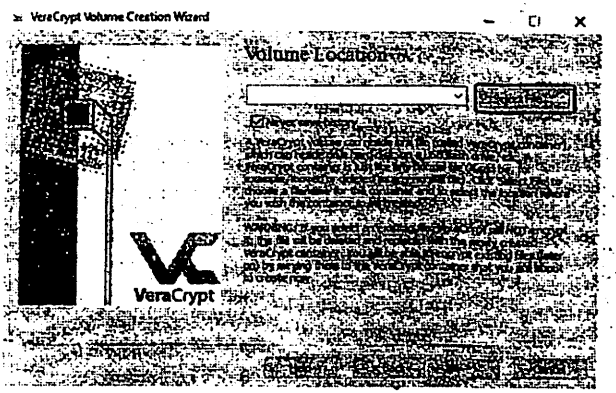


Рис.3.4. Диалоговое окно выбора места хранения криптоконтейнера

Далее откроется окно выбора места для сохранения файла, имени и расширения создаваемого файла. Вы можете выбирать любые расширения и места сохранения файлов, однако не рекомендуется указывать имена,

дублирующие уже существующие файлы. Как видно на скриншоте, криптоконтейнер назван data1.dat и сохранен в папке «Рабочий стол».

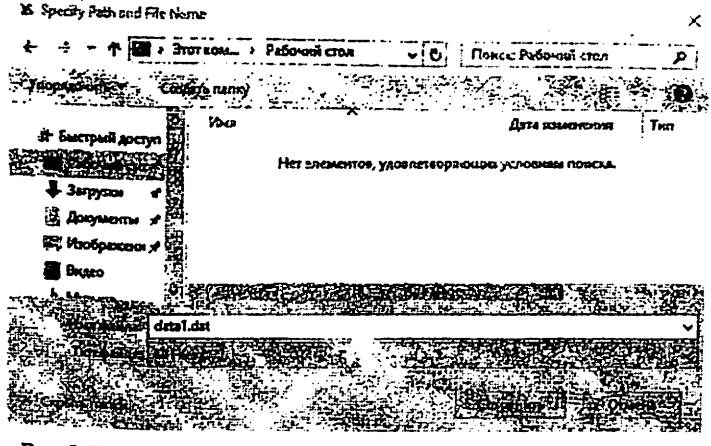


Рис.3.5. Диалоговое окно выбора имени криптоконтейнера

Следующим шагом будет *выбор алгоритма шифрования*. Алгоритм шифрования - это метод, который будет использоваться для шифрования данных - выберите *Serpent-Twofish-AES*.

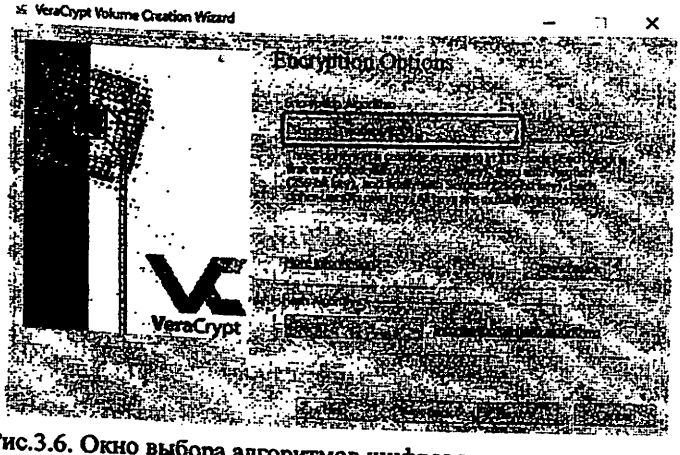


Рис.3.6. Окно выбора алгоритмов шифрования и хеширования

Далее система предложит указать объем памяти создаваемого криптоконтейнера. Обратите внимание на необходимость создания

криптоконтейнера с учетом использования 5% (но не более 100 МБ) под системную информацию и ключ для дешифрования информации.

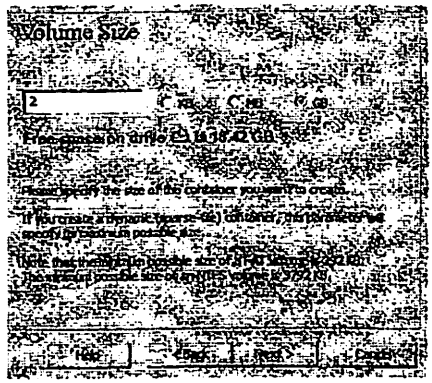


Рис.3.7. Указание объема памяти для создаваемого криптоконтейнера

После выбора выделяемого объема памяти необходимо будет создать пароль для дешифрования криптоконтейнера. Для максимальной защиты рекомендуется использование пароля в связке с файлом-ключом. Для этого активируйте опцию *Use keyfiles.*

Перед созданием пароля и файла-ключа рекомендуем познакомиться с этой главой. Для добавления ключа нажмите на кнопку Keyfiles.

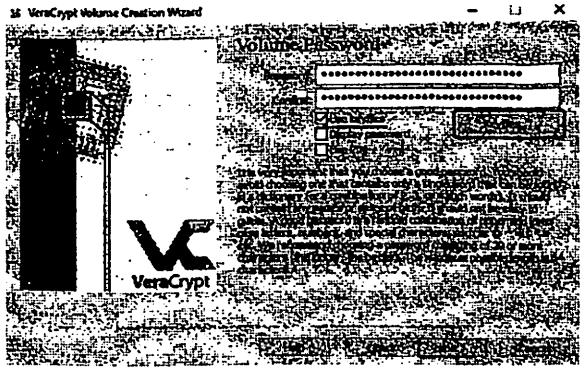


Рис.3.8. Диалоговое окно создания пароля и файл-ключа

В открывшемся окне выберите *Add Files*, если хотите добавить свой файл в качестве ключа, или *Generate Random Keyfile*, если хотите создать файл-ключ.

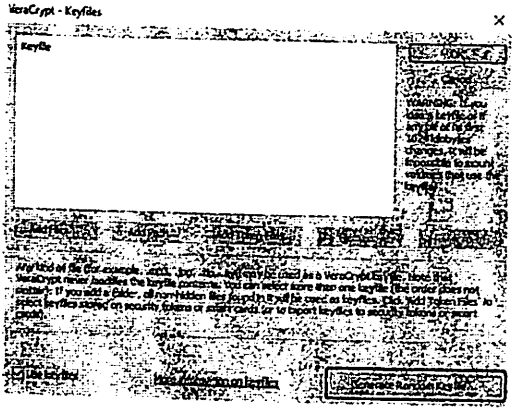


Рис.3.9. Окно генерации файл-ключа

Обычно рекомендуется именно генерация нового ключа. Для этого поводите мышкой по экрану, пока ключ не сгенерируется, затем укажите его имя и нажмите *Generate and Save Keyfiles*. Система потребует выбрать место сохранения созданного файла-ключа.

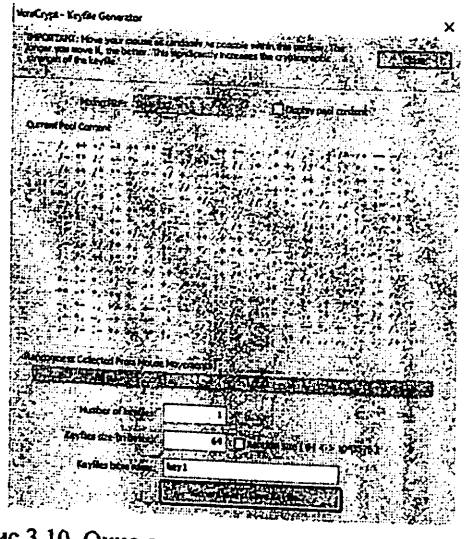


Рис.3.10. Окно генерации нового файл-ключа

Закончив создание ключа, нажмите *Add Files...* и добавьте созданный ключ в список ключей *VeraCrypt / TrueCrypt*, затем выберите его в списке и нажмите *OK*.

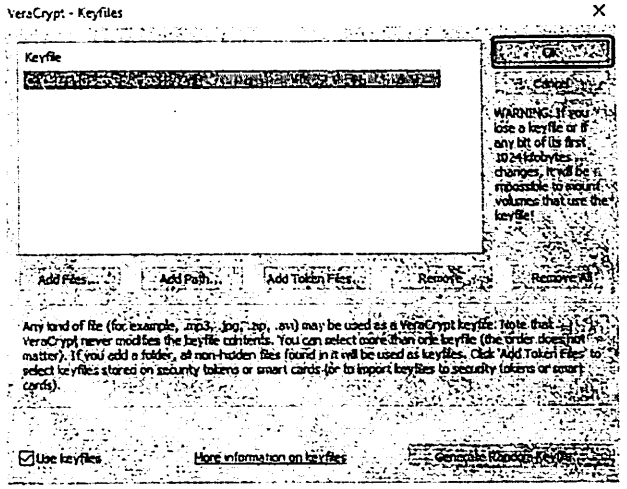


Рис.3.11. Окно выбора файл-ключа

На следующем этапе программа предложит выбрать файловую систему. Пользователям Windows рекомендуется выбор NTFS. После выбора файловой системы для создания криптоконтейнера нажмите *Format*.

Не забудьте основательно поводить мышкой, так как это повлияет на безопасность созданного криптоконтейнера (хотя и весьма косвенно).

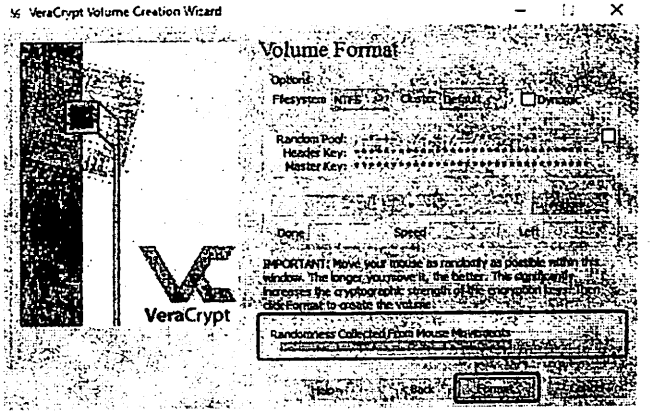


Рис.3.12. Выбор типа файловой системы для криптоконтейнера

Время создания криптоконтейнера зависит от его объема и используемых алгоритмов шифрования. По завершении программа предложит

создать еще один криптоконтейнер. Многих новичков вводит в заблуждение данное окно, и они начинают сомневаться, создался криптоконтейнер или нет. На самом деле, это обычное для VeraCrypt / TrueCrypt завершение создания криптоконтейнера. Просто закройте окно и переходите к использованию созданного криптоконтейнера.

ЧАСТЬ 2. Полнодисковое шифрование с помощью TrueCrypt (для Windows)

Программы полного шифрования диска, (к примеру TrueCrypt), обеспечивает шифрование каждого байта данных на жестком диске компьютера. Она даже шифрует файлы, которые позволяют загрузиться в Windows. TrueCrypt выполняет шифрование файлов, которые позволяют выполнять загрузку Windows. Таким образом, TrueCrypt будет запрашивать пароль при каждой перезагрузке компьютера - до того, как начнется загрузка Windows. Если ваш компьютер попадет в чужие руки, ваши данные будут в безопасности.

Процедура полного шифрования диска предназначена для персонального компьютера на базе Windows. В системах, управляемых Bucknell, используется шифрование Bitlocker от Microsoft, которое предназначено для больших сетей с централизованным управлением. TrueCrypt идеально подходит для автономных систем.

Скачать программу TrueCrypt можно по ссылке: http://www.truecrypt.org/downloads, либо осуществив поиск в Интернете самостоятельно.

!!! Примечание. Создайте резервную копию вашего компьютера! Прежде чем вносить какие-либо серьезные изменения в свой компьютер, всегда полезно создать резервную копию важных файлов.

Запустите программу установки (TrueCrypt Setup N.NN.exe) и

выполните установку по умолчанию. Запустите TrueCrypt, нажав на значок в меню "*Пуск*".

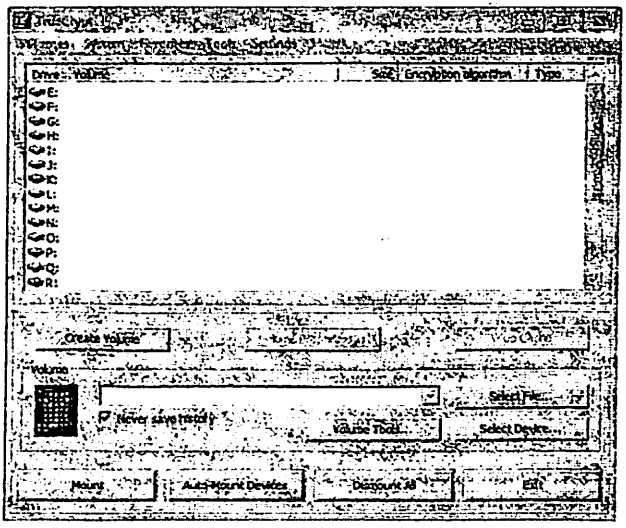


Рис.3.13. Главное окно программы TrueCrypt

Далее в меню *Система* выберите *Шифровать системный раздел/Диск...* Выберите *Обычный*, затем нажмите *Далее*.

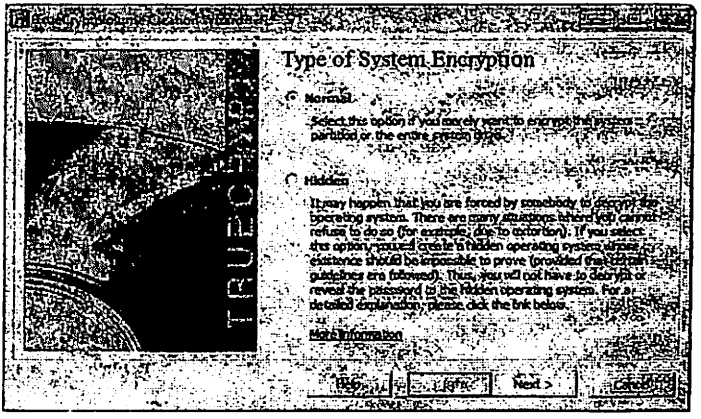


Рис.3.14. Выбор типа шифрования

Выберите *Шифровать системный раздел или весь системный диск*, затем нажмите *Далее*.

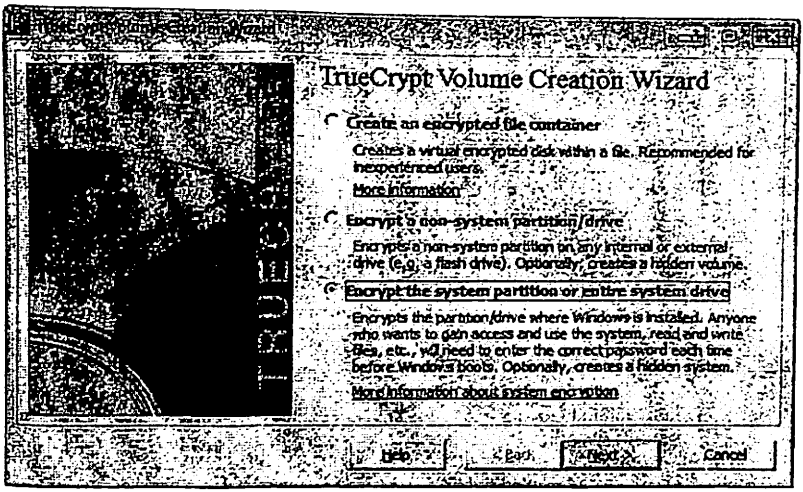


Рис.3.15. Окно выбора типа криптоконтейнера

Выберите *Нет* для шифрования защищенной области хоста, затем нажмите *Далее*.

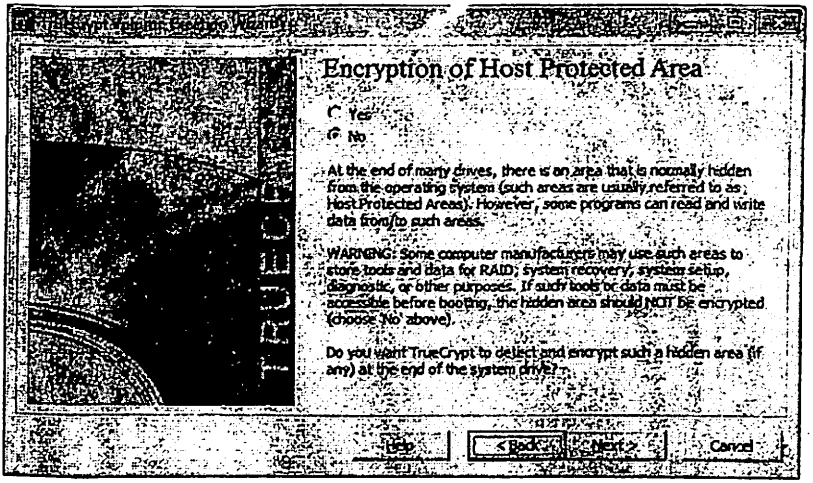


Рис.3.16. Выбор шифрования защищенной области хоста

Выберите *Однозагрузочный*. (Если у вас установлена функция двойной загрузки, в данном случае, вы не сможете использовать полнодисковое шифрование TrueCrypt).

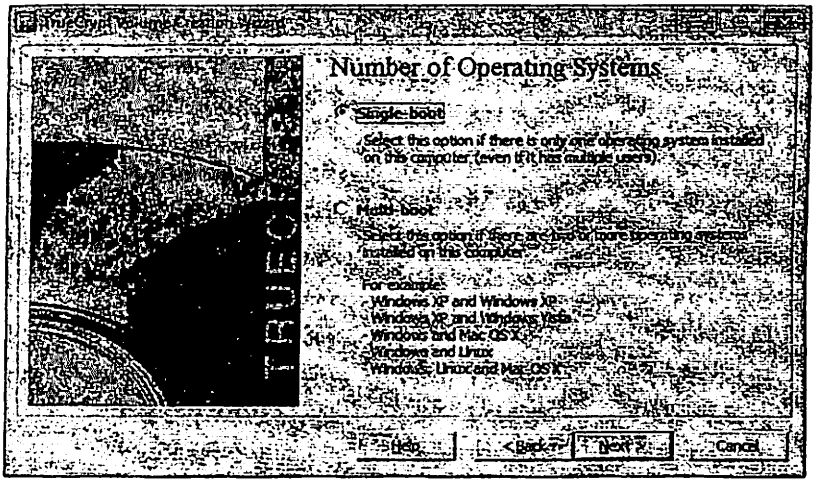


Рис.3.17. Окно выбора количества установленных операционных систем

Примите значения *по умолчанию* на экране Параметры шифрования, затем нажмите *Далее*.

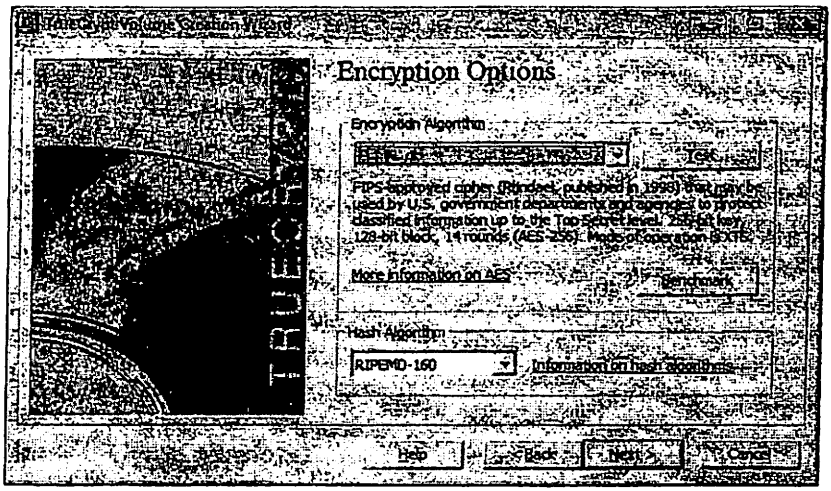


Рис.3.18. Окно выбора параметров шифрования

Выберите надежный пароль и введите его в окне *Пароль*. Выбор надежного пароля - важная часть полного шифрования диска.

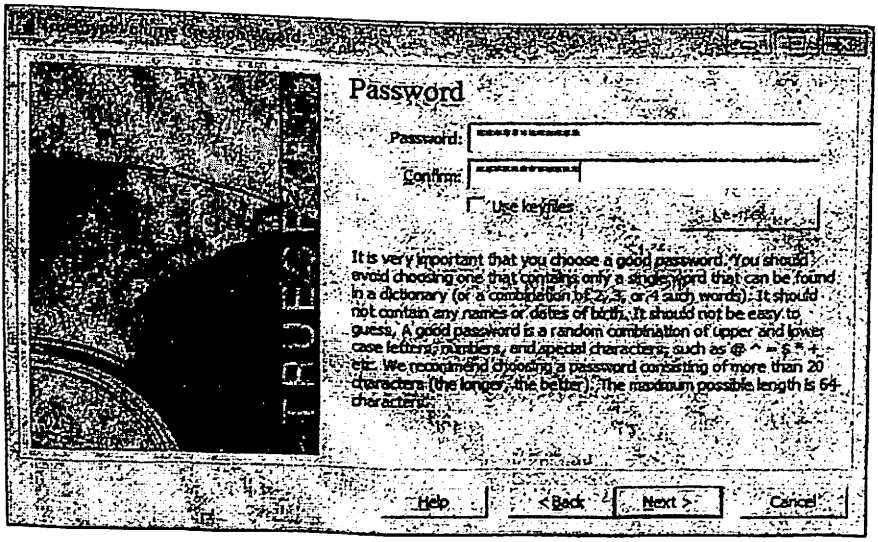


Рис.3.19. Диалоговое окно задания пароля

На экране *"Сбор случайных данных"* поводите мышью случайным образом. TrueCrypt будет использовать показания вашей мыши для генерации высококачественного случайного числа, которое будет использоваться в процессе шифрования. Нажмите кнопку *Далее*.

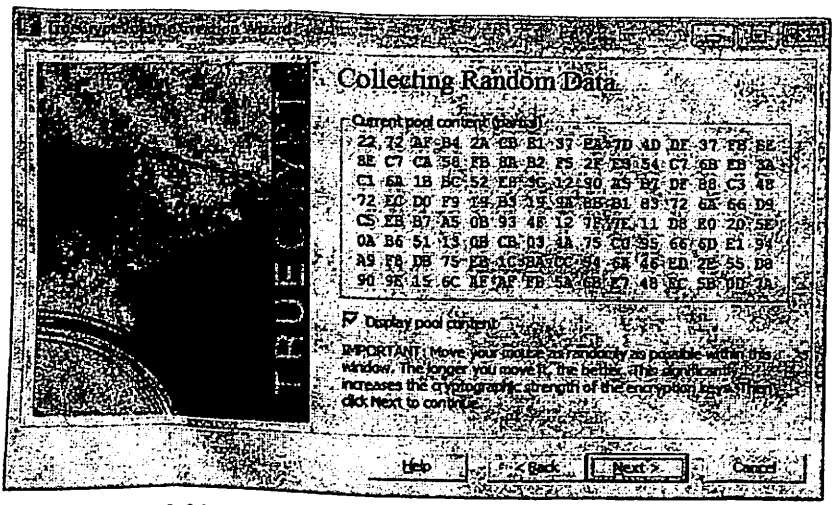


Рис.3.20. Окно генерации случайного значения ключа

На экране создания аварийного диска нажмите *Далее*. TrueCrypt создаст образ CD-ROM в папке *Документы*.

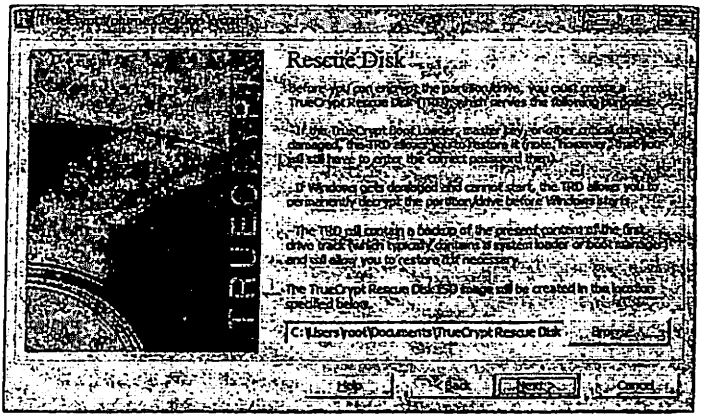


Рис.3.20. Окно создания аварийного диска

На экране *"Создание аварийного диска"* нажмите Далее. Теперь вы должны записать образ диска аварийного восстановления на CD. Этот диск очень важен - если вы потеряете или забудете свой пароль, этот диск будет единственным способом восстановить доступ к компьютеру.

Далее откроется экран программы *записи образа диска Windows*. Вставьте чистый компакт-диск в дисковод, затем нажмите кнопку *Записать*.

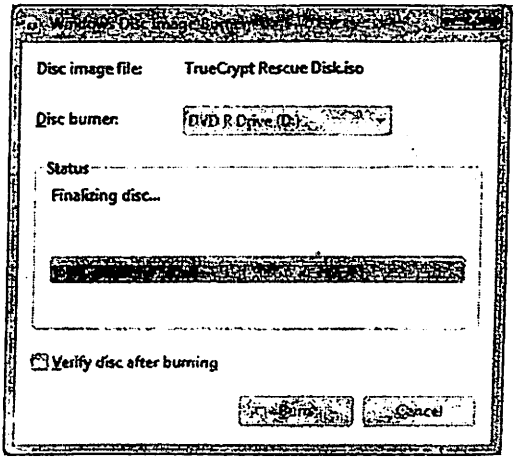


Рис.3.21. Окно записи образа диска

После завершения записи диска система извлечет его из устройства. Вставьте диск обратно, затем нажмите *Далее* на экране записи диска аварийного восстановления.

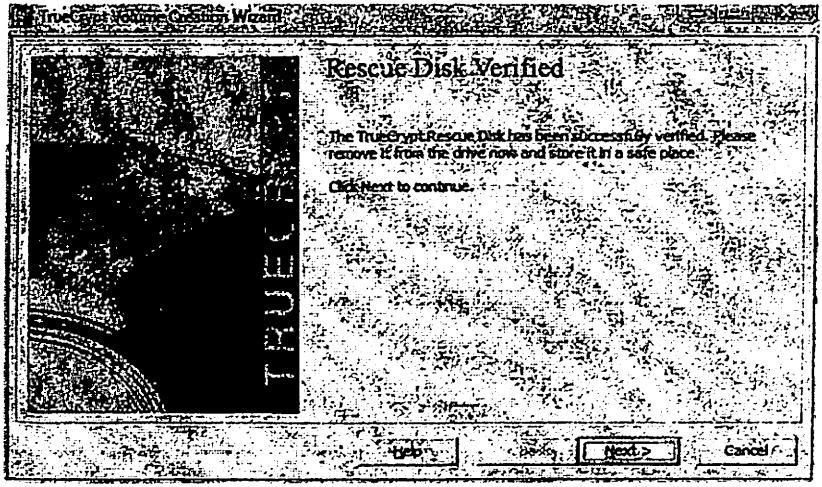


Рис.3.22. Окно завершения создания аварийного диска

На экране режима стирания выберите значение *Никакой* (быстрее всего) None (faster). Нажмите Далее.

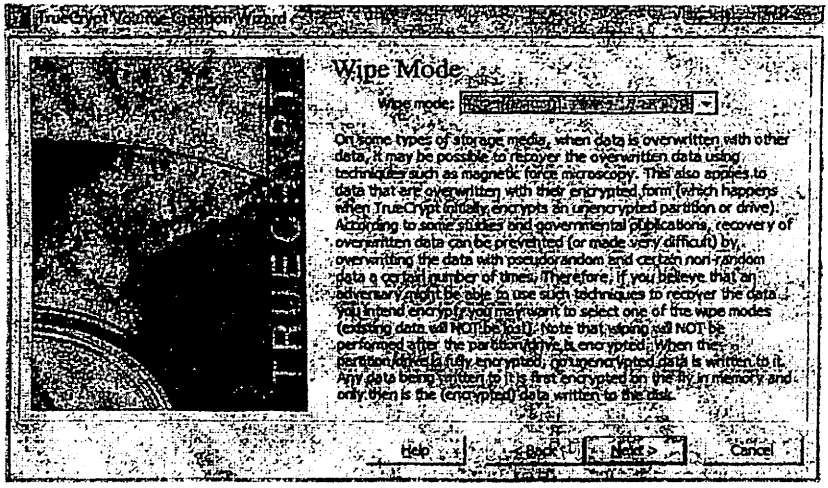


Рис.2.23. Окно выбора режима стирания диска

После этого программа TrueCrypt будет готова перезагрузить систему и начать процесс шифрования. Для этого необходимо выбрать *Да* в диалоговом окне о перезагрузке системы.

После перезагрузки компьютера, но до начала загрузки Windows, TrueCrypt предложит вам ввести пароль. Введите его и нажмите *Enter*.

После появления рабочего стола появится окно TrueCrypt *Предварительная проверка завершена*. Нажмите кнопку *Зашифровать*.

После этого программа Truecrypt начнет шифрование жесткого диска. Это займет определенного времени, в зависимости от скорости компьютера и размера жесткого диска.

