МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

ФАКУЛЬТЕТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра обеспечения информационной безопасности

З.И. Азизова

Методические пособие к выполнению практических работ по дисциплине «Основы кибербезопасности»

Ташкент 2021

В данном методическом пособии рассматриваются такие вопросы, как анализ и оценка рисков безопасности, криптографические методы защиты информации, модели логического контроля доступа пользователей информационной системы, наглядно представлены способы восстановления данных в ОС Windows, настройка ограничения доступа пользователей системы, процесс восстановления данных со съемных носителей с помощью программного средства TestDisk и др.

Каждая практическая работа включает в себя цель работы, 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. — ассистент кафедры обеспечения информационной безопасности ТУИТ им. Мухаммада ал-Хоразмий

Рецензенты:

Иргашева Д.Я. — декан факультета информационной безопасности ТУИТ им. Мухаммада ал-Хоразмий, к.т.н., доцент

Зокиров О.Ё. — начальник отдела контроля за качеством образования Филиала Российского государственного университета нефти и газа (НИУ) им. И.М.Губкина, PhD, доцент

Практическая работа №1

Тема: Методы оценки рисков

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).

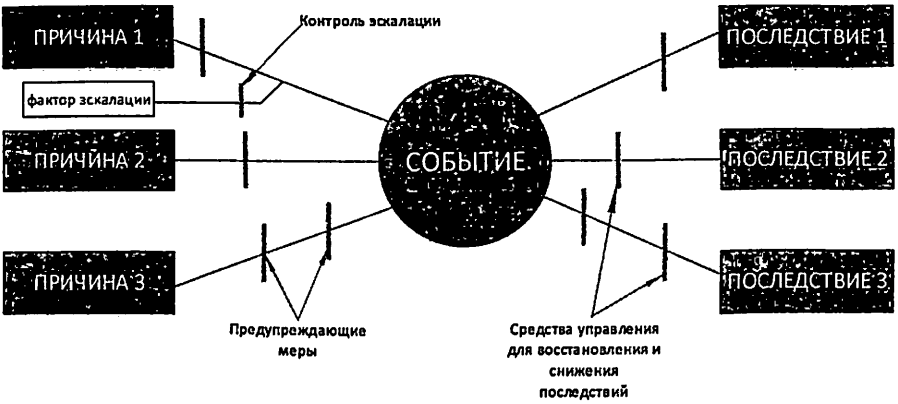


Рис 1.1. Пример диаграммы «галстук-бабочка»

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.

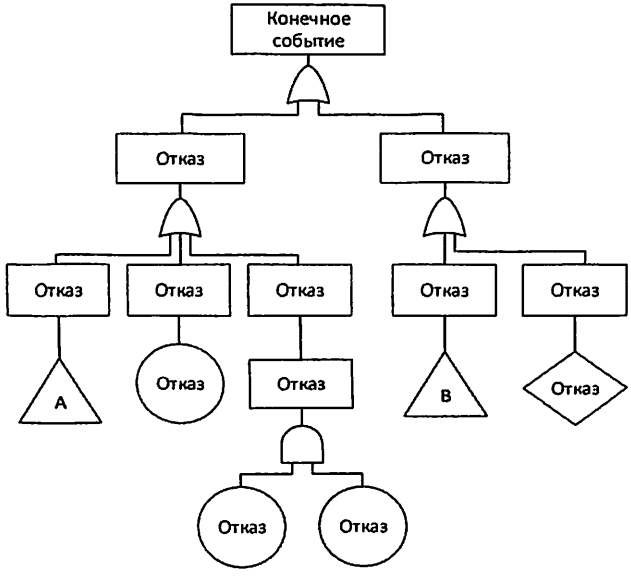


Рис.1.2. Пример диаграммы анализ «дерева» неисправностей

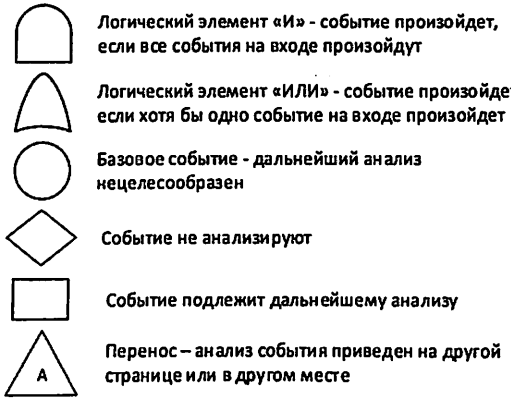


Рис.1.3. Символьные обозначения анализа дерева неисправностей

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.

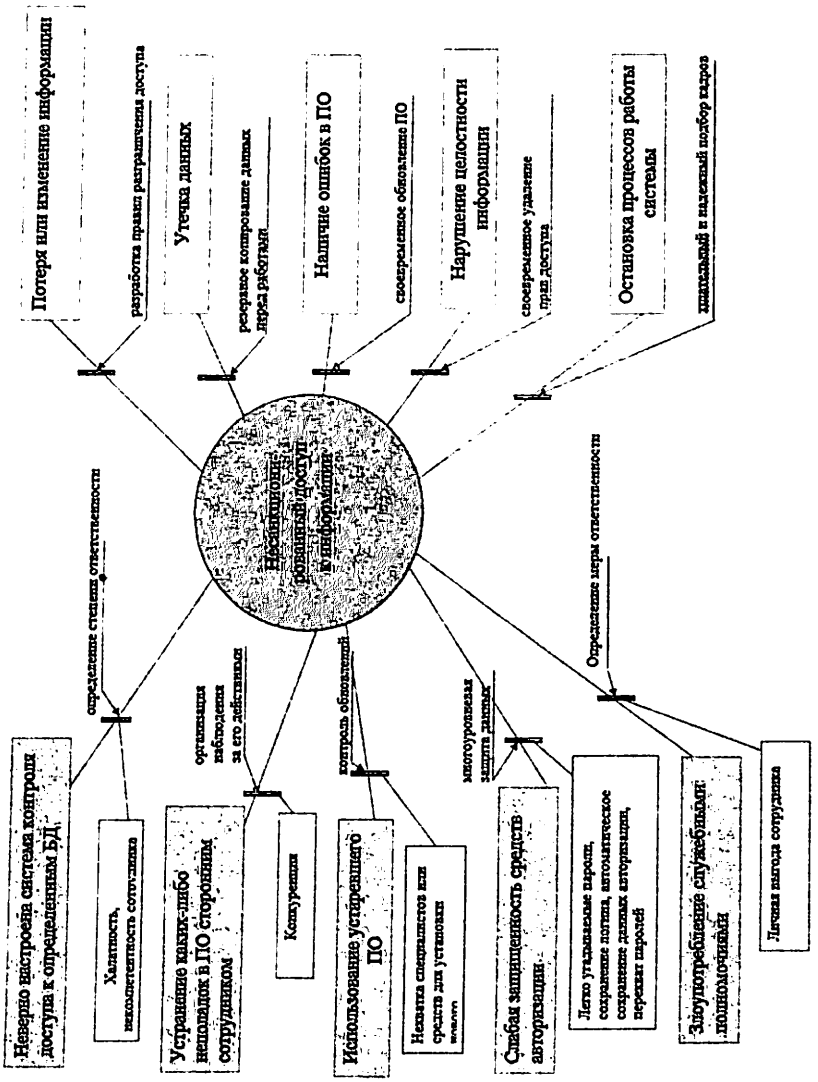


Рис.1.4. Пример заполнения диаграммы анализа «галстук-бабочка» для события «Несанкционированный доступ к информации»

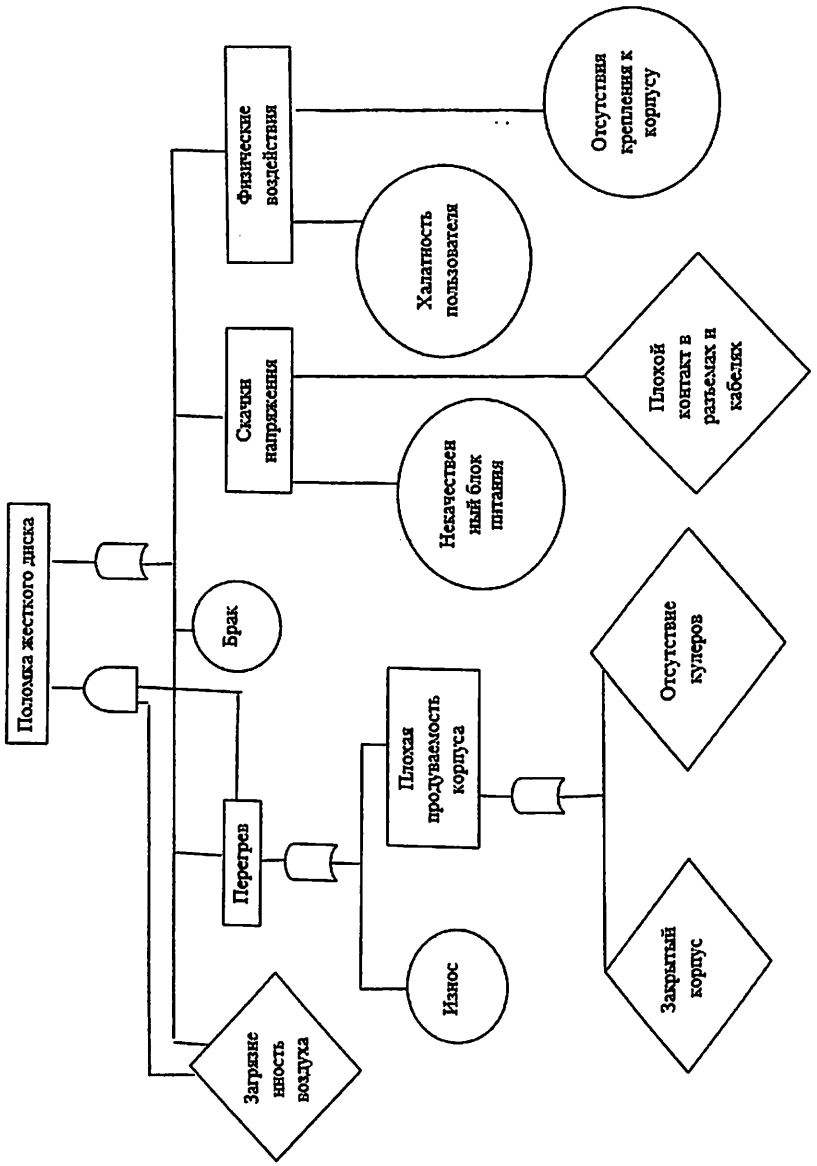


Рис.1.4. Пример заполнения диаграммы анализ «дерева» неисправностей для нежелательного события «Поломка жесткого диска»

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?

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) 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
3) 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.
4) Mike Chapple, James Michael Stewart, Darril Gibson, CISSP Official Study Guide, Sybex, 2018.
5) 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
6) Malcolm Harkins, Managing Risk and Information Security: Protect to Enable, Intel Corporation, 2013. – 152 p. ISBN 978-1-4302-5113-2.

Практическая работа №2

Тема: Исследование криптографических методов защиты информации

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.

