# Методические указания по организации практической работы студентов по учебной дисциплине Информационная безопасность

09.02.07 Информационные системы и программирование

2023

Методические рекомендации по учебной дисциплине «Информационная безопасность» разработаны с учетом по специальности среднего профессионального образования (далее - СПО) технического профиля: Информационные системы (по отраслям) предназначены для обучающихся и преподавателей колледжа.
Методические рекомендации разработаны на основе требований ФГОС среднего общего образования, предъявляемых к структуре, содержанию и результатам освоения учебной дисциплины «Информационная безопасность».

Составитель (автор): преподаватель колледжа

Рассмотрены на заседании предметной (цикловой) комиссии специальности общеобразовательных дисциплин

Протокол № от «_____ » _____ 2023 г

Председатель предметной (цикловой) комиссии _____
личная подпись

и одобрены решением учебно-методического совета колледжа.

Протокол № от «30» июня 2023 г

Председатель учебно-методического совета колледжа
комиссии _____
личная подпись

Рекомендованы к практическому применению в образовательном процессе

**Содержание:**

# Лабораторная работа №1 Правовые основы информационной безопасности РФ

**Цель:** изучение законов и правовых актов по обеспечению информационной безопасности РФ

Время:2 часа

**Теоретическая часть**

Нормативно-правовые акты, направленные на защиту информации условно можно разделить на уровневую структуру:

- Первый уровень составляет конституционное законодательство;
- Второй уровень составляют общие законы и кодексы, которые включают нормы по вопросам информационной безопасности;
- На третьем уровне находятся законы по организации управления, которые касаются отдельных структур, эти законы обеспечивают реализацию отдельных норм по правовой защите информации и должны устанавливать функционал конкретного органа исполнительной власти.
- Четвертый уровень характеризует специальные законы, которые в полном объеме относятся к конкретным отраслям.
- Пятый уровень - это законодательство субъектов РФ в сфере защиты информации.
- На шестом уровне подзаконные нормативно-правовые акты по защите информации.

Особое место в ряде нормативно-правовых актов отведено Закону «Об информации, ее защите и об информационных технологиях» - он определяет и обеспечивает основы правового регулирования всех важных компонентов информационной деятельности.

К ним можно отнести:

- информацию и информационные системы;
- субъекты участниками информационных процессов;
- правоотношения потребителей и производителей информационной продукции;
- владельцев информации.

**Практические задания**

**№ 1**

Откройте законов РФ в области информационной безопасности и заполните таблицу

| Название ФЗ | Дата принятия | Дата последнего изменения | Номер закона | Что регулирует закон |
|---|---|---|---|---|
| «Доктрина информационной безопасности Российской Федерации» | | | | |
| «Об информации, информационных технологиях и о защите информации» | | | | |
| «О безопасности» | | | | |
| «Об электронной подписи» | | | | |
| «О персональных данных» | | | | |
| «О государственной тайне» | | | | |
| «О правовой охране программ для электронных вычислительных машин и баз данных» | | | | |
| «О коммерческой тайне» | | | | |
| «О лицензировании отдельных видов деятельности» | | | | |

**№ 2**

Выпишите из указанных законов РФ по информационной безопасности основные определения и понятия

**A. Доктрина информационной безопасности Российской Федерации_**

- Под информационной безопасностью Российской Федерации понимается - (*текст из закона*)
- Интересы личности в информационной сфере заключаются - (*текст из закона*)
- Интересы общества в информационной сфере заключаются - (*текст из закона*)
- Интересы государства в информационной сфере заключаются - (*текст из закона*)
- Первая составляющая национальных интересов Российской Федерации в информационной сфере включает - (*текст из закона*)
- Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает- (*текст из закона*)
- Третья составляющая национальных интересов Российской Федерации в информационной сфере включает - (*текст из закона*)
- Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает- (*текст из закона*)

**B. Об электронной цифровой подписи**:

- Электронный документ - (*текст из закона*)
- Электронная цифровая подпись - (*текст из закона*)
- Владелец сертификата ключа подписи - (*текст из закона*)
- Средства электронной цифровой подписи - (*текст из закона*)
- Сертификат средств электронной цифровой подписи - (*текст из закона*)
- Закрытый ключ электронной цифровой подписи - (*текст из закона*)
- Открытый ключ электронной цифровой подписи - (*текст из закона*)
- Сертификат ключа подписи - (*текст из закона*)
- Подтверждение подлинности электронной цифровой подписи в электронном документе - (*текст из закона*)
- Пользователь сертификата ключа подписи - (*текст из закона*)
- Информационная система общего пользования - (*текст из закона*)
- Корпоративная информационная система - (*текст из закона*)

**C. О лицензировании отдельных видов деятельности**

- Лицензия - (*текст из закона*)
- Лицензируемый вид деятельности - (*текст из закона*)
- Лицензирование - (*текст из закона*)
- Лицензирующие органы - (*текст из закона*)
- Лицензиат - (*текст из закона*)

**D. Об информации, информационных технологиях и о защите информации**^

- информация -(*текст из закона*)
- информационные технологии - (*текст из закона*)
- информационная система -(*текст из закона*)
- информационно-телекоммуникационная сеть - (*текст из закона*)
- обладатель информации - (*текст из закона*)
- доступ к информации - (*текст из закона*)
- конфиденциальность информации - (*текст из закона*)
- предоставление информации - (*текст из закона*)
- распространение информации - (*текст из закона*)

**E. О персональных данных**

- персональные данные - (*текст из закона*)
- оператор - (*текст из закона)*
- обработка персональных данных - (*текст из закона*)
- распространение персональных данных - (*текст из закона*)
- использование персональных данных - (*текст из закона*)
- блокирование персональных данных - (*текст из закона*)

- уничтожение персональных данных - (*текст из закона*)

**F. О правовой охране программ для электронных вычислительных машин и баз данных**

- программа для ЭВМ - (*текст из закона*)
- база данных - (*текст из закона*)
- адаптация программы для ЭВМ или базы данных - (*текст из закона*)
- модификация (переработка) программы для ЭВМ или базы данных - (*текст из закона*)
- декомпилирование программы для ЭВМ - (*текст из закона*)
- воспроизведение программы для ЭВМ или базы данных - (*текст из закона*)
- распространение программы для ЭВМ или базы данных - (*текст из закона*)
- выпуск в свет (опубликование) программы для ЭВМ или базы данных - (*текст из закона*)
- использование программы для ЭВМ или базы данных - (*текст из закона*)

**G. УК РФ**

- статья138. (*текст из закона*)
- статья183. (*текст из закона*)
- статья 272. (*текст из закона*)
- статья 273. (*текст из закона*)
- статья 274. (*текст из закона*)

**H. О Г осударственной тайне**

- государственная тайна - (*текст из закона*)
- носители сведений, составляющих государственную тайну - (*текст из закона*)
- система защиты государственной тайны - (*текст из закона*)
- допуск к государственной тайне -(*текст из закона*)
- доступ к сведениям, составляющим государственную тайну -(*текст из закона*)
- гриф секретности - (*текст из закона*)
- средства защиты информации - (*текст из закона*)

**1. О коммерческой тайне**

- коммерческая тайна - (*текст из закона*)
- информация, составляющая коммерческую тайну -(*текст из закона*)
- обладатель информации, составляющей коммерческую тайну - (*текст из закона*)
- доступ к информации, составляющей коммерческую тайну -(*текст из закона*)
- контрагент - (*текст из закона*)
- предоставление информации, составляющей коммерческую тайну -(*текст из закона*)
- разглашение информации, составляющей коммерческую тайну -(*текст из закона*)

**Контрольные вопросы.**

1. Перечислите составляющие национальных интересов Российской Федерации в информационной сфере
2. Дать определение государственной и коммерческой тайны и их различие.
3. Какое наказание предусматривается УК РФ за преступление в сфере информационной безопасности.

## Лабораторная работа №2 «Кодирование и подсчет количества информации»

**Цель работы:** Изучить основные виды и свойства информации. Научиться определять количество представленной информации в ЭВМ.

Время 2 часа

**Теоретическая часть**

Термин **ИНФОРМАЦИЯ** происходит от латинского слова informatio - разъяснение, изложение. Первоначальное значение этого термина - «сведения, передаваемые людьми устным, письменным или иным способом».

**Свойства информации**

На свойства информации влияют как свойства данных, так и свойства методов её обработки.

1 **Объективность информации**. Понятие объективности информации относительно. Более

объективной является та информация, в которую методы обработки вносят меньше субъективности. Например, в результате наблюдения фотоснимка природного объекта образуется более объективная информация, чем при наблюдении рисунка того же объекта. В ходе информационного процесса объективность информации всегда понижается.

2 **Полнота информации**. Полнота информации характеризует достаточность данных для принятия решения. Чем полнее данные, тем шире диапазон используемых методов их обработки и тем проще подобрать метод, вносящий минимум погрешности в информационный процесс.

3 **Адекватность информации**. Это степень её соответствия реальному состоянию дел. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостоверных данных. Однако полные и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

4 **Доступность информации**. Это мера возможности получить информацию. Отсутствие доступа к данным или отсутствие адекватных методов их обработки приводят к тому, что информация оказывается недоступной.

5 **Актуальность информации**. Это степень соответствия информации текущему моменту времени. Поскольку информационные процессы растянуты во времени, то достоверная и адекватная, но устаревшая информация может приводить к ошибочным решениям. Необходимость поиска или разработки адекватного метода обработки данных может приводить к такой задержке в получении информации, что она становится ненужной.

**Виды информации**

Информация может быть представлена в разных видах, формах, способах хранения и кодирования.

1 По способу восприятия информация может быть визуальной (я вижу), аудиальной (я слышу), тактильной (я трогаю, ощущаю на ощупь), обонятельной (я чувствую запах), вкусовой (я ощущаю вкус).

2 По форме представления: текстовая (в виде текста), графическая (в виде рисунка, схемы, фото и т.д.), музыкальная (в форме музыки, звука), числовая (в виде чисел), видео (в форме видеофайла), комбинированная (сочетает в себе разные формы представления, например, музыкальный клип - формы видео и аудио) и т.д.

3 По специальности: научная, техническая, производственная и т.д. информация.

4 По значению для общества: массовая, ориентированная на отдельного человека, экономическая, политическая, эстетическая и т.д.

**Основные понятия**

1 Сообщение несет информацию для человека, если содержащиеся в нем сведения являются для него новыми и понятными.

2 Сообщение, уменьшающее неопределенность знаний в два раза, несет 1 бит информации.

3 Неопределенность знаний о некотором событии — это количество возможных результатов события.

4 Количество информации, содержащееся в сообщении о том, что произошло одно из N равновероятных событий, определяется из решения показательного уравнения: $2^i = N$.

5 Количество информации, содержащейся в сообщении о результатах нескольких (независимых) выборов, должно быть равно сумме количеств информации, содержащейся в сообщениях об этих выборах по отдельности

6 При алфавитном подходе к измерению информации количество информации зависит не от содержания, а от размера текста и мощности алфавита.

7 Алфавит - множество символов, используемых при записи текста. Мощность (размер)

алфавита - полное количество символов в алфавите.