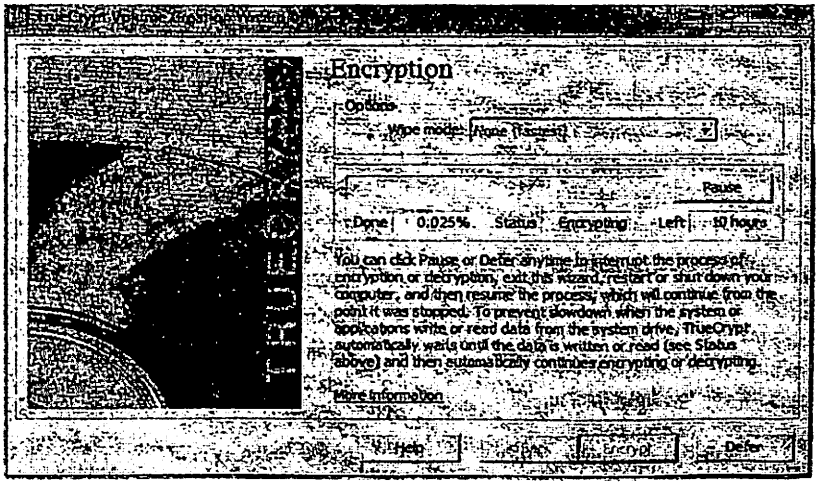


Рис.2.24. Процесс шифрования жесткого диска в программе Truecrypt

После завершения процесса шифрования можете использовать свой компьютер точно так же, как и раньше. Единственное изменение, которое станет заметным - это запрос пароля TrueCrypt, который будет появляться при каждой загрузке системы.

Задание к практической работе: осуществите шифрование данных с помощью программы TrueCrypt или VeraCrypt, выполнив следующие шаги:

1. Установить TrueCrypt. Нам потребуется версия 7.1a. (или VeraCrypt)

2. Создать криптоконтейнер, примонтировать его как виртуальный диск.
3. Поместить в криптоконтейнер какую-то информацию.
4. Отмонтировать диск и переместить криптоконтейнер.
5. Повторно примонтировать криптоконтейнер как виртуальный диск. Убедиться, что криптоконтейнер может передаваться и использоваться независимо.
6. Каждый этап работы с программой отразите в отчете к практической работе с подробным описанием выполняемых действий и скриншотами.

Содержание отчета:

1. Титульный лист.
2. Выполнение задания к практической работе.
3. Выводы по выполнению задания к практической работе.
4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. Что такое шифрование диска?
2. Какие способы шифрования диска вы знаете?
3. Что Вы знаете о шифровании диска и шифровании на уровне файловой системы?
4. Что такое криптоконтейнер?
5. Какие варианты шифрования (режимы) предлагаются в программе VeraCrypt?
6. Какие функциональные возможности программы TrueCrypt Вы знаете?
7. В чем заключаются различие между программами VeraCrypt и TrueCrypt?

Практическая работа №4

Тема: Установка и настройка механизмов аутентификации на основе пароля в ОС Windows

Цель работы: формирование навыков конфигурирования параметров аутентификации, а также сброса пароля в операционной системе Windows 10.

Теоретические сведения:

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации.

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации операционных систем выполняется в рамках локальной политики безопасности.

Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «Локальная политика безопасности» можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на Вашем компьютере;

- включение и отключение записи действий пользователя или группы в журнале событий.

Парольная аутентификация применяется для идентификации и аутентификации пользователей в большинстве современных компьютерных систем. В этом случае *для идентификации пользователь должен ввести свое имя, а для аутентификации ввести пароль* — текстовую строку, известную только ему. Имя пользователя, как правило, назначается ему администратором системы.

Процедура идентификации и аутентификации с использованием пароля предельно проста. Пользователь вводит с клавиатуры имя и пароль, операционная система ищет в списке пользователей запись, относящуюся к данному пользователю, и сравнивает пароль, хранящийся в списке пользователей, с паролем, введенным пользователем. Если запись, относящаяся к входящему в систему пользователю, присутствует в списке пользователей и соответствующий ей пароль совпадает с введенным, считается, что идентификация и аутентификация прошли успешно и начинается авторизация пользователя. В противном случае пользователь получает отказ в доступе и не может работать с операционной системой до тех пор, пока он не будет успешно идентифицирован и аутентифицирован.

Если идентификация и аутентификация пользователя происходят в процессе входа пользователя на удаленный сервер, имя и пароль пользователя пересылаются по сети (как правило, в зашифрованном виде).

Для обеспечения надежной защиты операционной системы пароль каждого пользователя должен быть известен только этому пользователю и никому другому, в том числе и администраторам системы. На первый взгляд то, что администратор знает пароль некоторого пользователя, не отражается негативно на безопасности системы, поскольку администратор, войдя в систему от имени обычного пользователя, получает права, меньшие, чем те, которые он получит, зайдя в систему от своего собственного имени. Однако, входя в систему от имени другого пользователя, администратор получает

возможность обходить систему аудита, а также совершать действия, компрометирующие данного пользователя, что недопустимо в защищенной системе.

Из вышеизложенного следует, что пароли пользователей не должны храниться в операционной системе в открытом виде. Поскольку администратор системы для выполнения своих обязанностей должен иметь доступ к списку пользователей (это необходимо, например, для регистрации новых пользователей), то, если пароли хранятся там открыто, администратор получает к ним доступ. Тем самым администратор получает возможность входить в систему от имени любого зарегистрированного пользователя.

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации операционных систем выполняется в рамках локальной политики безопасности. Оснастка *«Локальная политика безопасности»* используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «Локальная политика безопасности» можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на Вашем компьютере;
- включение и отключение записи действий пользователя или группы в журнале событий.

Наиболее актуальные параметры безопасности собраны в разделе *Локальные политики.*

Политика аудита. Здесь вы можете определить, какие события будут записываться в журнал безопасности. Для включения аудита дважды щелкните на нужном событии и в появившемся окне установите нужные флажки: Успех – для занесения в журнал удачных попыток, Отказ – для фиксации неудачных попыток выбранного действия.

Назначение прав пользователя. В этой категории имеется довольно обширный список параметров, определяющих, что можно и что нельзя делать на компьютере отдельным пользователям и группам. Например, вы можете указать, каким пользователям разрешить локальный вход, а каким – доступ по сети, кто может выполнять завершение работы или изменять системное время.

Параметры безопасности. Здесь собраны различные административные параметры, определяющие поведение системы при входе в нее, доступе к компьютеру из сети, работе с устройствами и др.

По умолчанию Windows учетные данные проверяются в базе данных диспетчера учетных записей безопасности (SAM) на локальном компьютере или в Active Directory на компьютере, присоединенном к домену, через службу Winlogon. Учетные данные собираются с помощью пользовательского интерфейса входа в систему или программно через интерфейс программирования приложения (API), который будет представлен целевому объекту проверки подлинности.

Windows управление учетными данными — это процесс, с помощью которого операционная система получает учетные данные от службы или пользователя и защищает эти сведения для будущей презентации в целевом объекте проверки подлинности. В случае компьютера, присоединенного к домену, целевым объектом проверки подлинности является контроллер домена. Учетные данные, используемые при проверке подлинности, — это цифровые документы, которые связывают удостоверение пользователя с

какой-либо формой проверки подлинности, например сертификатом, паролем или ПИН-кодом.

Сведения о локальной безопасности хранятся в реестре в **HKEY_LOCAL_MACHINE\SECURITY**. Хранимые сведения включают параметры политики, значения безопасности по умолчанию и сведения об учетной записи, такие как кэшированные учетные данные для входа. Копия базы данных SAM также хранится здесь, хотя она защищена записью.

На схеме (рис.4.1) показаны необходимые компоненты и пути, которые учетные данные проходят через систему для проверки подлинности пользователя или процесса успешного входа.

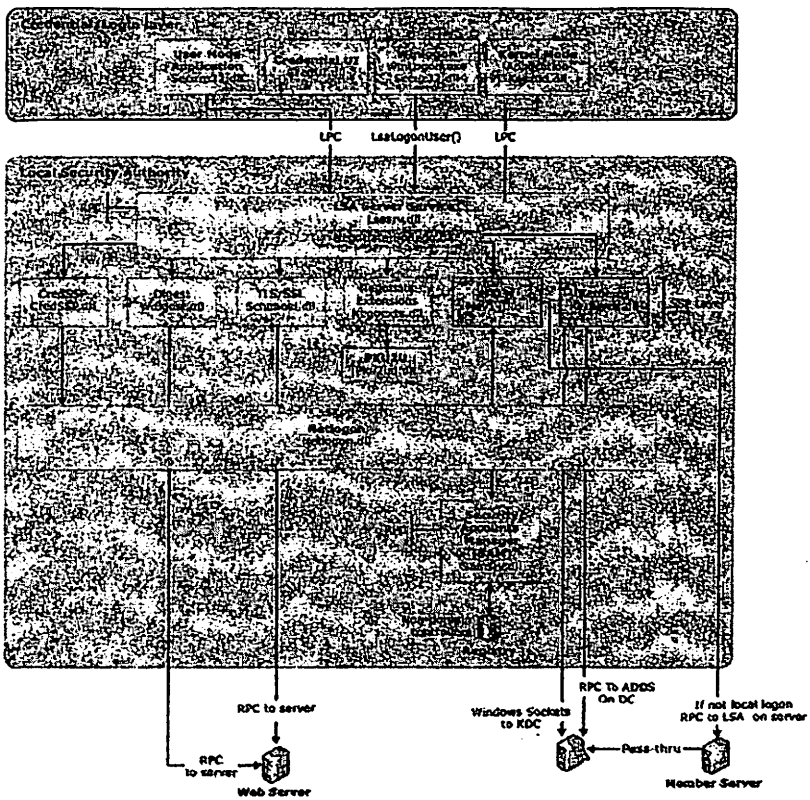


Рис.4.1. Схема проверки подлинности в ОС Windows

В таблице 4.1 приведено описание каждого компонента, который управляет учетными данными в процессе проверки подлинности на момент входа.

Таблица 1. Компоненты проверки подлинности для всех систем

КОМПОНЕНТ	ОПИСАНИЕ
Вход пользователя в систему	Winlogon.exe — это исполняемый файл, отвечающий за управление безопасным взаимодействием с пользователем. Служба Winlogon инициирует процесс входа в Windows операционных систем, передав учетные данные, собранные действием пользователя на защищенном рабочем столе (пользовательский интерфейс входа) в локальный центр безопасности (LSA) через Secur32.dll.
Вход в приложение	Входы в приложение или службу, для которых не требуется интерактивный вход. Большинство процессов, инициированных пользователем в пользовательском режиме, используют Secur32.dll тогда как процессы, инициированные при запуске, такие как службы, выполняются в режиме ядра с помощью Ksecdd.sys. Дополнительные сведения о пользовательском режиме и режиме ядра см. в разделе "Приложения", "Режим пользователя" или "Службы" и "Режим ядра" в этом разделе.
Secur32.dll	Несколько поставщиков проверки подлинности, образующих основу процесса проверки подлинности.
Lsasrv.dll	Служба сервера LSA, которая применяет политики безопасности и выступает в качестве диспетчера пакетов безопасности для LSA. LSA содержит функцию Negotiate, которая выбирает протокол NTLM или Kerberos после определения протокола, который должен быть успешным.
Поставщики поддержки безопасности	Набор поставщиков, которые могут вызывать один или несколько протоколов проверки подлинности по отдельности. Набор поставщиков по умолчанию может изменяться с каждой версией операционной системы Windows, а настраиваемые поставщики могут быть записаны.
Netlogon.dll	Службы, которые выполняет служба net Logon, приведены ниже. — поддерживает защищенный канал компьютера (не следует путать с Schannel) на контроллер домена. — передает учетные данные пользователя через безопасный канал контроллеру домена и возвращает идентификаторы безопасности домена (SID) и права пользователя. — публикует записи ресурсов службы в системе доменных имен (DNS) и использует DNS для разрешения имен в IP-адреса контроллеров домена. — реализует протокол репликации на основе удаленного вызова процедуры (RPC) для синхронизации основных контроллеров домена (PDCs) и контроллеров домена резервного копирования (BDCs).
Samsrv.dll	Диспетчер учетных записей безопасности (SAM), в котором хранятся локальные учетные записи безопасности, применяет локально хранимые политики и поддерживает API.
Реестр	Реестр содержит копию базы данных SAM, параметры локальной политики безопасности, значения безопасности по умолчанию и сведения об учетной записи, доступные только системе.

Практическая часть:

ЧАСТЬ 1. Настройка параметров локальной политики безопасности операционной системы. Для просмотра и изменения параметров

аутентификации пользователей выполните следующие действия: Выберите кнопку **Пуск** панели задач. Откройте меню **Настроить – Панель управления.** В открывшемся окне выберите ярлык **Система и безопасность – Администрирование - Локальная политика безопасности.**

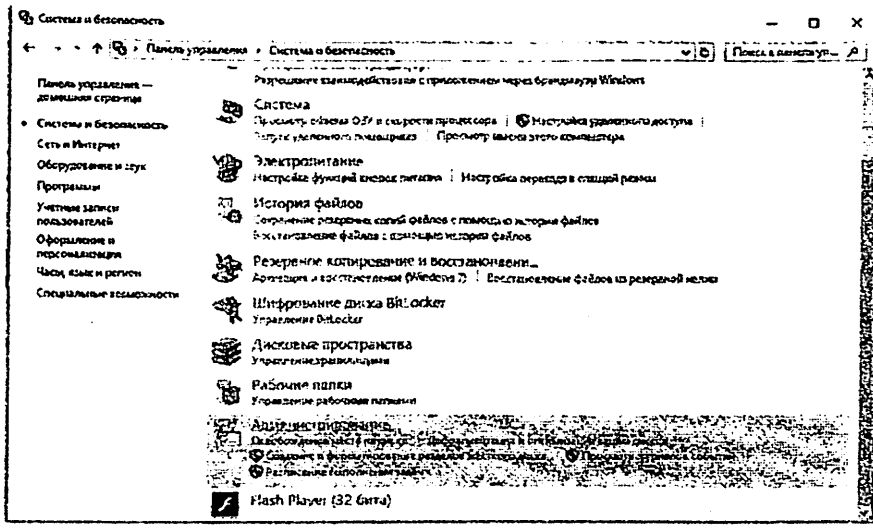


Рис.4.2. Диалоговое окно «Система и безопасность»

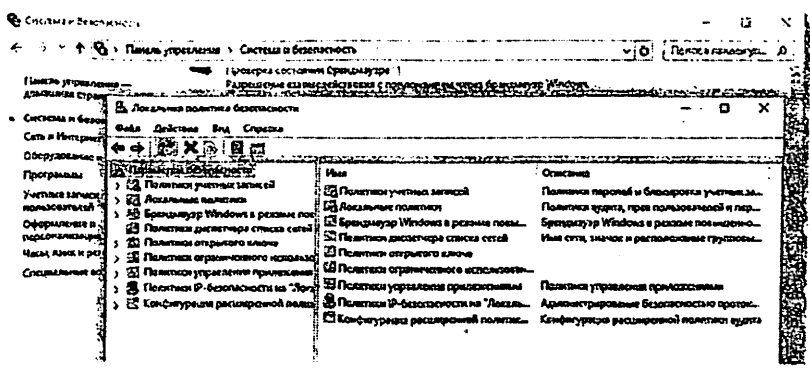


Рис. 4.3. Диалоговое окно «Локальная политика безопасности» - «Параметры безопасности»

Выберите пункт **Политика учетных записей** (этот пункт включает два подпункта: Политика паролей и Политика блокировки учетной записи).

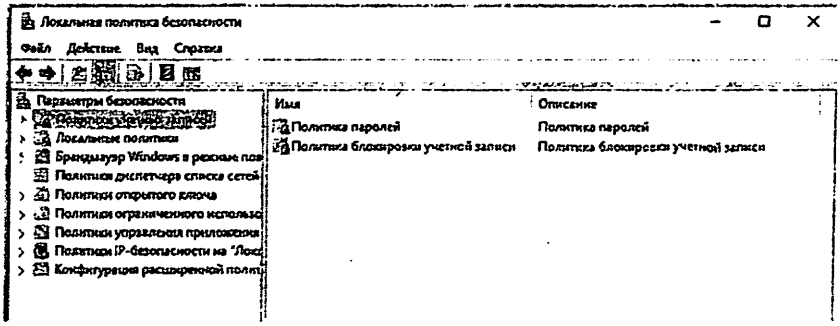


Рис.4.4. Диалоговое окно «Локальная политика безопасности» - «Политики учетных записей»

Откройте подпункт **Политика паролей**. В правом окне появится список настраиваемых параметров (рис.4.4.)

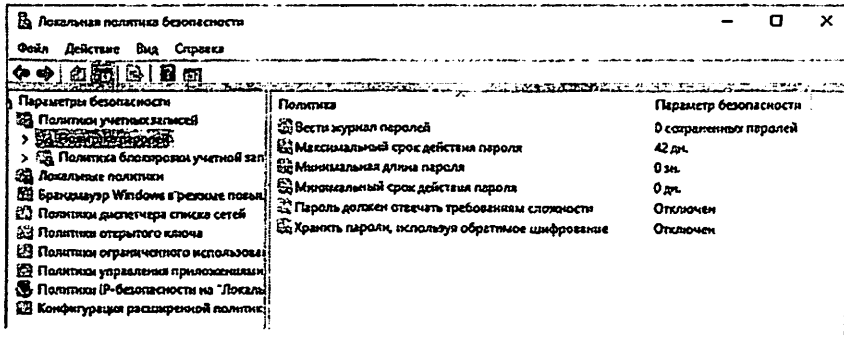


Рис.4.5. Диалоговое окно «Локальная политика безопасности» – «Политика паролей»

В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Ознакомьтесь со свойствами всех параметров.

Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щелкните на изменяемом параметре).

В результате этого действия появится одно из окон, показанных на рисунке 4.6:

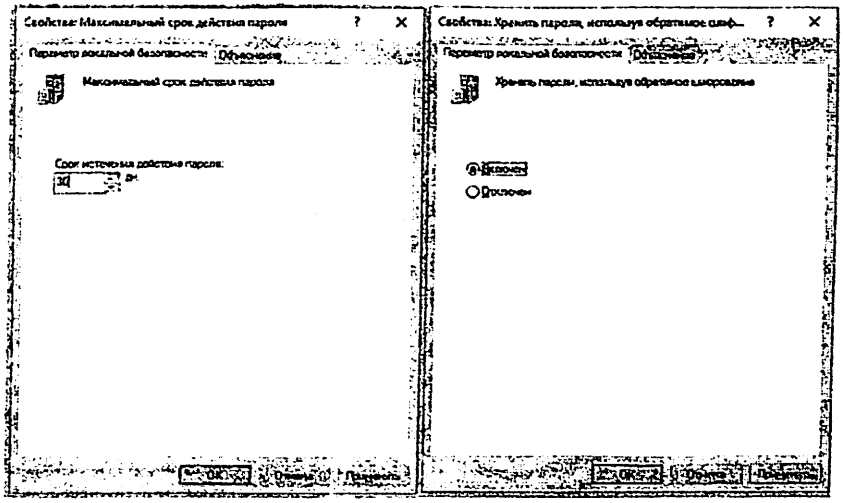


Рис.4.6. Окно настройки свойств политики паролей

Измените значение параметра и нажмите Ок. Например (*обязательно выполнить и сохранить*), выберите параметр **Требовать неповторяемости паролей** и измените его значение на 1.

Для настройки **Политики блокировки учетной записи** выберите этот подпункт и откройте его.

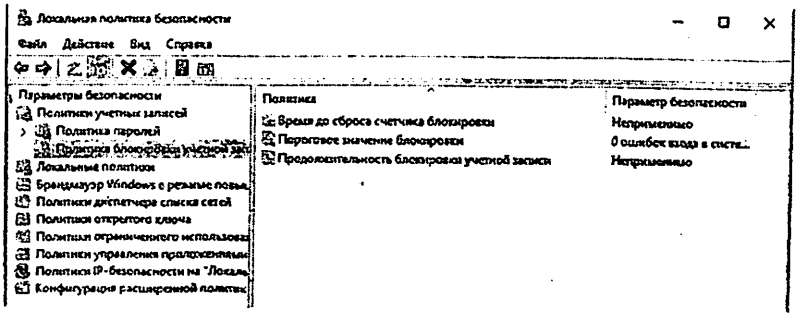


Рис.4.7. Диалоговое окно «Локальная политика безопасности» – «Политика блокировки учётной записи»

Значения параметров данного подпункта **Политики учетных записей** приведены в таблице 2. Ознакомьтесь со свойствами всех параметров. Внесите необходимые изменения.

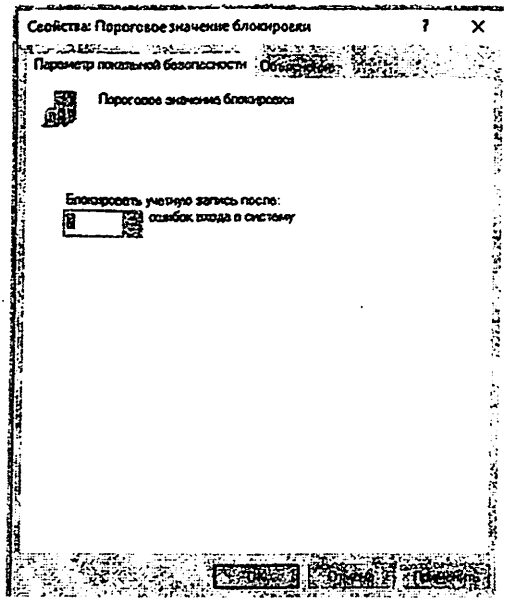


Рис.4.8. Пример конфигурации порогового значения блокировки

Таблица 2. Значения параметров Политики блокировки учетных записей

ПАРАМЕТР	ЗНАЧЕНИЕ
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока она не будет сброшена администратором или пока не истечет ее интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0.
Блокировка учетной записи на	Определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99 999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала *Блокировка учетной записи на.*

ЧАСТЬ 2. Сброс пароля в ОС Windows 10.

Способ 1: изменение пароля в Windows 10 из панели управления.

1. Откройте Панель управления. Установите для параметра «**Просмотр**» значение «**Крупные значки**». Щелкните **Учетные записи пользователей.**

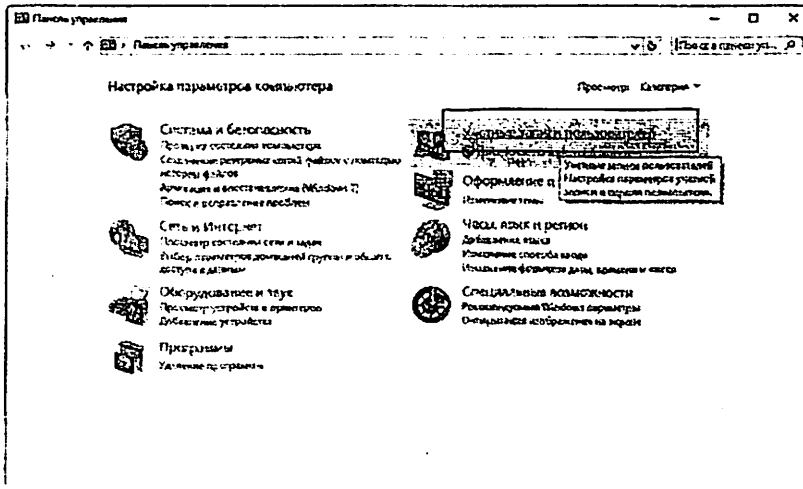


Рис.4.9. Окно настройки параметров компьютера

2. Щелкните ссылку **Управление другой учетной записью.**

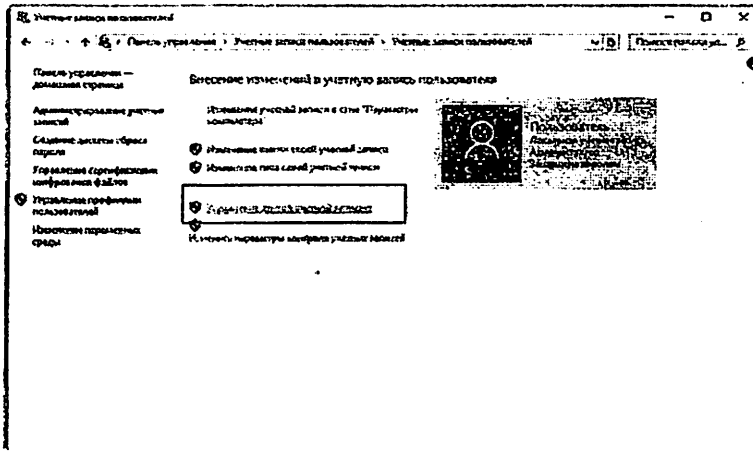


Рис.4.10. Окно управления профилями пользователей

3. Щелкните учетную запись пользователя, для которой вы хотите изменить пароль.
4. На следующем экране нажмите «**Изменить пароль**».

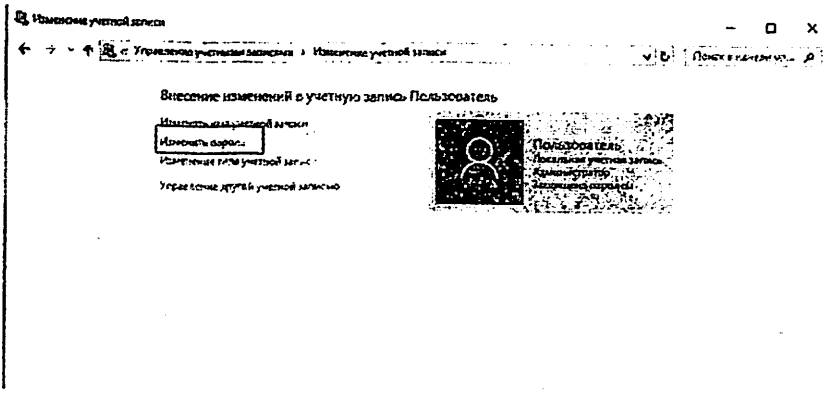


Рис.4.11. Окно внесения изменений в учетную запись Пользователь

5. Введите свой текущий пароль, а затем введите новый, который вы хотите использовать. Щелкните **Изменить пароль**.

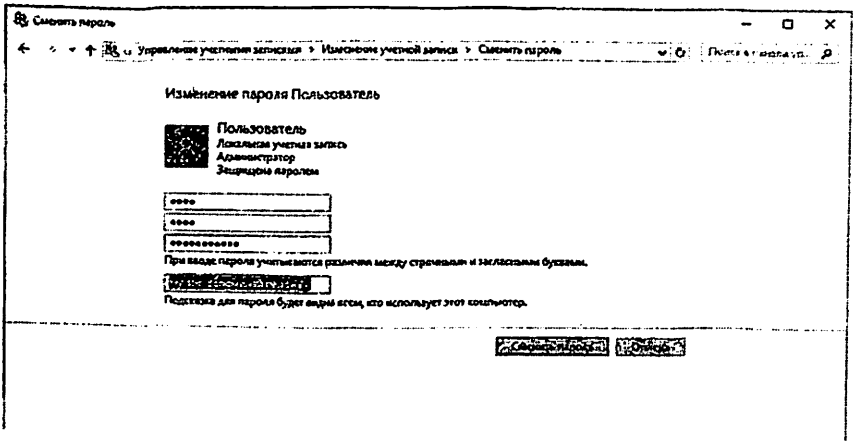


Рис.4.12. Окно смены пароля Пользователя

Способ 2: изменение пароля в Windows 10 в настройках ПК.

1. Нажмите клавиши Windows + I вместе, чтобы открыть приложение «**Настройки**». Нажмите **Учетные записи**.

Рис.4.13. Окно настройки параметров ОС Windows

2. Нажмите «**Параметры входа**» слева и нажмите кнопку «**Изменить**» в разделе «**Пароль**» справа.

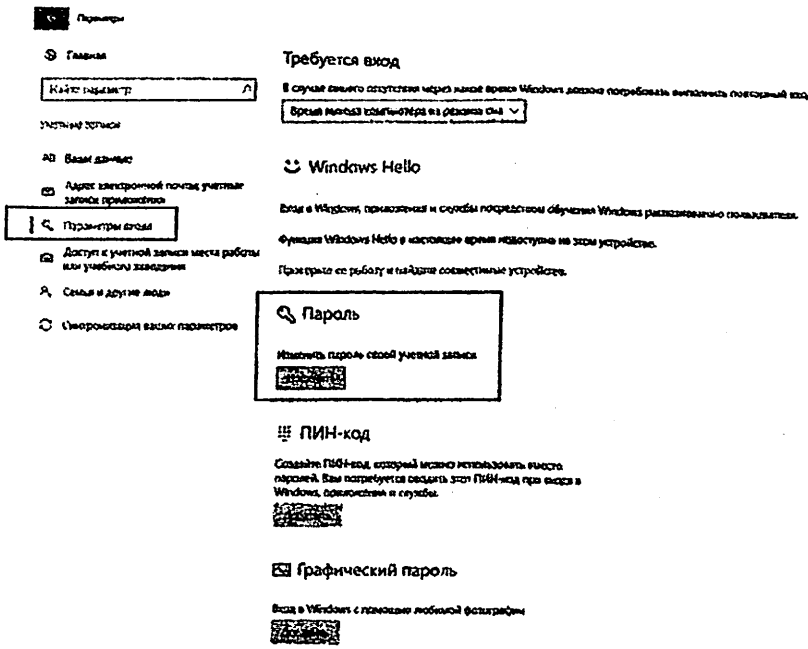


Рис.4.14. Окно настройки параметров входа в ОС Windows

3. Введите текущий пароль и нажмите «Далее».

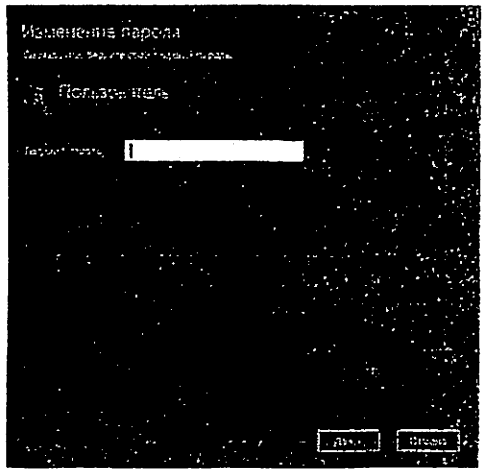


Рис.4.15. Окно ввода текущего пароля пользователя

4. Введите и повторно введите новый пароль, а также установите подсказку для пароля. Нажмите «Далее».