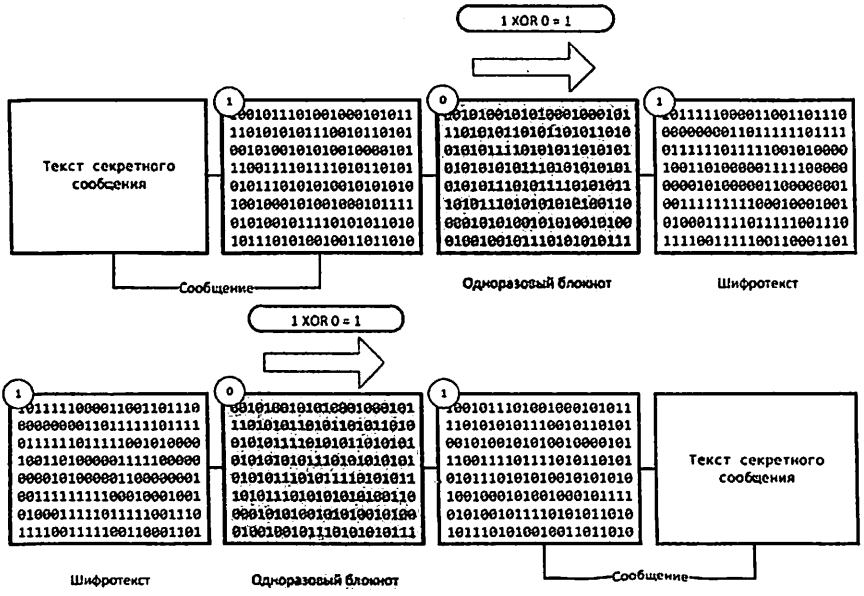


Рис.2.1. Одноразовый шифровальный блокнот

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: $y = x \oplus k$

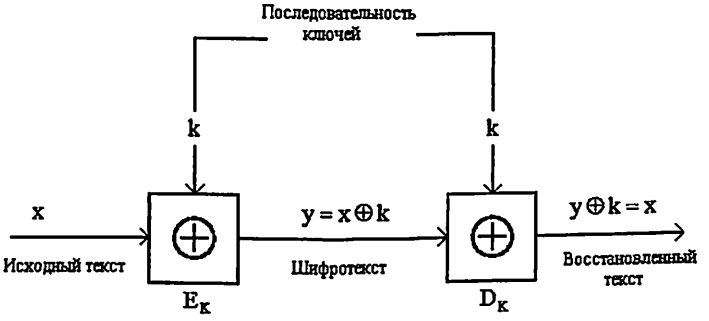


Рис. 2.2. Схема шифрования и расшифрования сообщений по методу Вернама

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 $\boldsymbol{p}$ и $\boldsymbol{q}$.
2. Определение их произведения: $\boldsymbol{n = p * q}$.
3. Определение функции Эйлера: $\boldsymbol{\phi\,(n) = (p-1)(q-1)}$.
4. Выбор открытого ключа $\boldsymbol{e}$ с учётом условий:

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

5. Определение секретного ключа d, удовлетворяющего условию

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

Алгоритм шифрования сообщения M (действия отправителя):

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

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

2. Шифрует текст сообщения в виде последовательности блоков:

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

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

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.

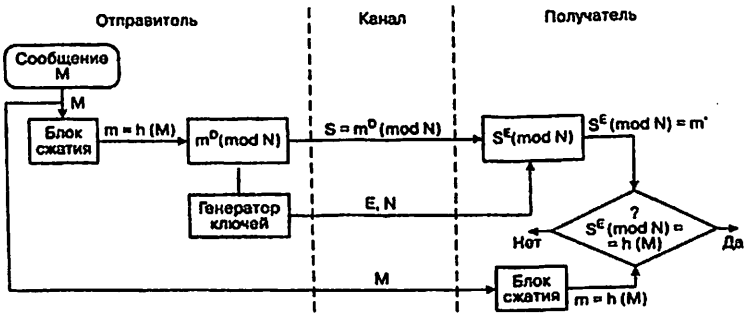


Рис.2.3. Схема электронной цифровой подписи RSA

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. № 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 М 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 М
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. Чем отличаются шифры перестановки от шифров замены?
2. Дайте определение и объясните суть симметричного шифрования. Объясните сущность симметричного шифрования.
3. Алгоритмы асимметричного шифрования.
4. Преимущества и недостатки алгоритма шифрования RSA.

Литература:

1) 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.
2) CISSP Official Study Guide (Mike Chapple, James Michael Stewart, Darril Gibson) (2018, Sybex).
3) William Stallings, "Cryptography and network security" (principles and practice, 5-th edition), 2011 (ISBN 13: 978-0-13-609704-4).
4) 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.
5) 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.

Практическая работа №3

Тема: Логический контроль доступа к данным

Цель работы: приобретение навыков по организации защиты от несанкционированного доступа к данным путем ограничения доступа пользователей системы.

Теоретические сведения:

Логический доступ — это комплекс мер, обеспечивающих защиту от несанкционированного доступа к персональным компьютерам, компьютерным сетям и информации, хранящейся в них.

Разграничение доступа к элементам защищаемой информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий. В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, программам обработки информации, полям (областям ОЗУ, ПЗУ) и массивам (базам) данных. Само разграничение может осуществляться несколькими способами, а именно:

1) списки контроля доступа (*ACL* – Access Control Lists);
2) избирательное или дискреционное управление доступом (*DAC* – Discretionary Access Control, матрицей контроля доступа);
3) полномочное (мандатное) управление доступом (*MAC* – Mandatory Access Control) – по уровням секретности;
4) Управление доступом на основе ролей (*RBAC* – Role Based Access Control).

Разграничение доступа по *спискам контроля доступа* заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа. Наиболее

полной моделью распределения полномочий является матрица доступа, в строках которой перечислены субъекты, в столбцах – объекты; в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия, текущие права других субъектов) и разрешенные виды доступа. В таблице 1 представлен пример разграничения доступа в структуре университета, права пользователь соответствуют следующим сокращениям: *X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление.

Избирательное или дискреционное управление доступом (разграничение доступа по матрицам полномочий) предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента. Недостатком метода разграничения доступа на основе матрицы полномочий является то, что с увеличением масштаба данная матрица может оказаться слишком громоздкой. Преодолеть данный недостаток можно путем применения следующих рекомендаций по сжатию матрицы установления полномочий:

– пользователей, имеющих идентичные полномочия, в группы;

– объединение ресурсов, полномочия на доступ к которым совпадают.

Пример *таблицы разграничения доступа по списку контроля доступа* представлен ниже (см.таблицу)

Субъект	*Объект*			
	персональные данные	*финансовые отчеты*	*учебно-методические комплексы*	*приказы*
Ректорат	*R*	*R*	*R*	*R, W, C, D*
Бухгалтерия	*R*	*W, C, E*	*R*	*R*
Преподаватели	*X*	*X*	*W, R, C, E, D*	*R*
Студенты	*X*	*X*	*R*	*R*

Далее следует *пример таблицы избирательного разграничения доступа*:

Субъект	*Объект*			
	персональные данные	*финансовые отчеты*	*учебно-методические комплексы*	*приказы*
Ректор	*R*	*R*	*R*	*R, W, C, D*
Главный бухгалтер	*R*	*W, C, E*	*R*	*R*
Преподаватель	*X*	*X*	*W, R, C, E, D*	*R*
Студент	*X*	*X*	*R*	*R*

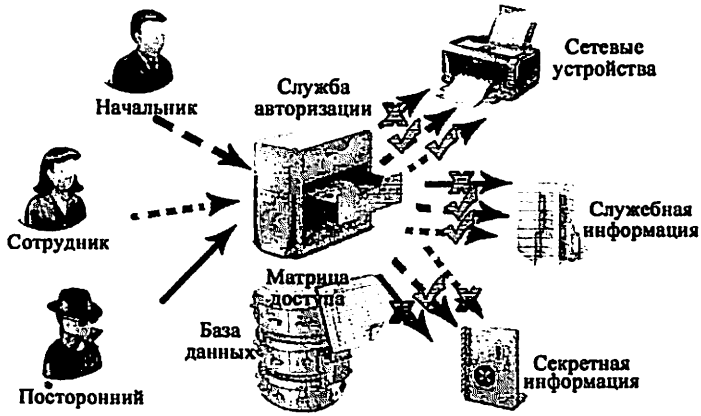


Рис. 3.1. Схема реализации дискреционного управления доступом

Access Control List (ACL) — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей). В типичных ACL каждая запись определяет субъект воздействия и операцию.

Полномочное (мандатное) управление доступом есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

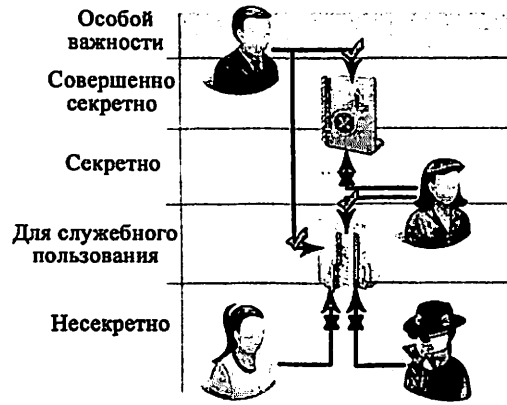


Рис.3.2 Схема реализации мандатного управления доступом

Система безопасности платформы Windows основана на модели безопасности для каждого пользователя или группы пользователей. Каждый пользователь, зарегистрированный в системе, имеет собственную учетную запись, которая содержит персональную информацию о пользователе. Эти данные система использует для проверки подлинности пользователя и для авторизации его при доступе к ресурсам домена. После прохождения процедуры аутентификации пользователю присваивается *маркер доступа*, идентифицирующий пользователя, его группу, а также определяющий доступные пользователю привилегии в системе для доступа к ресурсам. При этом каждому объекту системы, включая файлы, принтеры, сетевые службы, контейнеры Active Directory и другие, присваивается *дескриптор безопасности*. Дескриптор безопасности объекта определяет права доступа к объекту и содержит список контроля доступа (ACL – Access Control List), в котором явно определяется, каким пользователям разрешено выполнять те или иные действия с этим объектом. Дескриптор безопасности объекта также определяет, для каких событий должен вестись аудит. Авторизация Windows основана на сопоставлении маркера доступа субъекта с дескриптором безопасности объекта. Управляя свойствами объекта, администраторы могут устанавливать разрешения, назначать право владения и отслеживать доступ

пользователей. Каждый дескриптор безопасности может содержать списки двух типов. Системный список управления доступом (SACL – System Access Control List) позволяет отслеживать права и ограничения, установленные для объекта на системном уровне. В этот список могут вносить изменения только те пользователи, которые обладают правами доступа на уровне системы.

Пользовательский список управления доступом (DACL – Discretionary Access Control List) позволяет отслеживать права и ограничения, установленные владельцем данного объекта. DACL может быть изменен пользователем, который указан как текущий владелец объекта.

Оба списка имеют одинаковую структуру. Они могут не содержать ни одной записи либо содержать одну или несколько записей. Каждая запись (ACE – Access Control Entry) состоит из трех частей: в первой указываются пользователи или группы, к которым относится данная запись, во второй – права доступа, а третья информирует о том, предоставляются эти права или отбираются. Дескрипторы безопасности могут быть представлены либо в абсолютном, либо в относительном формате. Абсолютный формат предусматривает запись дескриптора безопасности в память в виде структуры указателей и, поэтому, он более удобен для обновления содержимого дескриптора.