8 Если мощность алфавита обозначить N, тогда, согласно известной формуле $N = 2^i$, каждый символ алфавита несет i бит информации. Количество информации одного символа называется весом символа

9 Чтобы найти количество информации во всем тексте, нужно посчитать число символов в нем и умножить на вес одного символа. J = K*I (K - количество символов в тексте, J - количество информации текста или информационный объем текста)

10 Скорость передачи информации (скорость передачи данных) - это количество бит, передаваемых за единицу времени, измеряется в бит/с: V = J/t

11 Если события не являются равновероятными, то для вычисления количества информации события необходимо использовать понятие вероятности (отношение благоприятных исходов к общему количеству исходов события)

12 Количественная зависимость между вероятностью события p и количеством возможных исходов события N выражается формулой:

$$\mathbf{N = 1/p}$$

**Единицы измерения информации**

- 1 байт = 8 бит
- 1 Кбайт = $2^{10}$ байт=1024 байт
- 1 Мбайт = $2^{10}$ Кбайт=1024 Кбайт
- 1 Гбайт = $2^{10}$ Мбайт=1024 Мбайт
- 1 Тбайт = $2^{10}$ Гбайт=1024 Гбайт
- 1 Пбайт = $2^{10}$ Тбайт=1024 Тбайт

Если сообщение состоит из символов некого алфавита (и все символы равно вероятны). То количество информации I в сообщении вычисляется по формуле:

$$\mathbf{I = \log_2 N}$$

Отсюда:

$\mathbf{N = 2^I}$, где: N-количество возможных информационных сообщений;

I-количество информации, которое несет одно сообщение.

Скорость передачи информации измеряется в битах в секунду и вычисляется по формуле:

$$\mathbf{V=I/t}$$

где **I** - количество информации в сообщении

**t** - время передачи сообщения

**Примеры решения:**

**Вопрос:** Сколько бит памяти займет слово «Микропроцессор»?

**Решение:**

Слово состоит из 14 букв. Каждая буква - символ компьютерного алфавита, занимает 1 байт памяти. Слово занимает 14 байт =14*8=112 бит памяти.

**Ответ:** 112 бит

2. Текст занимает 0, 25 Кбайт памяти компьютера. Сколько символов содержит этот текст?

**Решение:**

Переведем Кб в байты: 0, 25 Кб * 1024 =256 байт. Так как текст занимает объем 256 байт, а каждый символ - 1 байт, то в тексте 256 символов.

Ответ: 256 символов

3. Текст занимает полных 5 страниц. На каждой странице размещается 30 строк по 70 символов в строке. Какой объем оперативной памяти (в байтах) займет этот текст? ([1], с.133, №32)

**Решение**:

30*70*5 = 10500 символов в тексте на 5 страницах. Текст займет 10500 байт оперативной памяти.

Ответ: 10500 байт

**Практические задания:**

**Решить задачу в соответствии с вариантом:**

1. Сколько вопросов надо задать, чтобы отгадать задуманное целое число от 1 до 16?
2. В озере обитает 12500 окуней, 25000 пескарей, а карасей и щук по 6250. Какое количество информации несет сообщение о ловле рыбы каждого вида. Сколько информации мы получим, когда поймаем окуня?
3. Сколько информации содержит красный сигнал светофора?
4. Скорость передачи данных через ADSL-соединение равна 8000 байт/сек. Через данное соединение передают файл размером 375 Кбайт. Определите время передачи файла в секундах.
5. Можно ли уместить на одну дискету книгу, имеющую 432 страницы, причем на каждой странице этой книги 46 строк, а в каждой строке 62 символа? Емкость дискеты 1,44 МБ
6. Сообщение «Алиса живет в доме № 23 на улице Вишневая» содержит 5 бит информации. Сколько всего домов на улице?
7. В коробке лежат кубики: 10 красных, 8 зеленых, 2 желтых, 12 синих. Вычислите количество информации доставания зеленого кубика.
8. Сколько секунд потребуется модему, передающему сообщение со скоростью 216000 байт/мин, чтобы передать 100 страниц текста в 30 сток по 60 символов каждая, при условии, что для передачи используется алфавит из 256 символов.
9. Для записи текста использовался 256-символьный алфавит. Каждая страница содержит 30 строк по 70 символов в строке. Какой объем информации содержат 5 страниц текста?
10. Во время игры в кости на игральном кубике выпало число 1. Сколько информации содержит это сообщение?
11. В непрозрачном мешочке хранятся 10 белых, 20 красных, 30 синих и 40 зеленых шариков. Какое количество информации будет содержать сообщение о том, что вынули зеленый шарик?
12. Сколько Кбайт составит сообщение из 200 символов 20-символьного алфавита?
13. Сколько бит информации получит второй игрок после первого хода первого игрока в игре «Крестики-нолики» на иоле размером 4 х 4?
14. Если на озере живет 500 уток и 100 гусей, то какое количество информации в том, что подстрелили на охоте гуся?
15. «Ты меня любишь?» — спросил влюбленный юноша девушку. «Да», — ответила та. Сколько бит информации содержит ее ответ?
16. В течении 5 минут со скоростью 20 (байт/с) вождь племени передавал информационное сообщение. Сколько символов оно содержало, если алфавит племени состоит из 32 символов?
17. Подсчитать в Кбайт количество информации в тексте, если текст состоит из 800 символов, а мощность используемого алфавита - 128 символов
18. В доме 16 этажей. На каждом этаже по несколько квартир. Сообщение о том, что Саша живет в квартире №40, содержит 6 бит информации. Сколько квартир на каждом этаже?
19. В ящике лежат перчатки (белые и черные). Среди них - 2 пары черных. Сообщение о том, что из ящика достали пару черных перчаток, несет 4 бита информации. Сколько всего пар перчаток было в ящике?

20. Сколько символов в тексте, если мощность алфавита — 32 символа, а объем информации, содержащийся в нем - 1,5 Кбайт?

**КОНТРОЛЬНЫЕ ВОПРОСЫ**

1. Что такое отказоустойчивость?
2. Дать определение понятию «Кодирование».
3. Опишите требования к кодированию.
4. Привести примеры методов кодирования

**Лабораторная работа №3 Настройка параметров безопасности в ОС Windows**

**Цель работы:** Ознакомиться с механизмами аутентификации и идентификации, локальными политиками безопасности, встроенными в ОС Windows.

Время 2 часа

**Теоретическая часть:**

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации. Идентификация и аутентификация применяются для ограничения доступа случайных или незаконных субъектов (пользователей, процессов) к информационной системе, объектам - ресурсам (аппаратным, программным, информационным).

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

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

Настройка параметров аутентификации в ОС Windows выполняется в рамках локальной политики безопасности. Вкладка «Локальная политика безопасности» используется для изменения политики учетных записей и локальных политик безопасности на компьютере. При помощи вкладки «Локальная политика безопасности» можно определить:

- Кто имеет доступ к компьютеру;
- Какие ресурсы могут использовать пользователи на компьютере;
- Включение и выключение записи действий пользователей или группы пользователей в журнале событий.

**Группы политик, отвечающих за безопасность**

Рассмотрим подробнее расширение Параметры безопасности (Security Settings), с помощью которого конфигурируются параметры системы безопасности операционной системы. Политики, определяемые этим расширением, действуют на компьютеры и частично на пользователей.

**Политики учетных записей** (Account Policies). Настройка политик безопасности учетных записей в масштабах домена или локальных учетных записей. Здесь определяются политика паролей, политика блокировки паролей и политика Kerberos, распространяющаяся на весь домен.

**Локальные политики** (Local Policies). Настройка политики аудита, назначение прав пользователей и определение различных параметров безопасности.

**Журнал событий** (Event Log). Настройка политик безопасности, определяющих работу журналов событий приложений, системы и безопасности.

**Группы с ограниченным доступом** (Restricted Groups). Управление членством пользователей в заданных группах. Сюда обычно включают встроенные группы, такие как Администраторы (Administrators), Операторы архива (Backup Operators) и другие, имеющие по умолчанию права администратора. В эту категорию могут быть включены и иные группы, безопасность которых требует особого внимания и членство в коюрых должно регулироваться на уровне политики.

**Системные службы** (System Services). Настройка безопасности и параметров загрузки для работающих на компьютере служб.

**Реестр** (Registry). Настройка прав доступа к различным разделам реестра. (Значения параметров реестра можно задавать в доменных GPO объектах с помощью предпочтений

(preferences).)

**Файловая система** (File System). Настройка прав доступа к определенным файлам.

**Политики проводной сети** *(IEEE 802.3) (*Wired Network (IEEE 802.3) Policies). Настройка параметров клиентов, подключающихся к проводным сетям, принадлежащим разным доменам.

**Брандмауэр Windows в режиме повышенной безопасности (**Windows Firewall with Advanced Security). Настройка правил и других параметров встроенного брандмауэра Windows (Windows Firewall).

**Политики диспетчера списка сетей** (Network List Manager Policies). Настройка типов размещения для сетей, доступных компьютеру.

**Политики беспроводной сети** *(IEEE 802.111) (*Wireless Network (IEEH 802.11) Policies). Централизованная настройка параметров (включая методы проверки подлинности) клиентов беспроводной сети в доменах Active Directory.

**Политики открытого ключа** (Public Key Policies). Настройка политик безопасности в отношении шифрования информации с помощью EFS и BitLocker, авторизации корневого сертификата в масштабах домена, авторизации доверенного сертификата и т.д.

**Политики ограниченного использования программ** (Software Restriction Policies). Политики, указывающие на то, какие приложения могут, а ка кие программы не могут выполняться на локальном компьютере.

**Защита доступа к сети** *(*Network Access Protection). Настройка поли тик, определяющих требования к клиенту, подключающемуся к сети, и предоставляющих полный или ограниченный доступ к сети в зависимости от того, насколько клиент соответствует этим требованиям. В процессе проверки могут анализироваться различные аспекты безопасности: наличие обновлений программных средств и антивирусной защиты, параметры конфигурации и брандмауэра, список открытых и закрытых портов TCP/IP и т.д.

**Политики управления приложениями** (Application Control Policies). Управление средством AppLocker, представляющим собой новую функцию в системах Windows и Windows Server 2008 R2, предназначенную для контроля за установкой и использованием приложений в корпоративной среде.

**Политики IP-безопасности** (IP Security Policies). Настройка политик безопасности IP для компьютеров, находящихся в определенной области действия.

Конфигурация расширенной политики аудита (Advanced Audit Policy Configuration). Политики, позволяющие централизованно настраивать аудит в системах Windows и Windows Server 2008 R2.