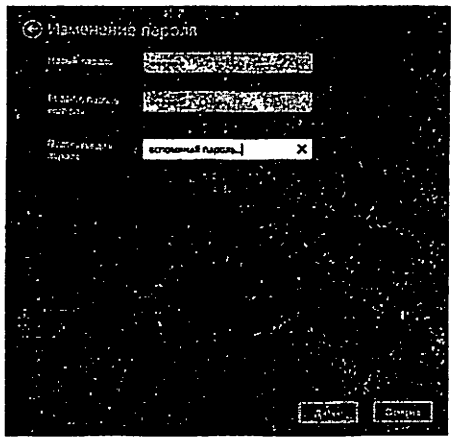


Рис.4.16. Ввод нового пароля пользователя в ОС Windows

Способ 3: изменение пароля Windows 10 в разделе «Управление компьютером».

1. Щелкните правой кнопкой мыши значок «Этот компьютер» на рабочем столе и выберите «Управление».

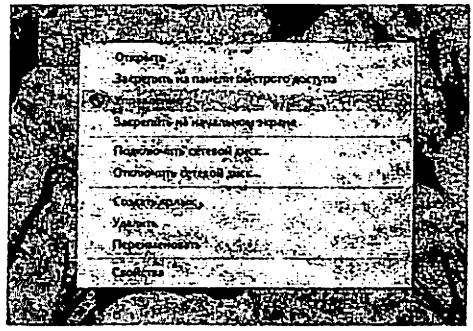


Рис.4.17. Выбор параметра Управление

2. В разделе «Управление компьютером» разверните **«Локальные пользователи и группы» -> «Пользователи»** на левой панели. Щелкните правой кнопкой мыши нужного пользователя в средней панели и выберите **«Задать пароль»**.

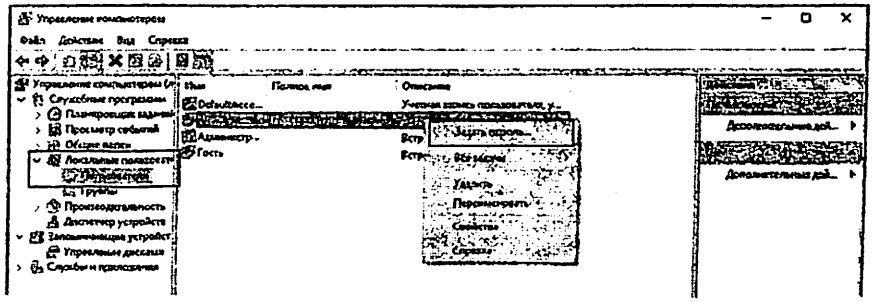


Рис.4.18. Окно управления компьютером в ОС Windows

3. Нажмите кнопку **«Продолжить»** для подтверждения.

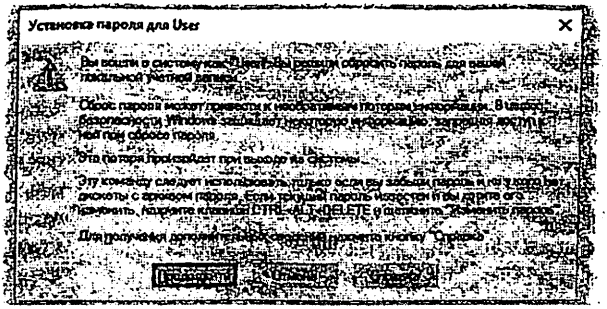


Рис.4.19. Окно подтверждения действий по смене пользовательского пароля

4. Дважды введите новый пароль и нажмите **OK**.

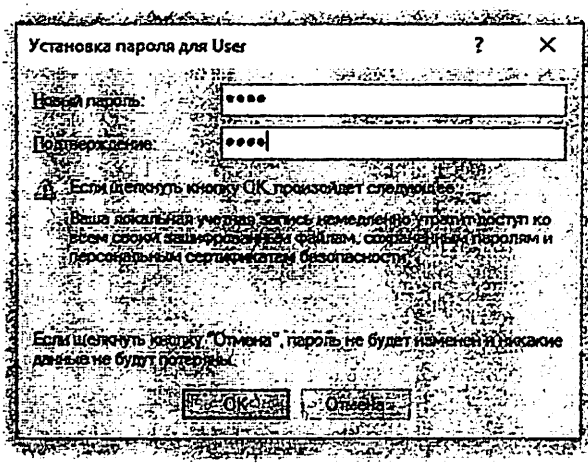


Рис.4.20. Задание нового пароля для учетной записи пользователя

Способ 4: изменить пароль Windows 10 с помощью Netplwiz

1. Нажмите одновременно клавиши Windows + R, чтобы открыть окно «Выполнить». Введите **netplwiz** и нажмите Enter.

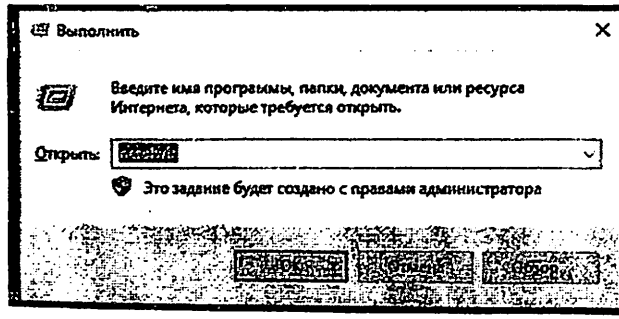


Рис.4.21. Вызов параметров настройки учетной записи пользователей

2. В окне «Учетные записи пользователей» выделите учетную запись пользователя, для которой вы хотите изменить пароль, и нажмите кнопку **«Сбросить пароль»**.

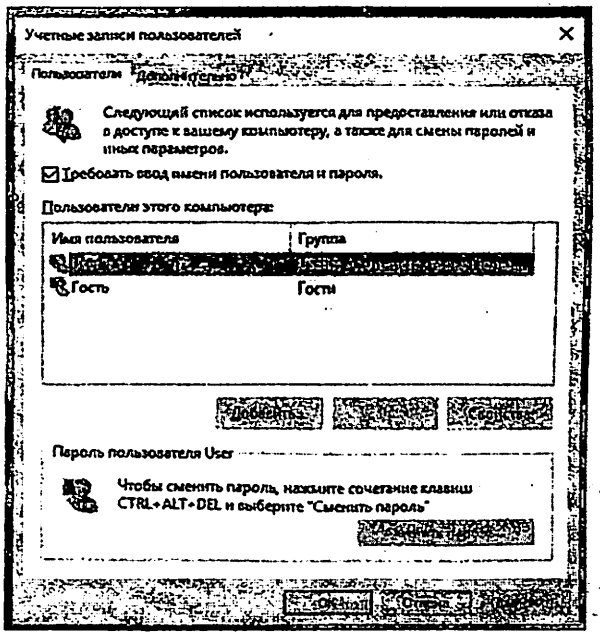


Рис.4.22. Изменение параметров учетной записи пользователя

3. Введите новый пароль для своей учетной записи пользователя и нажмите **OK**.

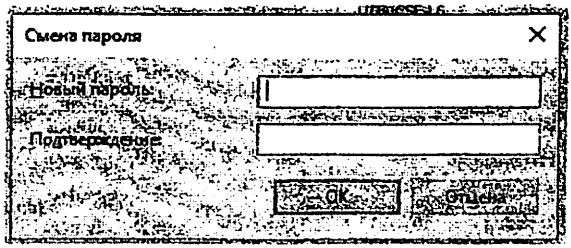


Рис.4.23. Окно смены пользовательского пароля

Способ 5: изменить пароль Windows 10 из командной строки

1. Откройте командную строку с повышенными привилегиями в Windows 10.
2. В командной строке введите **net user** и нажмите Enter. В нем будут перечислены все учетные записи пользователей на вашем компьютере, включая учетную запись, пароль которой вы хотите изменить.

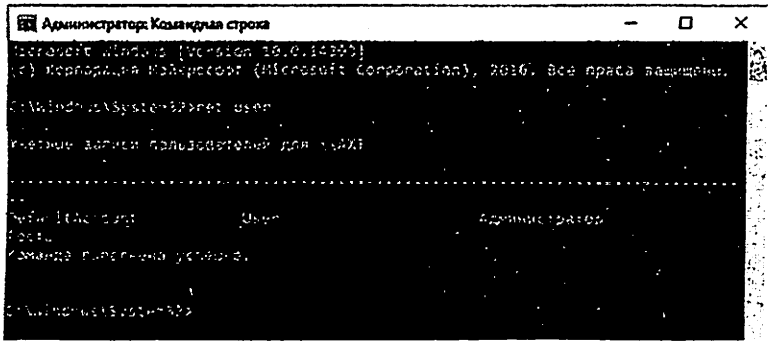


Рис.4.24. Окно с отображением текущих пользователи системы

3. Введите следующую команду, чтобы изменить пароль пользователя. Замените «*Гость*» на имя вашей учетной записи и «*123*» на ваш новый пароль.

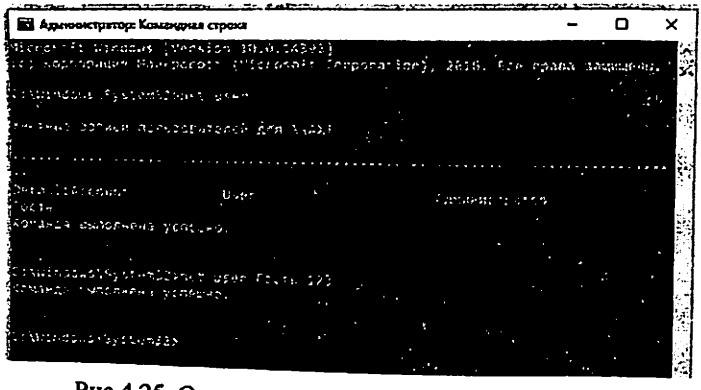


Рис.4.25. Окно смены пароля пользователя Гость

Последние 3 метода позволяют изменить пароль Windows 10 без ввода пароля администратора. Но все эти способы требуют входа в Windows 10 под учетной записью администратора. Если вы потеряете права администратора, вам может потребоваться использовать PCUnlocker для сброса забытого пароля администратора.

Задание к практической работе:

Задание №1. Измените параметр **«Пароль должен отвечать требованиям сложности»** *Политики паролей* на **«Включен»** и после этого

попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы (сделайте скриншоты), проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения *Вашего задания.*

Задание №2. После успешного выполнения первого задания, изменить пароль Вашей учетной записи, а в качестве нового пароля указать прежний пароль. Все сообщения зафиксировать, проанализировать и объяснить поведение системы безопасности.

Задание №3. Произведите настройку других параметрами Политики учетных записей. Выполняемые действия продемонстрируйте в виде скриншотов с подробным описанием всех шагов выполнения.

Задание №4. На основе изученных способов сброса паролей в ОС Windows 10 осуществите изменение пароля администратора системы.

Содержание отчета:

1. Титульный лист;
2. Выполнение заданий к практической работе
3. Выводы по выполнению практической части работы.
4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. Что можно настроить с помощью оснастки Локальная политика безопасности?
2. Поясните связь терминов «идентификация», «аутентификация», «авторизация», «администрирование»
3. Приведите определение и назначение параметра Политики паролей - «Вести журнал паролей».
4. Приведите определение и назначение параметра Политики блокировки учётной записи «Пороговое значение блокировки».

Практическая работа №5

Тема: Реализация разведывательных атак

Цель работы: изучение типов разведывательных атак и приобретение навыков по реализации атак и применения контрмер по их предотвращению.

Теоретические сведения:

Разведка (в рамках кибербезопасности) - несанкционированное выявление параметров ИС, ее точек уязвимости или получение конфиденциальной информации. Информация, полученная в результате атак разведки, может затем использоваться для проведения атак другого типа или для хищения важных данных.

Разведывательные атаки - несанкционированное обнаружение и сопоставление систем, служб или уязвимостей.

Злоумышленники извне могут использовать инструменты Интернета, например программные средства *nslookup* и *whois*, которые позволяют легко определить пространство IP-адресов, назначенное определённой корпорации или юридическому лицу. После определения пространства IP-адресов злоумышленник может выполнить проверку связи с общедоступными IP-адресами, чтобы выявить активные адреса. Для автоматизации этого этапа злоумышленник может использовать инструмент эхо-тестирования адресов (например, fping или gping), которые систематически выполняют проверку связи со всеми сетевыми адресами в пределах заданного диапазона или подсети. Этот процесс можно сравнить с просмотром раздела телефонной книги и звонком на каждый из номеров, чтобы проверить, кто ответит.

Рассмотрим наиболее распространенные виды разведывательных атак.

1. Выявление целей.

Выявление целей включает: *определение имен доменов и IP-адресов узлов* (серверов, маршрутизаторов и т.д.), *выявление списка доступных сервисов или какой-либо иной информации об этом узле.*

Способы реализации:

- *Сетевые команды и утилиты.* Для разведки можно использовать сетевые команды, доступные в UNIX и Windows, это ping (посылает Internet Control Message Protocol- пакеты), finger (показывает информацию о пользователях в системе), rusers (показывает, кто из пользователей работает на удаленной системе на данный момент), nslookup (интерактивное общение с DNS-серверами), dig (позволяет обращаться к DNS-серверам), telnet (команда для связи с другими узлами), nmap (утилита для исследования сети – сканер, позволяет определить открытые порты на узле, т.е. сервисы, которые на нем запущены), а также другие команды и утилиты, обеспечивающие информацию о сети и ее узлах.

Как видим, даже в стандартной поставке операционных систем есть немало команд для выявления узлов, запущенных на них сервисов и структуры сети.

- *Разведка ping.* Эта команда генерирует для конкретного узла (или по широковещательному адресу) сообщение ICMP Echo Request. Узел должен ответить соответствующим набором сообщений ICMP.

Хотя для сбора информации о сети и ее узлах можно использовать саму команду *ping*, были разработаны утилиты разведки ping, автоматизирующие выявление узлов внутри сети. Такие утилиты просматривают диапазон IP-адресов и используются для того, чтобы построить карту сети.

Во многие реализации ping встроена возможность послать так называемый *Flood ping*, при включении которого пакеты могут посылаться с очень большой частотой, что может затруднить работу узлов сети, маршрутизаторов или даже привести к «падению» сервисов на узле. Сделана эта возможность для благих целей (изучения сетевой производительности), но может использоваться для атаки. Команда *ping –f <host>* (запускается только в режиме супер-юзера).

- *Сканирование портов.* После выявления интересующего узла хакер может выполнить сканирование портов. *Утилита сканирования портов проверяет заданный диапазон портов TCP или UDP с целью выявления*

доступных сетевых службы типа Telnet, FTP, HTTP или RCP. Такое сканирование может быть общим, когда проверяется диапазон портов (порты с номерами 1-1023), или специальным, когда внимание концентрируется на определенных портах, чтобы выявить, например, информацию об операционной системе.

После выявления интересующих портов противник может приступить к проведению атаки против конкретного порта. Например, если хакер выяснит, что на данном узле доступна служба SMTP, он может послать соответствующие команды SMTP с целью получения доп. информации или несанкционированного доступа. Если хакер обнаружит, что на данном узле доступна служба DNS, он может попытаться получить доступ к записям HINFO службы DNS.

Сканеры портов могут исследовать открытые порты недостаточно защищенных пользователей. Существует большое количество легкодоступных (в том числе бесплатно распространяемых) сканеров.

Методы противодействия:

- ✓ отключение ответа на команды ping, finger, rusers и т.д.;
- ✓ отключение невостребованных сервисов на серверах и маршрутизаторах;
- ✓ использование системы обнаружения вторжений для выявления сканирования портов.

2. Перехват пакетов.

Перехват пакетов (сбор информации) является методом пассивного наблюдения за сетевым трафиком с помощью некоторого устройства или утилиты. Цель перехвата – выявление структуры потока данных для последующего анализа, а также с целью кражи информации. Синонимами понятия перехват являются *сетевое слежение* и *анализ пакетов.*

Типичным способом перехвата сообщений является *захват TCP/IP пакетов и декодирование их содержимого с помощью анализатора протокола.*

С помощью перехвата пакетов сетевые нарушители могут выяснять имена и пароли пользователей, извлечь из пакета такие данные, как номер кредитной карты или другую частную информацию.

Методы противодействия:

- ✓ ограничение физического доступа к сетевому оборудованию, исключающее возможность размещения анализаторов протокола в подходящих точка сети;
- ✓ использование коммутаторов для разбиения сети на сегменты (VLANы), с целью предотвращения захвата всего сетевого трафика с одной рабочей станции;
- ✓ принятие мер, гарантирующих невозможность несанкционированного доступа к хостам и размещения утилит захвата пакетов;
- ✓ использование программ проверки целостности систем и выявления файлов, размещенных без разрешения;
- ✓ использование на важных узлах сети интерфейсных плат, которые нельзя переключить в беспорядочный (promiscuous - беспорядочный, неразборчивый) режим работы (*объяснить, что это за режим*);
- ✓ применение шифрования данных для защиты содержимого пакетов при передаче через незащищенные сети.

3. Социальный инжиниринг.

Для проникновения в сети и компьютеры в сочетании с новыми технологиями широко применяются старомодные методы манипулирования людьми. ***Социальный инжиниринг*** - манипулирование людьми с целью проникновения в защищенные системы и сети.

Люди по своей природе непредсказуемы и подвержены манипуляции и убеждению. Исследования показывают, что у человека существуют определенные поведенческие тенденции, которые можно эксплуатировать при помощи тонкой манипуляции. Многие наиболее разрушительные проникновения в защищенные системы совершаются и будут совершаться методами социального инжиниринга.

Примеры: склонение пользователя к открытию ссылок и вложений электронной почты с целью внедрения троянов, открытие ссылок для ввода логина/пароля на ложные сайты.

Методы противодействия: противодействие данным методам наиболее затруднено.

- информирование пользователей об известных мошеннических методах;
- не предоставлять пользователям без необходимости лишние сервисы – web, e-mail и т.д.

4. Несанкционированный доступ.

Нарушитель может пытаться получить несанкционированный удаленный доступ к компьютерам сети или сетевым устройствам самыми различными способами. Общей целью нарушителя является получение прав корневого пользователя – *root'a* или *администратора* на том компьютере, где он имеет больше возможностей для управления интересующий его системой или для доступа к другим компьютерам сети.

Сетевому нарушителю обычно сначала требуется получить хотя бы *минимальный доступ* к любому узлу сети, чтобы затем попытаться выйти за рамки этого узла.

Нарушитель сначала пытается получить как можно больше информации об интересующем его узле с помощью методов разведки, а затем использует эту информацию для того, чтобы получить *первичный доступ*. После выявления IP адреса узла, в который можно проникнуть, нарушитель для получения первичного доступа может действовать разными способами.

Примеры способов получения первичного доступа:

1) *Посредством сканирования портов* нарушитель может искать доступные Internet-сервисы, и, используя их уязвимости, получить беспарольный доступ.
2) Использовать анализатор пакетов для перехвата имен и паролей пользователей.

3) Использовать программы-дозвонщики для перебора телефонных номеров и поиска незащищенных модемных соединений.
4) Для получения первичного или даже привилегированного доступа нарушитель может использовать методы социального инжиниринга и другие психологические методы (шантаж, подкуп и т.д.).
5) Нарушитель может работать и внутри организации, будучи легальным пользователем ее сети. Такой нарушитель может использовать свое служебное положение или доверие другого сотрудника.

Методы противодействия:

- сокращение числа точек доступа к сети, контроль и пресечение попыток несанкционированного доступа к сети внутренними пользователями;
- использование серверов AAA (аутентификации, авторизации и аудита) для управления привилегиями доступа (позволяют разграничить доступ для разных пользователей и отслеживать их действия);
- использование более защищенных протоколов удаленного доступа (например PPP).

5. Преодоление парольной защиты.

Существует большое разнообразие атак на систему парольной защиты. Зная учетное имя (login) одного из легальных пользователей системы, нарушитель может попытаться угадать пароль этого пользователя путем простого перебора вариантов (в надежде, что пользователь создал легко угадываемый пароль). Перебор может осуществляться вручную или программными средствами.

Пересылаемые в виде открытого текста имена и пароли пользователей нарушитель может захватить с помощью анализатора пакетов. В случае доступа к файлу всех паролей, например /etc/passwd в UNIX возможен подбор паролей с помощью утилиты взлома паролей. Эта утилита на самом деле не «взламывает» пароли, а просто угадывает их, используя компьютерную мощь для сравнения хэш-кодов паролей. Утилиты взлома паролей широко доступны как для UNIX, так и для Windows.

Нарушитель также может получить имя пользователя/пароль при помощи трояна или червя.

Защитится от атак парольной защиты можно с помощью последовательно проводимой политики выбора трудноугадываемых паролей. Пересылка паролей через незащищенные сети должна осуществляться только в зашифрованном виде, а файлы паролей должны тщательно охраняться от возможностей удаленного доступа к ним.

Для борьбы с перебором паролей необходимо отслеживать многократно повторяемые неудачные попытки вхождения в систему. Позволяют это сделать либо системы аудита, либо элементарные средства, входящие в состав ОС, например, команда lastb в UNIX.

Методы противодействия:

1. Проведение политики трудноугадываемых и труднораскрываемых паролей.
2. Выполнение программ взлома паролей для выявления слабых паролей.
3. Использование шифрования при передаче паролей.
4. Использование ограничений времени и параметров пароля, заставляющих пользователей периодически менять пароль.

Вариант использования сканирования Nmap. В тестовой среде Nmap был настроен на отправку зондов на отдельный IP-адрес от клиента, не прошедшего проверку подлинности. Результаты, хотя и ограничены определенным типом сканирования, возвращают множество информации, которая может помочь злоумышленнику в создании профиля об обнаруженном узле. Пример сканирования можно увидеть на снимке экрана ниже, который включает точки данных:

- Онлайн-статус сканируемой конечной точки.
- Роль или службы, работающие на конечной точке.
- Возможная версия операционной системы, установленной на конечной точке.

Этот тип информации имеет жизненно важное значение, поскольку он поможет направить злоумышленника к дальнейшему исследованию конкретных уязвимостей, которые можно использовать для успешной компрометации версии операционной системы или комбинации служб Windows, работающих на сканируемой конечной точке.

– Важно отметить, что, хотя эта информация представляет интерес для злоумышленника, сканирование зависит от взаимодействия с конечной точкой, что может оставить следы в службах безопасности, таких как брандмауэр Защитника Windows в режиме повышенной безопасности, которые можно проверить на наличие аномальной сети.

Практическая часть:

Сканирование портов в Nmap. Если вам нужно из Windows просканировать порты компьютеров и устройств в локальной сети или в Интернете, то одним из лучших вариантов является связка Nmap и Zenmap (графический интерфейс для Nmap). Nmap имеет большое количество опций сканирования, а графический интерфейс Zenmap делает использование программы крайне простым. Возможности Nmap включают: сканирование портов; определение операционной системы удалённого хоста; определение служб, программного обеспечения и их версий на удалённом хосте.

С помощью скриптов Nmap можно проверять удалённые хосты на наличие уязвимостей, на слабые пароли, собирать определённую информацию, искать службы, позволяющие анонимный вход и выполнять другие задачи, связанные с действиями администратора сети или тестера на проникновение.

Чтобы скачать программу для сканирования портов перейдите на страницу загрузки Nmap: https://nmap.org/download.html. Найдите там ссылку на .exe файл. Увидеть все доступные для загрузки файлы можно здесь: https://nmap.org/dist/.

Запустите установщик Nmap, кроме основной программы он также установит несколько компонентов, которые необходимы для работы Nmap в

Windows. Когда всё будет готово, на рабочем столе появится ярлык программы.

В поле **Цель** нужно указать адрес сайта (URL), IP или диапазон IP адресов для сканирования. В поле **Профиль** из выпадающего списка нужно выбрать желаемый профиль.

Как указать Цель в Zenmap (Nmap): Адреса сайтов следует указывать без протокола, например: mi-al.ru, suip.biz. Неправильным было бы указание вида https://mi-al.ru.

IP адреса можно указывать по-одному, например, 192.168.0.1; используя нотацию CIDR, например, 192.168.0.1/24; а также указывая диапазоны в одном или нескольких октетах, например, 192.168.0.1-100, или 192.160-170.50-100.1

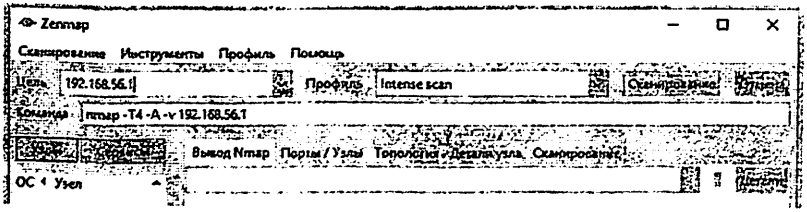


Рис.5.1. Главное окно программы Zenmap

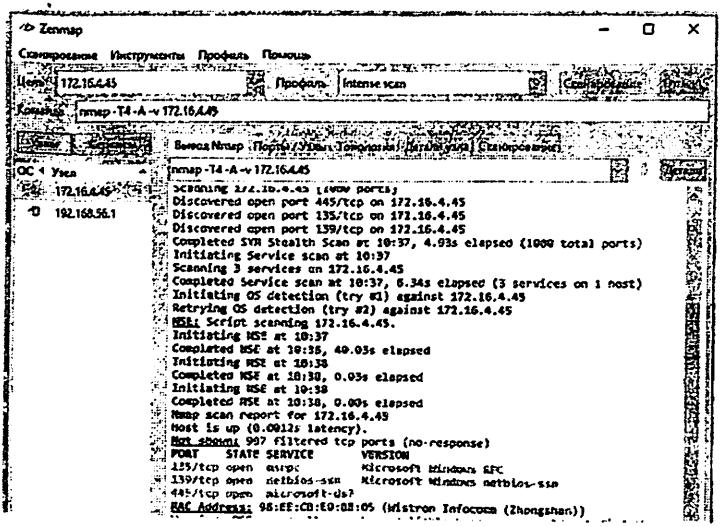


Рис.5.2. Результаты сканирования в программе Zenmap

Рис.5.3. Результаты сканирования в программе Zenmap

Что означают Профили в Zenmap: Профили в главном окне Zenmap – это набор опций типичных сканирований. Рассмотрим все профили Zenmap:

- ***Intense scan*** (Интенсивное сканирование). Интенсивное всестороннее сканирование. Опция **-A** включает сразу несколько других опций: определение версии ОС (**-O**), определение версий запущенных служб (**-sV**), сканирование с использованием скриптов (**-sC**) и трассировку (**--traceroute**). Без привилегий администратора запускается только определение версии и сканирование с помощью скриптов. Это считается интрузивным (навязчивым) сканированием.

- ***Intense scan plus UDP*** (Интенсивное сканирование плюс UDP). Делает определение ОС (**-O**), определение версий (**-sV**), сканирование с помощью скриптов (**-sC**) и трассировку (**--traceroute**) в дополнение к сканированию портов TCP и UDP.

- ***Intense scan, all TCP ports*** (Интенсивное сканирование, все TCP порты). Сканирует все TCP порты, затем делает определение ОС (**-O**), определение версий (**-sV**), сканирование скриптами (**-sC**) и трассировку (**--traceroute**).

- **Intense scan, no ping** (Интенсивное сканирование без пинга). Выполняет интенсивное сканирование без предварительной проверки, работают ли цели. Это может быть полезным, когда цели игнорируют обычные зондирования для обнаружения хостов.
- **Ping scan** (Пинг). Это сканирование только определяет, какие цели работают и не выполняет сканирование портов.
- **Quick scan** (Быстрое сканирование). Это сканирование быстрее обычного сканирования, поскольку оно использует агрессивный шаблон тайминга и сканирует меньше портов.
- **Quick scan plus** (Быстрое сканирование плюс). Быстрое сканирование, плюс определение ОС.
- **Quick traceroute** (Быстрая трассировка). Трассирует пути до целей без выполнения полного сканирования их портов.
- **Regular scan** (Обычное сканирование). Базовое сканирование без дополнительных опций.
- **Slow comprehensive scan** (Медленное всестороннее сканирование). Это всестороннее, медленное сканирование. Сканируется каждый TCP и UDP порт. Выполняется определение ОС (**-O**), определение версии (**-sV**), сканирование скриптами (**-sC**) и трассировка (**--traceroute**). Отправляется множество запросов зондирования для обнаружения хостов. Это очень интрузивное сканирование.

Например, если необходимо узнать, какие узлы подсети пингуются, то следует выбрать профиль **Ping scan**.

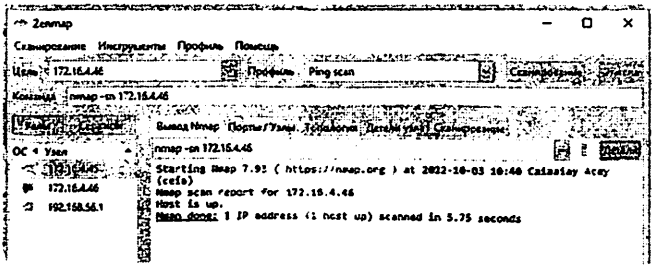


Рис.5.3. Результаты сканирования в профиле Ping scan.

С помощью удобного редактора профиля вы можете редактировать и создавать новые профили.