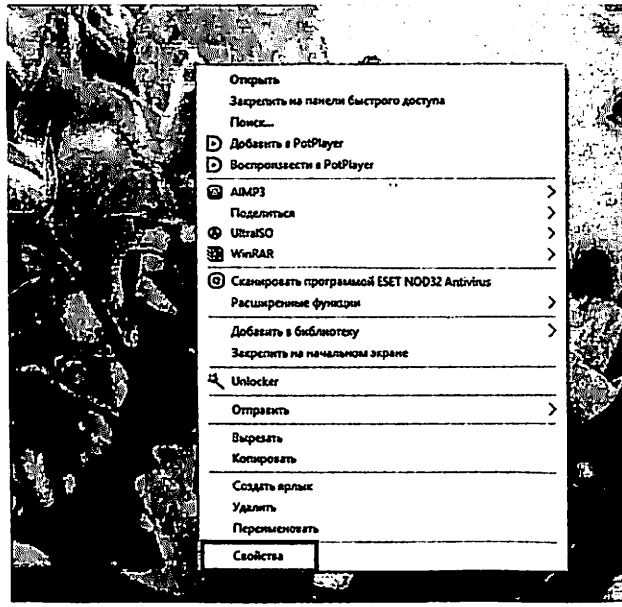
Практическая часть:

Настройка доступа к папкам и файлам

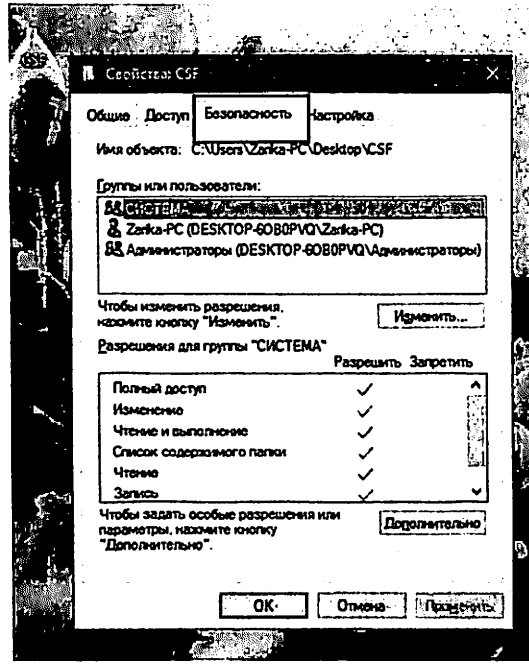
Откройте проводник (редактор реестра) и перейдите к папке/файлу/разделу реестра, к которому необходимо получить доступ.

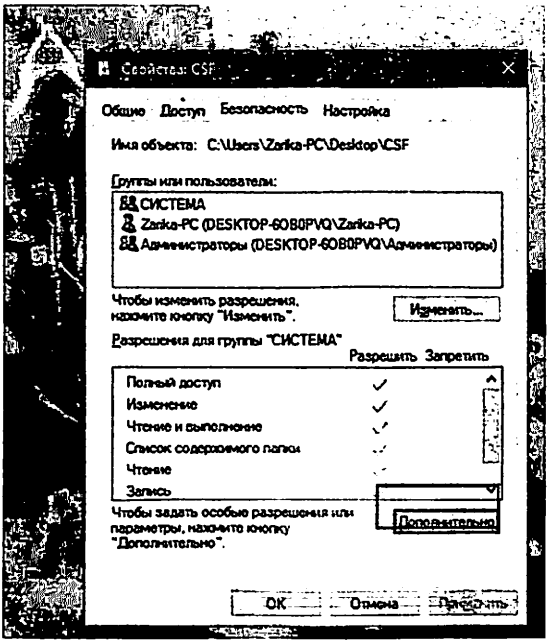
1) *Для файла или папки.*

1. Нажмите правую клавишу мыши и выберите в контекстном меню *Свойства*

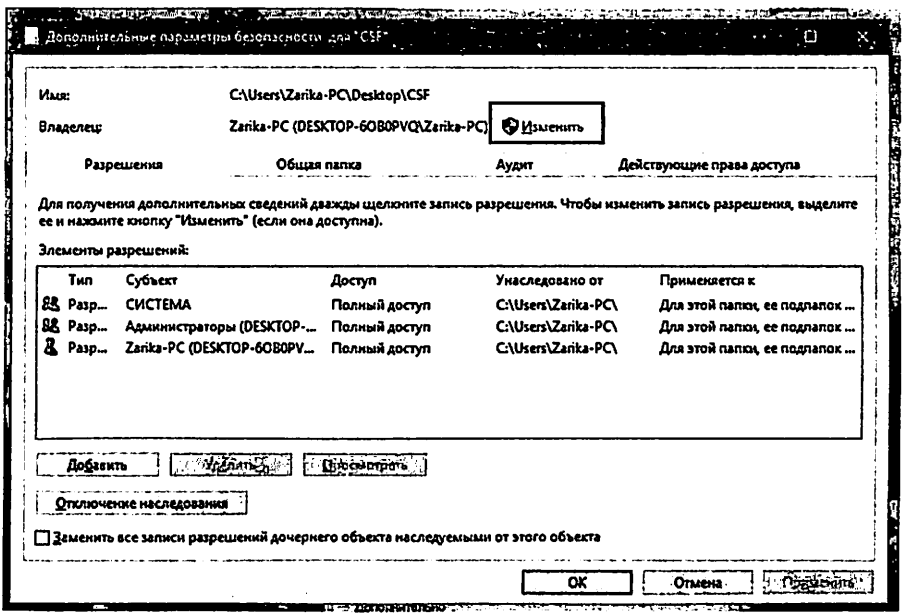


2. Перейдите на вкладку *Безопасность* и нажмите кнопку *Дополнительно*

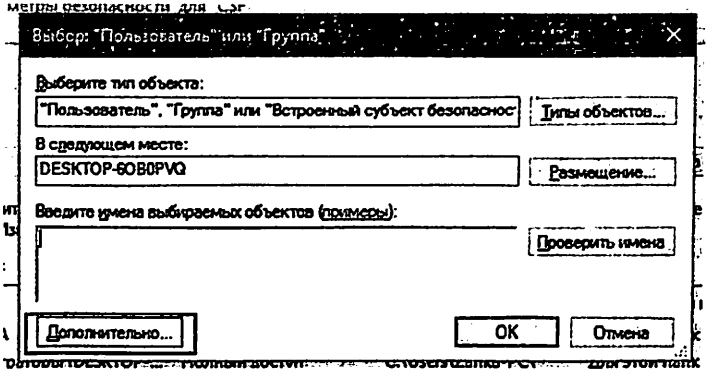




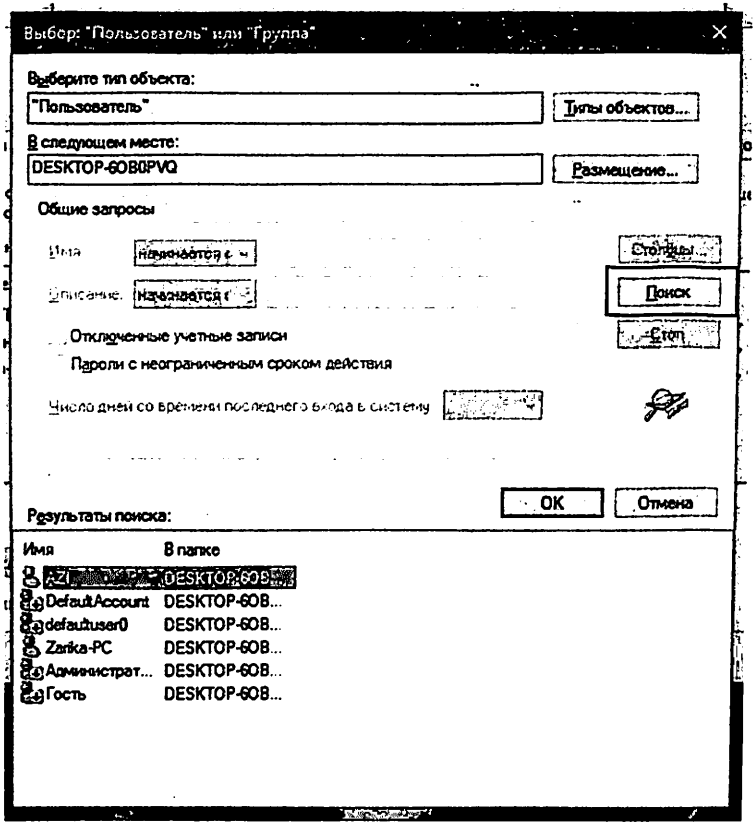
3. В строке с пунктом *Владелец* нажмите кнопку *Изменить*



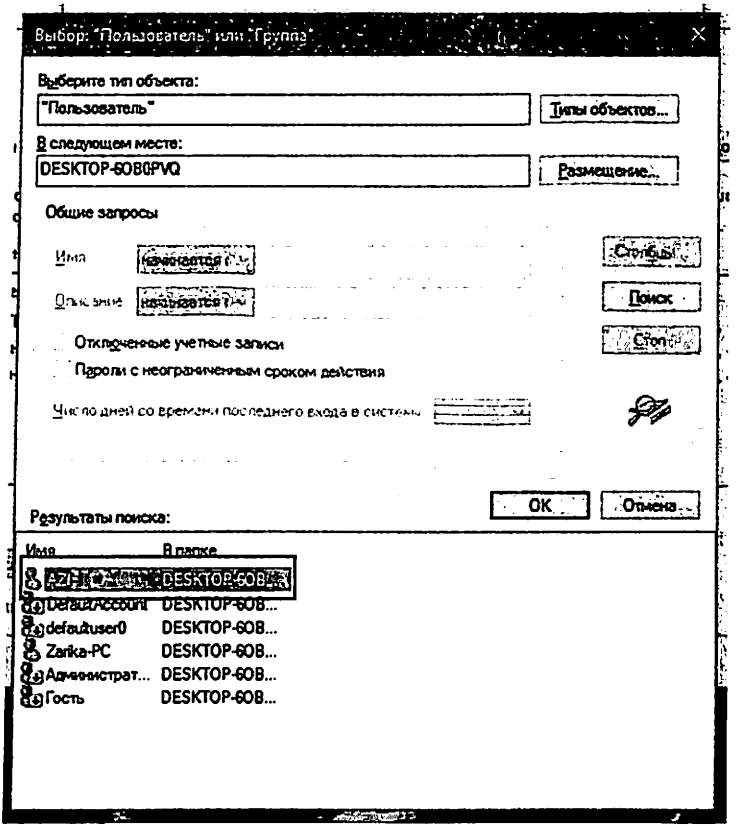
4. В появившемся окне выбора нажмите на *Дополнительно*, для выбора Пользователя



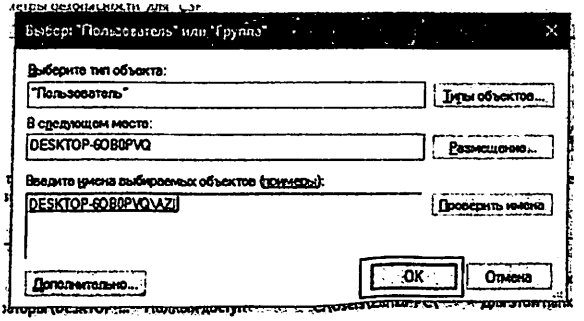
Нажмите на *Поиск* для просмотра имеющихся пользователей



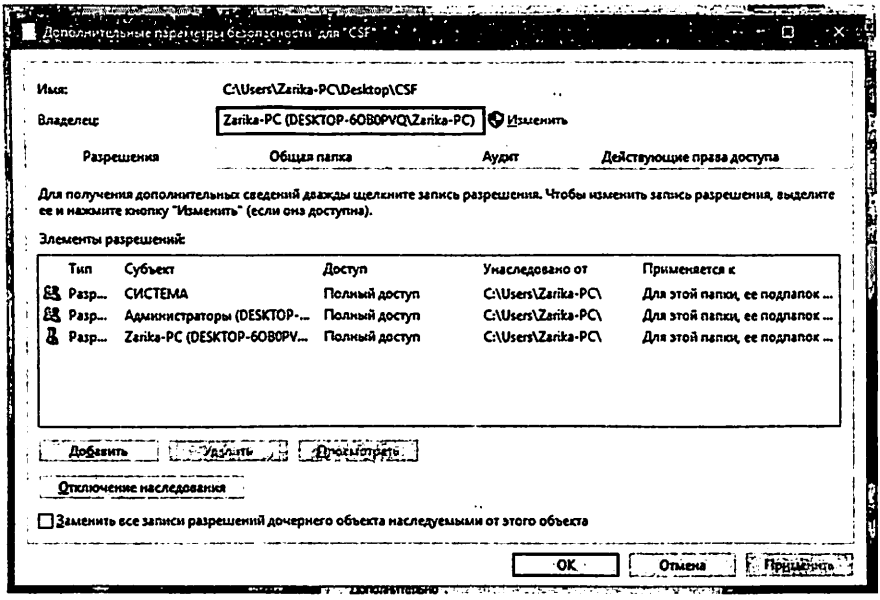
Выберите из предложенного списка пользователя, которому хотите передать права владения папкой (файлом, и т.п.). В моем случае это пользователь AZI.