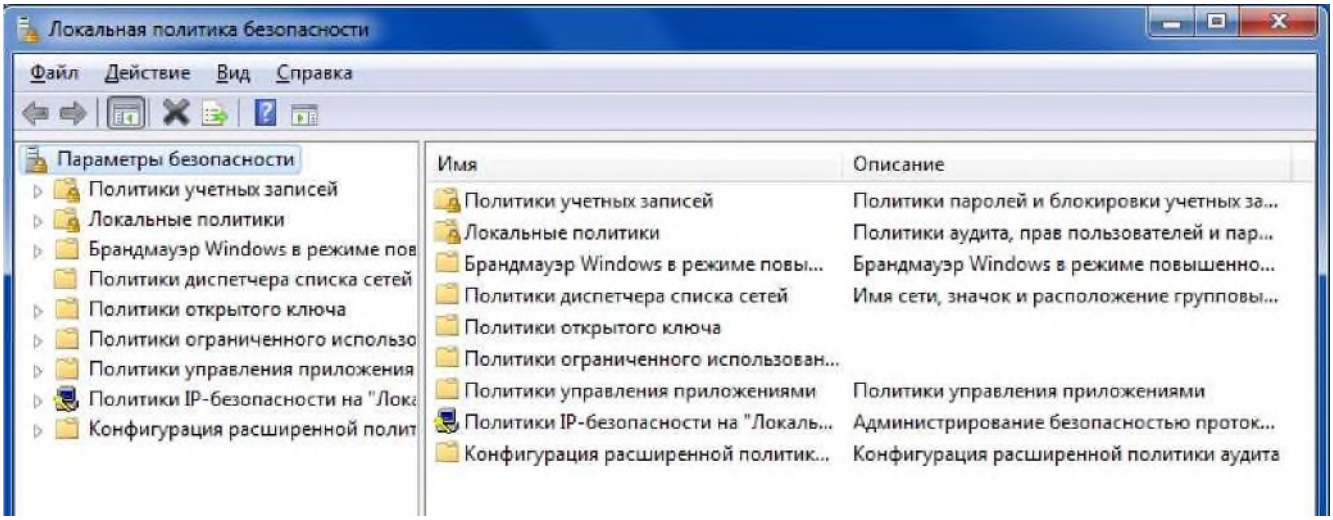
**Практические задания**

**№1** Настроить параметры локальной политики безопасности операционной системы Windows;

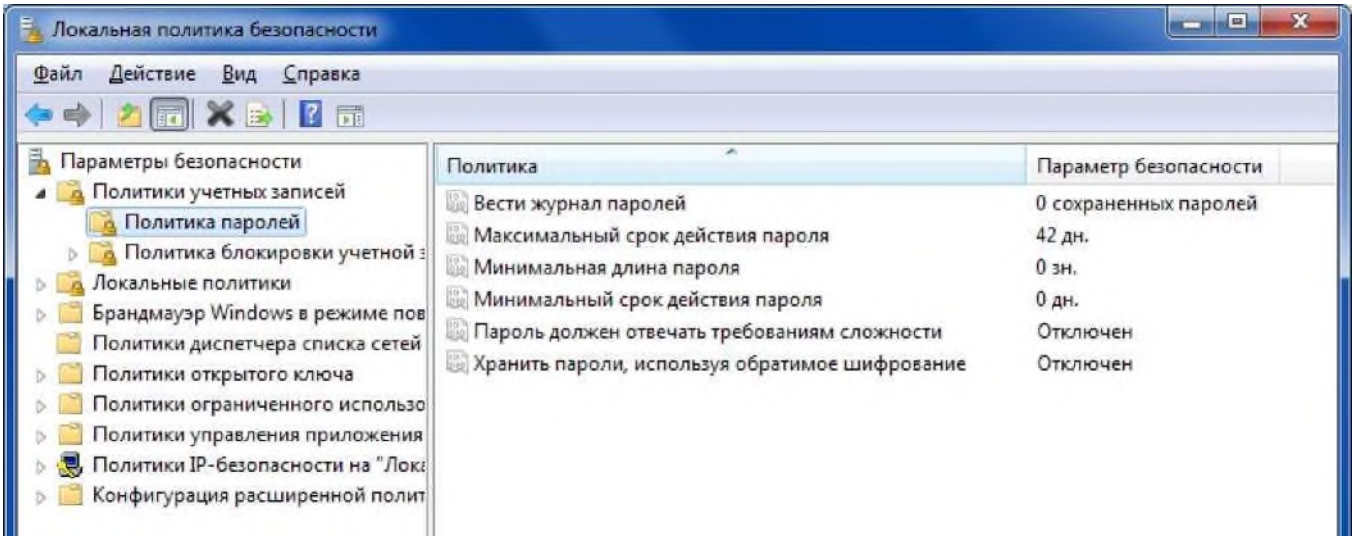
**Алгоритм выполнения работы:**

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку Пуск на панели задач.
2. Откройте меню Настроить - Панель управления.
3. В открывшемся окне выберите ярлык Администрирование - Локальная политика безопасности .




4. Выберите пункт **Политика учетных записей** (этот пункт включает два подпункта: **Политика паролей** и **Политика блокировки учетной записи**).
5. Откройте подпункт Политика паролей. В правом окне появится список настраиваемых параметров.



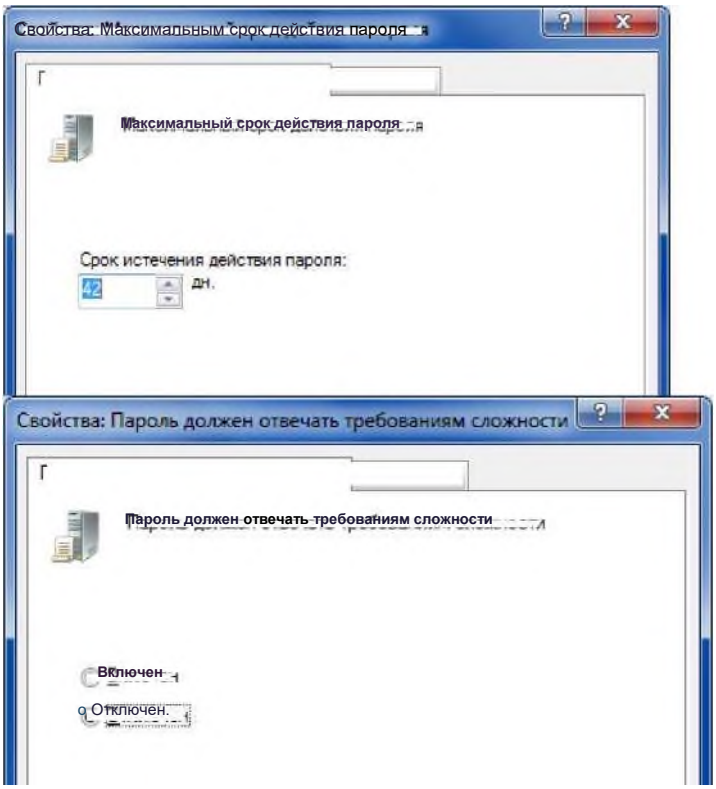

6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Возможные значения параметров приведены в таблице №1.

Таблица №1 - Значения параметров Политики паролей

| Параметр | Значение |
|---|---|
| Требовать повторяемости паролей | Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24. |
| Максимальный срок действия пароля | Определяет период времени (в Днях), в течение которого можно использовать пароль, чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0. |
| Минимальный срок действия пароля. | Определяет период времени (в Днях), в течение которого можно использовать пароль, чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0. |

| | |
|---|---|
| Минимальная длина пароля. | Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0 |
| Пароль должен отвечать требованиям сложности | Определяет, должны ли отвечать пароли требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. 0 Пароль не может содержать имя учетной записи пользователя или какую-либо его часть; 0 Пароль должен состоять не менее чем из 6 символов; 0 В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1. Прописные буквы английского алфавита от A до Z;<br>2. Строчные буквы английского алфавита от A до Z;<br>3. Символы не принадлежащие алфавитно-цифровому набору (например, !,$,#,%). |
| Хранить пароли всех пользователей в домене, используя обратимое шифрование. | Определяет, следует ли в системах Windows хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, это всё равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля. |

7. Ознакомитесь со свойствами всех параметров.
8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щёлкните на изменяемом параметре).
9. В результате этого действия появится одно из окон.




Параметр локальной безопасности Объяснение
Параметр локальной безопасности Объяснение

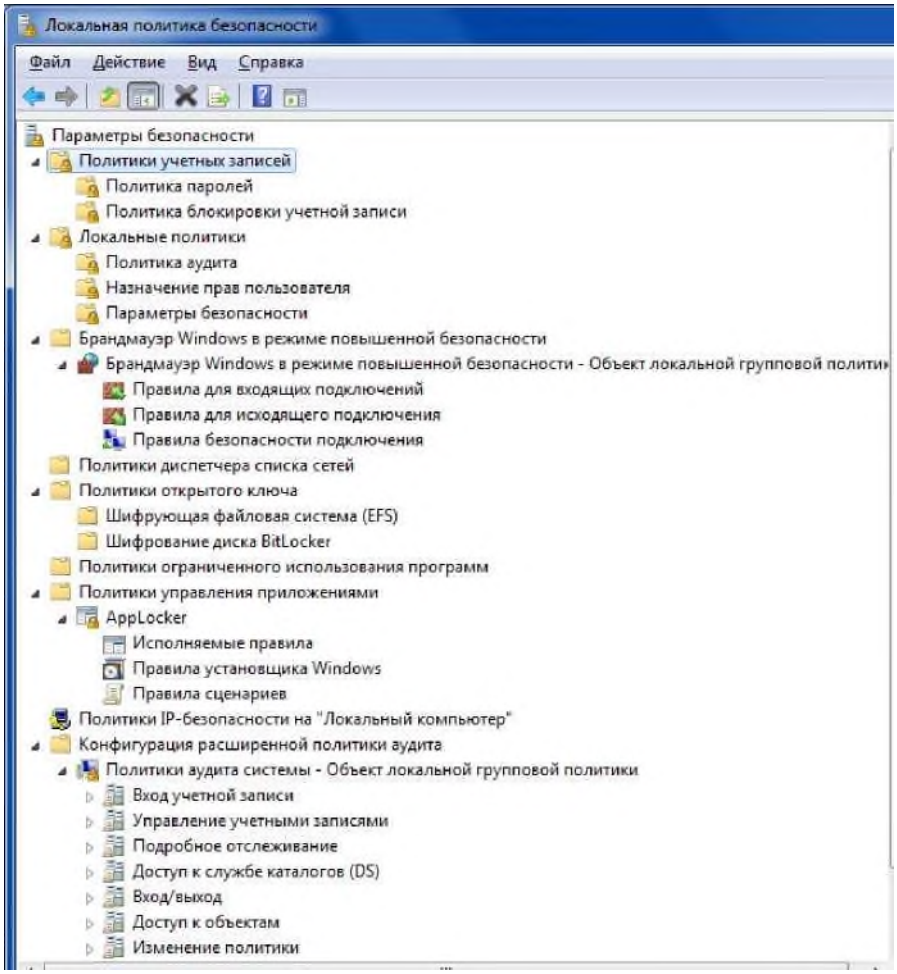
10. Измените, значение параметра и нажмите Ок.
11. Например (обязательно выполнить и сохранить), выберите параметр Требовать неповторимости паролей и измените его значение на 1.

12. Для настройки Политики блокировки учетной записи выберите этот подпункт и откройте его.
13. Значения параметров данного подпункта Политики учетной записи приведены в таблице №2.