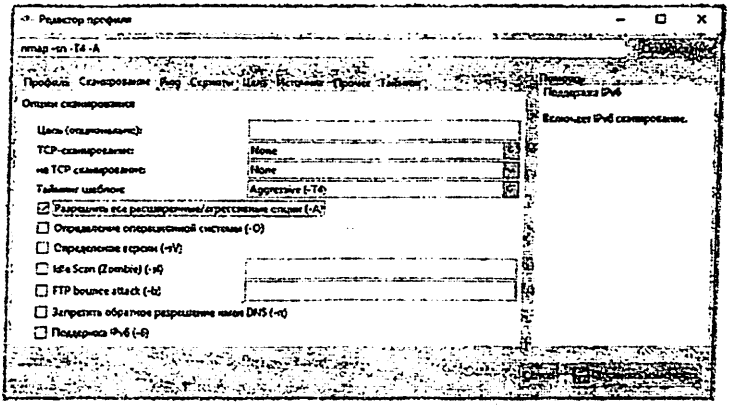


Рис.5.4. Окно редактора профилей в программе Zenmap

Хотя использование редактора профиля содержит описание выполняемых действий и, следовательно, не требует знания опций Nmap, для более глубокого понимания программы вы можете познакомиться с описанием всех опций Nmap на странице **https://kali.tools/?p=1317**. Если вы хотите просканировать все TCP порты, то укажите цель и в качестве команды введите **nmap -p 1-65535.**

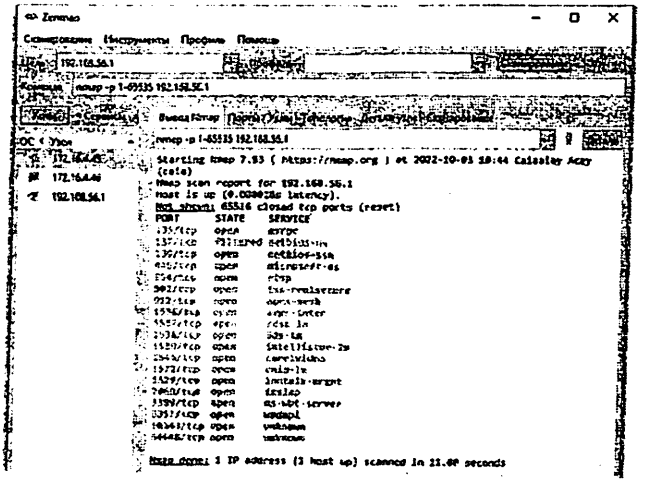


Рис.5.5. Результаты сканирования (для 198.168.56.1)

Результаты сканирования. Результаты, полученные при последнем сканировании видны во вкладке **Вывод** Nmap. В левой части вы можете переключаться между **Узлами** и **Сервисами**. При клике на определённый узел, вы увидите предыдущие результаты сканирования. При клике на сервис, вы увидите узлы, на которых данных сервис был обнаружен:

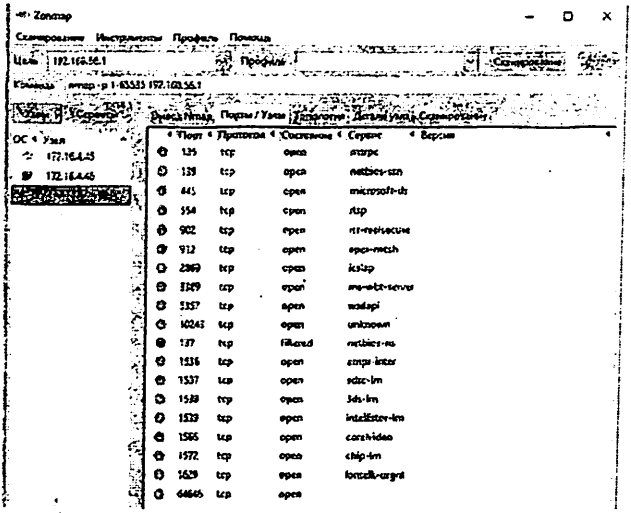


Рис.5.5. Результаты сканирования (для 192.168.56.1)

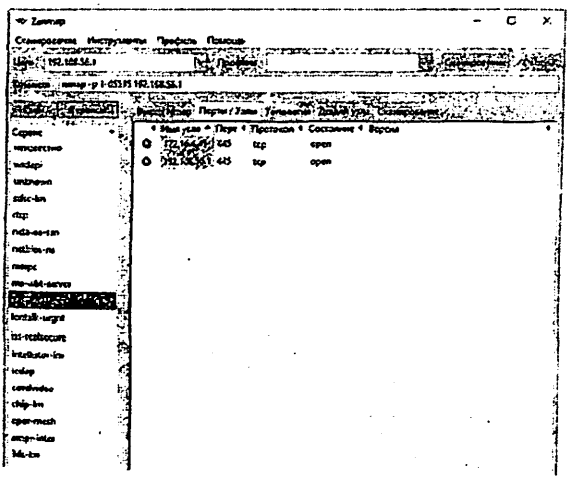


Рис.5.6. Результаты сканирования (доступные сервисы)

Для просмотра обобщённой информации по узлу, кликните на него и выберите вкладку **Детали узла**:

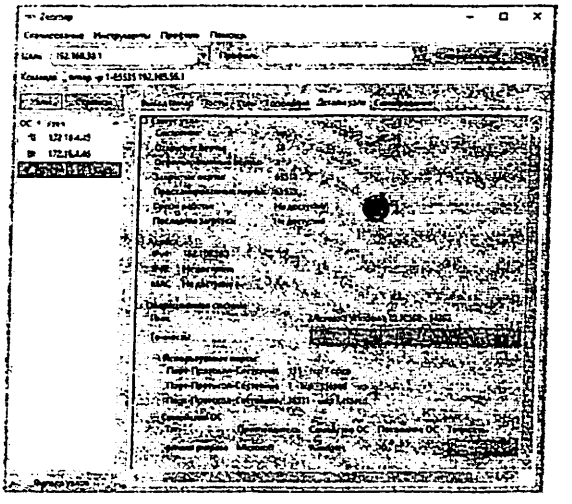


Рис.5.7. Просмотр обобщённой информации по узлу

Во вкладке **Топология** вы увидите информацию о связях между просканированными/обнаруженными узлами:

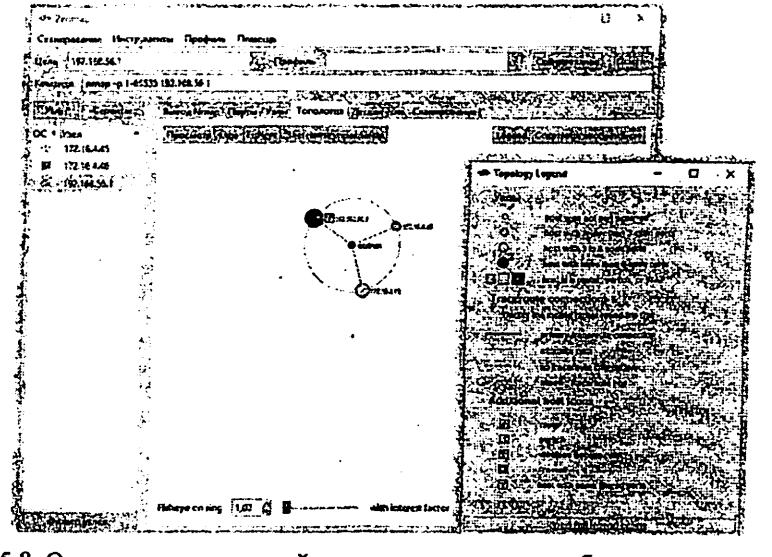


Рис.5.8. Окно просмотра связей просканированного и обнаруженных узлов

Программа Nmap позволяет из Windows проводить сканирование компьютеров и других устройств на наличие открытых портов. Также она способна определять запущенные на удалённом хосте службы, их версию.

Графический интерфейс позволяет упростить использование программы, но для получения навыков по различным техникам сканирования рекомендуется ознакомиться со всеми опциями программы: https://kali.tools/?p=1317.

Кроме своих основных функций – сканирование портов и определение версий установленного ПО – скрипты Nmap позволяют выполнять различные другие задачи, в том числе проверять на наличие уязвимостей, слабые пароли, выполнять сбор информации.

Задание к практической работе:

Реализуйте разведывательную атаку типа сканирование портов при помощи программы Nmap. Продемонстрируйте каждый этап выполнения в виде скриншотов с подробным описанием всех действий и приведением анализа полученных результатов.

Содержание отчета:

1. Титульный лист
2. Выполнение задания к практической работе, включая скриншоты и подробное описание выполненных действий;
3. Выводы по выполнению практической работы;
4. Ответы на контрольные вопросы

Контрольные вопросы:

1. Что вы понимаете под разведывательными атаками?
2. Какие виды разведывательных атак Вы знаете? Объясните принцип реализации каждой из названных разведывательных атак.
3. Объясните принцип реализации и контрмеры по отношению к атакам выявления целей.

4. Объясните принцип реализации и контрмеры по отношению к атакам социальной инженерии.
5. В чем заключается реализация разведывательных атак типа преодоление парольной защиты?
6. Какие основные профили (опции типичных сканирований) в Zenmap Вы знаете?
7. Какой профиль сканирования в Zenmap определяет то, какие цели работают и не выполняет сканирование портов?

Практическая работа №6

Тема: Применение инструментов межсетевого экранирования для защиты сети

Цель работы: приобретение навыков настройки межсетевого экрана в ОС Windows.

Теоретические сведения:

Межсетевой экран (брандмауэр, файрвол) — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Наиболее распространённое место для установки межсетевых экранов — граница периметра локальной сети для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов — в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.

Классификация межсетевых экранов. До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Однако в большинстве случаев поддерживаемый уровень сетевой модели OSI является основной характеристикой при их классификации. Учитывая данную модель, различают следующие типы межсетевых экранов: управляемые коммутаторы;

пакетные фильтры; шлюзы сеансового уровня; посредники прикладного уровня; инспекторы состояния.

Межсетевой экран — важнейшее звено обеспечения безопасности. Он создает оптимальные условия для защиты информации о внутренней структуре сети, участвует в организации демилитаризованной зоны, фильтрует трафик и поддерживает общую концепцию безопасности. В сочетании с другими защитными средствами Firewall предупреждает угрозу несанкционированного доступа к конфиденциальной информации, внедрения вредоносного ПО и вывода сетевых ресурсов из строя.

Практическая часть:

Для начала зайдите в панель управления и откройте управления брандмауэром, т.е нажмите правой кнопкой мышки на меню **"Пуск"**. Затем выберите пункт **"Панель управления"**, в которой переключитесь на маленькие значки (справа вверху) и выберите из списка **"Мелкие значки"**, после чего выберите **"Брандмауэр Windows"**:

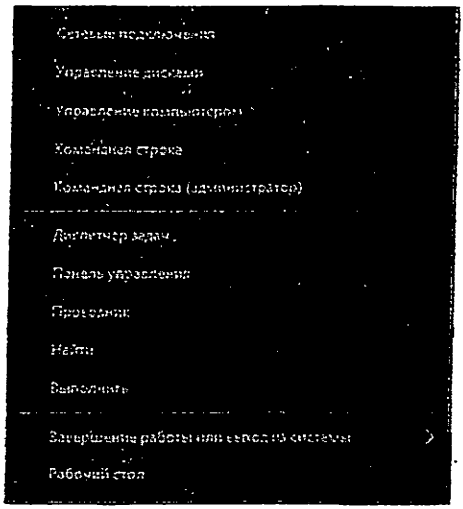


Рис.6.1. Окно доступа к параметрам запуска в ОС Windows

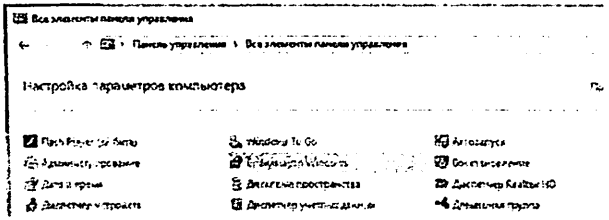


Рис.6.2. Окно настройки параметров компьютера

Далее перейдите к дополнительным настройкам выбрав в соответствующий пункт (**Дополнительные параметры**):

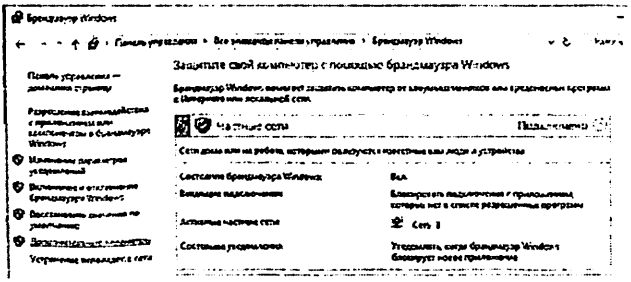


Рис.6.3. Окно параметров настройки брандмауэра Windows

Брандмауэр Windows и настройка профилей. Далее Вы увидите **3** набора профилей (**Общий профиль, Профиль домена** и **Частный профиль**), а так же параметры **IPSec.**

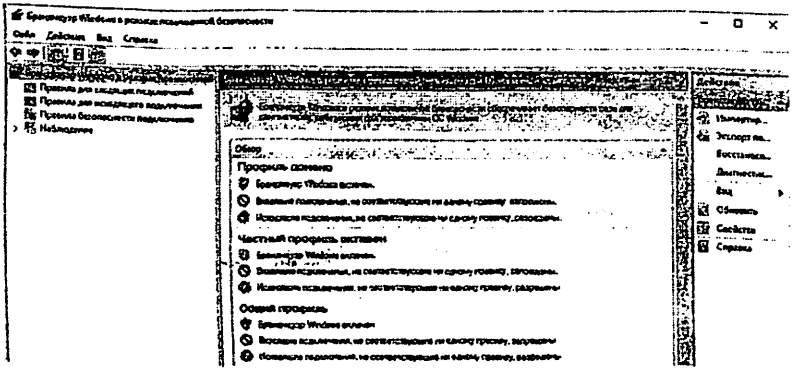


Рис.6.4. Окно настройки брандмауэра Windows в режиме повышенной безопасности

Выберите пункт «**Свойства брэндмауэра**». Здесь для каждого (т.е. три раза) из профилей нужно включить брандмауэр Windows (*первый выпадающий список*), включить блокировку всех входящих подключений (*второй выпадающий список*) и блокировать исходящие подключения (*третий список*).

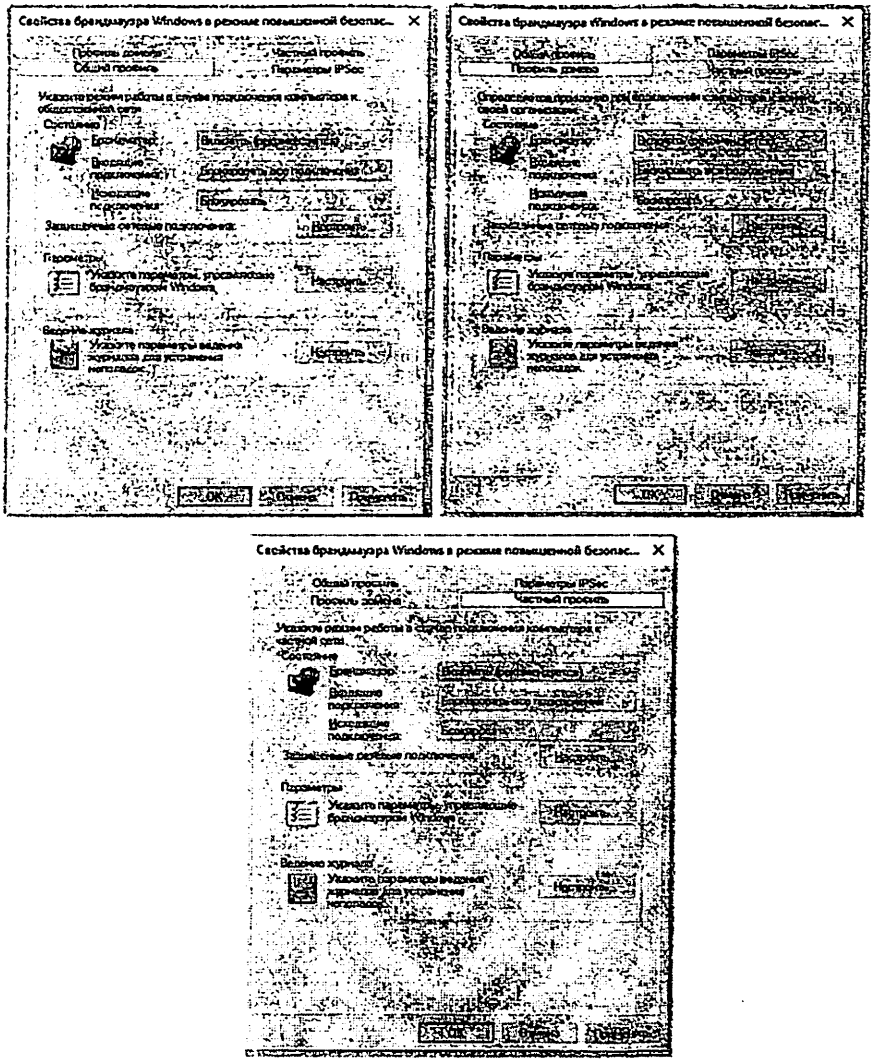


Рис.6.5. Диалоговые окна свойств брандмауэра для разных профилей

На выходе, на каждой из вкладок профиля Вы должны видеть то, что видите на скриншотах выше.

ПРИМЕЧАНИЕ! *После применения, скорее всего, Вы сразу потеряете соединения с интернетом для всех программ (в том числе браузера), которые не были в исключениях.*

Результатом должно являться нечто следующее (см.описание профилей в колонке **"Обзор"**):

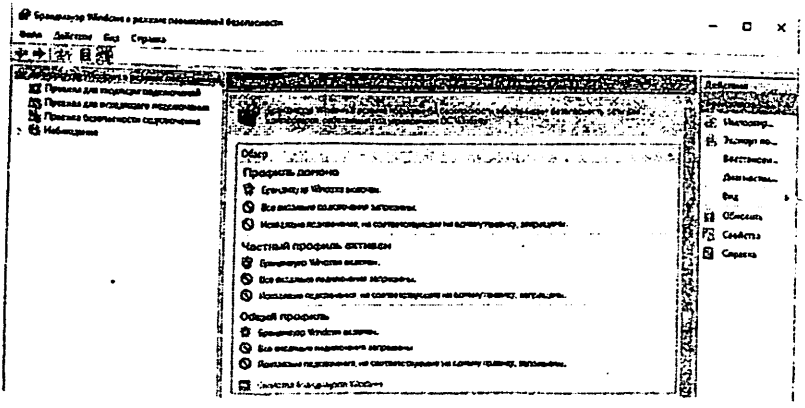


Рис.6.6. Запрет всех входящих и исходящих подключений

В данный момент запрещены все входящие подключения и все исходящие, кроме тех правил, что заданы изначально приложениями или самой системой.

Правила для исходящих соединений.

В большинстве случаев для входящих соединений ничего настраивать не нужно и их стоит держать заблокированными (за исключением установленных локально FTP-Web и прочих серверов), но требуют настройки правила для исходящих соединений.

Для того, чтобы это сделать, перейдите на вкладку **"Правила для исходящего подключения"**, где Вы увидите существующие (*все*) и активные (*зеленая галочка*), правила, которые есть в системе.

Чаще всего здесь **стоит оставить всё** как есть изначально, либо удалить все правила, **кроме** отмеченных зелёной галочкой, т.е включенных самой системой (и приложениями) в данный момент.

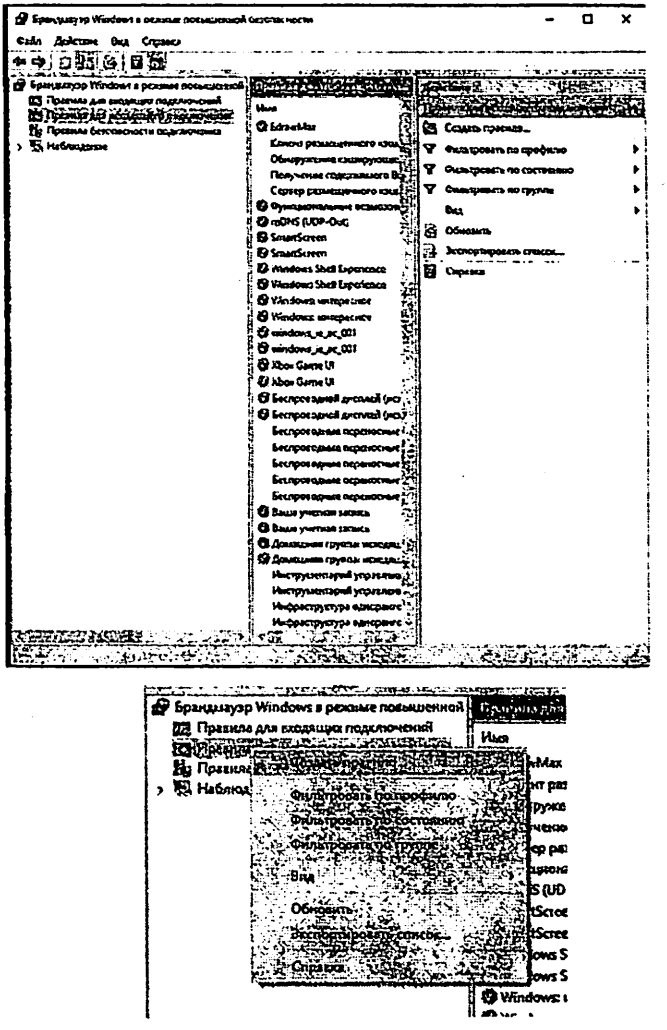


Рис.6.7. Создание правила для исходящего подключения

В правой колонке вы найдите кнопку **"Создать правило"**, которая так же доступна при клике правой кнопкой мышки на пункте **"Правила для исходящего подключения"**. С помощью этой самой кнопки необходимо

создать правила для всех приложений, которые, по Вашему мнению, должны иметь доступ в интернет.

Создание правил работы брандмауэра. Например, давайте сделаем правило для браузера. Для этого создаем правило, тип которого выбираем как: **"Для программы"**, после чего, используя кнопку **"Обзор"**, указываем путь до exe-файла программы, которой мы хотим дать доступ для исходящего трафика (при учете, что Вы создаете правило в разделе исходящих).

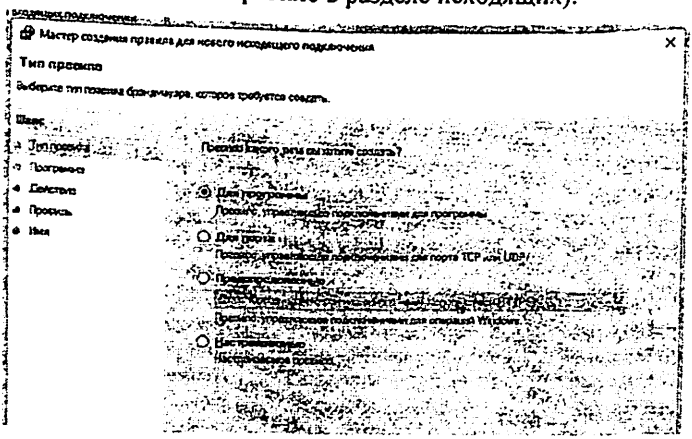


Рис.6.8. Создание правила для исходящего подключения для программы

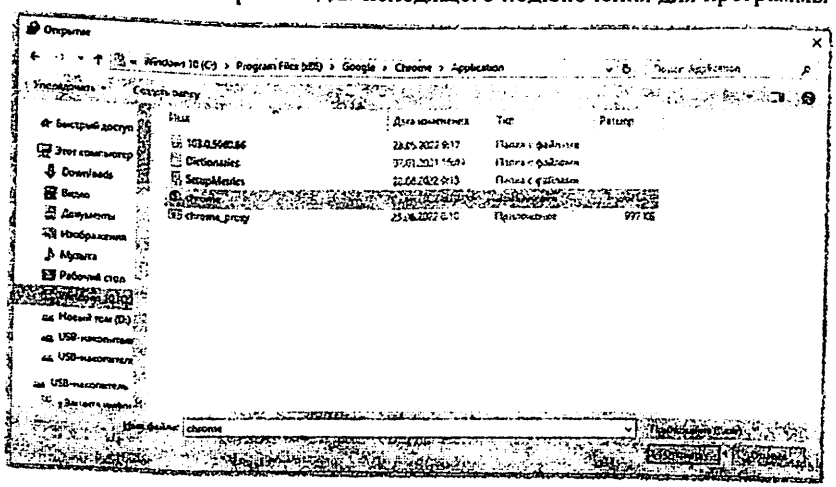


Рис.6.9. Выбор программы для которой создается правило

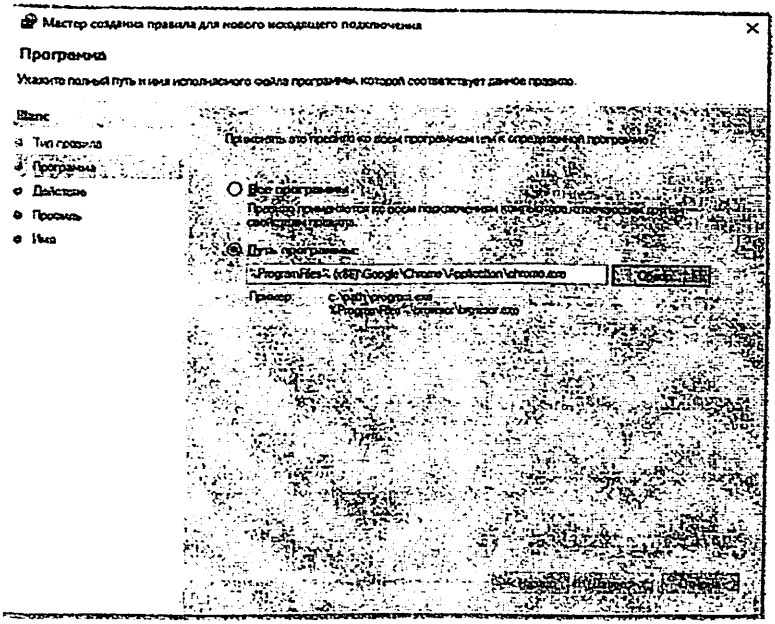


Рис.6.10. Указание пути программы для которой создается правило

На следующей вкладке выбираем пункт **"Действие"** как **"Разрешить подключение"**.

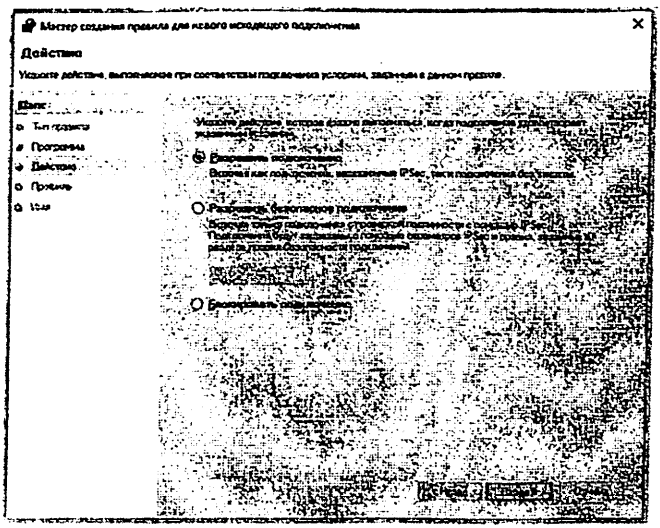


Рис.6.11. Выбор действия для заданного правила

На вкладке "**Профиль**" выбираем разрешения для всех профилей, т.е ставим все галочки:

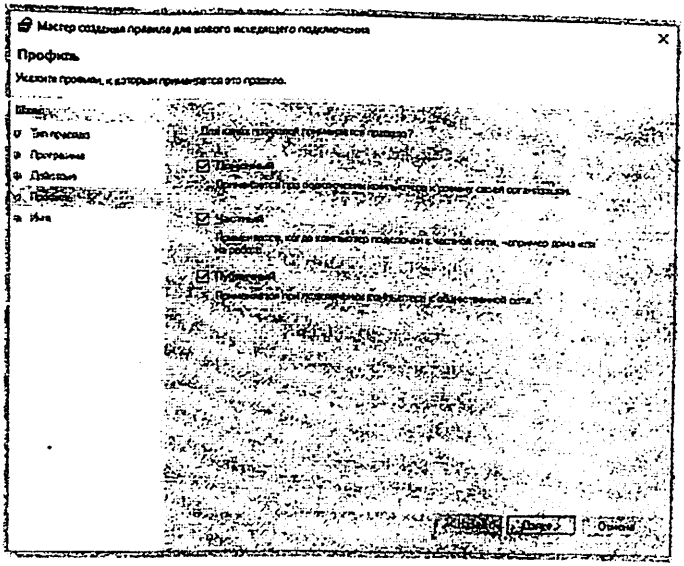


Рис.6.12. Выбор профилей для которых применяется правило

И на вкладке "**Имя**" мы задаём имя для своего профиля (рекомендуется начинать имя с одной и той же буквы, а лучше с одного и того же *символа*, что позволит быстро находить свои правила в списке):

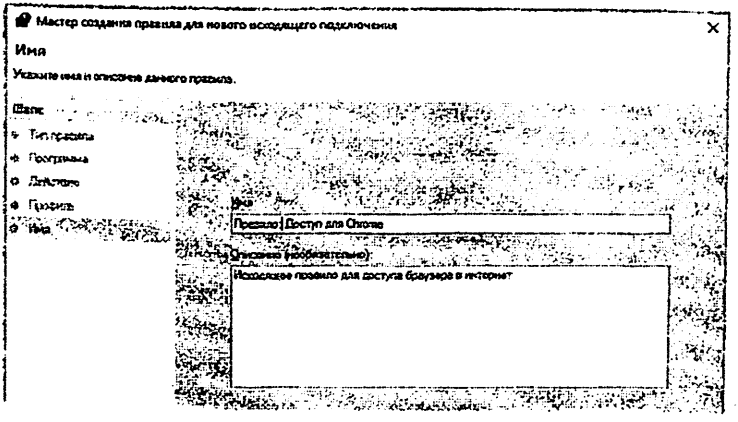


Рис.6.13. Задание имени для созданного правила

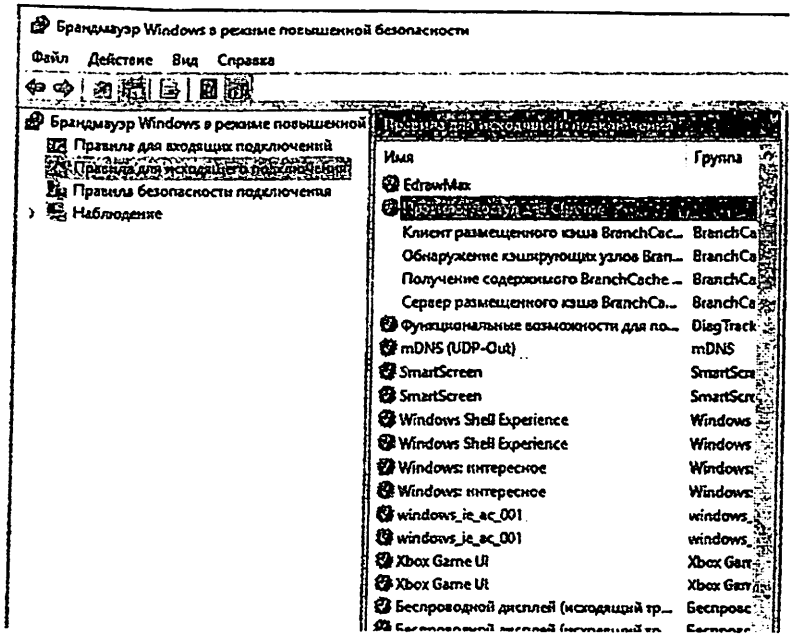


Рис.6.14. Отображение созданного правила исходящего подключения в списке правил

Теперь, когда Вы создали правило (и если Вы его сделали правильно) браузер должен успешно соединятся с интернетом. По тому же принципу добавьте правила для всех приложений, которым, по Вашему мнению, нужен доступ в интернет.