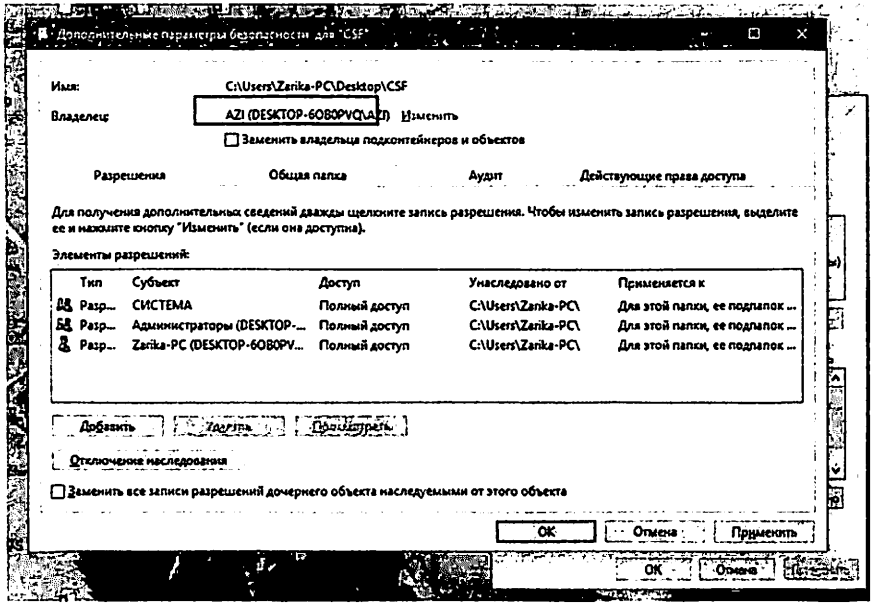


Далее в появившемся диалоговом окне нажмите **Ок**



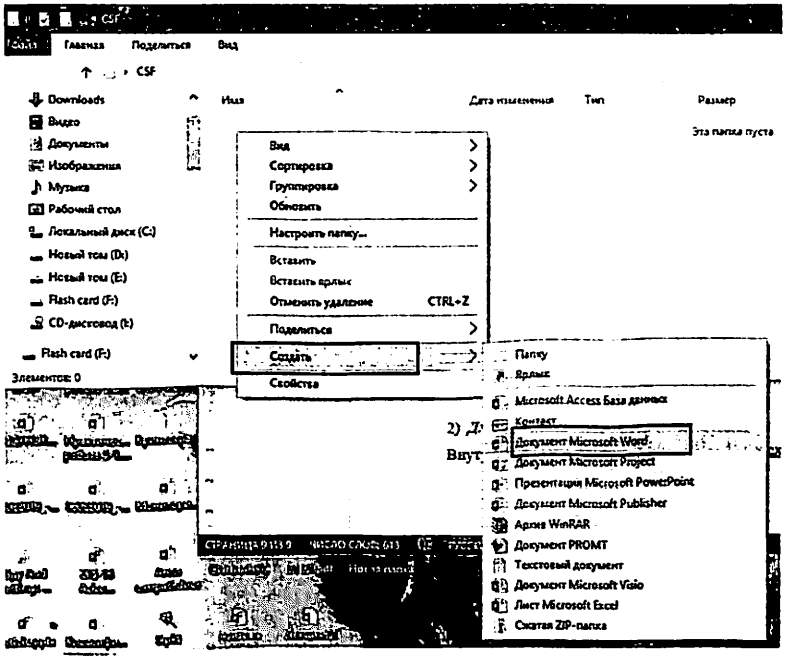
Теперь можно увидеть, что владельцем папки CSF является пользователь AZI, хотя изначальным владельцем был пользователь Zarika-PC.



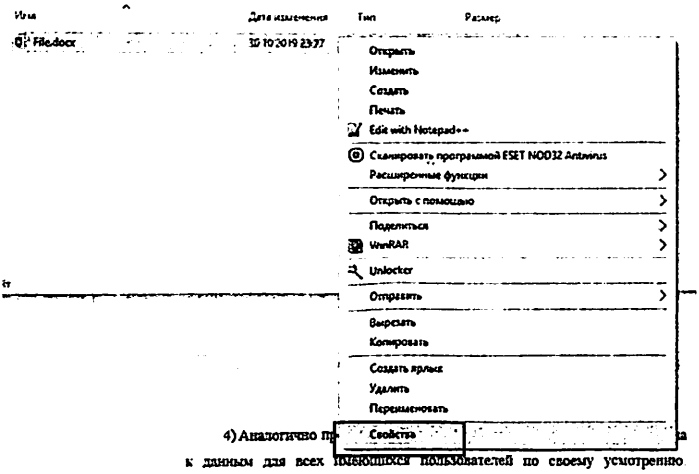


2) *Для отдельного файла*

Внутри созданной папки создадим файл File.docx

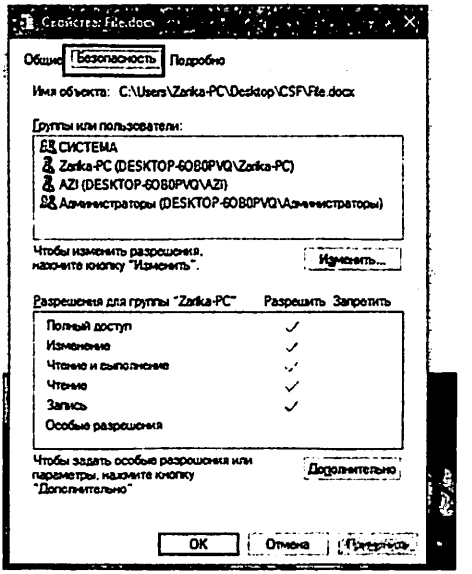


Для того, чтобы ограничить пользователя AZI в правах доступа к файлу File.docx нам необходимо открыть свойства данного файла (кликнув правой клавишей мыши на этот файл) выбрав пункт *Свойства*



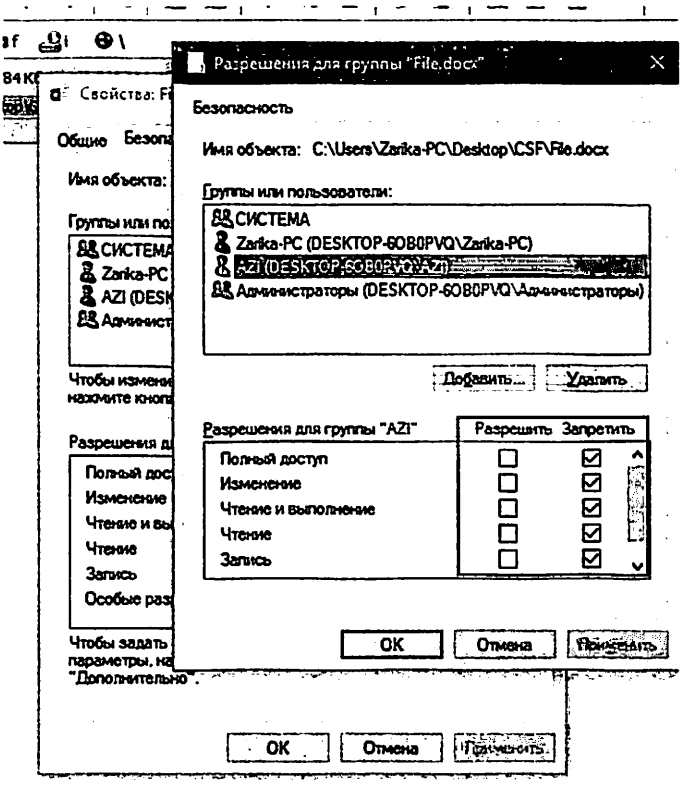
4) Аналогично пр а
к данным для всех имеющихся пользователей по своему усмотрению

В появившемся диалоговом окне *Свойств файла* выберем вкладку *Безопасность*

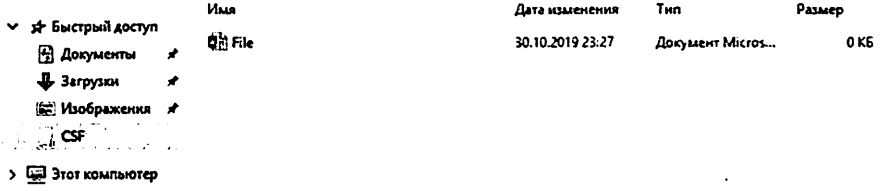


Далее выберем пользователя AZI из списка пользователей (если нужного пользователя нет в списке, необходимо добавить его нажав на кнопку ***Изменить – Добавить – Дополнительно – Поиск*** и выбрав из списка нужных

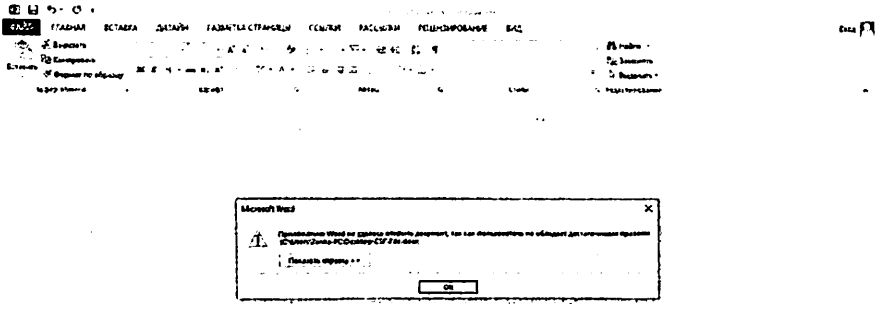
пользователей нажать *Ок*) и настраиваем права доступа пользователя AZI к файлу File.docx (например, разрешить «только чтение», запретить «запись», предоставить «полный доступ», либо вообще запретить доступ к файлу, и так далее)

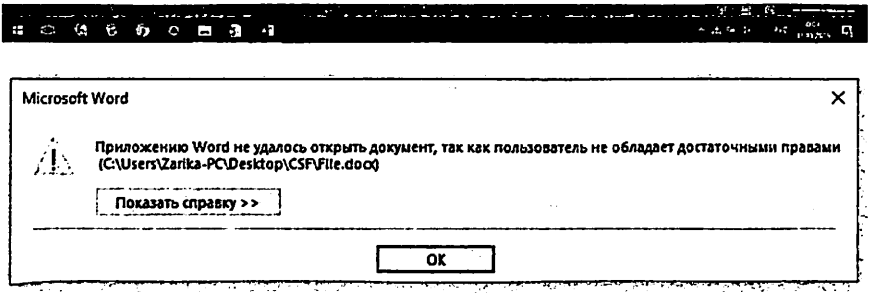


Для проверки заданных прав доступа к файлу *File.docx* мне необходимо зайти в систему от имени пользователя AZI и открыть данный файл.