Таблица №2

| Параметр | Значение |
|---|---|
| Пороговое значение блокировки | Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока не будет сброшена администратором или пока не истечёт её интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0. |
| Блокировка учетной записи | Определяет число минут, в течении которых учетная запись остаётся блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99999 минут. Если установить Значение 0, учетная запись будет блокирована на всё время до тех пор, пока администратор не разблокирует её явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса. |
| Сброс счетчика блокировки | Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала Блокировка учетной записи на. |

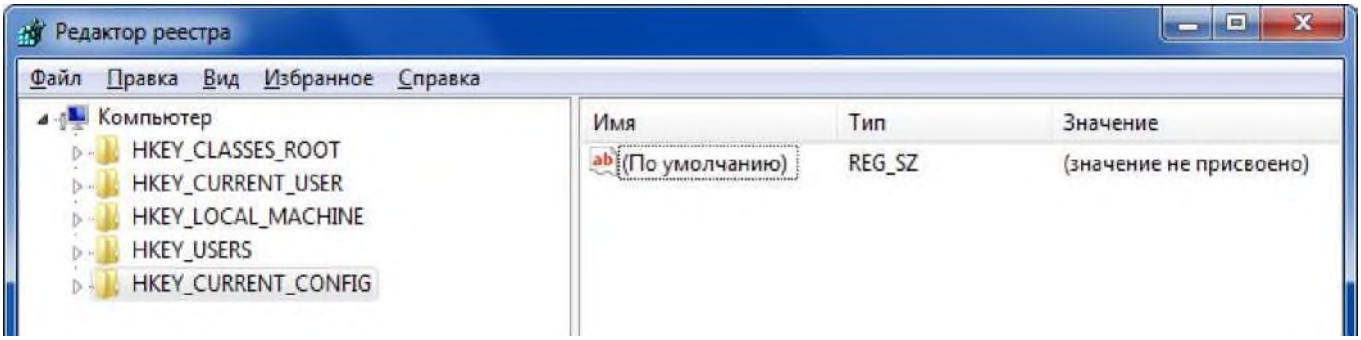
14. Ознакомитесь со свойствами всех параметров.
15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.



**Задания для самостоятельной работы:**

1. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.
2. После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.
3. Проведите эксперименты с другими параметрами Политики учетных записей.
4. Поработайте с параметрами безопасности регистра. Выполните задания 4.1-4.15:

Редактор реестра (**regedit**) - инструмент, предназначенный для **опытных пользователей**. Этот инструмент предназначен для просмотра и изменения параметров в системном реестре, в котором содержатся сведения о работе. Изменения параметров безопасности реестра так же способны повысить уровень безопасности данных.




**Отключить редактирование меню Пуск**
Откройте раздел
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
и создайте в нем параметр типа DWORD с именем **NoChangeStartMenu** и значение параметра должно быть равно **1**

**Запрет запуска Панели управления**
В разделе
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
создайте параметр типа DWORD с именем **NoControlPanel** и установите значение параметра **1**

**Отключить запуск Диспетчера задач**
В разделе:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
создайте дополнительный подраздел с именем **System** (если его нет) и в этом разделе создайте параметр типа DWORD с именем **DisableTaskMgr** и значение **1**. Теперь при вызове Диспетчера задач этот пункт в меню **Панели задач** будет не активен

**Отключить автозагрузку USB-устройст, приводов, съемных дисков, сетевых дисков.**
Открываем раздел реестра
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
и создаем новый раздел с именем **Explorer** В этом разделе создаем параметр типа DWORD с именем **NoDriveTypeAutoRun** Значение параметра выбираем на своё усмотрение
**0x1** - отключить автозапуск на приводах неизвестных типов
**0x4** - отключить автозапуск съёмных устройств **0x8** - отключить автозапуск Несъёмных устройств
**0x10** - отключить автозапуск сетевых дисков
**0x20** - отключить автозапуск CD-приводов
**0x40** - отключить автозапуск RAM-дисков

**0x80** - отключить автозапуск на приводах неизвестных типов **0xFF** - отключить автозапуск вообще всех дисков

**Отключить просмотр общих ресурсов анонимным пользователям**
В разделе
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa измените значение параМетра**restrictanonymous** на **1**

**Отключаем «расшаренные» административные ресурсы C$, D$, ADMIN$**
Открываем редактор реестра и в разделе
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters создаем параметр типа DWORD и именем **AutoShareWks**. Значение параметра - **0**. Теперь если открыть Управление компьютером - Общие папки - Общие ресурсы, то кроме IPC$ ничего не должно быть.

**Отключение запуска Командной строки**
Откройте раздел
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows и создайте дополнительный подраздел System с параметром типа DWORD **DisableCMD**, значение параметра могут иметь следующие:
0 - разрешить использовать Командную строку
1 - запретить использовать Командную строку
2 - разрешить запуск командных файлов

**Отключить изменение обоев рабочего стола**
В разделе
HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies создайте подраздел **ActiveDesktop** и в нем параметр типа DWORD с именем
**NoChangingWallPaper** со значением 1

**Отключение Рабочего стола**
Откройте раздел
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer и создайте в нем параметр типа DWORD с именем **NoDesktop** и значением **1**. Вернуть **Рабочий стол** можно изменить параметр на **0** или удалить его.

**Запрет запуска Редактора реестра (regedit)**
Откройте раздел
HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies
и создайте в нем подраздел **System**. В этом подразделе создайте параметр типа DWORD с именем **DisableRegistryTools**с именем **1**.
**Примечание**. Если не сделать экспорт этого раздела где параметр DisableRegistryTools имеет значение **0**, или не создать заранее reg-файл, для возврата запуска Редактора реестра, то запуск будет невозможен. Для создания reg-файла откройте блокнот и скопируйте в него эти строки
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
«DisableRegistryTools»=dword: 00000000
Сохраните этот файл под любым, удобным для вас именем, и поменяйте расширение txt на reg. Теперь для возврата запуска **Редактора реестра** запустите этот файл.

**Отключение автоматического обновления Internet Explorer**
Откройте раздел
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

и установите значение параметра **NoUpdateCheck** равное **1**

**Запретить автоматическое обновление Media Player**
Откройте раздел
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\PlayerUpgrade
и создайте строковый параметр **AskMeAgain** со значение **no**. И проверьте параметр **EnableAutoUpgrade**, его значение установите **no**

**Запрет запуска определенных программ**
Задать список программ, которые не будут запущены пользователем можно в разделе HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun. Если подраздела **DisallowRun** нет - создайте его. Создайте строковый параметр (REZ_SZ) с именем**1** (порядковый номер программ, вторая программа будет с именем 2, и т. д) Значени е параметров - это имя программы с расширение exe, например AkelPad. Exe

**Отключение сообщения о недостатке свободного места**
Откройте раздел
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer, создайте в нем параметр типа DWORD с именем **NoLowDiskSpaseChecks** и установите значение параметра **1**
Откройте раздел
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\Gather
и измените значение параметра **LowDiskMinimumMBytes** на **0**
Откройде раздел
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\Gathering Manager

и измените значение параметра **BackOffLowDiskThresholdMB** на **0 Примечание**: Чтобы менять значения в разделе могут понадобится права администратора. Для этого надо сделать следующее: Пуск - Все программы - Стандартные. Правой клавишей на **Командная строка** - Запуск от имени администратора. Ведите команду **regedit**. Теперь на разделе **Gathering Мападег**кликните правой кнопкой и выберите **Разрешения**. В открывшемся окне выберите **Дополнительно**. Перейдите во вкладку **Владелец** и выберите свою учетную запись (У вас должны быть права администратора). **Применить** и ОК.
После этих изменений, если на диске будет меньше 10% свободно места, не будет работать система восстановления и дефрагментация диска.

**Запрет на установку простого пароля**
Дополнительная функция для усложнения пароля. По мимо установки минимальной длины, это параметр задает еще и буквенно-цифровой пароль. Откройте раздел HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies, создайте подраздел **Network** і в этом подразделе создайте параметр типа DWORD с именем **AlphanumPwds** и значение параметра установите **1**

## КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое аутентификация и идентификация?
2. Для чего применяются эти механизмы?
3. Что можно настроить с помощью вкладки Локальные политики безопасности?
4. Для чего предназначен реестр?
5. Как зайти в Редактор реестра?
6. Как запретить запуск определённых программ?

# Лабораторная работа №4 «Групповые политики в Windows »

**Цель работы:** Познакомиться с редактором локальных групповых политик и освоить работу по настройке локальных групповых политик.
Время 2 часа

## Теоретическая часть

Групповые политики нужны для управления операционной системы Windows. Они применяются во время персонализации интерфейса, ограничения доступа к определенным ресурсам системы и многого другого.

Используют данные функции преимущественно системные администраторы. Они создают однотипную рабочую среду на нескольких компьютерах, ограничивают доступ пользователям. В этой статье мы подробно разберем групповые политики в Windows , расскажем про редактор, его настройку и приведем некоторые примеры групповых политик.

### Редактор групповой политики

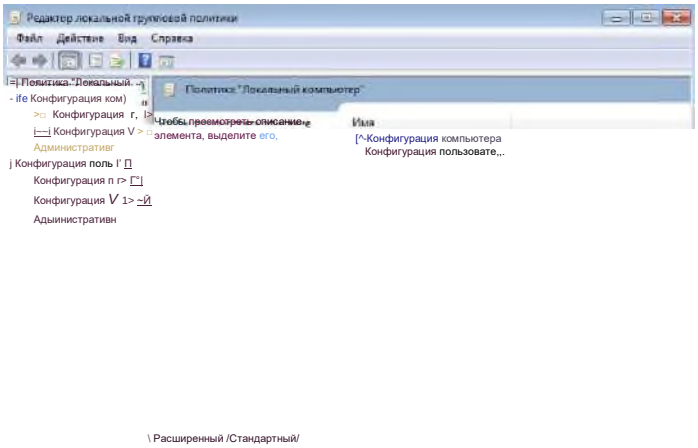
В Windows Домашняя Базовая/Расширенная и Начальная редактор групповых политик просто отсутствует. Разработчики позволяют использовать его только в профессиональных версиях Windows, например, в Windows Максимальная.

Запуск редактора групповой политики

Для перехода к среде работы с параметрами и настройками необходимо:

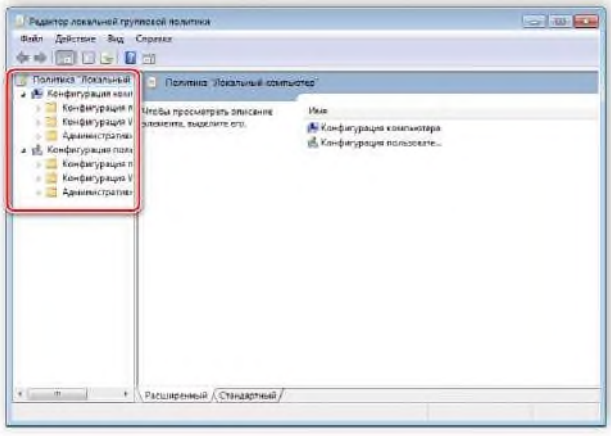
Зажать клавиши **Win + R**, чтобы открыть **«Выполнить»**.