Исключения, работа с проблемами, изоляция. Если после всех настроек работа нормализовалась, но не полностью, то возможно настроить разрешение для входящих соединений брандмауэра для конкретной программы (настраивается аналогично, просто на соседней вкладке, а именно на вкладке **"Правила для входящих подключений"**).

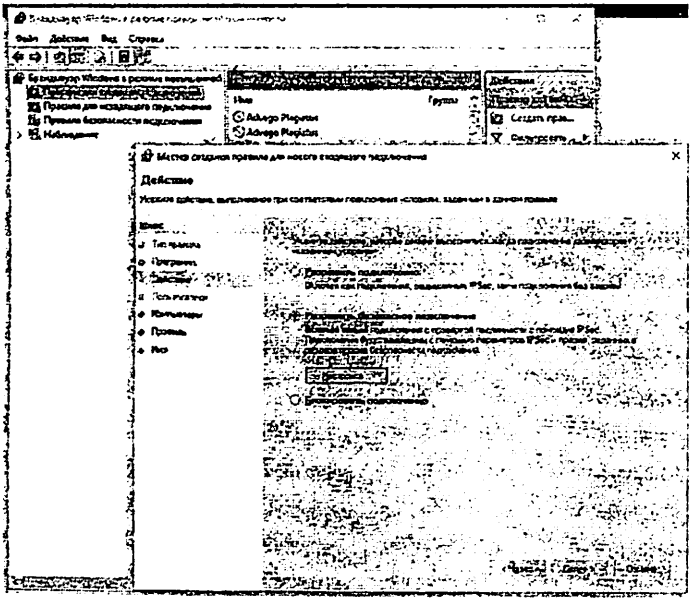


Рис.6.15. Выбор действия для правила входящего подключения

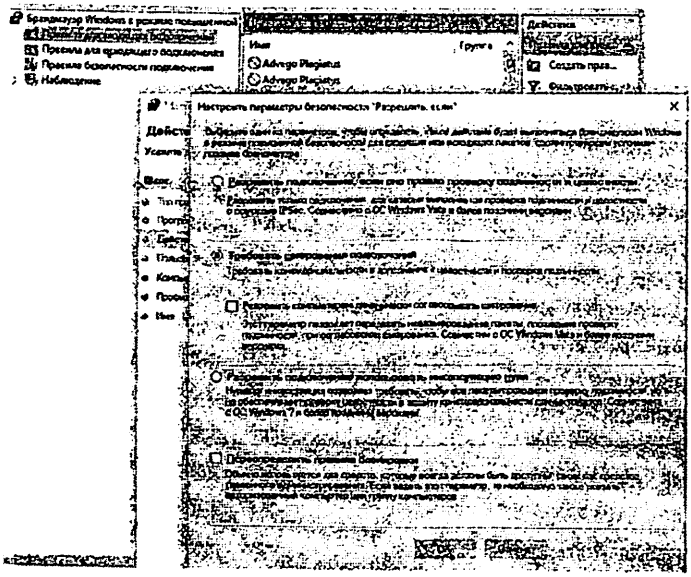


Рис.6.16. Настройка параметров безопасности для создаваемого правила входящего подключения

Экспорт и импорт готовых настроек. Имея несколько компьютеров схожей конфигурации, не всегда удобно настраивать все правила по новому, поэтому здесь предусмотрена, во-первых, выгрузка глобальной политики (правая кнопка мышки по пункту "**Брандмауэр Windows в режиме повышенной безопасности - Экспорт политики**").

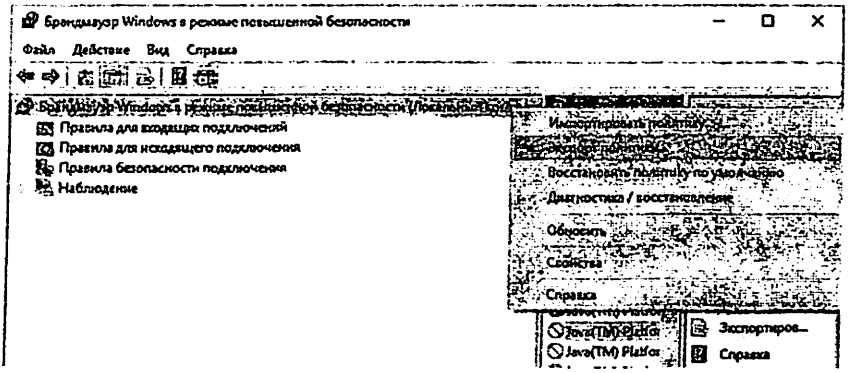


Рис.6.17. Экспорта списка правил Брандмауэра Windows

Во-вторых, предусмотрена выгрузка списков правил (входящих и исходящих отдельно) в виде **txt**, что делается в меню справа, где Вы создавали, собственно, правила:

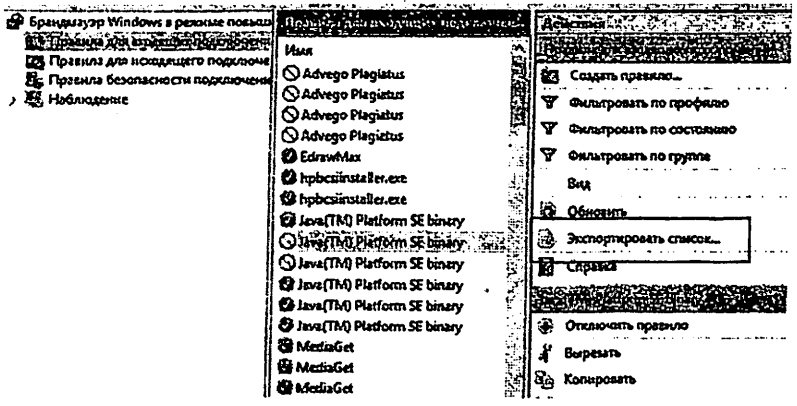


Рис.6.18. Окно экспорта списка правил в txt-формате

Это позволит быстрее восстанавливать уже настроенные правила, переносить пути, настройки и другие нюансы, локально или между машинами:

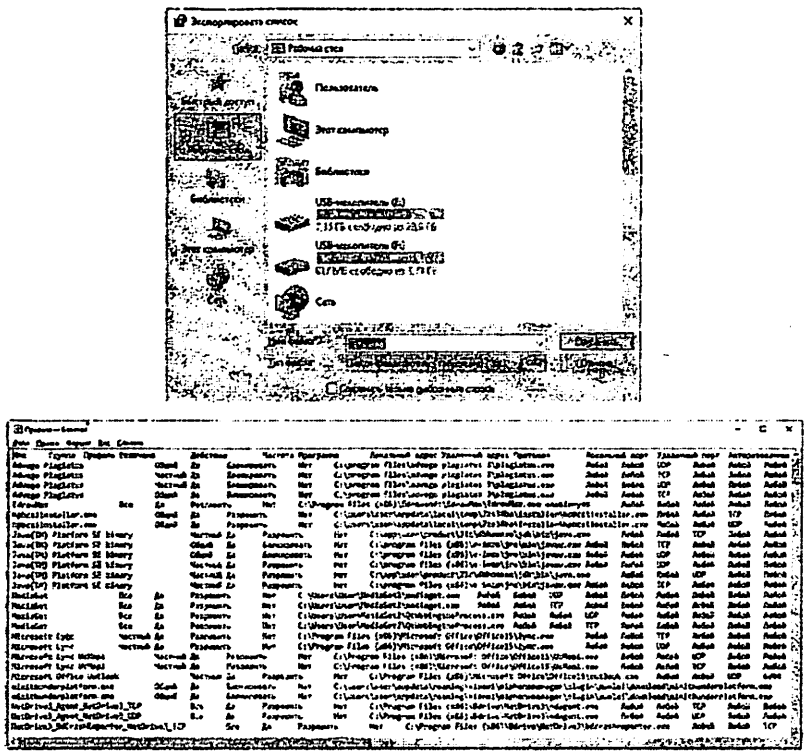


Рис.6.19. Экспорт списка правил Брандмауэра Windows

Вы всегда можете включить-или выключить брандмауэр Windows, используя соответствующий пункт **"Включение и отключение брандмауэра Windows"**, если что-то пойдет (или настроили) не так, или сбросить все настройки, выбрав пункт **"Восстановить значения по умолчанию"**:

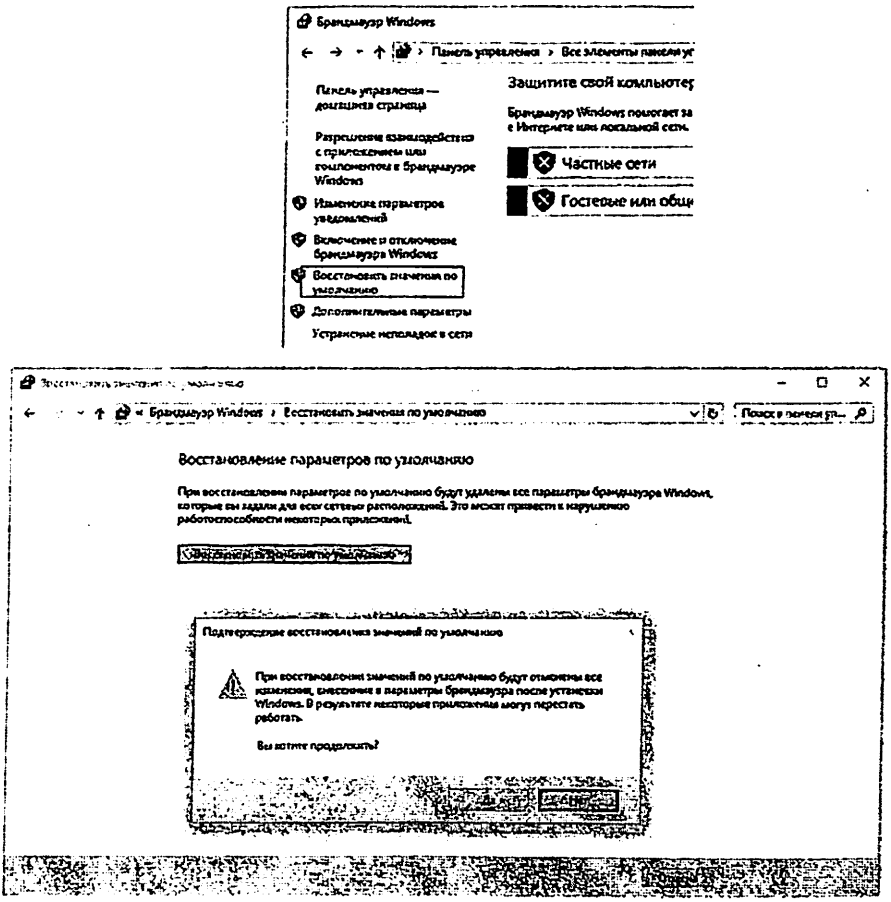


Рис.6.20. Окно восстановления параметров значений брандмауэра Windows по умолчанию

Задание к практической работе:

1. Подробно изучите классификацию межсетевых экранов и способы их размещения.
2. Осуществите настройку брандмауэра Windows создав правила для входящих и исходящих подключений (как минимум 5 правил для 5 приложений).
3. В дополнение к представленному в практической работе материалу, изучите способы конфигурации брандмауэра Windows:

https://learn.microsoft.com/ru-ru/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security.

Содержание отчета:

1. Титульный лист
2. Выполнение задания к практической работе, включая скриншоты и подробное описание выполненных действий;
3. Выводы по выполнению практической работы;
4. Ответы на контрольные вопросы

Контрольные вопросы:

1. Что такое межсетевой экран? Какие виды межсетевых экранов Вы знаете?
2. В чем заключается различие пакетного фильтра и шлюза сеансового уровня?
3. Объясните назначение межсетевого экрана с контролем состояния сеансов.
4. Приведите основные функциональные возможности посредников прикладного уровня.
5. Какие функции брандмауэра Windows с расширенной безопасностью (WFAS) и протоколом IPsec Вы знаете?
6. Как осуществляется реализация проекта базовой политики брандмауэра.

Практическая работа №7

Тема: Построение безопасной сети Wi-Fi

Цель работы: приобретение навыков построения и настройки защищенной беспроводной сети Wi-Fi.

Теоретические сведения:

Беспроводные локальные сети или как работает Wi-Fi по стандарту IEEE 802.11.

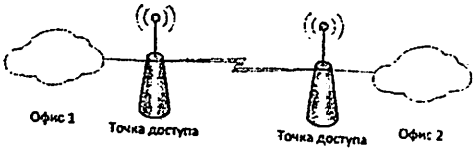
Стандарт IEEE 802.11 был разработан институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers). Данный стандарт определяет локальные сети Ethernet; поэтому модель TCP/IP не определяет сети Ethernet в своих запросах на комментарии, а ссылается на документы IEEE Ethernet.

Концепция беспроводных сетей. Многие пользователи регулярно пользуются услугами и устройствами беспроводных локальных сетей (Wireless LAN — WLAN). На текущий момент времени растёт тенденция использования портативных устройств, таких как ноутбуки, планшеты, смартфоны. Также сейчас активно развиваются концепции «умного дома», большинство устройств которого подключаются «по воздуху». В связи с этим возникла потребность беспроводного подключения во всех людных местах: на работе, дома, в гостинице, в кафе или книжном магазине. С ростом количества беспроводных устройств, которые подключаются через сеть WLAN, выросла популярность беспроводных сетей.

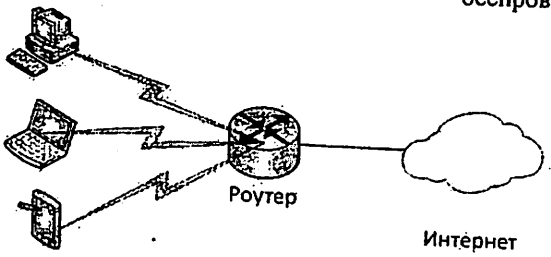
Стандарты беспроводных локальных сетей. IEEE определяет четыре основных стандарта WLAN 802.11: 802.11a, 802.11b, 802.11g и 802.11n. Наибольшее влияние на стандарты беспроводных сетей оказали следующие четыре организации.

Основные способы использования Wi-Fi

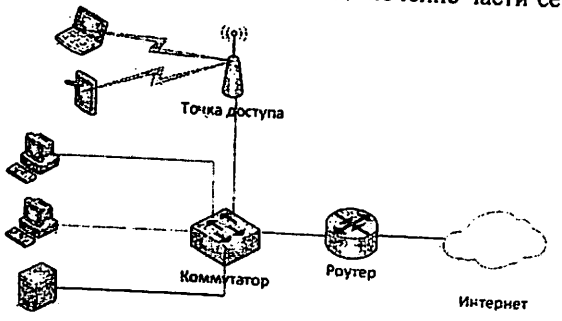
1. **Wi-Fi мост** – соединение двух точек доступа по Wi-Fi



2. **Wi-Fi роутер** – подключение всех устройств к роутеру по Wi-Fi (вся сеть подключена беспроводным способом).



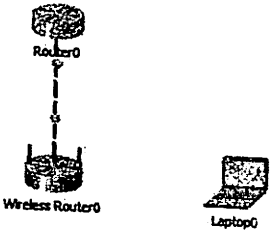
3. **Wi-Fi точка доступа** – подключение части сети для беспроводной работы



Практическая часть:

Для выполнения задания Вам потребуется установить программу Cisco Packet Tracer.

Создайте модель локальной сети, состоящей из обычного домашнего wi-fi роутера и маршрутизатора, который имитирует провайдера Интернета. Используйте интерфейс Fast Ethernet. Добавьте также пользовательское



устройство, например ноутбук. Установите модуль Wi-Fi (WPC300N) в ноутбук.

Настройка модели:

1) *Настройки маршрутизатора провайдера* **Router0** (жирным выделено то, что необходимо ввести с клавиатуры:

```
Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#int fa0/0
Router (config-if)#ip address 210.210.0.1 255.255.255.252
Router (config-if)#no shutdown

Router (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Router (config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
```

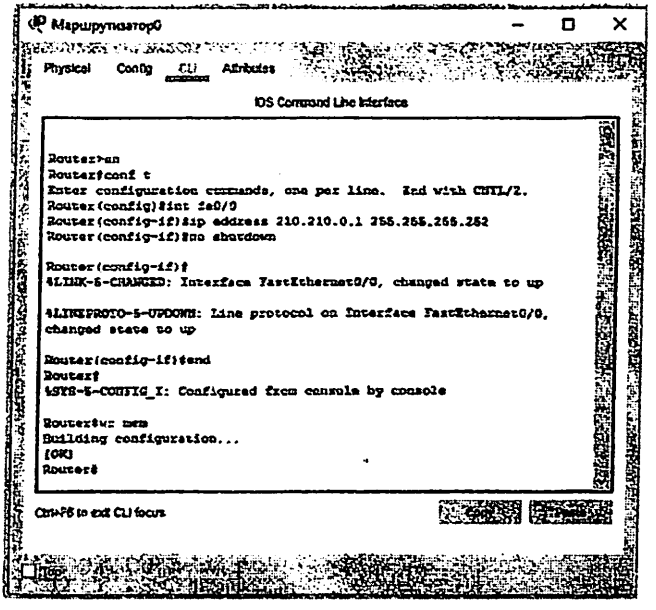


Рис.7.1. Ввод команд для настройки Маршрутизатора 0

2) *Настройки домашнего Wi-Fi маршрутизатора* **Wireless Router0** выполняется с помощью веб интерфейса. Настройка внешнего интерфейса во вкладке Setup показана на рисунке.

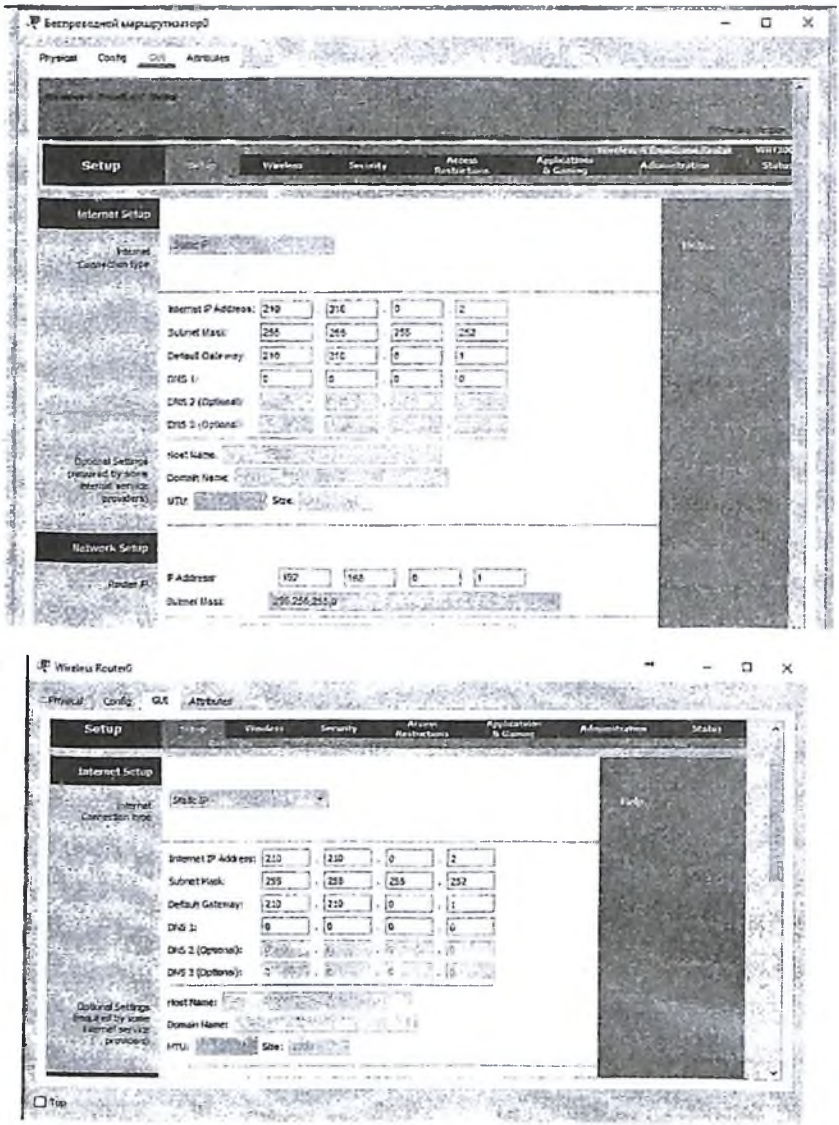


Рис.7.2. Задание IP-адреса и маски подсети для Маршрутизатора 0

Настройка локальной сети (Network Setup). Выбираем по умолчанию ip-адрес 192.168.0.1, маска 24-битная 255.255.255.0, разрешён DHCP-сервер, начало раздачи с адреса 192.168.0.100 и всё. После чего незабываем сохранить настройки, нажать на кнопку внизу формы Save Settings.

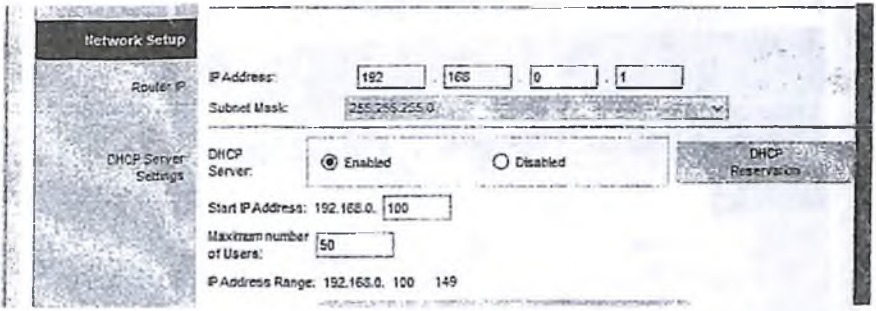


Рис.7.3. Окно ввода IP-адреса и маски подсети

Настройки во вкладке Wireless, т.е. wi-fi. Выбираем основные настройки *wi-fi*: режим (mode), мы выбираем смешанный (mixed); идентификатор сети (SSID) — WirelessNetwork; ширина канала (Radio Band) — auto; частоту — 1-2.412HGz; видимость сети (SSID Broadcast) — видимая (enable). Сохраняем настройки.

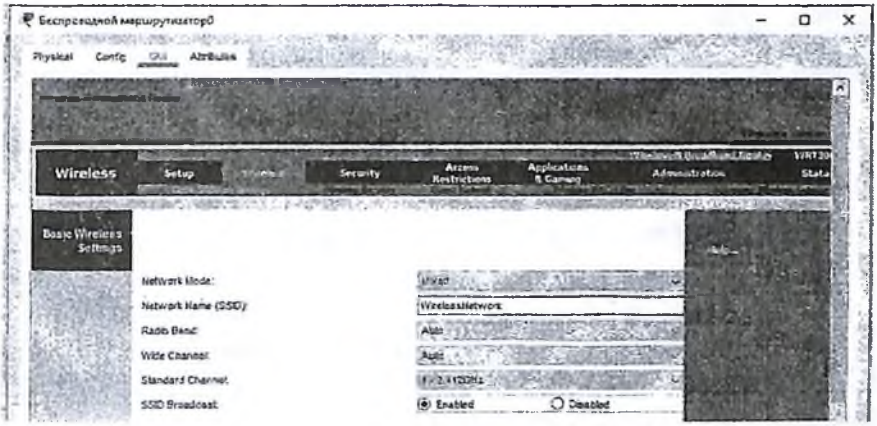


Рис.7.4. Настройки беспроводной сети

Переходим ко вкладке Wireless Security. Выбираем режим шифрования WPA2 Personal, алгоритм шифрования AES, ключевое слово для выбранного режима шифрования не менее 8 символов. Сохраняем.

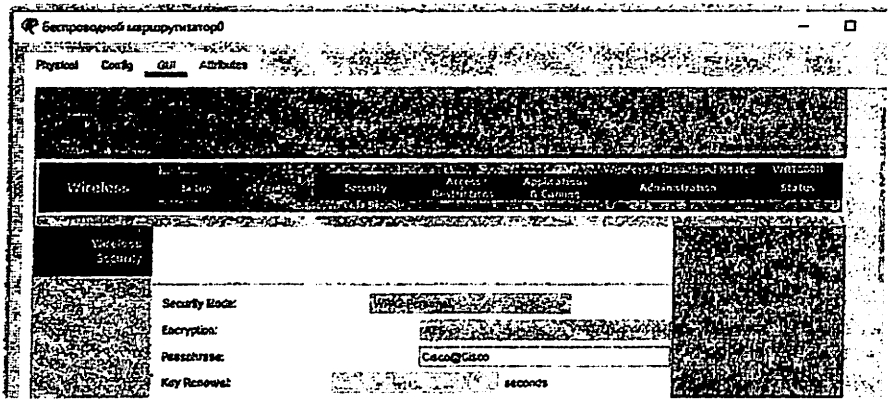


Рис.7.5. Выбор режима и алгоритма шифрования

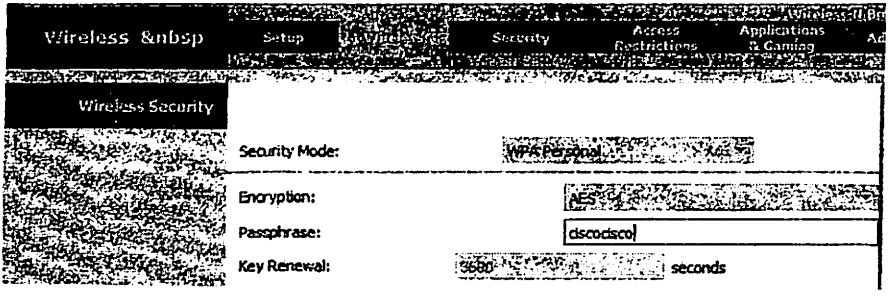
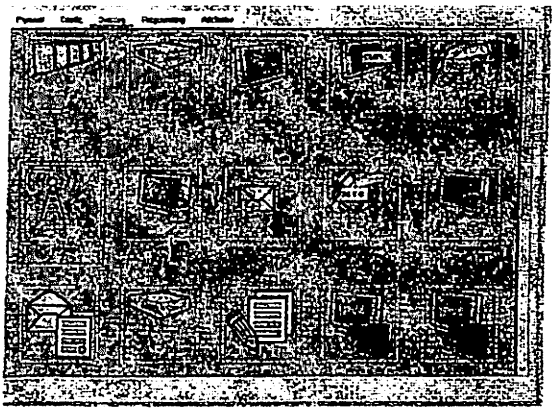


Рис.7.6. Ввод ключевого слова для выбранного шифрования

3) **Настройка wi-fi адаптера на ноутбуке.** Вкладка Desktop->PC Wireless->Connect. Смотрим доступные нам сети. Нажимаем кнопку Connect для подключения к сети WirelessNetwork.

Примечание. Сначала необходимо заменить модуль PT-LAPTOP-NM-1CFE на модуль Linksys-WPC300N (беспроводной интерфейс беспроводной интерфейс 2.4ГГц) на устройстве. Для этого отключите устройство кликнув на кнопку питания, извлеките модуль Linksys-WPC300N (перетащив его во

вкладку MODULES) и заменив его на на модуль Linksys-WPC300N включите вновь устройство.



Настройка wi-fi адаптера на ноутбуке. Вкладка Desktop->PC Wireless->Connect. Смотрим доступные нам сети. Нажимаем кнопку Connect для подключения к сети WirelessNetwork.