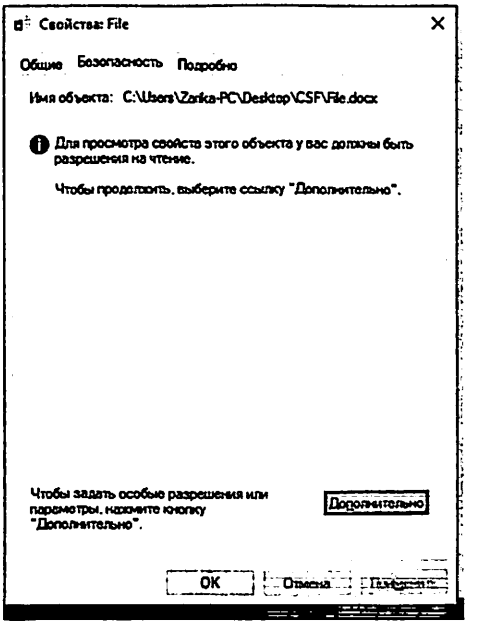


После попытки открыть файл появилось следующее сообщение





Далее для проверки, открыв окно Свойства файла File.docx во вкладке Безопасность можно прочитать информацию о том, что данный пользователь не имеет соответствующих прав доступа к выбранному объекту, т.е. файлу File.docx



Задания к практической работе:

Задание №1:

1) Создайте трех пользователей у себя на ПК (именуйте пользователей следующим образом: Фамилия_Имя_1, Фамилия_Имя_2, Фамилия_Имя_3)
2) Создайте одну папку общего доступа для всех трех пользователей.
3) Создайте в папке общего доступа две новые папки и поместите в них несколько файлов разного типа, либо создайте их заново.
4) Аналогично представленной настройке выполните контроль доступа к данным для всех имеющихся пользователей по своему усмотрению. (Например, ограничьте доступ первого пользователя Фамилия_Имя_1 к файлам в первой папке, либо к какому-то отдельному файлу, дайте право «только чтения» какого-либо файла для пользователя Фамилия_Имя_3, и т.д.)
5) После настройки контроля доступа к папкам или файлам, продемонстрируйте как именно ограничили доступ каждому пользователю

(для этого необходимо будет проверять созданные папки и файлы от имени всех пользователей по отдельности), при этом необходимо включить в работу скриншоты с описанием этого процесса.

б) *Продемонстрируйте и опишите другие способы контроля доступа к данным в ОС Windows.*

7) Предоставьте выполнение задания в виде скриншотов и подробным описанием всех настроек контроля доступа.

Задание №2. Приведите таблицу сравнения моделей контроля доступа Белла-ЛаПадулы и Биба.

Содержание отчета:

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

Контрольные вопросы:

1. Опишите модель дискреционного контроля доступа (DAC) к данным. Приведите примеры использования данной модели.
2. Что такое логический контроль доступа?
3. Укажите возможности и назначение списков управления доступом (ACL).
4. Мандатное управление доступом (MAC), достоинства и недостатки использования данного подхода.
5. Управление доступом на основе ролей (RBAC): характерные черты, достоинства и недостатки.

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) В.Ф.Шаньгин, "Комплексная защита информации в корпоративных системах", Москва, 2018.
3) 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.
4) П.Н.Девянин, Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб.пособие, Москва : Горячая линия – Телеком, 2016. – 338 с.
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) Mike Chapple, James Michael Stewart, Darril Gibson, CISSP Official Study Guide, Sybex, 2018.
7) 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.

Практическая работа №4

Тема: Политика резервного копирования и восстановления данных

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

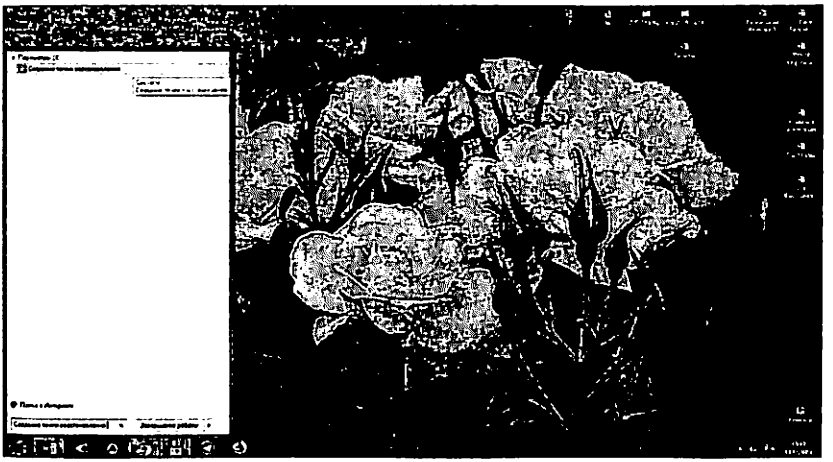
Операционная система от Microsoft имеет функцию Восстановление Системы, которая поможет восстановить работу компьютера если что-то пойдёт не так. Восстановление Системы даёт возможность восстановить состояние компьютера до предыдущего, отменив изменения, которые могли повредить компьютеру. Это изменения 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.

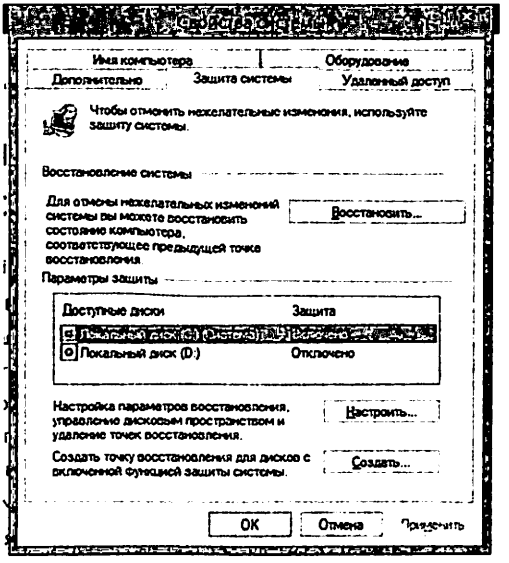
Это похоже на резервную копию, но с тем отличием, что нет возможности вернуть документы и настройки в состояние до момента создания точки восстановления. Также данная функция удалит все приложения, драйвера, обновления системы и изменения реестра, которые были сделаны до создания точки восстановления.

Включение функции восстановления системы

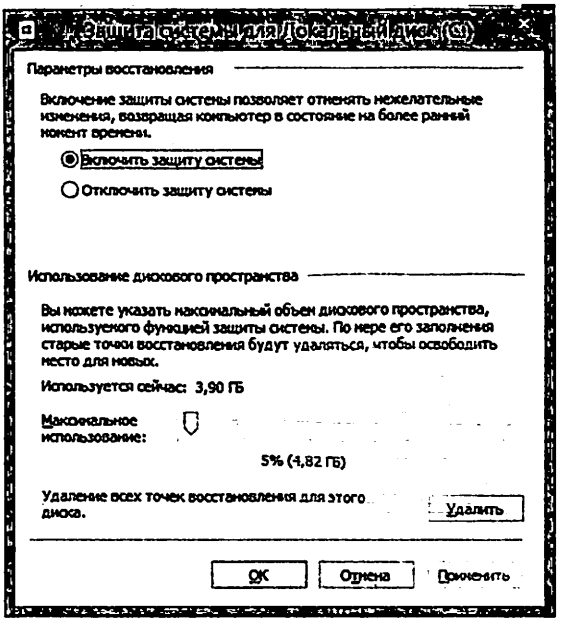
1. Перейдите в меню «Пуск» или кликните окошко поиска, наберите «Создание точки восстановления» и нажмите Enter. Откроется вкладка «Защита системы» в окошке «Свойства системы», в котором можно внести изменения в настройку необходимой нам функции.



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…».



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



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.

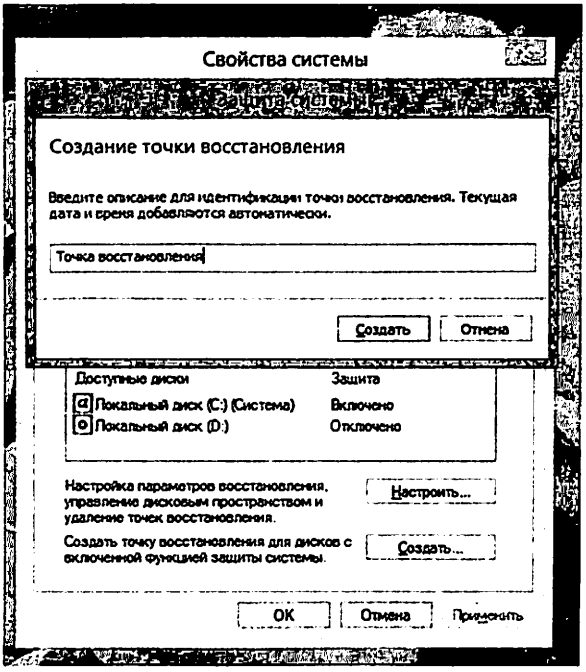
Также, обратите внимание на кнопку «Удалить», с помощью которой можно удалить все существующие точки восстановления. Она будет полезна, когда необходимо создать точку восстановления вручную, и для этого будет недостаточно места.

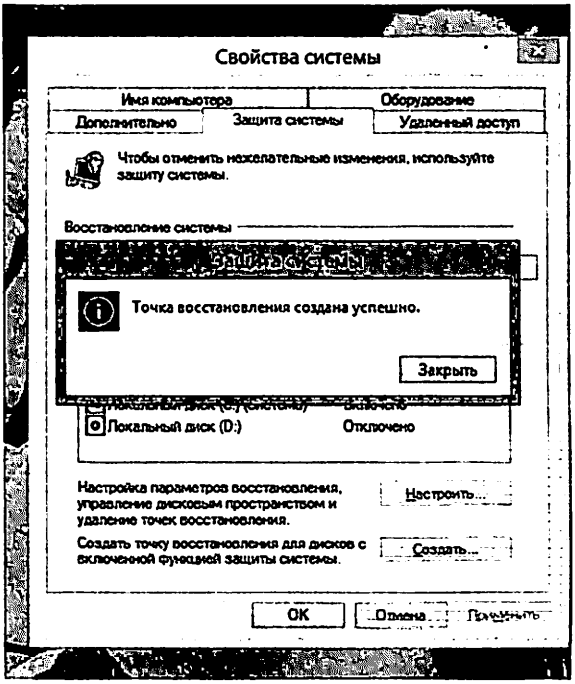
5. После осуществления необходимых настроек нажмите «Применить» и «ОК». После этого функция защиты диска будет включена.

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.