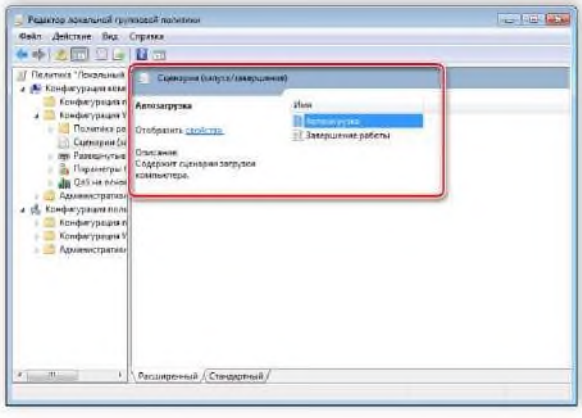
Напечатать в строке **gpedit.msc** и подтвердить действие, нажав **«ОК»**. Далее запустится новое окно.




### Работа в редакторе

Окно редактора групповых политик разделяется на две части.



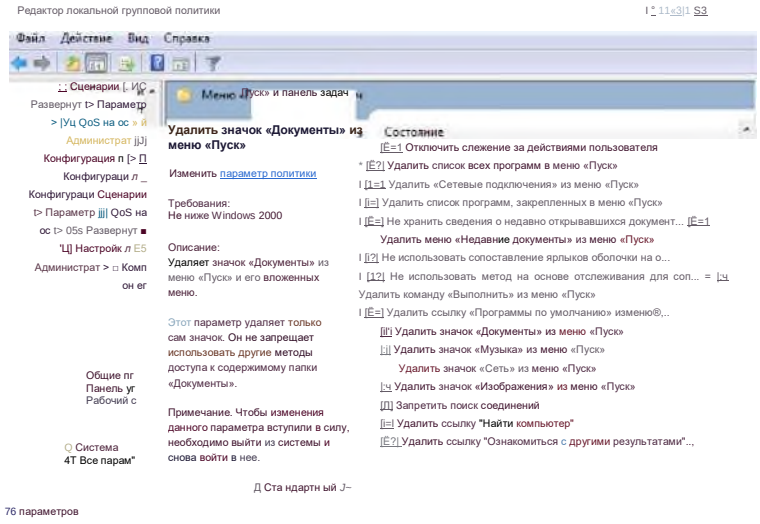



Слева располагается структурированные категории политик.

Они в свою очередь делятся еще на две различные группы - настройка компьютера и настройка пользователя. В правой части отображается информация о выбранной политике из меню слева.

Работа в редакторе осуществляется путем перемещения по категориям для поиска необходимой настройки.

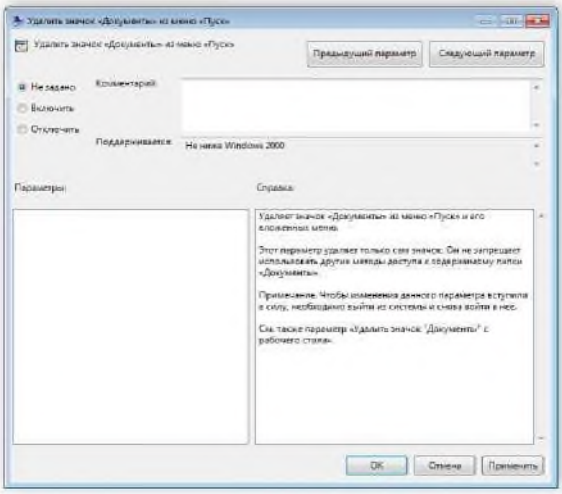
Например, **«Административные шаблоны»** в **«Конфигурации пользователя»** и перейдите в папку **«Меню «Пуск» и диспетчер задач»**. Теперь справа отобразятся параметры и их состояния.




Нажмите на любую строку, чтобы открыть ее описание.

## Настройки политики

Каждая политика доступна для настройки. Открывается окно редактирования параметров по двойному щелчку на определенную строку. Вид окон может отличаться, все зависит от выбранной политики.

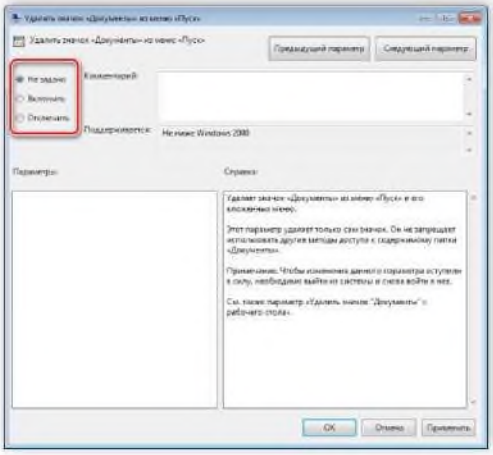



Стандартное простое окно имеет три различных состояния, которые настраиваются пользователем. Если точка стоит напротив **«Не задано»**, то политика не действует.

**«Включить»** - она будет работать и активируются настройки. **«Отключить»** - находится в

рабочем состоянии, однако параметры не применяются.

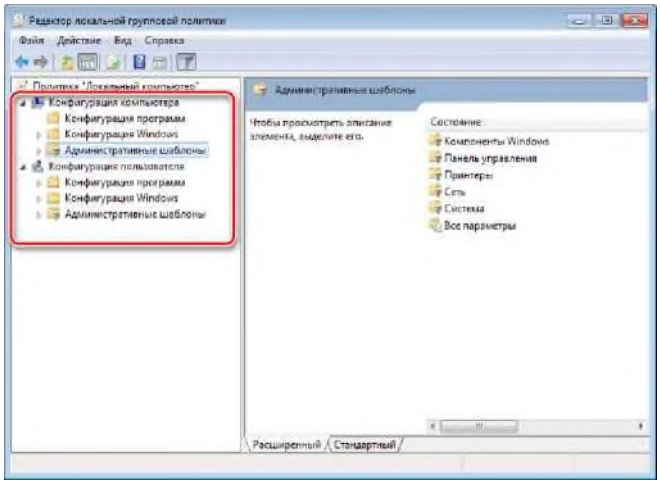
Рекомендуем обратить внимание на строку **«Поддерживается»** в окне, она показывает, на

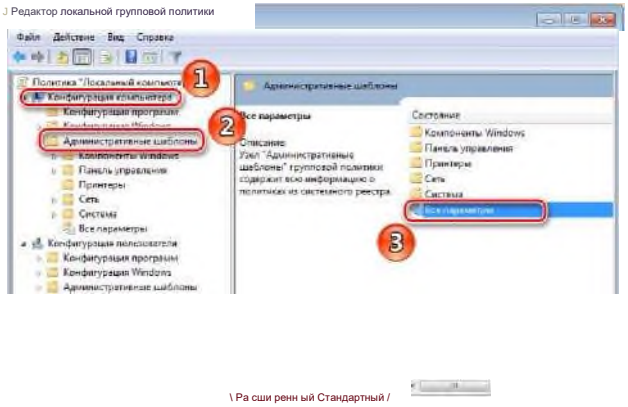


какие версии Windows распространяется политика.

**Фильтры политик**

Существует множество различных настроек и параметров, их больше трех тысяч, все они разбросаны по отдельным папкам, а поиск осуществляется вручную. Однако данный процесс упрощается благодаря структурированной группе из двух ветвей, в которых расположились тематические папки.





Например, в разделе **«Административные шаблоны»**, в любой конфигурации, находятся политики, которые никак не связаны с безопасностью. В этой папке находится еще несколько папок с определенными настройками, однако можно включить полное отображение всех параметров, для этого нужно нажать на ветвь и выбрать пункт в правой части редактора **«Все параметры»**, что приведет к открытию всех политик данной ветви.

Экспорт списка политик

Если все-таки появляется необходимость найти определенный параметр, то сделать это можно только путем экспорта списка в текстовый формат, а потом уже через, например Word, осуществлять поиск.

В главном окне редактора есть специальная функция **«Экспорт списка»**, он переносит все политики в формат TXT и сохраняет в выбранном месте на компьютере.

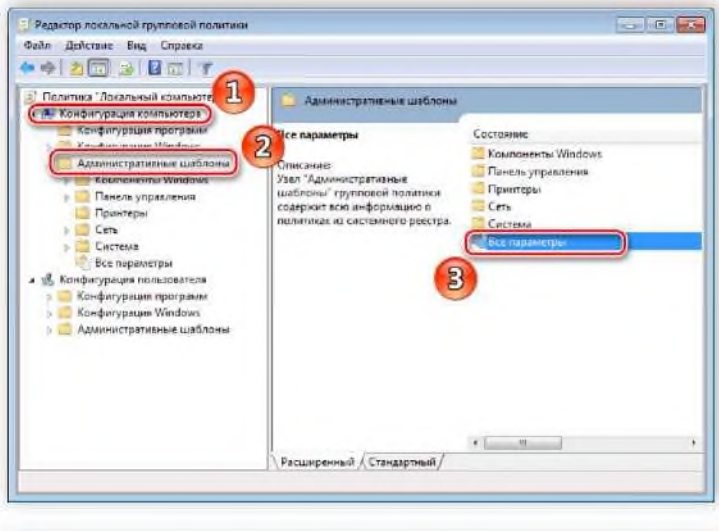
Применение фильтрации

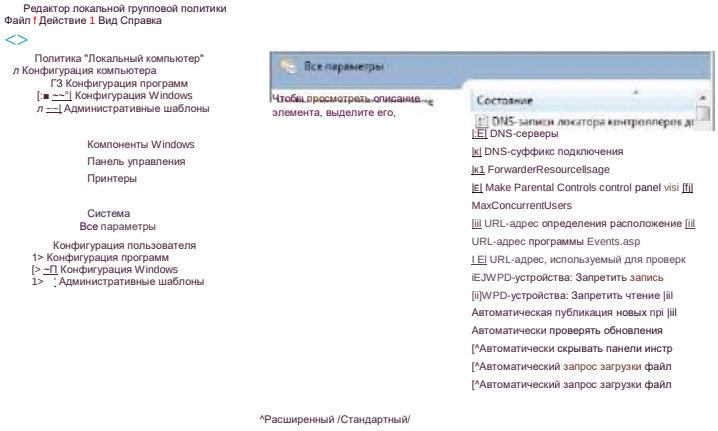
Через **«Все параметры»** и функцию фильтрация лишнее откидывается путем применения

фильтров, отображаться будут только необходимые политики.