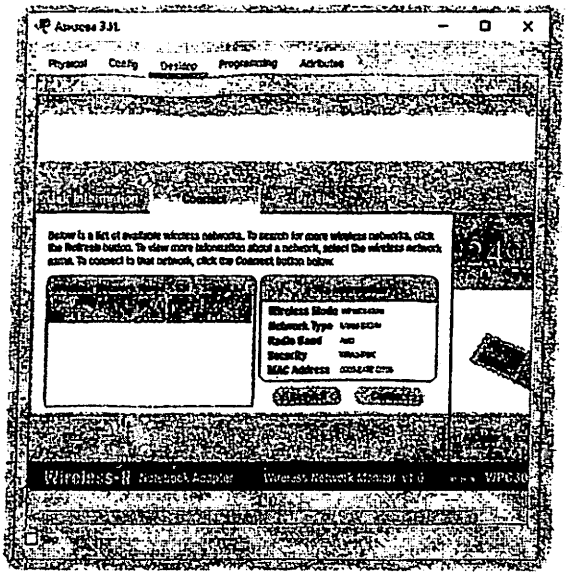


Рис.7.7. Выбор доступной беспроводной сети

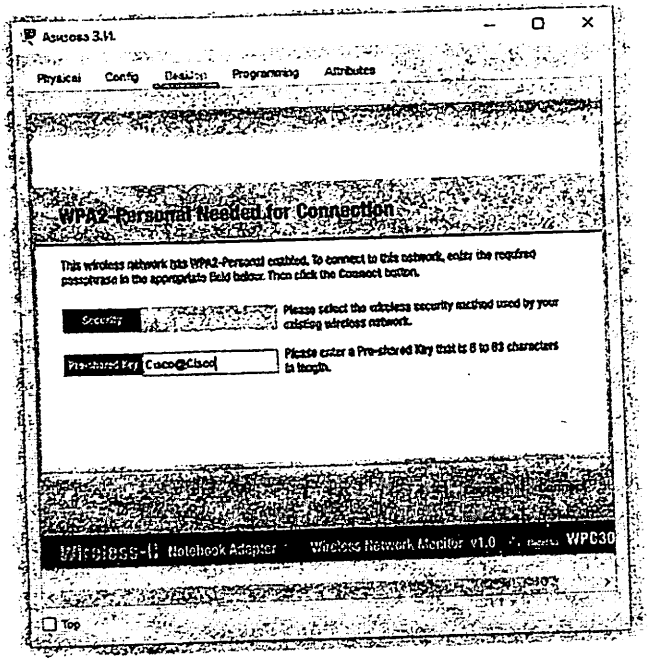
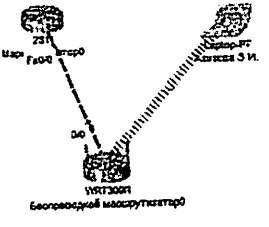


Рис.7.8. Ввод пароля для подключения к беспроводной сети

Если настройки произведены верно, то появится пунктирная линия между wi-fi маршрутизатором и ноутбуком как на рисунке.



Введём на ноутбуке в командной строке (Command Prompt) команду **ipconfig**, чтобы проверить правильность настроек. Из рисунка видно, что DHCP - сервер присвоил правильный ip **192.168.0.100**. Осуществим проверку ping шлюза (wi-fi маршрутизатор) и адреса интернет провайдера. На рисунке видно, что в обоих случаях происходит передача пакетов без потерь.

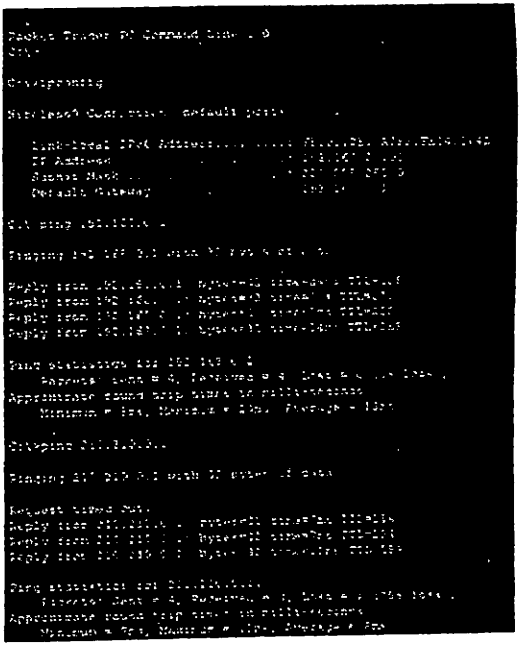


Рис.7.9. Проверка подключения к беспроводной сети

Задание к практической работе:

Задание 1. Создайте модель локальной сети и осуществите ее настройку как это показано в практической части работы, указав в качестве наименований устройств свои имя и фамилию.

Содержание отчета:

1. Титульный лист
2. Выполнение задания, включая скриншоты и подробное описание выполненных действий;
3. Выводы по выполнению практической работы;
4. Ответы на контрольные вопросы

Контрольные вопросы:

1. Что такое компьютерная сеть и какие ее типы Вы знаете?
2. Перечислите сетевые устройства и их основные функции.

3. Какие сетевые протоколы Вы знаете? Опишите их функции.
4. В чем заключаются основные причины возникновения сетевых проблем?
5. Какие типы угроз в беспроводных сетях Вы знаете? Приведите их примеры
6. Как нарушение сетевой безопасности влияет на деятельность бизнеса?

Практическая работа №8

Тема: Восстановление данных с помощью специальных программных средств

Цель работы: совершенствование практических навыков программного восстановления данных, создания точки восстановления системы и восстановления удаленных файлов со съемных носителей.

Теоретические сведения:

Политика резервного копирования (Backup Policy) — это свод правил для копирования данных, включающих в себя: имя политики, статус, время выполнения работ по резервному копированию, период копирования и правила хранения копий данных. Правила хранения определяют продолжительность хранения, количество сохраненных резервных копий и порядок удаления более ранних копий.

Политика резервного копирования, как правило, содержит:

- виды текущих и планируемых ресурсов данных;
- порядок их использования и резервного копирования;
- требования к резервному оборудованию;
- список ответственных лиц;
- общий порядок резервирования;
- условия дополнительного резервирования (дублирующие ресурсы) и прочее.

Цель всякого *резервного копирования* — понижение затрат от незапланированного уничтожения данных в нештатных ситуациях. Достигается эта путём дублирования ценных данных с рабочих машин в сторонние хранилища.

Следующие *задачи* определяются из целей *резервного копирования*:

1. Выделение целевых данных.
2. Сохранение указанных данных для последующего восстановления.
3. Восстановление сохранённых данных.

4. Обеспечение устойчивости хранимых данных к изменению и уничтожению.
5. Разграничение доступа к хранимым данным.
6. Обеспечение контроля системы и процесса резервного копирования.

Практическая часть:

I. Восстановление системы в Windows 10

Операционная система от Microsoft имеет функцию Восстановление Системы, которая поможет восстановить работу компьютера если что-то пойдёт не так. Восстановление Системы даёт возможность восстановить состояние компьютера до предыдущего, отменив изменения, которые могли повредить компьютеру. Это изменения в системных файлах и настройках, реестре, и в установленных приложениях. Это как возвращение назад во времени.

Если всё правильно настроено, в момент установки нового приложения, драйвера или обновления Windows создаёт точку восстановления, но такую точку восстановления можно также создавать и вручную. Например, если необходимо изменить настройки реестра или установить какое-то большое приложение.

Это похоже на резервную копию, но с тем отличием, что нет возможности вернуть документы и настройки в состояние до момента создания точки восстановления. Также данная функция удалит все приложения, драйвера, обновления системы и изменения реестра, которые были сделаны до создания точки восстановления.

Включение функции восстановления системы

1. Перейдите в меню «Пуск» или кликните окошко поиска, наберите «Создание точки восстановления» и нажмите Enter. Откроется вкладка «Защита системы» в окошке «Свойства системы», в котором можно внести изменения в настройку необходимой нам функции.

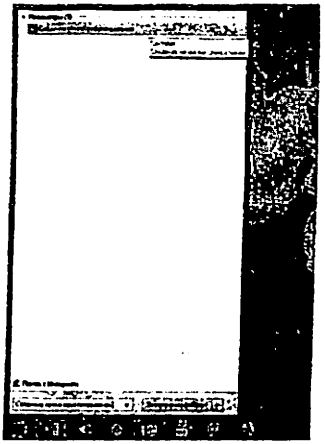


Рис.8.1.Окно поиска элемента «Создание точки восстановления»

2. В открытом окошке необходимо убедиться, что активирована функция защиты системного диска (как правило диск С) – напротив диска прописано «Включено».
3. Если функция защиты системного диска не активирована, кнопка «Создать...» будет неактивна. В таком случае необходимо будет указать системный диск и кликнуть кнопку «Настроить...».

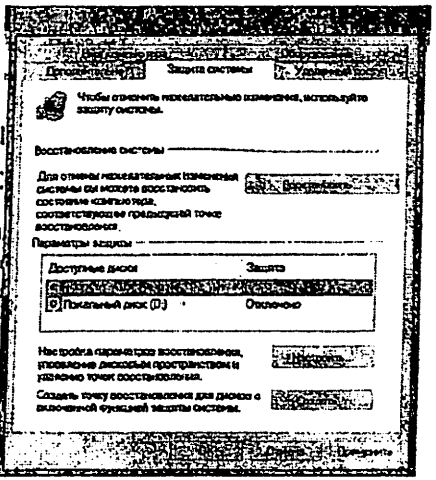


Рис.8.2. Диалоговое окно «Свойства системы»

4. В открытом окошке настроек выберите «Включить защиту системы» для её активации.

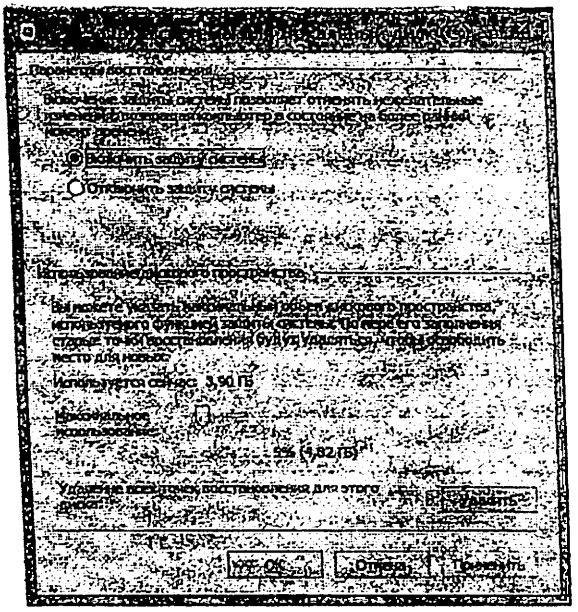


Рис.8.3. Окно настройки параметров восстановления

Функция «Восстановление системы» может быть активирована только для системного диска, но не для всего компьютера. Вы не сможете её настроить для других встроенных или съёмных носителей.

В разделе «Использование дискового пространства» можно определить максимальный размер дискового пространства, предназначенного для хранения точек восстановления. По умолчанию, Windows использует небольшой процент пространства диска и по мере его заполнения, удаляет старые точки восстановления для сохранения более новых.

Также, обратите внимание на кнопку «Удалить», с помощью которой можно удалить все существующие точки восстановления. Она будет полезна, когда необходимо создать точку восстановления вручную, и для этого будет недостаточно места.

5. После осуществления необходимых настроек нажмите «Применить» и «ОК». После этого функция защиты диска будет включена.

Создание точки восстановления

Теперь, когда в системе активирована Точка Восстановления, операционная система будет автоматически создавать точки восстановления каждый раз, когда будут происходить важные изменения. Но, иногда требуется создание точки восстановления вручную. Например, перед тем, как в систему будут вноситься изменения, а уверенности в том, что они не повредят работоспособности системы – нет.

Для настройки ручного создания точки восстановления, просто нажмите кнопку «Создать...», и введите описание точки восстановления, с помощью которой вы сможете её идентифицировать (например: Точка восстановления перед установкой «....»). После этого нажмите кнопку «Создать» для завершения процесса.

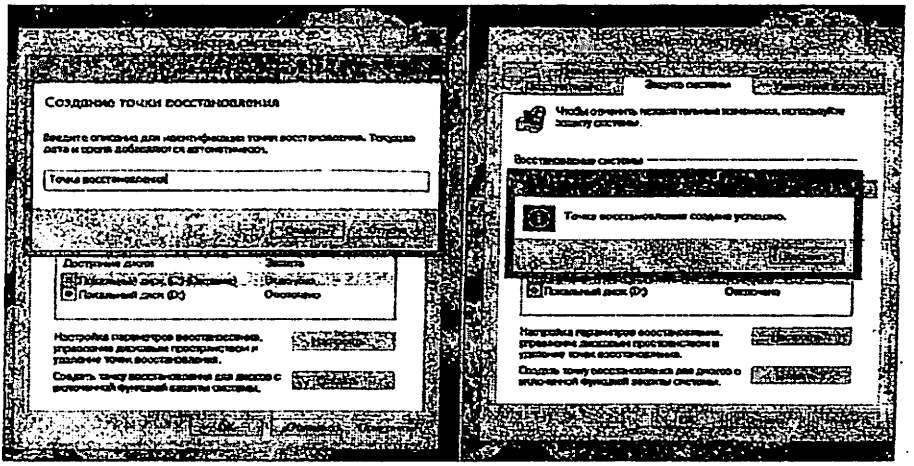


Рис.8.4. Ввод описания точки восстановления для её последующей идентификации

В любой момент времени, в случае возникновения каких-либо проблем, перед использованием резервной копии данных или функции «Возвращения

компьютера в исходное состояние» в Windows 10, попробуйте воспользоваться точкой восстановления, что намного быстрее и проще. Для отмены нежелательных изменений системы и восстановления компьютера до состояния, которое было до изменений необходимо сделать следующее:

1. Перейдите в меню «Пуск» или кликните окошко поиска, наберите «Создание точки восстановления» и нажмите Enter. Откроется вкладка «Защита системы» в окошке «Свойства системы».
2. Нажмите кнопку «Восстановить...» и кликните «Далее».

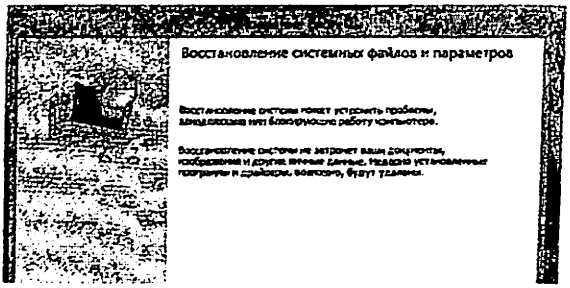


Рис.8.5. Окно восстановления системных файлов и параметров

3. В следующем окне вы увидите доступные точки восстановления с датой, описанием, и что более важно – тип точки восстановления, указывающий была она создана вручную или системой.

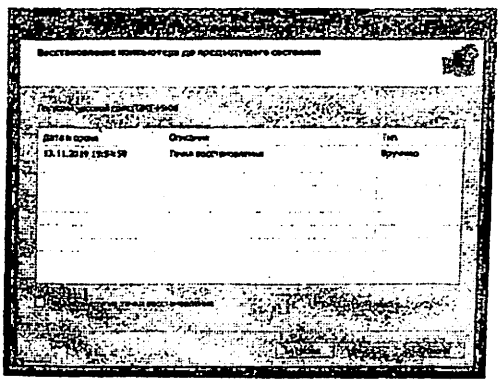


Рис.8.6. Окно восстановления компьютера до предыдущего состояния

После того как будет выбрана точка восстановления можно выбрать «Поиск затрагиваемых программ», чтобы увидеть приложения, которые были установлены после создания точки восстановления и будут удалены после её восстановления.

Для завершения процесса восстановление нажмите «Далее».

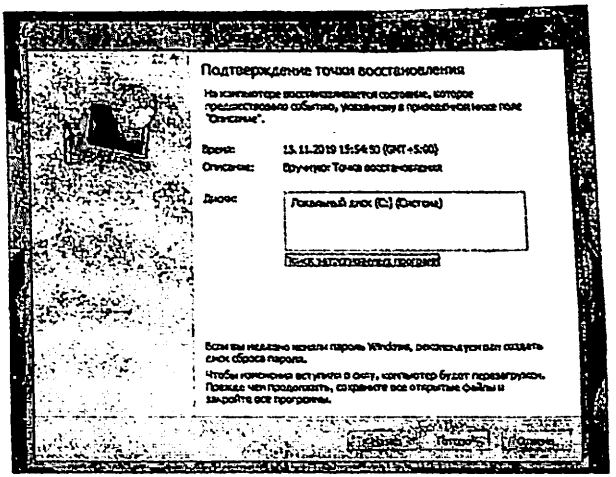


Рис.8.10. Завершение процесса создания точки восстановления

После завершения процесса, состояние системы вернётся в то состояние при котором была создана точка восстановления.

Режим автоматического восстановления системы

До этого, мы рассматривали как использовать точку восстановления в случае необходимости восстановления системы, когда она ещё работоспособна. Но бывают случаи, когда точка восстановления создана, но после внесения определённых изменений Windows не загружается.

В таких случаях, для доступа к функции «Восстановления системы» используются дополнительные параметры при загрузке. Просто, попробуйте загрузить компьютер трижды, чтобы вызвать режим автоматического восстановления в Windows 10, после чего:

1. Выберите «Особые варианты загрузки».

2. Далее: «Диагностика», «Дополнительные параметры», «Восстановление системы».
3. После чего загрузится «Восстановление системы» и далее можно будет следовать указанными раннее шагами начиная с раздела «Использование восстановления системы».

Также, для того чтобы загрузить систему можно использовать загрузочный диск, после чего:

1. Нажать «Далее» и «Восстановить компьютер».
2. Далее: «Диагностика», «Дополнительные параметры», «Восстановление системы».
3. После чего загрузится «Восстановление системы» и далее можно будет следовать указанными раннее шагами начиная с раздела «Использование восстановления системы».

II. Восстановление файлов в программе TestDisk

TestDisk — свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или человеческих ошибок (например, потеря MBR).

1. Установка *<sudo api-get install testdisk>*.
2. Запускаем TestDisk *<sudo testdisk>*.
3. Появляется окошко приветствия TestDisk, нам предлагается вести лог работы (для выполнения данной работы лог не требуется).
4. Выбираем нужный диск и нажимаем *Enter*.
5. Предлагается выбрать тип таблицы разделов, обычно TestDisk определяет все правильно, так что нажимаем *Enter*.
6. Выбираем *Analise*.
7. Выбираем *QuickSearch*.
8. Нам выводят таблицу разделов. Выбираем раздел и нажимаем *P*, чтобы вывести список файлов.
9. Выбираем файлы для восстановления и нажимаем *C*.

10.Выбираем папку, куда будут сохранены файлы и нажимаем *C*.

Если раздел на жестком диске, карте памяти или USB флешке оказался поврежден или случайно удален, во многих случаях его может оказаться возможным восстановить. Существуют различные утилиты для восстановления разделов, как платные, так и бесплатные. Среди программ с возможностью бесплатного использования можно выделить TestDisk и DMDE.

На первом экране вам предложат создать журнал производимых TestDisk операций: выбираем Create для его создания или No Log.

Как восстановить раздел диска в TestDisk. В приведенном далее примере будет демонстрироваться простая ситуация: с флешки был удален файл и его требуется восстановить. Аналогично процесс будет выглядеть и для подобных ситуаций с жестким диском или картой памяти, при условии, что на них не были созданы новые разделы и записаны дополнительные данные.

Следующие шаги по восстановлению раздела с диска будут выглядеть следующим образом: на первом экране вам предложат создать журнал производимых TestDisk операций: выбираем «Create» для его создания или «No log», если он не требуется.

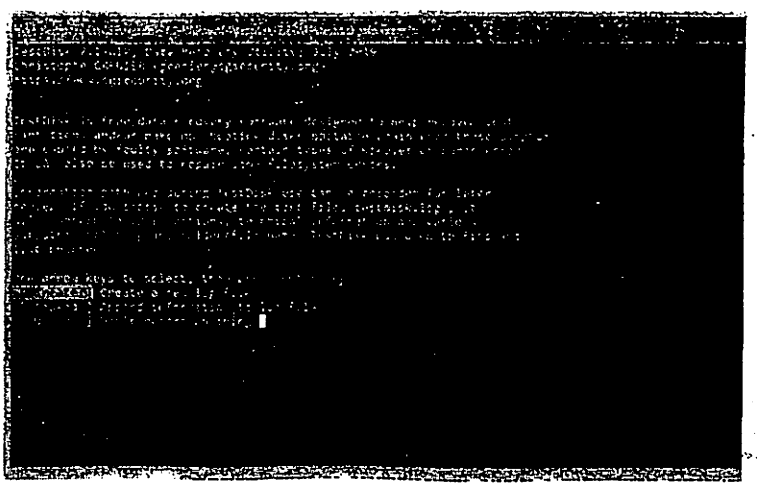


Рис.8.11. Окно выбора режима работы программы TestDisk

Следующий этап — выбор физического диска, на котором будет выполнен поиск разделов. После выбора с помощью стрелок нажимаем Enter для продолжения.

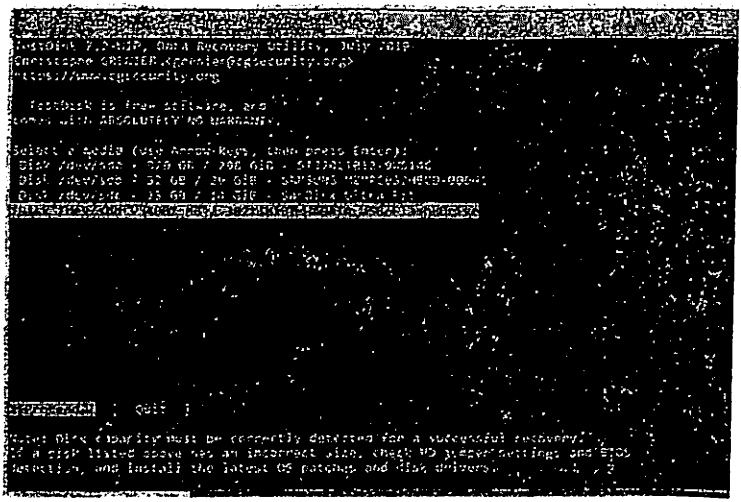


Рис.8.12. Выбор раздела жесткого диска

На 3-м этапе следует выбрать, какой тип разделов следует найти. Обычно требуется первый пункт — Intel/PC partition, включающий поиск разделов NTFS и различных вариантов FAT.

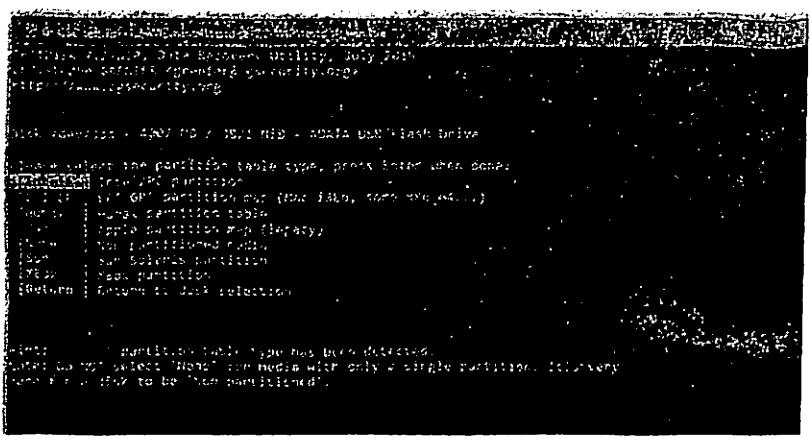


Рис.8.13. Выбор типа таблицы разделов

В результате поиска отобразится список найденных на накопителе потерянных разделов. Если вы не уверены, тот ли это раздел, вы можете нажать по клавише P на этом экране для просмотра содержимого найденного раздела. При просмотре содержимого вы можете перемещаться по папкам (учитывайте, что кириллические имена будут отображаться неверно), сохранять файлы с раздела. Для возврата на экран со списком разделов нажмите клавишу Q.

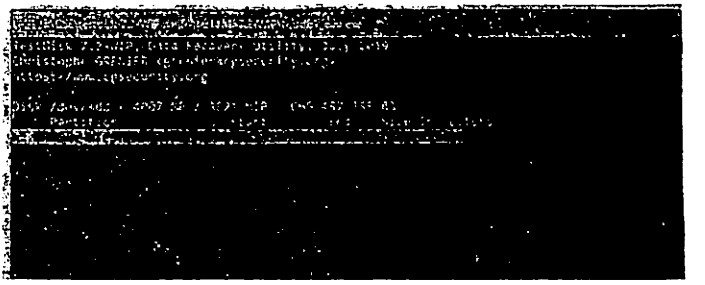


Рис.8.14. Выбор потерянных разделов из списка предложенных

Нажмите Enter, а на следующем экране, если вы решили восстановить найденный раздел, выберите пункт «Write» (записать изменения) и нажмите Enter. Обратите внимание, что здесь же присутствует пункт «Deeper Search» (глубокий поиск) на случай, если до этого разделы не были найдены.

Теперь необходимо выбрать файл для восстановления: Логический контроль доступа 3.docx. Выбираю файл и команду C для копирования файла, как показано на рисунке выше.

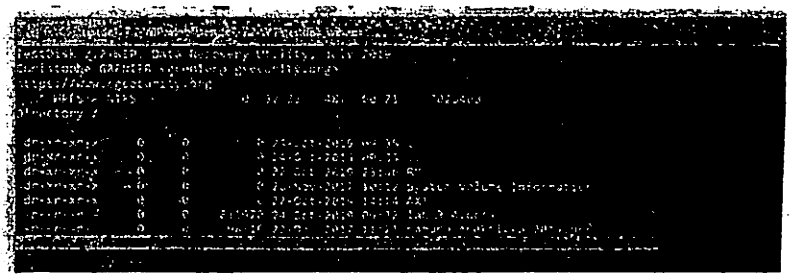


Рис.8.15. Выбор требуемого для восстановления файла

После этого необходимо выбрать путь для сохранения файла. По умолчанию предлагается путь расположения самой программы TestDisk. Выбираем необходимый путь сохранения восстанавливаемых данных:

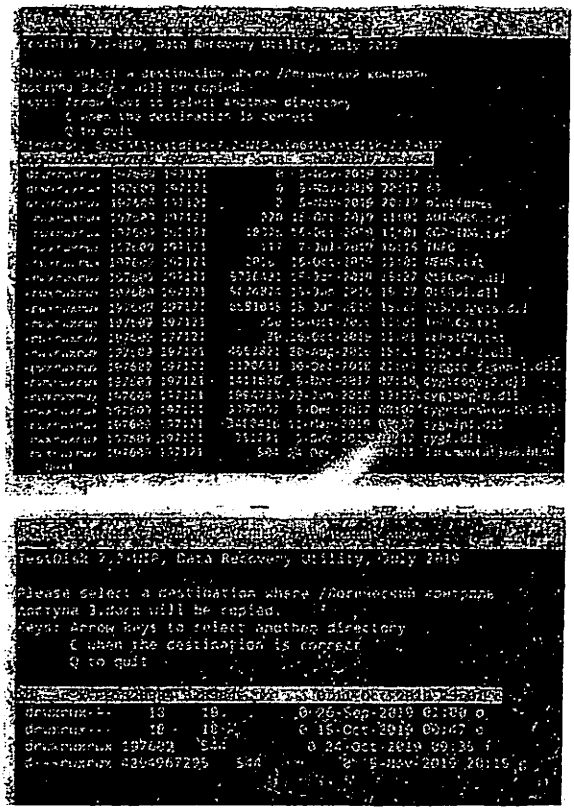


Рис. 8.16. Выбор пути для сохранения восстановленного файла

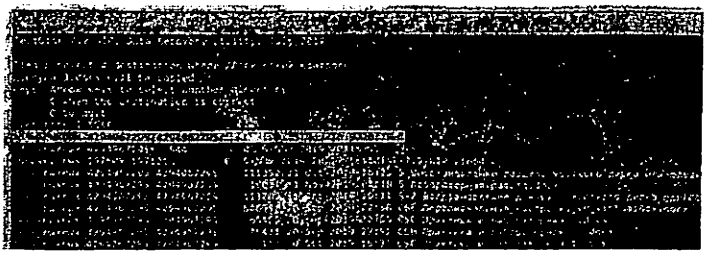


Рис.8.17. Выбор конечного пути для сохранения восстановленного файла

Определив конечный путь сохранения файла вновь необходимо выбрать команду копирования файла C.

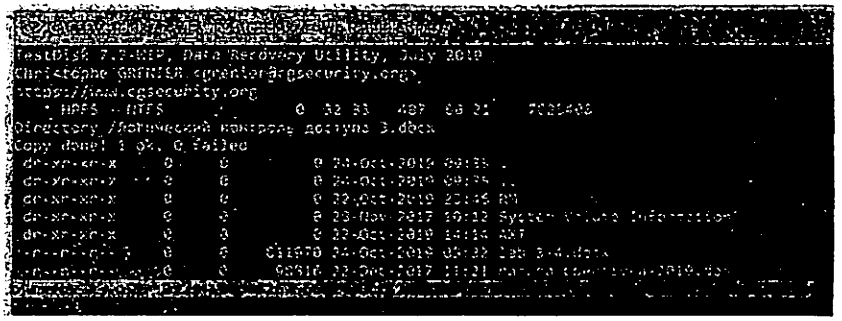


Рис.8.18. Успешное восстановление требуемого файла

При проверке папки CSE видно что скопированный файл Логический контроль доступа 3.docx находится в указанной папке.

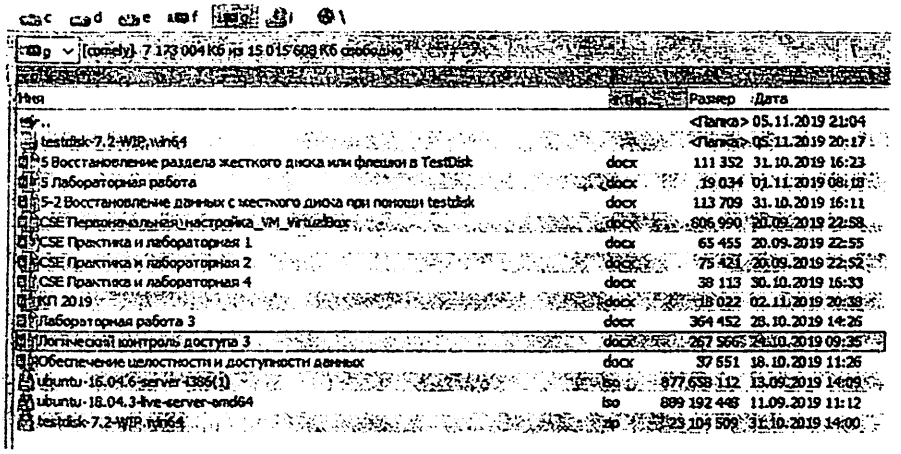


Рис.8.19. Отображение восстановленного файла в указанной папке

Задание к практической работе:

Задание 1. Создайте резервные копии данных и выполните восстановление системы в ОС Windows. Продемонстрируйте каждый этап выполнения в виде скриншотов с подробным описанием всех действий.