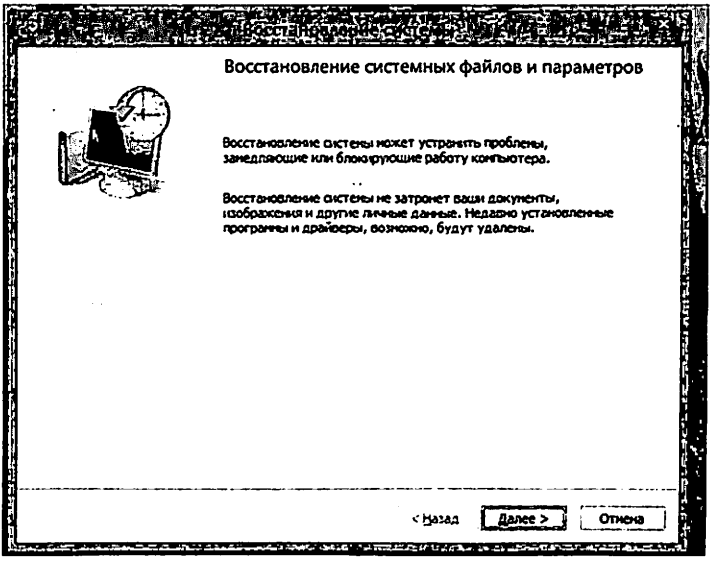




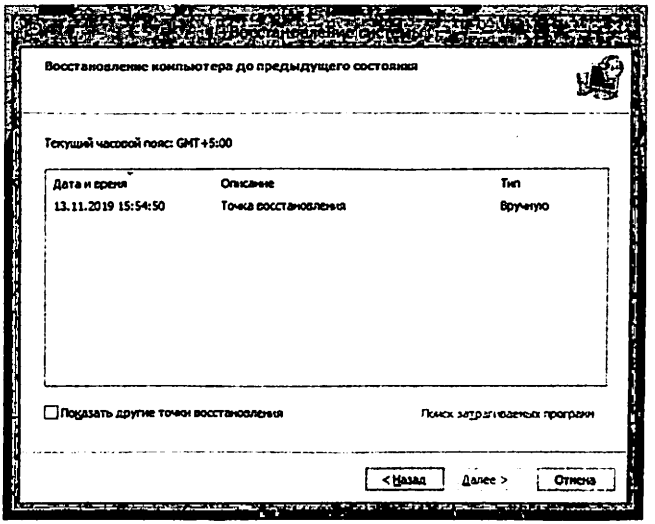
• В любой момент времени, в случае возникновения каких-либо проблем, перед использованием резервной копии данных или функции «Возвращения компьютера в исходное состояние» в Windows 10, попробуйте воспользоваться точкой восстановления, что намного быстрее и проще.

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».

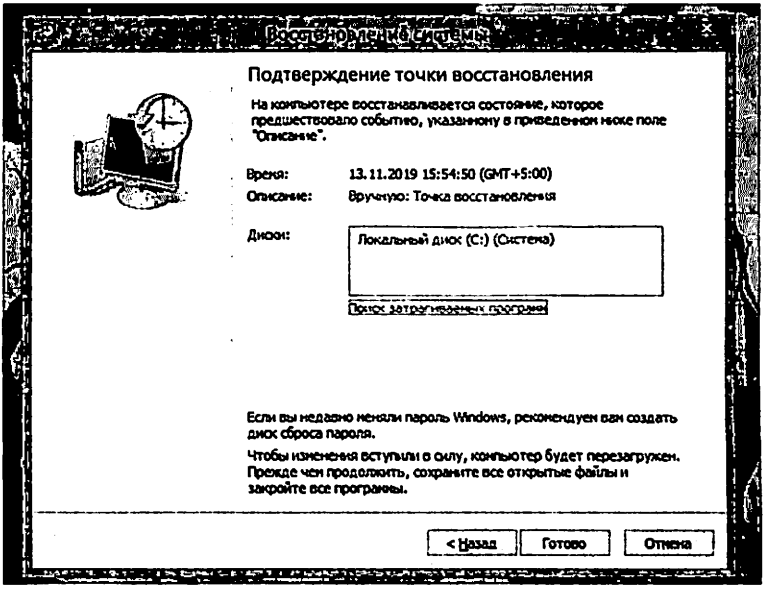


3. В следующем окне вы увидите доступные точки восстановления с датой, описанием, и что более важно – тип точки восстановления, указывающий была она создана вручную или системой.



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».



После завершения процесса, состояние системы вернётся в то состояние в 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 apt-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.

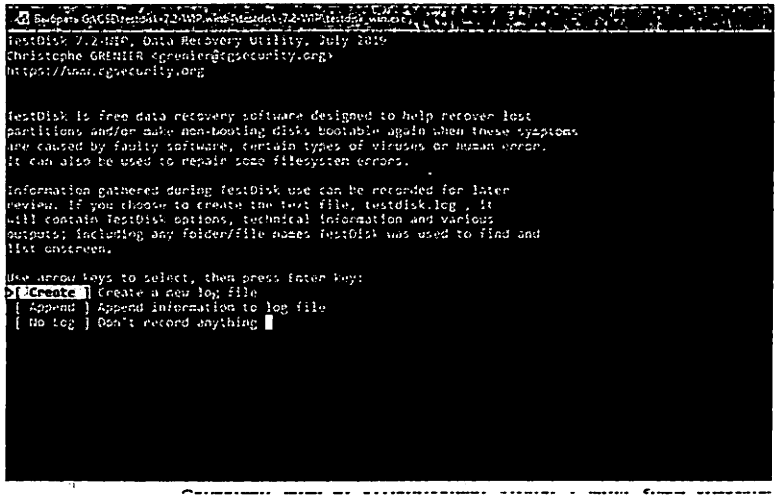
На первом экране вам предложат создать журнал производимых TestDisk операций: выбираем Create для его создания или No Log.

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.

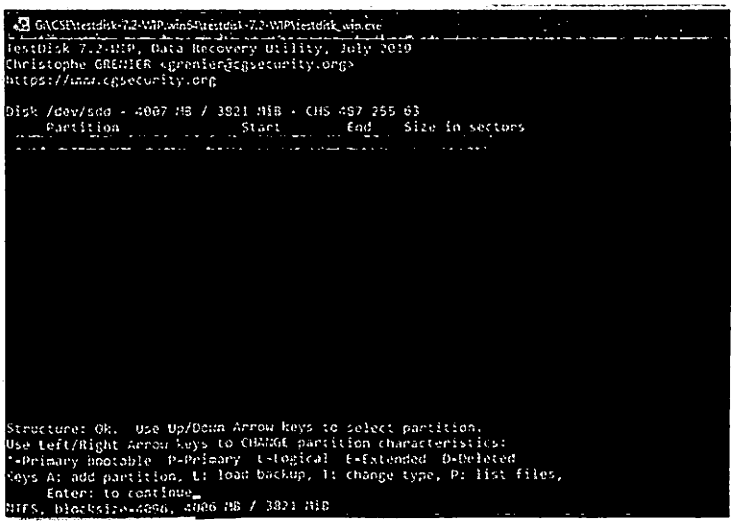


Следующий этап — выбор физического диска, на котором будет выполнен поиск разделов. После выбора с помощью стрелок нажимаем Enter для продолжения.

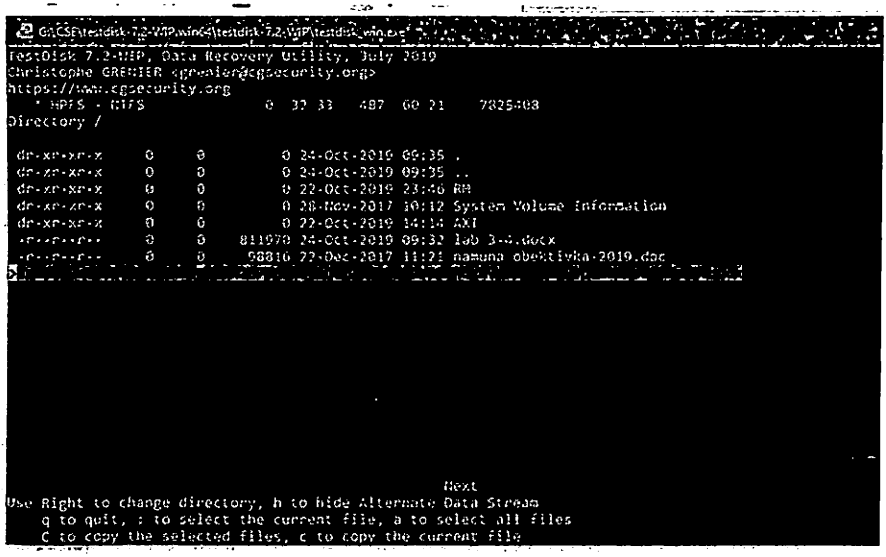
На 3-м этапе следует выбрать, какой тип разделов следует найти. Обычно требуется первый пункт — Intel/PC partition, включающий поиск разделов NTFS и различных вариантов FAT.

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.

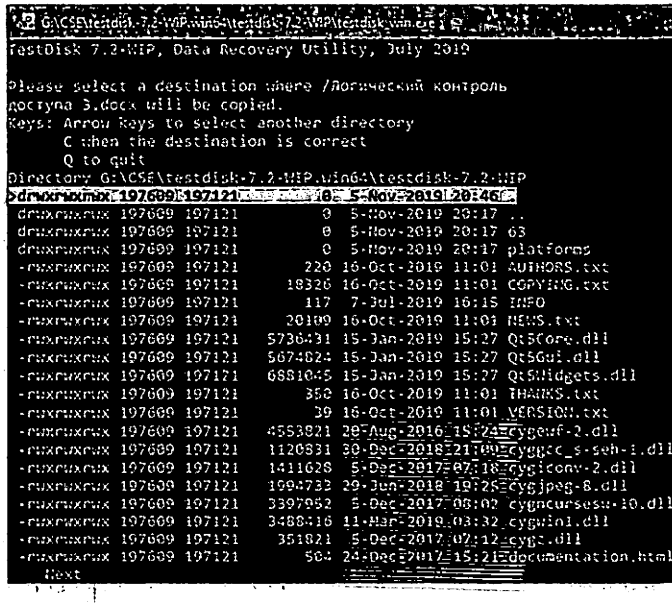


Нажмите Enter, а на следующем экране, если вы решили восстановить найденный раздел, выберите пункт «Write» (записать изменения) и нажмите Enter. Обратите внимание, что здесь же присутствует пункт «Deeper Search» (глубокий поиск) на случай, если до этого разделы не были найдены.

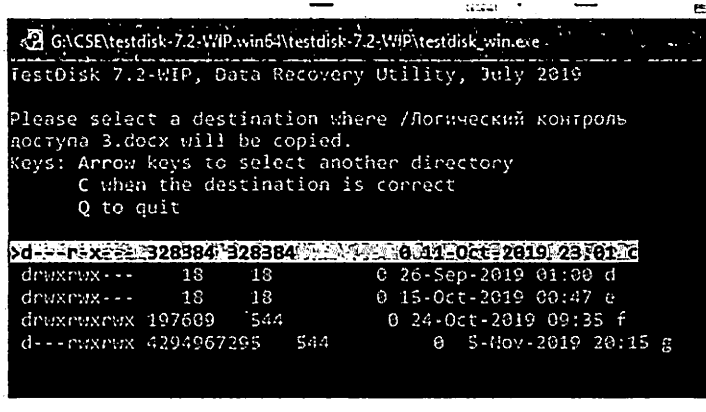


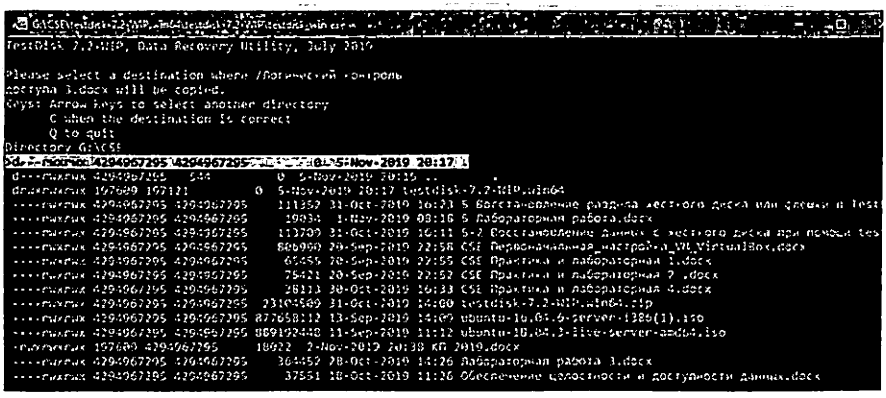
Теперь необходимо выбрать файл для восстановления: Логический контроль доступа 3.docx. Выбираю файл и команду **C** для копирования файла, как показано на рисунке выше.