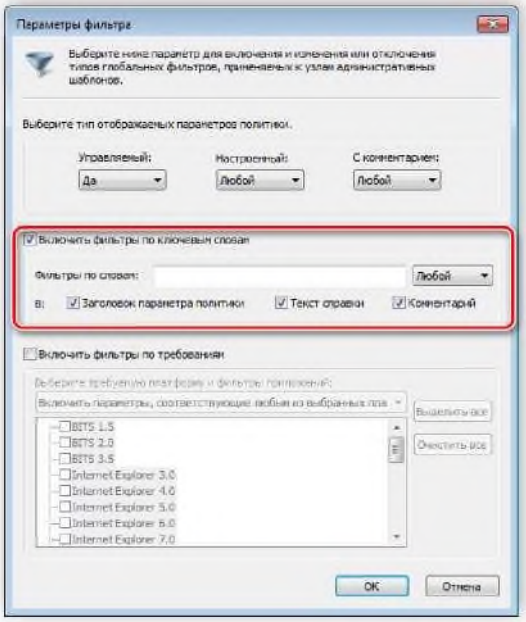
Для этого подробнее рассмотрим процесс применения фильтрации:

1. Выберите, например, **«Конфигурация компьютера»**, откройте раздел **«Административные шаблоны»** и перейдите в **«Все параметры»**.
2. Разверните всплывающее меню **«Действие»** и перейдите в **«Параметры фильтра»**.

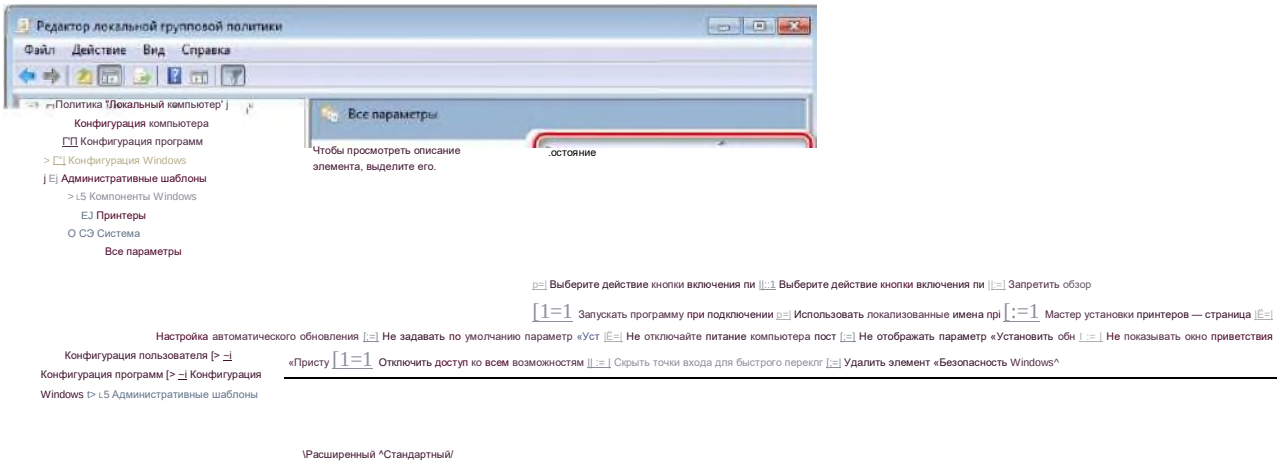


Поставьте галочку возле пункта **«Включить фильтры, по ключевым словам,»**. Здесь имеется несколько вариантов подбора соответствий. Откройте всплывающее меню напротив строки ввода текста и выберите **«Любой»** - если нужно отображать все политики, которые соответствуют хотя бы одному указанному слову, **«Все»** - отобразит политики, содержащие текст из строки в любом порядке, **«Точный»** - только параметры, точно соответствующие заданному фильтру по словам, в правильном порядке. Флажками снизу строки соответствий отмечаются места, где будет осуществляться выборка.




3. Нажмите **«ОК»** и после этого в строке **«Состояние»** отобразятся только подходящие параметры.




В том же всплывающем меню **«Действие»** ставится или убирается галочка напротив строки **«Фильтр»**, если нужно применить или отменить заранее заданные настройки подбора соответствий.

Принцип работы с групповыми политиками

Рассматриваемый в этой статье инструмент позволяет применять множество самых разнообразных параметров. К сожалению, большинство из них понятно только профессионалам, использующим групповые политики в рабочих целях. Однако и обычному пользователю есть что настроить, используя некоторые параметры. Разберем несколько простых примеров.

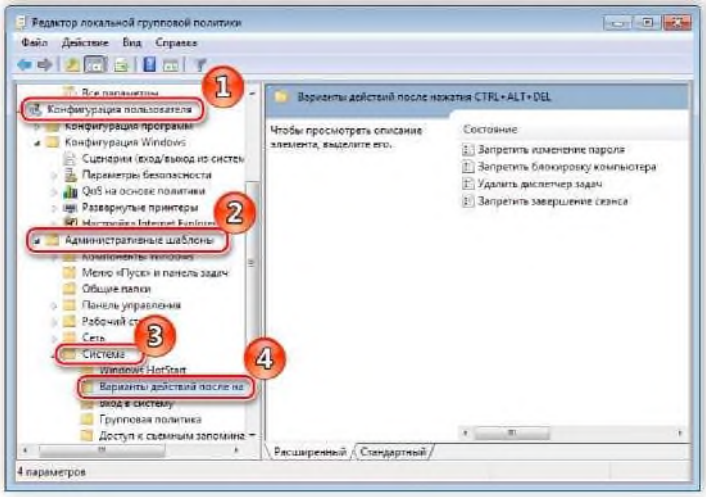
**Изменение окна безопасности Windows**

Если в Windows зажать сочетание клавиш **Ctrl + Alt + Delete**, то будет запущено окно безопасности, где осуществляется переход к диспетчеру задач, блокировка ПК, завершение сеанса системы, смена профиля пользователя и пароля.

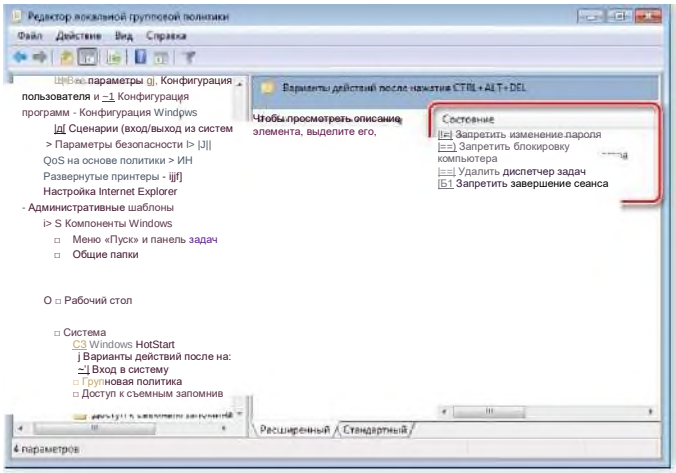
Каждая команда за исключением **«Сменить пользователя»** доступна для редактирования путем изменения нескольких параметров. Выполняется это в среде с параметрами или путем изменения реестра. Рассмотрим оба варианта.

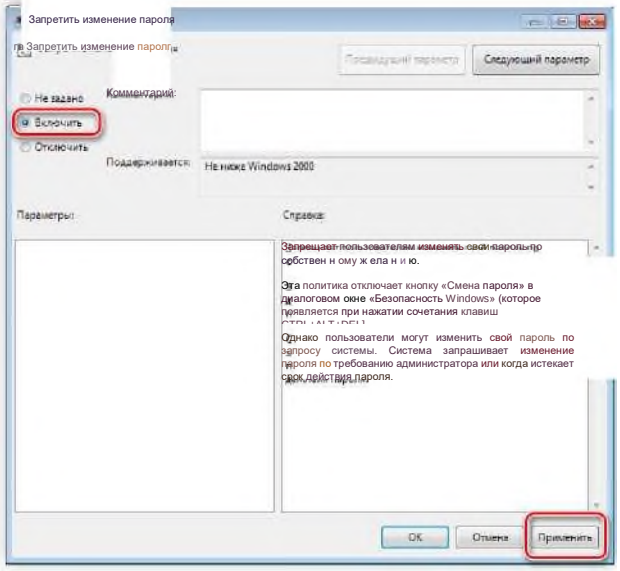
1. Откройте редактор.

2. Перейдите в папку **«Конфигурация пользователя»**, **«Административные шаблоны»**, **«Система»** и **«Варианты действий после нажатия Ctrl + Alt + Delete»**.




Откройте любую необходимую политику в окне справа.




В простом окне управления состоянием параметра поставьте галочку напротив **«Включить»** и не забудьте применить изменения.

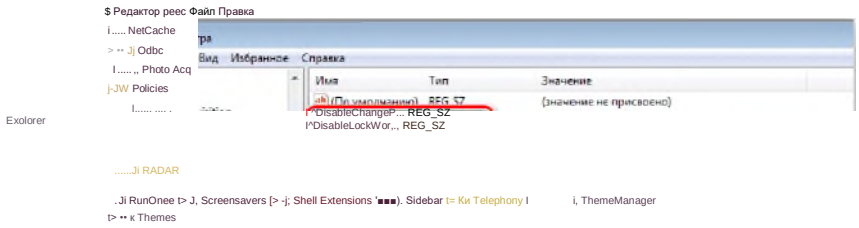
Пользователям, у которых нет редактора политик, все действия нужно будет выполнять через реестр.

Давайте рассмотрим все действия пошагово:

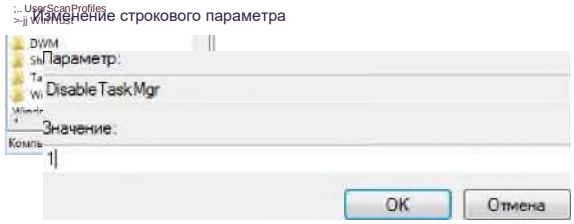
1. Перейдите к редактированию реестра.

2. Перейдите к разделу **«System»**. Он находится по этому ключу:
**HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System**

3. Там вы увидите три строки, отвечающие за появление функций в окне безопасности.



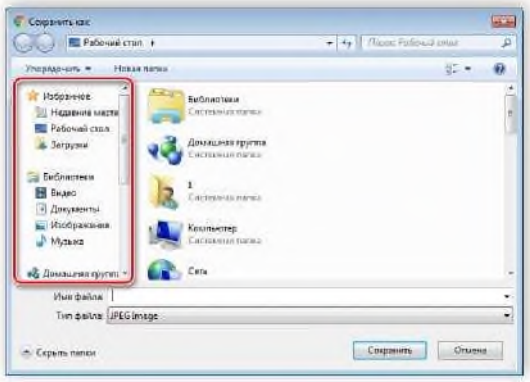

Откройте необходимую строку и поменяйте значение на **«1»**, чтобы активировать параметр.