Задание 2. Выполните резервное копирование и восстановление данных с flash-накопителя в программе TestDisk. Действия по восстановлению отразите в отчете к практической работе.

Содержание отчета:

1. Титульный лист
2. Выполнение заданий №1 и №2, включая скриншоты и подробное описание выполненных действий;
3. Выводы по выполнению практической работы;
4. Ответы на контрольные вопросы

Контрольные вопросы:

1. Что вы понимаете под резервным копированием данных?
2. Какие виды резервного копирования данных вы знаете? В чем их различия?
3. Какие способы резервного копирования вы знаете?
4. Каким образом происходит процесс восстановления данных в программе TestDisk?
5. С каким программными средствами резервного копирования и восстановления данных вы работали?
6. Как часто необходимо осуществлять резервное копирование (бэкап)?

Практическая работа №9

Тема: Установка антивирусной защиты на персональные компьютеры

Цель работы: приобретение навыков установки и настройки антивирусного программного обеспечения на персональном компьютере.

Теоретические сведения:

Антивирусными называются программы, предназначенные для защиты данных от разрушения, обнаружения и удаления компьютерных вирусов. Различают следующие разновидности антивирусных программ: фильтры, или сторожа; детекторы; доктора, или фаги; ревизоры; иммунизаторы, или вакцины.

Фильтр представляет собой резидентную программу, которая контролирует опасные действия, характерные для вирусных программ, и запрашивает подтверждение на их выполнение. К таким действиям относятся:

- изменение файлов выполняемых программ;
- размещение резидентной программы;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные секторы диска; форматирование диска.

Достоинством программ-фильтров является их постоянное отслеживание опасных действий, повышающее вероятность обнаружения вирусов на ранней стадии их развития. С другой стороны, это же является и недостатком, так как приводит к отвлечению пользователя от основной работы для подтверждения запросов по подозрительным операциям.

Детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях. Различают детекторы универсальные и специализированные. ***Универсальные детекторы*** в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью причин искажения файлов. ***Специализированные***

детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы Детектор, позволяющий обнаруживать несколько вирусов, называют *полидетектором*.

Доктором называют антивирусную программу, позволяющую обнаруживать и обезвреживать вирусы. При обезвреживании вирусов среда обитания может восстанавливаться или не восстанавливаться.

Полифаг – программа, предназначенная для обнаружения и уничтожения компьютерных вирусов (Фаг – программа для обнаружения и уничтожения одного вируса). Как правило, полифаги используют базу данных, содержащую данные о вирусах, с которыми умеет бороться полифаг. Кроме того, современные полифаги, как правило, имеют эвристический анализатор, который позволяет обнаруживать вирусы, информация о которых не содержится в базе данных полифага. К их числу принадлежат получившие широкое распространение программы Doctor Web, Norton Antivirus, Virusscan, AVP и др. Основной нюанс их работы, заключается в необходимости постоянного обновления базы данных, содержащей сведения о вирусах. При этом важно помнить, что каждый месяц появляется от 100 до 200 и более новых вирусов, поэтому программа, не обновленная несколько месяцев, может не обеспечить Вашему ПК должную защиту от новых вирусов.

Ревизор представляет собой программу, запоминающую исходное состояние программ, каталогов и системных областей и периодически сравнивающую текущее состояние с исходным. Сравнение может выполняться по параметрам: длина и контрольная сумма файла и т.п. Достоинством ревизоров является их способность обнаруживать стелс-вирусы. К числу ревизоров относится хорошо известная программа ADinf.

Иммунизатор представляет собой резидентную программу, предназначенную для предотвращения заражения рядом известных вирусов путем их вакцинации. Суть вакцинации заключается в модификации программ или диска таким образом, чтобы это не отражалось на нормальном

выполнении программ. В то же время вирусы воспринимали их как уже зараженные и поэтому не пытались внедриться.

Антивирусные программы - это программы, основной задачей которых является защита от вирусов и вредоносных программ. Из всех методов антивирусной защиты можно выделить две основные группы:

- *Сигнатурные методы* - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.
- *Эвристические методы* - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Практическая часть:

Установка Антивируса Kaspersky Anti-Virus.

Шаг 1. Установка и активация Антивируса Касперского. Скачать исполняемый файл можно пройдя по ссылке: https://www.kaspersky.ru/downloads/antivirus?icid=ru_sup-site_trd_ona_oth__onl_b2c__tri-dl__kav__&_ga=2.211412880.426716304.1668683077-1964581452.1664801915.

Запустите Мастер установки Антивируса Касперского. Чтобы сделать это, выполните запуск исполняемого файла.

Рис.9.1. Запуск Мастера установки программы

В результате запустится Мастер установки Антивируса Касперского. Чтобы запустить стандартную установку Антивируса Касперского, нажмите кнопку *Продолжить*.

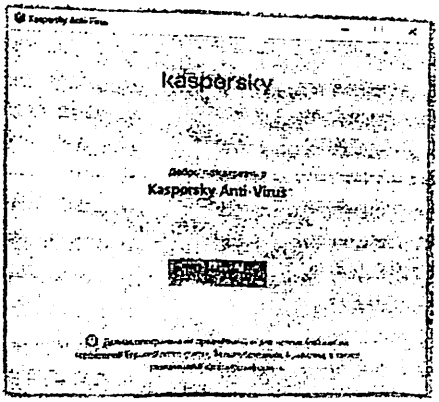


Рис.9.2. Запуск стандартной установки Антивируса Касперского

Шаг 2. Ознакомьтесь с Лицензионным соглашением Лаборатории Касперского. Внимательно прочтите соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку *Принять*. Установка программы на ваш компьютер будет продолжена. Для отказа от установки нажмите на кнопку *Назад*.

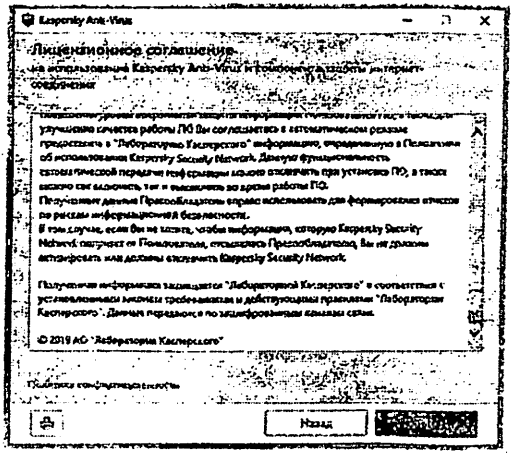


Рис.9.3. Окно ознакомления с Лицензионным соглашением

Также изучите Положение о компоненте защиты интернет-соединения Kaspersky Security Network и, если вы согласны со всеми его пунктами, нажмите на кнопку *Принять*. Участие в программе Kaspersky Security Network предусматривает отправку в Лабораторию Касперского информации о новых угрозах, обнаруженных на вашем компьютере, отправку уникального идентификатора, присвоенного вашему компьютеру Антивирусом Касперского, и информации о системе. При этом гарантируется, что персональные данные отправляться не будут. Установка программы на ваш компьютер будет продолжена. Для отказа от установки нажмите на кнопку *Отказаться*.

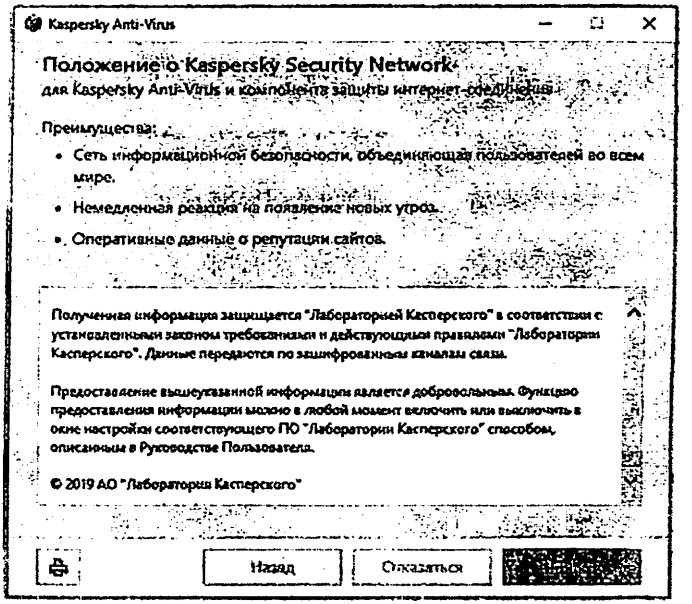


Рис.9.4. Положение о компоненте защиты интернет-соединения Kaspersky Security Network

После этого для перехода к процессу установки кликните на кнопку *Установить*

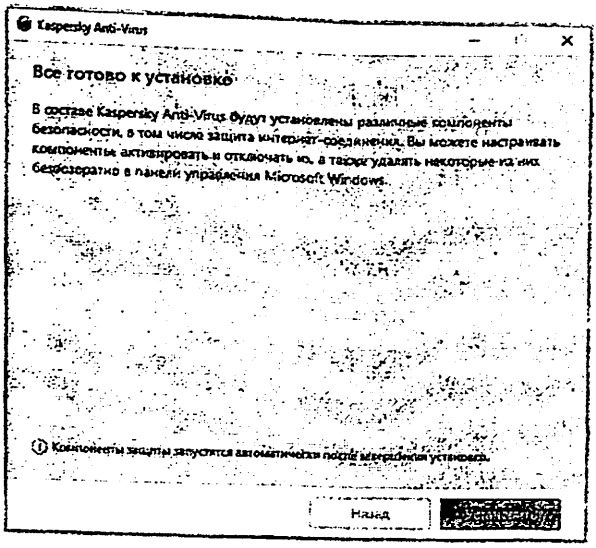


Рис. 9.5. Запуск процесса установки программы

Далее начнётся процесс установки программы.

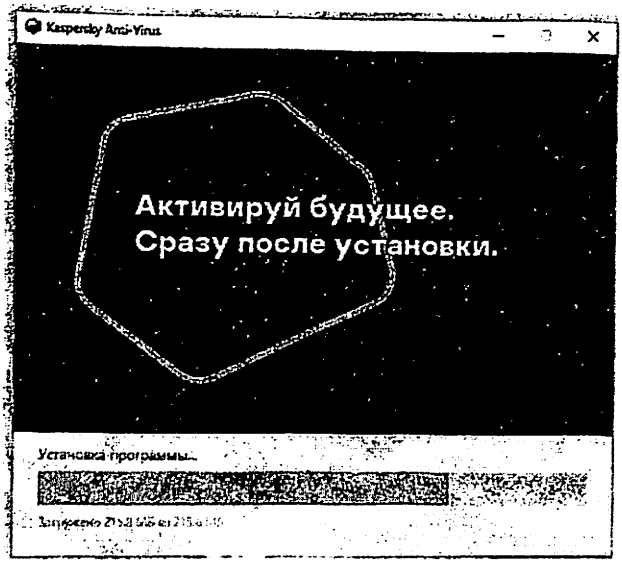


Рис.9.6. Процесс установки программы

После этого появится окно с рекомендуемыми настройками. Выберите необходимые настройка и нажмите на кнопку *Применить*.

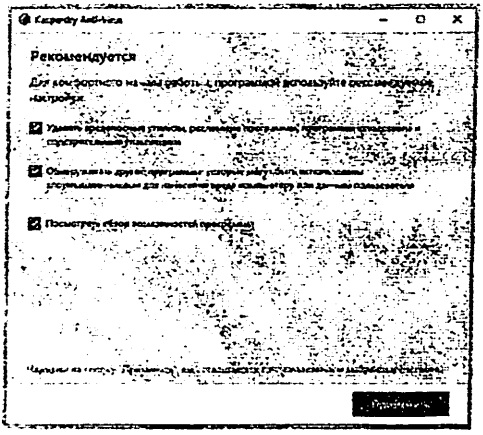


Рис.9.10. Рекомендуемые настройки антивируса

Далее появится диалоговое окно с сообщением об успешной установке программы. Нажмите *Готово* и приступите к активации и настройке программы.

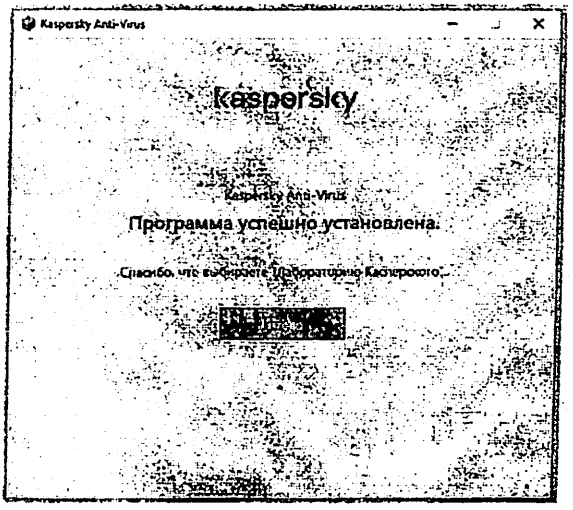


Рис.9.11. Завершение установки программы

Шаг 3. Активация Kaspersky Anti-Virus. Для активации пробной версии Антивируса Касперского необходимо подключение к Интернет.

После копирования файлов *Мастер установки* предлагает активировать копию Антивируса Касперского. Предлагается 3 варианта активации:

- *Активировать коммерческую версию*- необходимо ввести 20-значный код активации. Для активации необходим доступ в Интернет, Мастер установки скачает и установит ключевой файл автоматически.
- *Активировать пробную версию* - Мастер установки скачает и установит ключевой файл сроком на 30 дней. Для активации необходим доступ в Интернет. Пробная версия полностью функциональна. По истечении срока пробного ключа обновление баз будет не доступно.

(Примечание. Пункт **Активировать пробную версию** может быть недоступен, в случаях если пробная версия была использована ранее или активирована в данный момент.)

- *Активировать позже* - пропустить активацию на данном этапе. Обновление антивирусных баз будет доступно сразу после активации.

Введите код активации и нажмите на кнопку *Активировать*. После чего можете приступить к настройке программы.

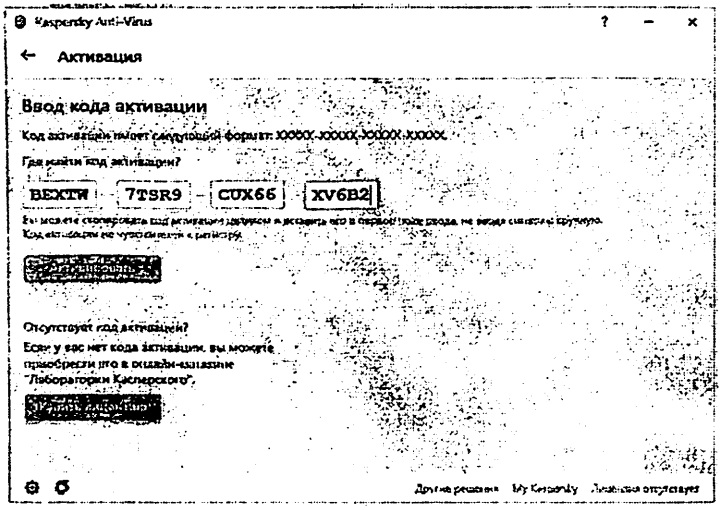


Рис.9.12. Активация программы Kaspersky Anti-Virus

Шаг 4. Настройка антивируса.

Изучите каждый из представленных пунктов меню *Настройка* (Защита, Общие, Угрозы и исключения, Отчеты и карантин, Настройки сети, Интерфейс, Управление настройками и Дополнительно). Осуществите настройку каждого из пунктов согласно личным предпочтениям и целям использования программы.

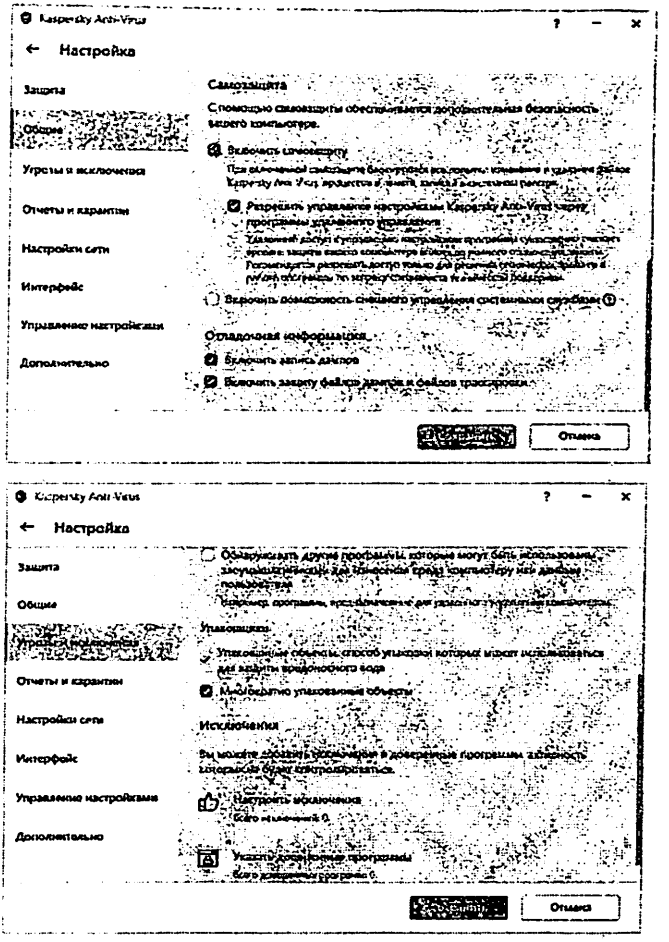


Рис. 9.13. Настройка программы Kaspersky Anti-Virus

Вы можете добавить в исключения программу или файл, которые не нужно будет антивирусу сканировать на наличие вредоносного кода.

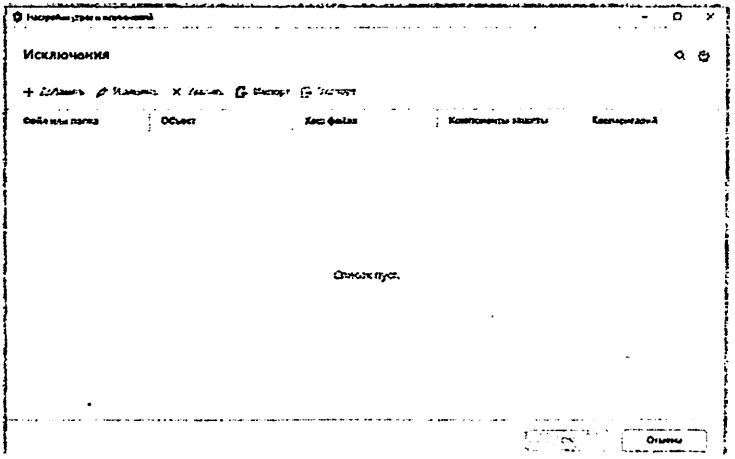


Рис.9.14. Окно настройки угроз и исключений

Также настроить периодичность формирования отчётов о результатах сканирования и периоде хранения файлов в папке Карантин.

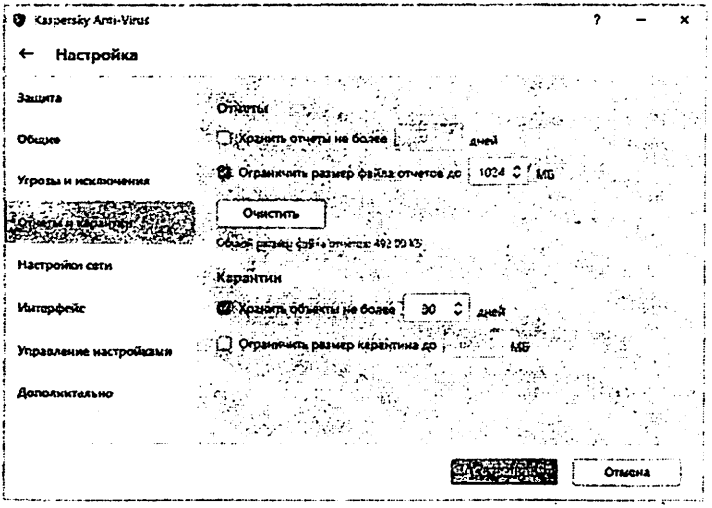


Рис.9.15. Окно настройки параметров формирования отчетов и хранения объектов

Во вкладке *Настройки сети* необходимо отметить нужные настройки и сохранить их.

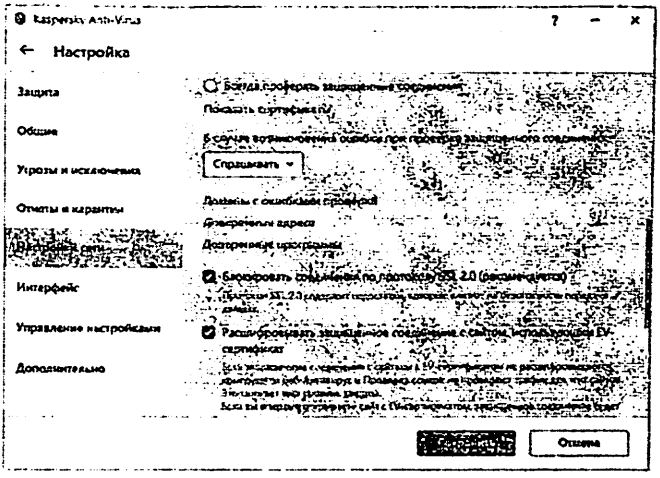


Рис.9.16. Окно настройки параметров сети

Можно скрыть стандартный значок антивируса в настройках Интерфейса.

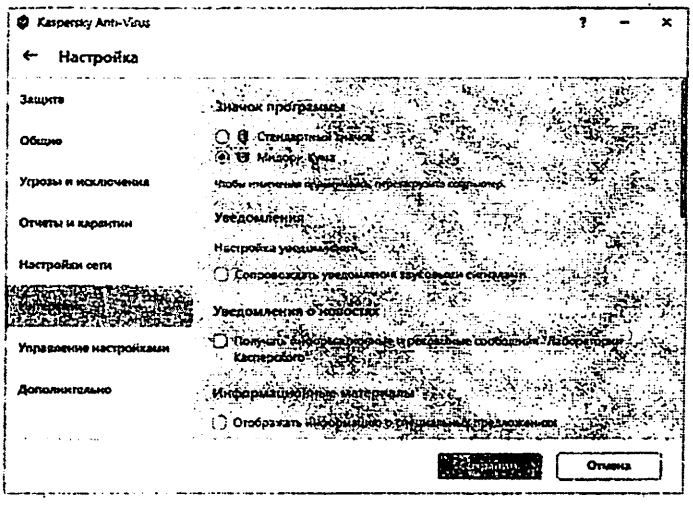


Рис.9.17. Окно настройки интерфейса программы

При необходимости сохранения настроек антивируса их можно *экспортировать* в единый файл, либо наоборот, при наличии файла настроек антивируса можно настроить антивирус путем *импортирования* готовых настроек. Можно вернуть все настройки по умолчанию выбрав *Восстановить*.

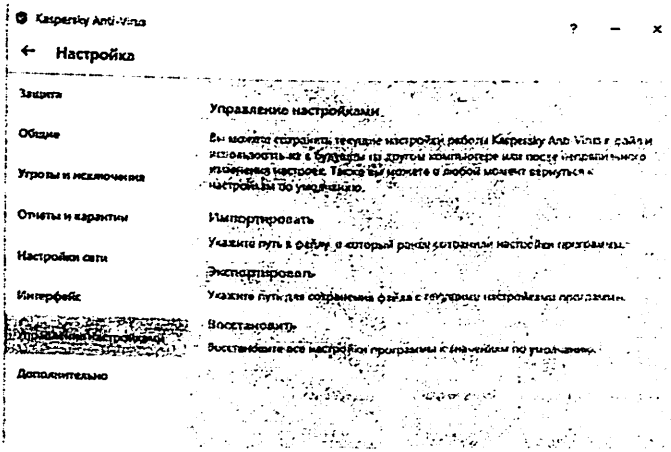


Рис.9.18. Окно управления настройками программы

Для осуществления проверки устройства или съемного носителя на наличие вредоносных программ и вирусов выбираем пункт *Проверка*.

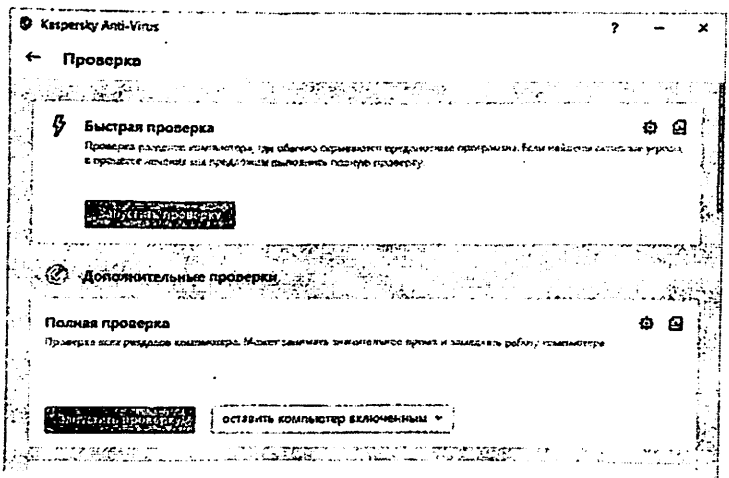


Рис.9.19. Окно запуска проверки на наличие вредоносных программ

Далее выбираем *Проверка съемных носителей* и указываем либо весь носитель, либо отдельную папку для проверки (как это сделано в данном примере)

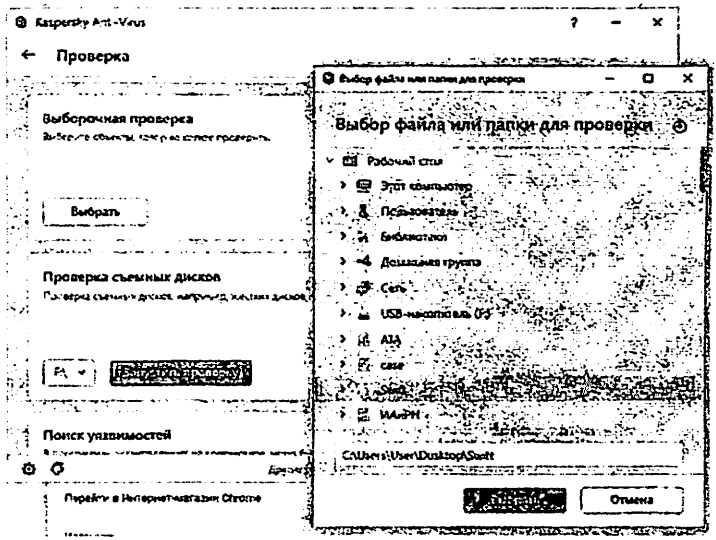


Рис.9.20. Выбор объекта проверки

И нажимаем на Запустить проверку

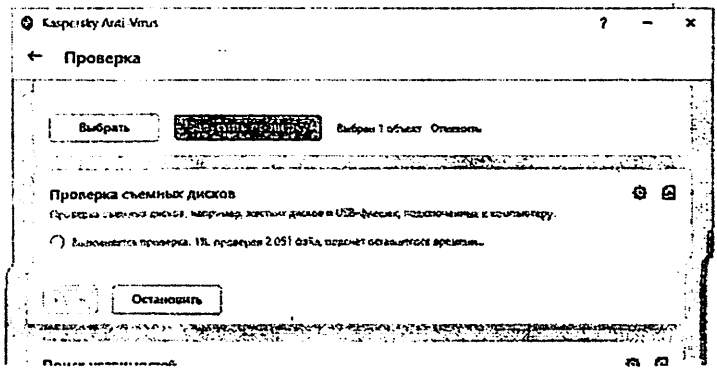


Рис.9.21. Запуск проверки на наличие вредоносных программ

По завершению проверки будут выведены результаты сканирования с указанием обнаруженных вредоносных программ, либо сообщение об их отсутствии.

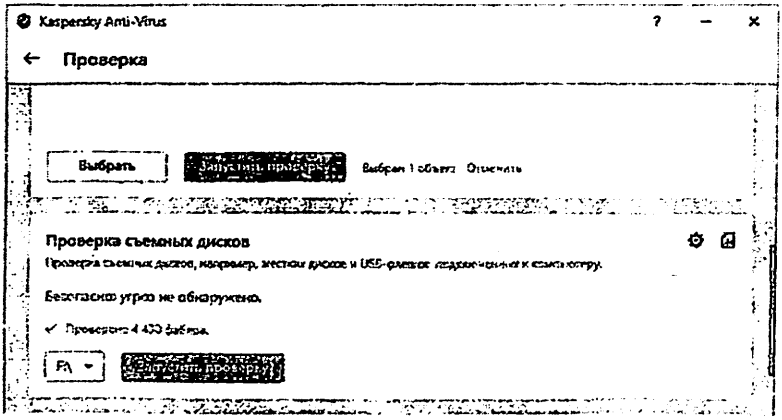


Рис.9.22. Результаты произведенной проверки

Задание к практической работе:

Задание 1. Установите на свой персональный компьютер программу Kaspersky Anti-Virus (либо любую другую выбранную вами программу-антивирус, например, Защитник Windows (Windows Defender), Comodo Antivirus, AVG AntiVirus FREE, Avast! Free Antivirus, Eset NOD32, и др.).