После этого необходимо выбрать путь для сохранения файла. По умолчанию предлагается путь расположения самой программы TestDisk.

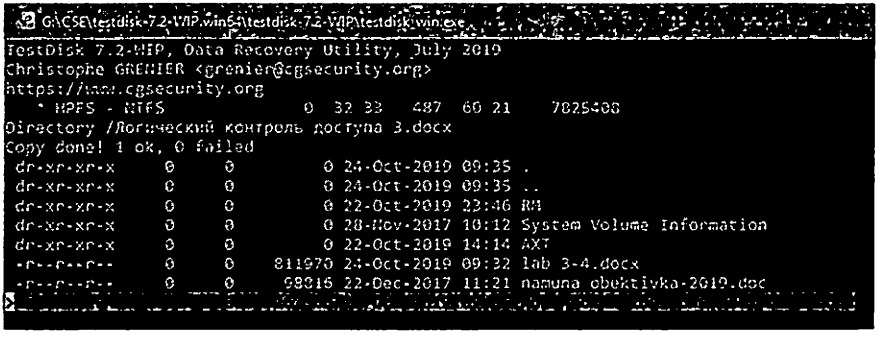


Выбираем необходимый путь сохранения восстанавливаемых данных:

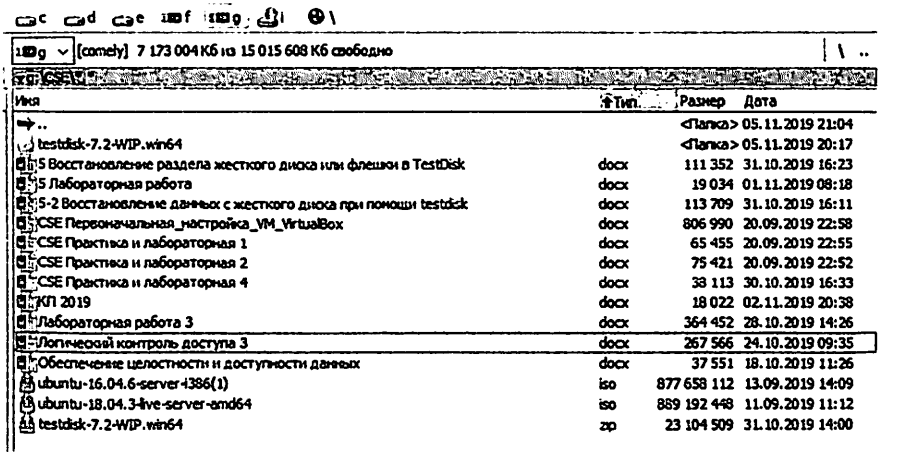




Определив конечный путь сохранения файла вновь необходимо выбрать команду копирования файла **C**.



При проверке папки CSE видно что скопированный файл Логический контроль доступа 3.docx находится 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)?

Литература:

1) С.К.Ганиев, З.Т.Худойқулов, Н.Б.Насруллаев, "Основы кибербезопасности": Учебное пособие / -Т.: «Iqtisod-Moliya», 2021. – 240. ISBN 978-9943-13-9 88-6 .
2) 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.
3) Mike Chapple, James Michael Stewart, Darril Gibson, CISSP Official Study Guide, Sybex, 2018.
4) Разработка политики резервного копирования в компании. URL: http://info-bryansk.ru/about_the_software/backup/development_of_backup_policy_in_the_company.

Практическая работа №5

Тема: Анализ рисков информационной безопасности

Цель работы: формирование и закрепление навыков проведения анализа рисков информационной безопасности, а также исследование методики их количественного и качественного оценивания.

Теоретические сведения:

Анализ рисков, который на самом деле представляет собой инструмент для управления рисками, является *методом выявления уязвимостей и угроз, оценки возможного воздействия, что позволяет выбирать адекватные защитные меры именно для тех систем и процессов, в которых они необходимы.* Анализ рисков позволяет сделать безопасность экономически эффективной, актуальной, своевременной и способной реагировать на угрозы. Он также помогает компании приоритезировать список рисков, определить и обосновать разумную стоимость защитных мер.

Анализ рисков имеет четыре основные *цели*:

1) Идентификация активов и их ценности для компании.
2) Идентификация угроз и уязвимостей.
3) Количественная оценка вероятности и влияния на бизнес этих потенциальных угроз.
4) Обеспечение экономического баланса между ущербом от воздействия угроз и стоимостью контрмер.

Анализ рисков позволяет сравнить годовую стоимость защитных мер с потенциальным ущербом. Годовая стоимость защитных мер не должна превышать потенциальный годовой ущерб. Также, анализ рисков позволяет связать программу безопасности с целями и требованиями бизнеса компании, что крайне важно для успеха и в том, и в другом.

Перед началом работы по выявлению и анализу рисков важно понять цель данной работы, ее объем и ожидаемый результат. Следует учитывать, что

попытка проанализировать все риски во всех областях за один раз может оказаться невыполнимой.

Анализ рисков должен осуществляться при поддержке и управлении со стороны высшего руководства. Только в этом случае он будет успешным. Руководство должно определить цели и масштабы анализа, назначить членов группы для проведения оценки, а также выделить необходимое время и средства для проведения этой работы. Крайне важно, чтобы высшее руководство внимательно отнеслось к результатам проведенной оценки.

Идентификация угроз. *Риск – это вероятность того, что источник угрозы воспользуется уязвимостью, что приведет к негативному воздействию на бизнес.* Существует множество видов источников угрозы, которые могут использовать разные типы уязвимостей, что может привести к определенным угрозам. Некоторые примеры рисков показаны в таблице ниже.

Таблица 5.1. Взаимосвязь угроз и уязвимостей

Источник угрозы	Может использовать эту уязвимость	В результате возникнет угроза
Вирус	Отсутствие антивирусного программного обеспечения	Заражение вирусом
Хакер	Большое количество служб, запущенных на сервере	Несанкционированный доступ к конфиденциальной информации
Пользователи	Неверно настроенный параметр операционной системы	Неисправность системы
Пожар	Отсутствие огнетушителей	Здание и компьютеры повреждены, возможны человеческие жертвы
Сотрудник	Отсутствие обучения или требований Отсутствие контроля	Общий доступ к критичной информации Внесение изменений во вводимую информацию и выводимую из приложений обработку данных
Подрядчик	Слабые механизмы контроля доступа	Утечка конфиденциальной информации
Атакующий	Плохо написанное приложение Нестрогие настройки межсетевого экрана	Проведение атаки «переполнение буфера» Проведение DoS-атаки
Нарушитель	Отсутствие охраны	Похищение компьютеров и других устройств

Анализ рисков проводится для выявления рисков, связанных с продуктом, и возможных последствий их реализации, с которыми клиент может столкнуться при использовании этого разрабатываемого продукта. Обычно в рамках процесса анализа рисков задается множество вопросов, составляется длинный список уязвимостей и угроз, с указанием вероятности эксплуатации этих уязвимостей и последствий реализации каждой из угроз. Для различных продуктов задаются разные вопросы, они зависят от таких факторов, как цель продукта, ожидания в отношении среды, в которой он будет функционировать, задействованного персонала, а также типа бизнеса компаний, которые будут приобретать и использовать этот продукт. Ниже приводится краткий список вопросов, которые должны быть заданы в процессе анализа рисков программного обеспечения:

- Существует ли возможность переполнения буфера, как ее избежать и протестировать?
- Выполняет ли продукт надлежащую проверку формата / правильности всех данных, вводимых пользователем?
- Какие источники угроз существуют во внешней и внутренней среде? Что это за источники?
- Бизнес какого типа зависит от этого продукта, в бизнесе какого типа может возникнуть ущерб, если продукт не будет работать некоторое время?
- Существуют ли угрозы утечки информации через скрытые каналы, которые должны быть учтены?
- Отказоустойчивость какого типа должен обеспечивать продукт, и когда реализация этого будет инициирована?
- Необходимо ли шифрование? Какого типа? Какая требуется стойкость?
- Нужны ли планы действий на случай экстренных ситуаций?
- Будет другая сторона (например, интернет-провайдер или хостинг-провайдер) сопровождать этот продукт для клиента?
- Необходим ли мобильный код? Зачем? Как он может быть реализован?

- Будет ли этот продукт работать в среде, подключенной к сети Интернет? Какие последствия это может иметь для продукта?
- Нужно ли этому продукту взаимодействовать с уязвимыми системами?
- Уязвим ли этот продукт к DoS-атакам?
- Уязвим ли этот продукт для вирусов?
- Необходимы ли механизмы предупреждения о вторжениях?
- Будут ли у сотрудников клиента или внешних лиц мотивы саботировать этот продукт? Зачем? В чем может выражаться такой саботаж?
- Будут ли у компаний-конкурентов клиента мотивы совершить мошенничество с помощью этого продукта? Зачем? Как может быть реализовано такое мошенничество?
- Какие другие системы будут затронуты, если этот продукт выйдет из строя?

Команда физической безопасности должна провести анализ рисков, а рамках которого будут выявлены уязвимости, угрозы и их воздействие на бизнес компании. Результаты команда должна предоставить руководству и совместно с руководством определить приемлемый уровень риска для программы физической безопасности. Исходя из этого, команда должна разработать базисы (минимальный уровень безопасности) и метрики для правильной оценки и определения, достигаются ли эти базисы внедренными контрмерами. После определения и внедрения контрмер, эффективность этих контрмер должна постоянно отслеживаться и оцениваться на основе разработанных метрик. Значения эффективности контрмер должны сравниваться с набором базисов. Если базисы постоянно соблюдаются, программу безопасности можно считать успешной, поскольку в компании не превышается приемлемый для нее уровень рисков.

Количественный анализ рисков. Количественный анализ рисков пытается присвоить реальные и осмысленные числа всем элементам процесса анализа рисков. Этими элементами могут быть стоимость защитных мер, ценность актива, ущерб для бизнеса, частота возникновения угрозы, эффективность защитных мер, вероятность использования уязвимости и т.д.

Количественный анализ рисков позволяет получить конкретное значение вероятности (в процентах) реализации угрозы. Каждый элемент в процессе анализа вставляется в количественном виде в уравнение определения общего и остаточного риска.

Нужно понимать, что количественный анализ рисков в чистом виде невозможен, т.к. всегда есть некоторая степень неопределенности в значении отдельных количественных величин (особенно если угрозы сложны, а частота их возникновения невелика). Например, как узнать насколько часто уязвимостью будут пользоваться? Или как узнать точную денежную сумму потерь компании?

Шаги процесса анализа рисков:

Шаг 1: Определить ценность активов. Для каждого актива необходимо ответить на следующие вопросы для определения его ценности:

- В чем заключается ценность данного актива для компании?
- Сколько стоит его поддержка?
- Какую прибыль он приносит компании?
- Сколько за него готовы заплатить конкуренты?
- Сколько будет стоить его повторное создание или восстановление?
- Сколько стоило его получить или разработать?
- Какова мера ответственности в случае компрометации данного актива?