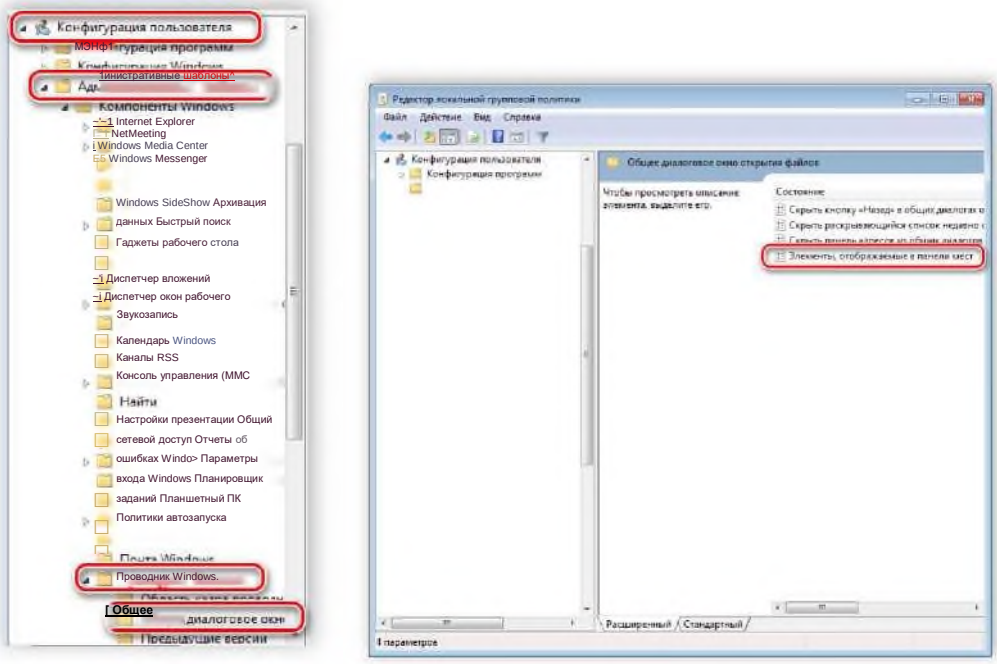

После сохранения изменений деактивированные параметры больше не будут отображаться в окне безопасности Windows .

Изменения панели мест

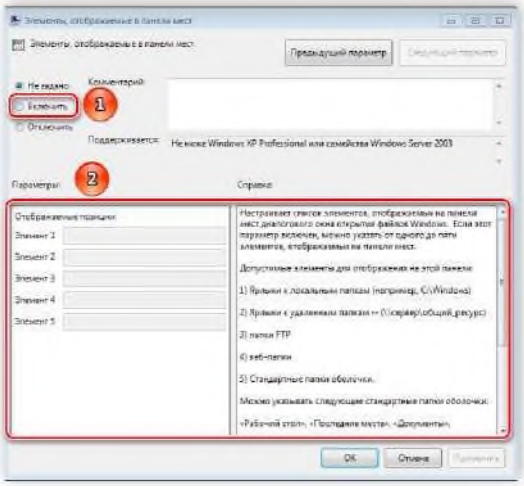
Многие используют диалоговые окна **«Сохранить как»** или **«Открыть как»**. Слева отображается навигационная панель, включая раздел **«Избранное»**. Данный раздел настраивается стандартными средствами Windows, однако это долго и неудобно. Поэтому лучше воспользоваться групповыми политиками для редактирования отображения значков в данном меню. Редактирование происходит следующим образом:



1. Перейдите в редактор, выберите **«Конфигурация пользователя»**, перейдите к **«Административные шаблоны»**, **«Компоненты Windows»**, **«Проводник»** и конечной папкой будет **«Общее диалоговое окно открытия файлов»**.




2. Здесь вас интересует **«Элементы, отображаемые в панели мест»**.
3. Поставьте точку напротив **«Включить»** и добавьте до пяти различных путей сохранения в соответствующие строки. Справа от них отображается инструкция правильного указания путей к локальным или сетевым папкам.

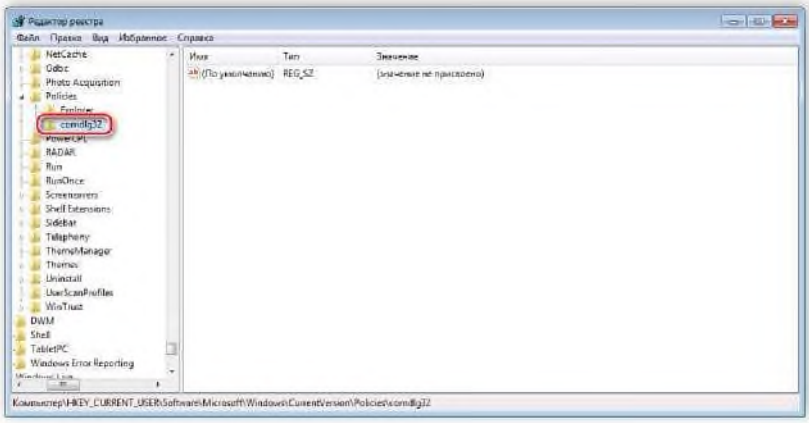



Теперь рассмотрим добавление элементов через реестр для пользователей, у которых отсутствует редактор.

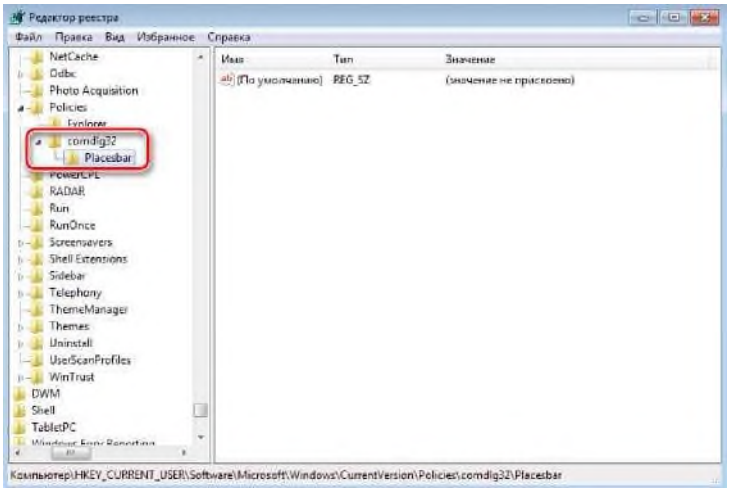
1. Перейдите по пути:

HKCU\Software\Microsoft\Wmdows\CuirentVersion\Policies\

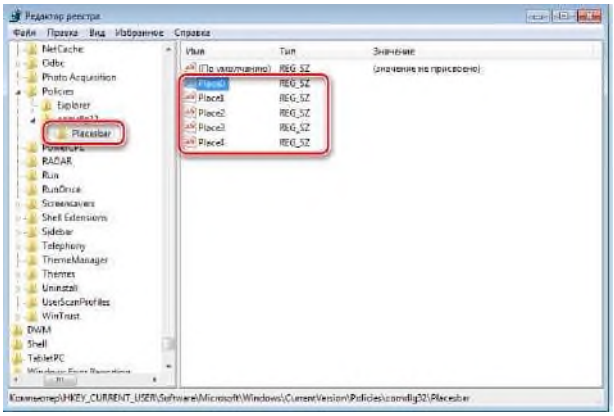
2. Выберите папку **«Policies»** и сделайте в ней раздел **comdlg32**.



3. Перейдите в созданный раздел и сделайте внутри него папку **Placesbar**.




4. В этом разделе потребуется создать до пяти строковых параметров и назвать их от **«PlaceO»** до **«Place4»**.




5. После создания откройте каждый из них и в строку введите необходимый путь к папке.

Изменение строкового параметра

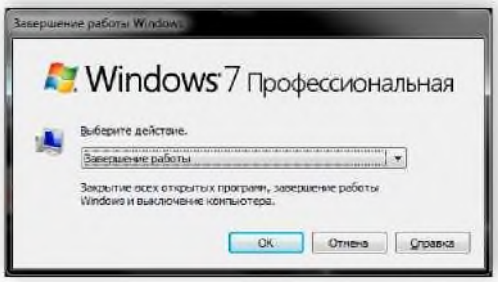
Параметр:
Place 3

Значение:
C:\Windows|

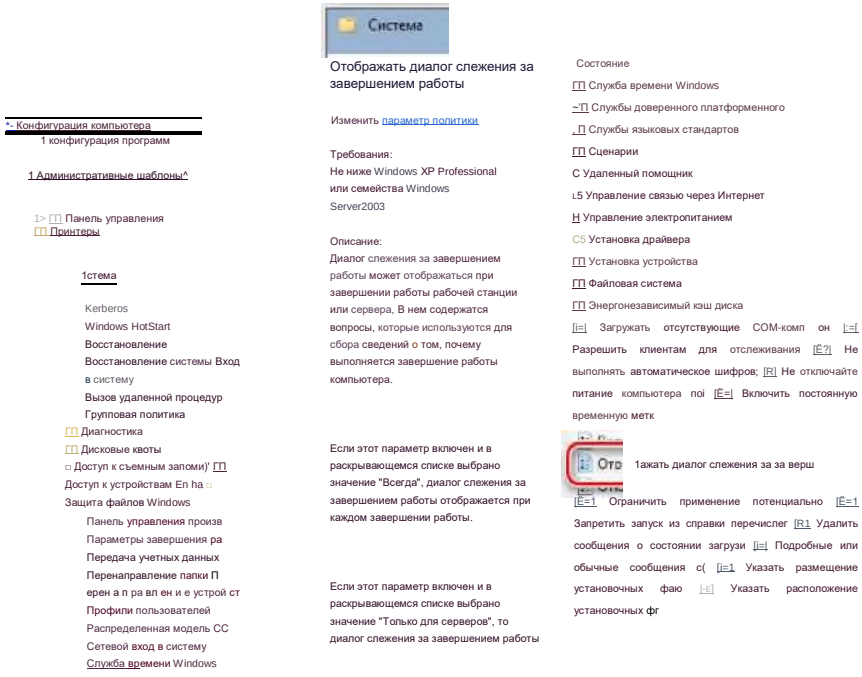
OK | Отмена

Слежение за завершением работы компьютера

Когда вы завершаете работу за компьютером, выключение системы происходит без показа дополнительных окон, что позволяет не быстрее выключить ПК. Но иногда требуется узнать почему происходит выключение или перезапуск системы. В этом поможет включение специального диалогового окна. Включается оно с помощью редактора или путем изменения реестра.

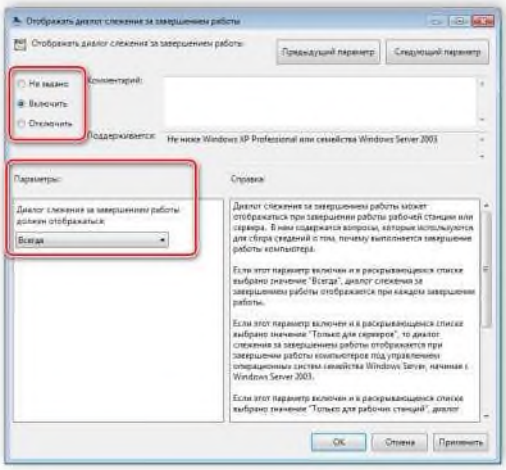



1. Откройте редактор и перейдите к **«Конфигурация компьютера»**, **«Административные шаблоны»**, после чего выберите папку **«Система»**.




2. В ней нужно выбрать параметр **«Отображать диалог слежения за завершением работы»**.