Задание 2. Осуществите настройку антивируса и сканирование своего персонального компьютера или съёмного носителя на наличие вредоносных программ и файлов. Результаты предоставьте в виде скриншотов с подробным описанием выполненных действий.

Содержание отчета:

1. Титульный лист.
2. Выполнение задания к практической работе, включая скриншоты и подробное описание выполненных действий.
3. Выводы по выполнению практической работы.

4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. В чём назначение антивирусных программ?
2. Какие альтернативные антивирусные программы вы знаете?
3. Что такое активация антивирусной программы Касперского?
4. Как правильно настроить антивирус для отдельного персонального компьютера?
5. Какие методы обновления антивирусных баз вы знаете?
6. Как настроить обновление антивирусных баз без выхода в Интернет?
7. Что такое антифишинг?
8. Как настроить файловый антивирус?
9. Как настроить почтовый антивирус?
10. Как настроить веб-антивирус?

Практическая работа №10

Тема: Управление паролями пользователей

Цель работы: приобретение навыков управления сохраненными паролями учётных данных пользователей в операционной системе Windows.

Теоретические сведения:

Windows Credential Manager *(Диспетчер учетных данных)* позволяет сохранять учетные записи и пароли для доступа к сетевым ресурсам, сайтам и приложениям. Благодаря диспетчеру учётных записей Windows вы можете подключаться к удаленным ресурсам автоматически, без ввода пароля. Приложения могут самостоятельно обращаться в Credential Manager и использовать сохраненный пароль.

Использование диспетчера учетных данных Windows для хранения паролей. Впервые Credential Manager появился в Windows 7 и позиционируется как достаточное безопасное место для хранения пользовательских паролей. В диспетчере учетных данных могут хранится следующие типы аккаунтов:

- *Учетные данные Windows (Windows Credentials)* – данные для входа в Windows, для доступа на удаленные компьютеры, сохраненные пароли для RDP подключений, пароли к сайтам, поддерживающих встроенную аутентификацию Windows и т.д; (*Примечание: в Windows Credential не хранятся данные для автоматического входа в Windows или доменные Cached Credentials.*)
- *Учетные данные на основе сертификатов (Certificate-Based Credentials)* – для аутентификации с помощью смарт-карт;
- *Общие учетные данные (Generic Credentials)* – используются сторонними приложениями, совместимые с Credential Manager;
- *Учетные данные для интернета (Web Credentials)* – сохранённые пароли в браузерах Edge и IE, приложениях Microsoft (MS Office, Teams, Outlook, Skype и т.д). Например, если при доступе к сетевой папке вы включите

опцию "Сохранить пароль", то введенный вами пароли будет сохранен в Credential Manager. Аналогично пароль для подключения к удаленному RDP/RDS серверу сохраняется в клиенте Remote Desktop Connection (mstsc.exe).

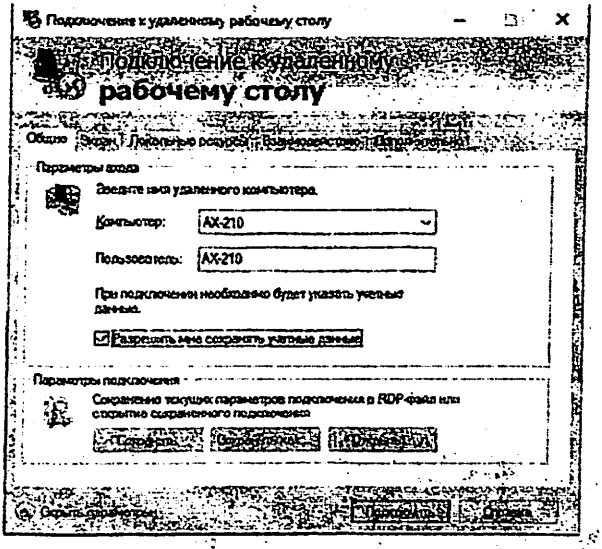


Рис.10.1. Окно подключения к удаленному рабочему столу

Также в менеджере паролей сохраняются пароли пользователей при их сохранении командой runas /savecred.

Практическая часть:

Управление сохраненными паролями с помощью Windows Credential Manager. Вы можете получить доступ к диспетчеру учетных данных в Windows 10 из классической панели управления **Панель управления -> Учетные записи пользователей -> Диспетчер учетных данных** (*Control Panel\User Accounts\Credential Manager*).

В диспетчере учетных данных Windows вы можете:

1. Добавить, изменить или удалить учетные данные Windows
2. Добавить общие учетные данные
3. Добавить учетные данные на основе сертификата

4. Резервное копирование хранилища Windows
5. Восстановить хранилище Windows

В Windows 10/8 вы также увидите еще один тип учетных данных, называемый *веб-учетными данными*, который помогает Internet Explorer хранить веб-пароли пользователей. VaultPasswordView позволяет расшифровывать пароли, хранящиеся в хранилище Windows.

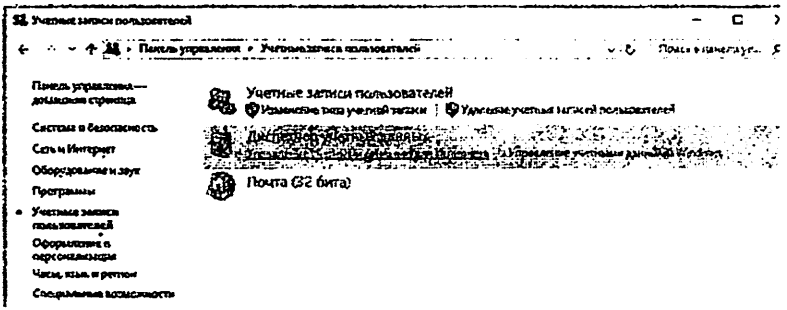


Рис.10.2. Окно Учетных записей пользователей

Как вы видите, в Credential Manager хранятся сохраненные пароли.

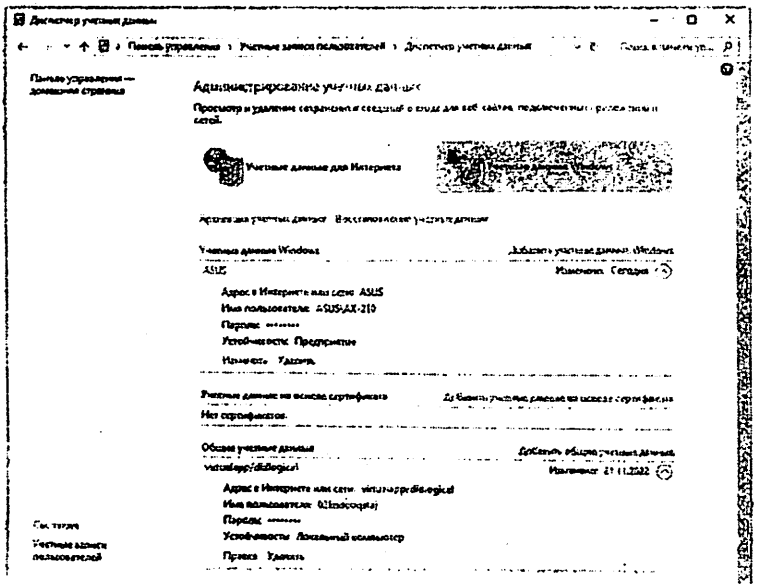


Рис.10.3. Окно Диспетчера учетных данных

Вы можете добавить сохранённый пароль, отредактировать (просмотреть сохраненный пароль из графического интерфейса нельзя) или удалить любую из записей. Также для работы с сохраненными паролями можно использовать классический диалоговый интерфейс Windows – *Сохранение имен пользователей и паролей*. Для его вызова, выполните:

rundll32.exe keymgr.dll,KRShowKeyMgr

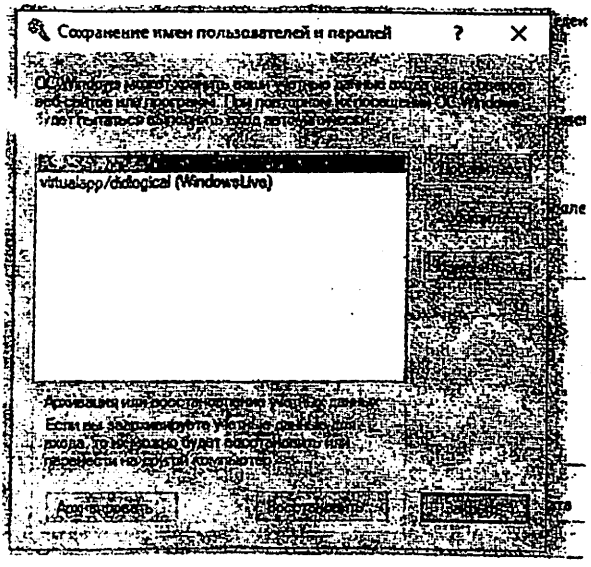


Рис.10.4. Окно сохранения имен пользователей и паролей

Можно управлять сохраненными учетными данными, а также есть функции резервного копирования и восстановления данных в Credential Manager (можно использовать для переноса базы Credential Manager на другой компьютер).

Для управления Credential Manager из командной строки используется утилита **vaultcmd**. Например, чтобы вывести список сохраненных учетных данных типа Windows Credentials выполните команду:

vaultcmd /listcreds:"Учетные данные Windows" или

vaultcmd /listcreds:"Windows Credentials"

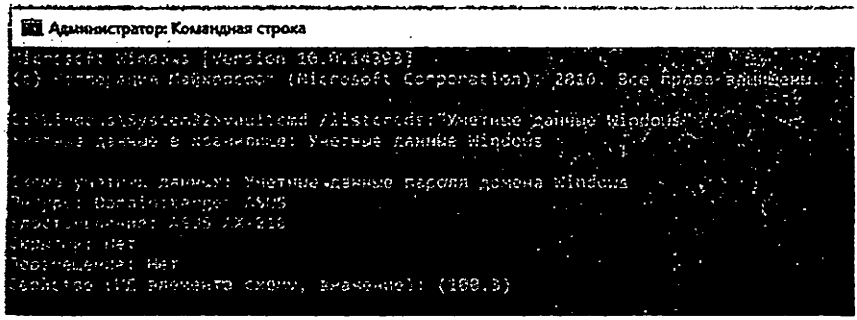


Рис.10.5. Список сохраненных учетных данных

Примеры испол ания VaultCmd.

1. **vaultcmd /list - отобразить** список хранилищ учетных данных.

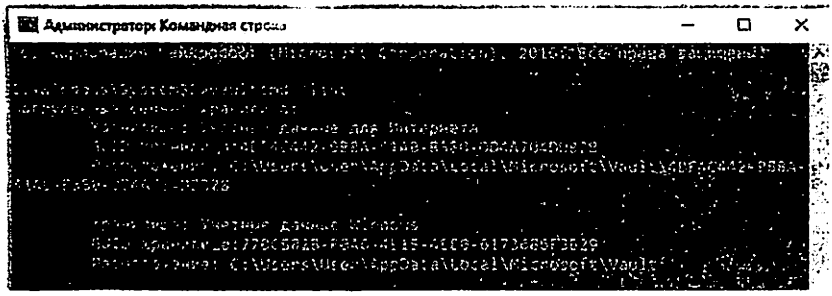


Рис.10.5. Список хранилищ учетных данных

Команда Vaultcmd выполняется по отношению к хранилищу, задаваемому названием или глобальным уникальным идентификатором GUID. Если в названии хранилища имеются пробелы, то оно должно быть заключено в двойные кавычки, например – "Учетные данные для Интернета". Если название содержит символы кириллицы, то они должны быть представлены в DOS-кодировке (кодовая страница 866).

2. **vaultcmd /listschema** - отобразить схему хранилища учетных данных.

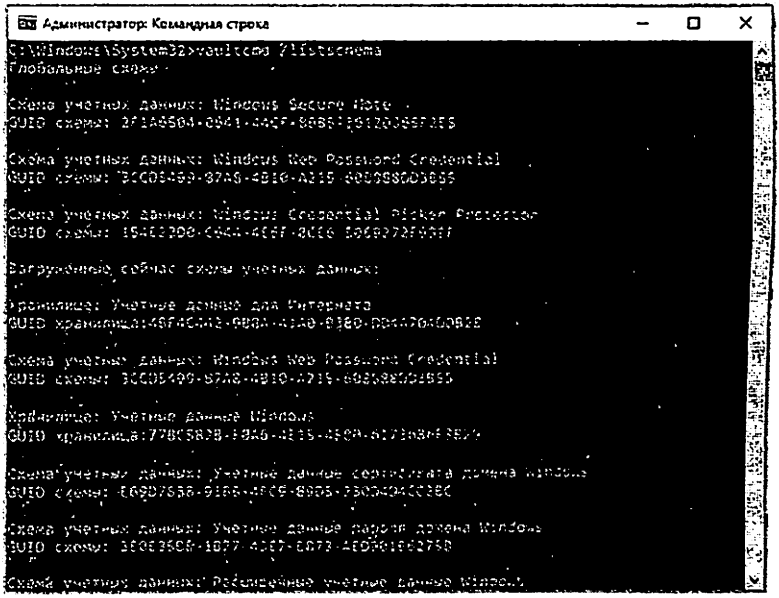


Рис.10.6. Схема хранилища учетных данных

3. vaultcmd /listproperties:"Учетные данные Windows" - отобразить свойства указанного хранилища.

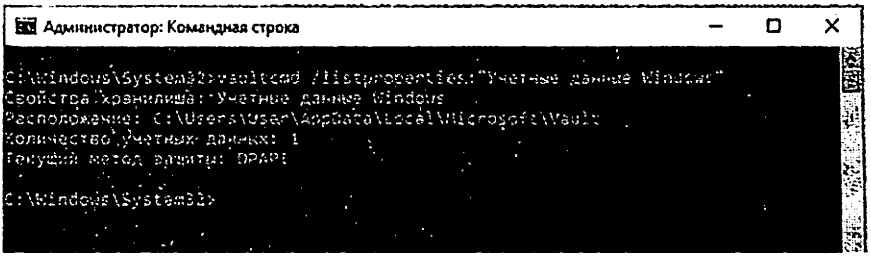


Рис.10.7. Свойства хранилища «Учетные данные Windows»

Все сохраненные пароли хранятся в хранилище Windows Vault. Windows Vault это защищенное хранилище секретов, паролей и другой информации пользователя. Данные в Windows Vault структурированы и представляют собой набор записей, принадлежащих определенной схеме Vault.

Набор ключей шифрования для записей Windows Vault хранится в файле **Policy.vpol.**

Для доменных он хранится в каталоге:

%userprofile%\AppData\Roaming\Microsoft\Vault.

Для локальных пользователей в:

%userprofile%\AppData\Local\Microsoft\Vault .

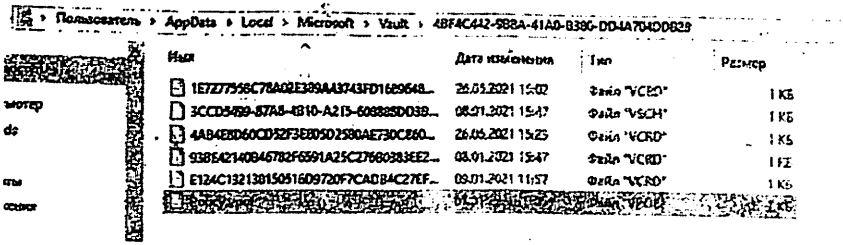


Рис.10.8. Набор ключей шифрования для записей Windows Vault

Если вы хотите заблокировать пользователям возможность сохранения сетевых паролей в Credential Manager, нужно включить политику **Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности** (*Network access: Do not allow storage of passwords and credentials for network authentication*) в разделе **Редактор локальной групповой политики -> Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности.** Для открытия Редактора локальной политики необходимо в меню *Выполнить* ввести **gpedit.msc.**

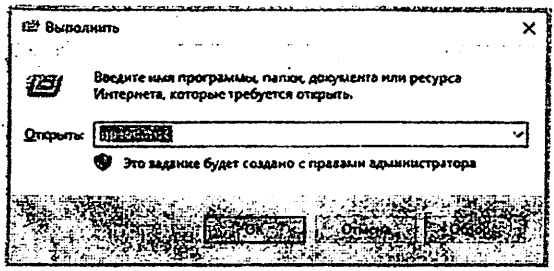


Рис.10.9. Запуск Редактора локальной политики

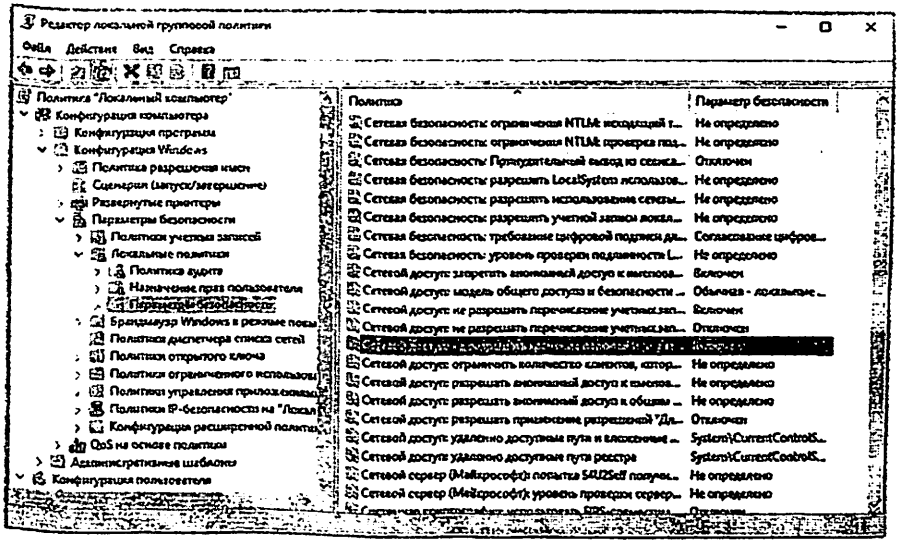


Рис.10.10. Запуск Редактора локальной групповой политики

После этого, если пользователь попытается сохранить пароль в хранилище.

Задание к практической работе:

Задание 1. Изучите возможности управления паролями пользователей с помощью *Диспетчера учетных данных* в ОС Windows. Осуществите настройку имеющихся учётных данных в меню Администрирование учётных данных.

Задание 2. Используя утилиту *VaultCmd* отобразите имеющийся список хранилищ учетных данных программ и файлов, схему хранилища учетных данных, а также свойства указанного хранилища. Изучите другие возможности утилиты *VaultCmd.* Результаты предоставьте в виде скриншотов с подробным описанием выполненных действий.

Содержание отчета:

1. Титульный лист.
2. Выполнение задания 1 и задания 2 к практической работе, включая скриншоты и подробное описание выполненных действий.

3. Выводы по выполнению практической работы.
4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. Что такое пароль? Какие виды паролей Вы знаете?
2. Какой пароль можно считать надежным?
3. В чем заключается основное назначение Диспетчера учетных данных (Windows Credentials)?
4. Где следует сохранять пароли и каким образом можно защищать пароли в операционной системе Windows?
5. Какие требования к хранению и передаче пароля по сети Вы знаете?

Практическая работа №11

Тема: Сбор данных из социальных сетей

Цель работы: приобретение навыков сбора и анализа данных из социальных сетей и других источников персональных данных.

Теоретические сведения:

Тестирование на проникновение является одной из методик выявления областей системы, уязвимых для вторжения и компрометации целостности и достоверности со стороны неавторизованных и злонамеренных пользователей или сущностей. Процесс тестирования проникновения включает в себя умышленные санкционированные атаки на систему, способные выявить как ее наиболее слабые области, так и пробелы в защите от сторонних проникновений, и тем самым улучшить атрибуты безопасности.

Данная методика также может быть использована в качестве дополнения к другим методам проверки для оценки эффективности комплекса защиты системы от различных типов неожиданных вредоносных атак.

Тестирование на проникновение в зависимости от используемых элементов и объектов может быть отнесено к следующим *типам*:

- *Социальная инженерия.* Тестирование с подключением «человеческого контингента», способного четко выявлять и получать конфиденциальные данные и другую информацию через Интернет или телефон (к этой группе могут относиться сотрудники организации или любые другие уполномоченные лица, присутствующие в сети организации).
- *Веб-приложение. Используется* для обнаружения прорех в безопасности и иных проблем в нескольких вариантах веб-приложений и сервисов, размещенных на стороне клиента или сервера.
- *Сетевая служба.* Тестирование проникновения в сеть для выявления и обнаружения возможности доступа хакерам или любому неавторизованному объекту.

- *Клиентская часть.* Как видно из названия, этот тест используется для тестирования приложений, установленных на клиентском сайте / приложении.
- *Удаленное подключение.* Тестирование vpn или аналогичного объекта, который может обеспечить доступ к подключенной системе.
- *Беспроводные сети.* Тест предназначен для беспроводных приложений и сервисов, включая их различные компоненты и функции (маршрутизаторы, фильтрационные пакеты, шифрование, дешифрование и т.д.).

Классифицировать тестирование на проникновение также можно и на основе используемых *подходов к тестированию*:

- ***Белый ящик.*** При таком подходе тестировщик будет иметь полный доступ к глубоким знаниям о функционировании и основных атрибутах системы. Это тестирование очень эффективно, так как понимание каждого аспекта системы очень полезно при проведении обширных испытаний на проникновение.
- ***Черный ящик.*** Тестировщикам предоставляется только высокоуровневая информация (например, URL или IP-адрес организации) для проведения тестирования на проникновение. Специалист может ощутить себя хакером, который ничего не знает о системе / сети. Это весьма трудоемкий подход, так как тестировщику требуется значительное количество времени для изучения свойств и деталей системы; кроме того, высока вероятность пропустить часть областей из-за недостатка времени и информации.
- ***Серый ящик.*** Тестировщик получает ограниченную информацию (например, знания алгоритма, архитектуры, внутренних состояний) для имитации внешней атаки на систему.

Ограничения тестирования на проникновение. У тестирования на проникновение существует ряд ограничений:

– недостаток времени и высокая стоимость тестирования;

- ограниченный объем испытаний, основанный на требованиях за данный период времени (что может привести к игнорированию других важных областей);
- возможность разрушения системы или потери системы в состоянии отказа в результате испытания на проникновение;
- уязвимость данных (потеря, коррупция или ущерб).

Инструмент UserRecon ***(!Дисклеймер! Использовать только в образовательных целях!)*** используется для поиска имен пользователей в более чем 75 социальных сетях. Это очень полезно, когда вы проводите расследование, чтобы определить использование одного и того же имени пользователя в разных социальных сетях, таких как Twitter, Instagram, MySpace, Youtube, Reddit, WordPress, GitHub и многих других. Одним нажатием кнопки следователь OSINT сможет узнать, существует ли одно и то же имя пользователя в разных социальных сетях. Это очень удобный и простой в использовании инструмент.

Практическая часть:

Шаг 1: Откройте терминал и введите следующую команду.

Git clone https://github.com/issamelferkh/userrecon.git

Шаг 2: После клонирования инструмента измените каталог на UserRecon: ***cd userrecon***

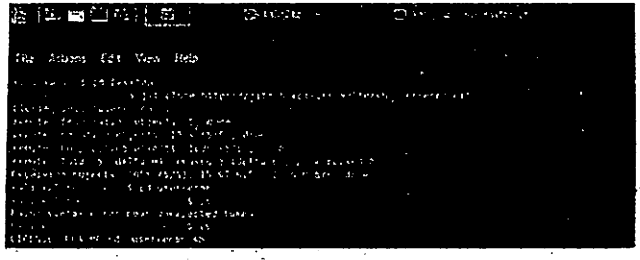


Рис.11.1. Изменение каталога на UserRecon

Шаг 3: Теперь перечислите все скрытые файлы, используя команду ls -la в вашем терминале.

ls –la

Шаг 4: Измените разрешение userrecon.sh.

chmod +x userrecon.sh

Шаг 5: После изменения разрешения userrecon.sh запустите инструмент с помощью следующей команды: *./userrecon.sh*

Рис.11.2. Запуск программы UserRecon

Либо запустите *userrecon.bat* если Вы работаете в ОС Windows.

После запуска инструмента с помощью команды ./userrecon.sh вы увидите экран, аналогичный показанному выше. Теперь просто введите имя пользователя, которое вы хотите найти:

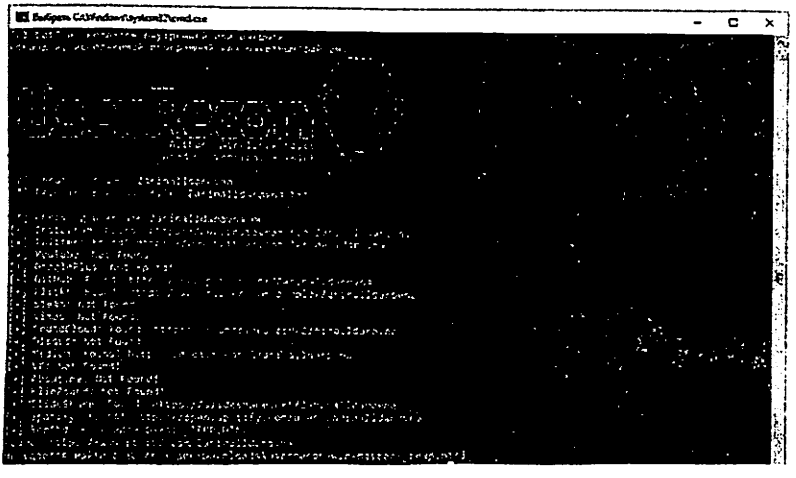


Рис.11.3. Начало работы в программе UserRecon

Как мы видим, UserRecon ищет имя пользователя «ZarinaIldarovna» на всех 75 сайтах и возвращает ссылку, если она существует. Все эти данные сохраняются в файле ZarinaIldarovna.txt. Доступ к нему можно получить в любом текстовом редакторе. Например, можно открыть его Блокноте.

Можно открыть любую из ссылок, чтобы увидеть профиль в этой социальной сети. Как видно из приведенных выше операций, UserRecon может быть очень полезным и экономящим время инструментом, если кто-то хочет найти имя пользователя в социальных сетях.

Рис.11.4. Результаты поиска сохраненные в txt-файле

Задание к практической работе:

Задание 1. Изучите возможности реализации тестирования на проникновение.

Задание 2. Используя утилиту *Userrecon* проанализируйте свои профили в социальных сетях. Опишите подробно результаты анализа и то, какую

информацию можно с легкостью обнаружить и определить исходя из анализа Ваших страниц в социальных сетях.

Содержание отчета:

1. Титульный лист.
2. Выполнение задания 1 и задания 2 к практической работе, включая скриншоты и подробное описание выполненных действий.
3. Выводы по выполнению практической работы.
4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. Что такое тестирование на проникновение?
2. Каковы цели проведения тестирования на проникновение?
3. С помощью каких программных средств можно осуществить сбор сведений о пользователе по профилю в социальных сетях?
4. Для чего применяется утилита UserRecon? Какие функциональные возможности она имеет?

СОДЕРЖАНИЕ:

ЛИТЕРАТУРА:

1) С.К.Ганиев, З.Т.Худойкулов, Н.Б.Насруллаев, Основы кибербезопасности: Учебное пособие / -Т.: «Iqtisod-Moliya», 2021. – 240. ISBN 978-9943-13-9 88-6.
2) Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учеб.пособие / В.Ф. Шаньгин. — Москва: ИД «ФОРУМ»: ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0411-4.
   URL: https://znanium.com/catalog/product/546679.
3) Mike Chapple, James Michael Stewart, Darril Gibson, CISSP Official Study Guide, Sybex, 2018.
4) William Stallings, Cryptography and network security (principles and practice, 5-th edition), 2011 (ISBN 13: 978-0-13-609704-4).
   URL: http://www.dut.edu.ua/ru/lib/1/category/1289/view/1134
5) Malcolm Harkins, Managing Risk and Information Security: Protect to Enable, Intel Corporation, 2013. – 152 p. ISBN 978-1-4302-5113-2.
6) Ronald L. Krutz and Russell Dean Vines, "The CISSP Prep Guide: Gold Edition".
   URL:http://index.of.es/Misc/pdf/Wiley.The.CISSP.Prep.Guide.Gold.Edition.eBook-kB.pdf.
7) William Stallings, "Cryptography and network security" (principles and practice, 5-th edition), 2011 (ISBN 13: 978-0-13-609704-4).
8) Jean-Philippe Aumasson, "Serious Cryptography. A Practical Introduction to Modern Encryption", No Starch Press, San Francisco 2018, -291. ISBN-13: 978-1-59327-826-7.
9) П.Н.Девянин, Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб.пособие, Москва : Горячая линия – Телеком, 2016. – 338 с.

10) Б.Шнайер, "Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С" 2-издание.
URL: http://www.dut.edu.ua/ru/lib/1/category/1289/view/1134.

11) Курило А.П., Ухлинов Л.М., Тенденции развития систем контроля доступа к информационным ресурсам.
URL:http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/de55ab383c4a2df0c325764300439fe2.

ИНТЕРНЕТ-РЕСУРСЫ:

1. International Standard, Risk management – Risk assessment techniques, IEC/FDIS 31010:2009(E).
URL: https://bambangkesit.files.wordpress.com/2015/12/iso-31010_risk-management-risk-assessment-techniques.pdf
2. Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology
URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
3. Handbook of Information Security Management, Domain 3, "Risk Management and Business Continuity Planning," Micki Krause and Harold F. Tipton, editors (CRC Press LLC). URL: www.cccure.org/Documents/HISM/223-228.html
4. Threat and Risk Assessment Working Guide. URL: www.cse-cst.gc.ca/en/documents/publications/gov_pubs/itsg/itsg04.pdf
5. Настройка контроля доступа пользователей и разрешений. URL:https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control.
6. Разработка политики резервного копирования в компании. URL: http://info-bryansk.ru/about_the_software/backup/development_of_backup_policy_in_the_company .