Шаг 2: Оценить потенциальные потери от угрозы. Для оценки потенциальных потерь, необходимо ответить на следующие вопросы:

- К каким физическим повреждениям может привести угроза и сколько это будет стоить?
- Какую потерю продуктивности может вызвать угроза и сколько это будет стоить?
- Какие потери понесет компания в случае разглашения конфиденциальной информации?
- Какова стоимость восстановления после воздействия угрозы?
- Какова стоимость потерь в случае неисправности критичных устройств?

- Каков ожидаемый ущерб от единичного инцидента (SLE – Single Loss Expectancy) для каждого актива и каждой угрозы?

Это только небольшой список вопросов, на которые необходимо получить ответы. Специфичные вопросы будут зависеть от типов угроз и выявленных группой особенностей.

Шаг 3: Выполнить анализ угроз. Для анализа угроз нужно выполнить следующие действия:

- Собрать информацию о вероятности каждой угрозы, опросив сотрудников каждого подразделения, проанализировав произведенные ранее записи, а также официальные источники по безопасности, которые предоставляют такую информацию.
- Рассчитать среднегодовую частоту возникновения инцидентов (ARO – Annualized Rate of Occurrence), которая показывает сколько инцидентов может произойти за год.

Шаг 4: Определить общие годовые потери на угрозу. Для этого нужно выполнить следующее:

- Объединить потенциальные потери и вероятность.
- Рассчитать ожидаемый среднегодовой ущерб (ALE – Annualized Loss Expectancy) на угрозу, используя информацию, собранную на первых трех шагах.
- Выбрать контрмеры для противодействия каждой угрозе.
- Выполнить анализ затрат/выгод выбранных контрмер.

Шаг 5: Уменьшить, перенести, избежать или принять риск. Для каждого риска необходимо выбрать меры по его снижению, переносу, либо принять его.

- *Методы снижения риска:*
  - внедрить защитные меры и средства управления;
  - усовершенствовать процедуры;
  - изменить окружение;

- внедрить методы раннего обнаружения для своевременного выявления факторов воздействия угрозы и снижения возможных последствий;
- разработать план действий в непредвиденных ситуациях, позволяющий продолжить работу в случае воздействия определенных угроз и снизить последствия от угрозы;
- создать препятствия для реализации угрозы;
- провести тренинг по вопросам безопасности.

- *Перенос риска* – например, застраховать некоторые риски.
- *Избежание риска* – прекратить деятельность, вызывающую риск.
- *Принятие риска* – смириться с риском и не тратить деньги на защиту от него (это целесообразно, если стоимость защитных мер превышает величину возможного ущерба). Однако при этом нужно учитывать, что реализация риска может вести к дополнительным последствиям (например, потере репутации).

При проведении количественного анализа рисков необходимы, реальные цифры и расчеты. Ранее уже были упомянуты показатели *SLE (ущерб от единичного инцидента)* и *ALE (ожидаемый среднегодовой ущерб)*. SLE – это потенциальная сумма (в деньгах) ущерба для компании в результате единичного факта реализации соответствующей угрозы:

$$\text{Ценность актива} \times EF = SLE$$

EF (Exposure Factor,фактор воздействия) – это процент ущерба для актива от реализовавшейся угрозы, т.е. часть значения (ценности), которую актив потеряет в результате инцидента. Например, ценность актива "хранилище данных" составляет $150,000. В случае пожара может быть повреждено 25% хранилища (но не более, т.к. установлена система пожаротушения, поблизости находится пожарная часть и т.д.). В этом случае SLE будет составлять $37,500. Значение SLE используется при расчете ALE:

$$SLE \times ARO = ALE$$

ARO (Annualized Rate of Occurrence, среднегодовая частота возникновения инцидентов) – это величина, представляющая собой

ожидаемую частоту реализации соответствующей угрозы в год. Значение ARO может быть от 0,0 (никогда) до 1,0 (по крайней мере, раз в год) и выше (несколько раз в год). Например, наводнения в той местности, в которой расположено здание компании, происходят в среднем раз в 1000 лет. Значит величина ARO составляет 0,001.

Таким образом, если SLE для хранилища данных компании при пожаре равно $37,500, а пожары в аналогичных условия случаются примерно раз в 10 лет (ARO равно 0,1), величина ALE будет равна $3,750 ($37,500 x 0,1 = $3,750).

Значение ALE используется при оценке целесообразности внедрения тех или иных мер защиты соответствующего актива от соответствующей угрозы – годовая стоимость защитных мер, обеспечивающих необходимый уровень безопасности актива, не должна превышать значение ALE. Применение более дорогих защитных мер не будет эффективным и целесообразным.

Практическая часть:

Пример 1. Количественная оценка рисков.

Рассмотрим пример результатов анализа рисков (таблица 5.2). Используя полученные данные компания может принять обоснованное решение о том, какие угрозы необходимо рассматривать в первую очередь, основываясь на их последствиях и вероятности реализации. Также компания может оценить целесообразный уровень затрат на защиту от каждой угрозы.

Таблица 5.2. Пример результатов анализа рисков

Актив	Угроза	SLE	ARO	ALE
Здание	Пожар	$230,000	0,1	$23,000
Коммерческая тайна	Хищение	$40,000	0,01	$400
Файловый сервер	Неисправность	$11,500	0,1	$1,150
Данные	Вирус	$6,500	1,0	$6,500
Информация о кредитной карте клиента	Хищение	$300,000	3,0	$900,000

Результаты анализа рисков: группа анализа рисков должна иметь четко определенные цели. Следующий список показывает, что в основном можно ожидать от результатов анализа рисков:

- ценность активов в денежном выражении;
- полный список всех возможных и существенных угроз;
- вероятная частота возникновения каждой угрозы;
- потенциальные потери компании от угроз, которые она может понести в 12-ти месячный срок;
- рекомендуемые меры безопасности, контрмеры и действия.

Хотя данный список следует по возможности детализировать, следует сделать краткое резюме для руководства, на основании которого можно быстро сделать выводы о результатах анализа.

Пример 2. Рассмотрим простой пример качественного анализа рисков. Группа анализа рисков написала одностраничный сценарий, описывающий угрозу получения хакером доступа к конфиденциальной информации, хранящейся на файловых серверах компании. Группа распространяет этот сценарий между пятью сотрудниками (*ИТ-директор, администратор базы данных, программист, системный инженер и руководители подразделения технической поддержки*), которые заполняют лист оценки, ранжируя (*от 1 до 5*) серьезность угрозы, уровень потенциального ущерба, эффективность каждой защитной меры. Результаты показаны в таблице 5.3. Затем на основе этих результатов один из членов группы готовит отчет для руководства, в котором указывает, что из проанализированных трех вариантов защиты (межсетевой экран, система IDS и honeypot), наиболее эффективной является защита с помощью межсетевого экрана.

Анализируя отчет по анализу рисков, руководство видит оценки серьезности угроз, вероятности их реализации, а также уровень потенциальных потерь от каждой угрозы. На основе этой информации руководство может выбрать наиболее критичные для компании риски, которые должны быть учтены в первую очередь.

Анализируя отчет по анализу рисков, руководство видит оценки серьезности угроз, вероятности их реализации, а также уровень потенциальных потерь от каждой угрозы. На основе этой информации

руководство может выбрать наиболее критичные для компании риски, которые должны быть учтены в первую очередь.

Таблица 5.3. Пример качественного анализа рисков

Угроза: Доступ хакера к конфиденциальной информации	*серьезность угрозы*	*вероятность реализации угрозы*	*потенциальный ущерб для компании*	*эффективность защиты с помощью межсетевого экрана*	*эффективность защиты с помощью IDS*	*эффективность защиты с помощью honeypot*
ИТ-директор	4	2	4	4	3	2
Администратор БД	4	4	4	3	4	1
Программист	3	3	3	4	2	1
Системный инженер	4	4	3	4	2	1
Руководитель тех.поддержки	5	4	4	4	4	2
Итог:	***3,6***	***3,4***	***3,8***	***3,8***	***3,0***	***1,4***

Задания к практической работе:

Задание 1. Рассмотрите предлагаемую проблемную ситуацию кейса *«Ситуация 1»*. Запишите решение кейса в отчете к практической работе.

Ситуация 1. Представьте себя работниками отдела информационной безопасности крупной банковской организации. В кратчайшие сроки Вам необходимо устранить уязвимости, приведшие к несанкционированному доступу к информации. Предложите варианты выявления причин и последствий данного нарушения, варианты проверки и использования контрмер. Для рассмотрения проблемной ситуации используйте метод анализа «Галстук-бабочка»

Вопросы кейса: Какие действия нужно произвести для того, чтобы устранить причины несанкционированного доступа к данным? Какие факторы могут влиять на выбор контрмер со стороны организации? Каким образом по вашему мнению осуществляется контроль нарушения целостности и конфиденциальности данных?

Задание 2. Проанализируйте проблемную ситуацию кейса *«Ситуация 2»*. Запишите решение в отчете к практической работе.

Ситуация 2. При работе оператора информационной системы произошел сбой аппаратной части обработки данных. В результате произошедшего инцидента произошла непредвиденная потеря конфиденциальных данных клиентов организации. Причиной произошедшего сбоя явилась поломка жесткого диска. Представьте себя работниками отдела информационной безопасности крупной организации. В кратчайшие сроки Вам необходимо выявить причины возникшей поломки, которая привела к нарушению целостности и доступности данных. Для рассмотрения проблемной ситуации используйте метод анализа «Дерево неисправностей».

Вопросы кейса: Какие аппаратные части вычислительных устройств могут стать причиной нарушения AIC-триады безопасности? Каким образом можно обезопасить организацию от подобного рода рисков потери данных?

Задание 3. Какой из перечисленных ниже ответов лучше всего описывает отношения между анализом рисков, приемлемым уровнем рисков, бизисами, контрмерами и метриками? Аргументируйте свой ответ.

a) Результаты анализа рисков используются для определения необходимых контрмер. Базисы используются для оценки этих контрмер. Метрики используются для отслеживания эффективности контрмер, чтобы убедиться в соблюдении базисов.

b) Результаты анализа рисков помогают руководству понять и установить приемлемый уровень рисков. Базисы основаны на этом уровне. Метрики используются для отслеживания эффективности контрмер, чтобы убедиться в соблюдении базисов.

c) Результаты анализа рисков помогают руководству понять и установить базисы. Приемлемый уровень рисков основан на базисах. Метрики используются для отслеживания эффективности контрмер, чтобы убедиться в соблюдении базисов.

d) Результаты анализа рисков помогают руководству понять и установить приемлемый уровень рисков. Базисы основаны на этом уровне. Метрики используются для отслеживания эффективности базисов.

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 риск?
2. В чем заключаются основные цели анализа рисков?
3. Что вы понимаете под качественным анализом рисков?
4. Что подразумевается под количественным анализом рисков?
5. Перечислите и разъясните каждый из шагов процесса анализа рисков.

Литература:

1) С.К.Ганиев, З.Т.Худойқулов, Н.Б.Насруллаев, Основы кибербезопасности: Учебное пособие / -Т.: «Iqtisod-Moliya», 2021. – 240. ISBN 978-9943-13-9 88-6.
2) Mike Chapple, James Michael Stewart, Darril Gibson, CISSP Official Study Guide, Sybex, 2018.
3) 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
4) 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
5) Threat and Risk Assessment Working Guide.
   URL: www.cse-cst.gc.ca/en/documents/publications/gov_pubs/itsg/itsg04.pdf

СОДЕРЖАНИЕ