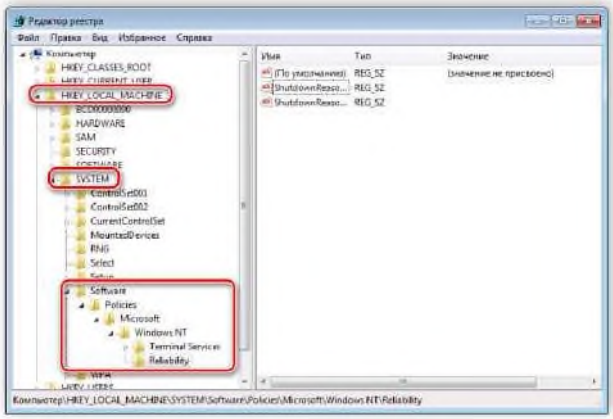
3. Откроется простое окно настройки, где необходимо поставить точку напротив **«Включить»**, при этом в разделе параметры во всплывающем меню необходимо указать **«Всегда»**. После не забудьте применить изменения.



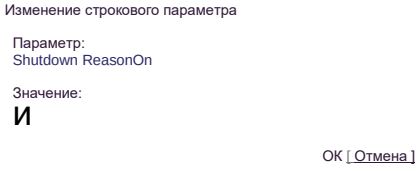
Данная функция включается и через реестр. Вам нужно совершить несколько простых действий:

1. Запустите реестр и перейдите по пути:

HKLM\Software\Policies\Microsoft\Windows NT\Reliability



2. Найдите в разделе две строки: **«ShutdownReasonOn»** и **«ShutdownReasonUI»**.
3. Введите в строку с состоянием **«1»**.




**Задание на самостоятельную работу с групповыми политиками**

В отчете отобразить путь, порядок и выполненные действия по заданиям

| № пп | Режим работы с консолью | Параметры групповой политики |
|---|---|---|
| 1 | Авторский | Запретить редактирование реестра. Ограничить размер профиля пользователя значением 5 МБ |
| 2 | Пользовательский - | Запретить использование командной строки. Запретить |

| | | |
|---|---|---|
| | полный доступ | изменение рисунка рабочего стола |
| 3 | Пользовательский - многооконный | Запретить использование сочетаний клавиш, включающих кнопку «Windows». Удалить имя пользователя из меню «Пуск» |
| 4 | Пользовательский - однооконный | Запретить использование диспетчера задач. Установить обязательный запрос пароля при выходе из спящего режима |
| 5 | Авторский | Запретить доступ к «Панели управления». Запретить запуск «Блокнота» |
| 6 | Пользовательский - полный доступ | Установить обязательный запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню «Пуск» |
| 7 | Пользовательский - многооконный | Скройте диск D: (CD-привод) из окна «Мой компьютер». Удалить значок «Мои документы» с «Рабочего стола» |
| 8 | Пользовательский - однооконный | Удалите «Общие документы» из окна «Мой компьютер». Скрыть общие группы программ из меню «Пуск» |
| 9 | Авторский | Запретите доступ к диску C: из окна «Мой компьютер». Удалить «Сетевые подключения» из меню «Пуск» |
| 10 | Пользовательский - полный доступ | Запретить вызов «Свойств» объекта «Мой компьютер». Установить очистку списка последних использованных документов при выходе из системы |

**Контрольные вопросы**

1. Для чего предназначена групповая политика безопасности ОС Windows ?
2. Какие настройки включает окно локальных групповых политик безопасности ОС Windows ?
3. Что такое Административные шаблоны локальных групповых политик безопасности ОС Windows ?
4. Какие ключи реестра доступны для редактирования локальных групповых политик безопасности ОС Windows ?

## Лабораторная работа №5 Настройка брандмауэр Windows.

**Цель работы**: изучить настройки брандмауэра ОС и его настройки для обеспечения защиты информации

Время 2 часа

**Теоретическая часть**

Брандмауэр или фаерволл — это системная утилита (сетевой экран) для контроля и фильтрации входящего/исходящего трафика. Брандмауэр стал неотъемлемой частью операционных систем Windows, начиная с версии XP SP2.

Брандмауэр может быть как для отдельного компьютера, так и для всей локальной сети. В общем случае брандмауэр выполняет следующие функции:

• **Защита системы от внешних атак.** В список таких угроз входят сканирование портов, IP-спуффинг, DDoS-атаки, подбор паролей.

• **Блокировка утечек.** Если вредоносное ПО проникло в компьютер через USB или CD, то брандмауэр при соответствующих настройках предотвратит дальнейшее распространение по сети.

• **Контроль приложений.** Брандмауэр позволяет настроить доступ в сеть для каждого отдельного приложения.

• **Зональная защита.** Обеспечение различных уровней доступа в рамках локальной сети.

• **Протоколирование и предупреждение.** Брандмауэр не только собирает статистику, но и предупреждает пользователей о различных действиях.

Брандмауэр есть не только в операционных системах. ПО маршрутизаторов также включает встроенный фаерволл, который обычно настраивается через

Брандмауэр способен анализировать абсолютно весь исходящий и входящий трафик, а также динамически открывать порты для конкретных приложений. Что конкретно из трафика будет блокировать брандмауэр, зависит от пользовательских настроек, а также внутренней базы, которая позволяет идентифицировать потенциально нежелательное содержимое.

Фильтры работают на нескольких уровнях модели OSI. Например, брандмауэр способен выполнять фильтрацию пакетов (сетевой уровень), контролировать шлюзы (сеансовый и прикладной уровни). Для каждого уровня используется свой гибкий фильтр.

Например, на сетевом уровне брандмауэр анализирует заголовок IP-пакета: адреса получателя и отправителя, информацию о протоколе и приложении, номера портов. Собранная информация сравнивается с таблицей правил, после чего принимается решение — пропустить или отбраковать пакет.

| **Модель OSI** | | |
|---|---|---|
| **Тип данных** | **Уровень** | **Функции** |
| Данные | 7. Прикладной | Доступ к сетевым службам |
| | 6. Представительский | Представление и шифрование данных |
| | 5. Сеансовый | Управление сеансом связи |
| Сегменты | 4. Транспортный | Прямая связь между конечными пунктами |
| Пакеты | 3. Сетевой | Определение маршрута и логическая адресация |
| Кадры | 2. Канальный | Физическая адресация |
| Биты | 1.Физический | Работа со средой передачи и двоичными данными |

Например, известный вирус WannaCry атаковал TCP-порт 445, который на большинстве компьютеров был открыт.

Брандмауэр — это первая линия обороны вашего компьютера, которая позволяет с высокой эффективностью справиться со следующими видами угроз:

- **Компьютерные черви и некоторые вирусы.** У червей собственный код, поэтому им не нужны определенные файлы для заражения. С этой точки зрения такие угрозы более опасны.

- **Взлом с использованием удаленного рабочего стола.** При отключенном брандмауэре злоумышленники могут получить доступ к вашим файлам и даже перехватить управление.

- **Различный шпионский софт.** Некоторые программы без вашего ведома отправляют информацию о системе или действиях самого пользователя сторонним лицам. Брандмауэр за счет ограничения исходящего трафика может предотвратить утечку данных.

- **Доступ через бэкдоры.** Хакеры часто используют различные уязвимости в ПО, в том числе открытые порты. Брандмауэр блокирует любой неавторизированный трафик, уменьшая шанс воспользоваться такими уязвимостями.

- **DDoS-атаки.** Используемые алгоритмы эффективно определяют подобные атаки, анализируя повторяющиеся запросы с определенных ip-адресов.

Брандмауэр не способен обеспечить полную защиту вашего компьютера. Есть ряд угроз, с которыми ему не справиться.

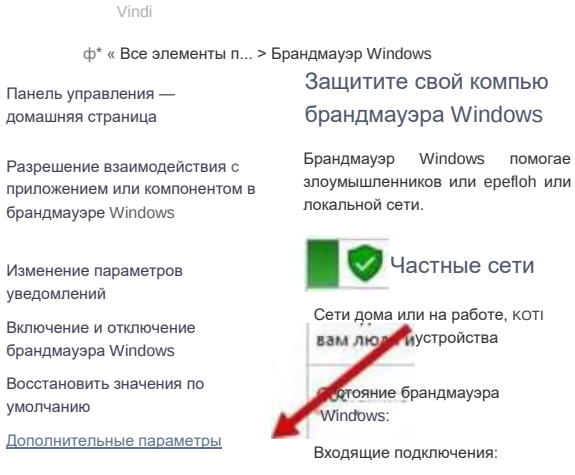
Первое — вирусы и черви, которые уже попали на компьютер. Брандмауэр сканирует только сетевой трафик и не анализирует непосредственно файловую систему. Именно поэтому на компьютерах обязательно должен быть полноценный антивирус, который обнаруживает и удаляет уже действующие вирусы.

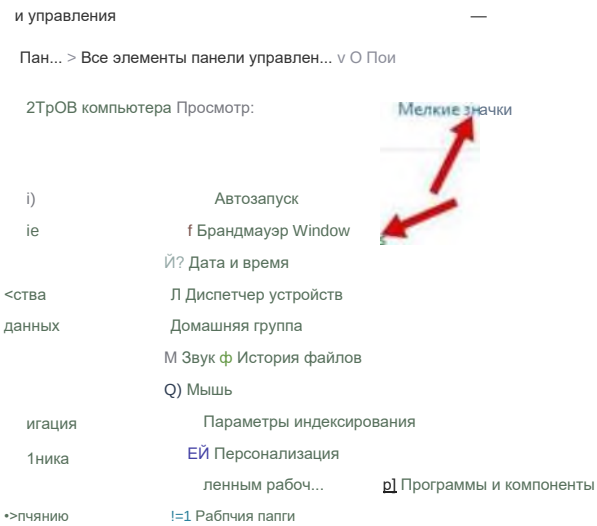
**Брандмауэр не способен защитить вас от вредоносных ссылок,** которые вы получаете через спам в электронной почте. Также компьютер может заразиться вредоносным ПО не через сеть — USB-накопители, оптические диски, карты памяти и так далее. Чтение и копирование файлов с этих носителей брандмауэр никак не контролирует.

**Практические задания**

**Первичный запуск и настройка**

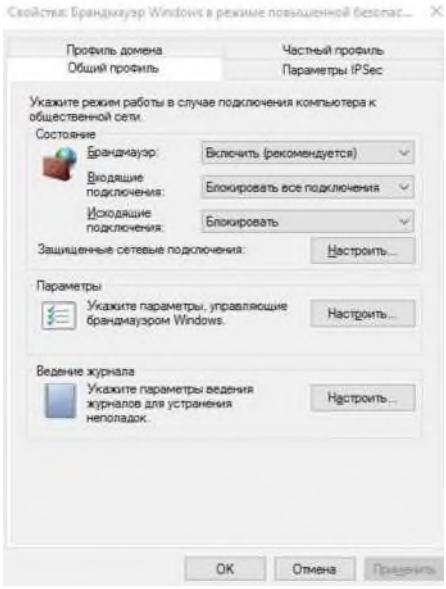
Открыть "**Панель управления**", в которой кликаем по "**Брандмауэр Windows**": Далее выбираем мышкой в соответствующий пункт (**Дополнительные параметры**):





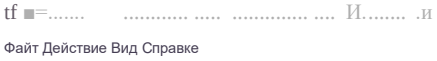

Брандмауэр Windows и настройка профилей

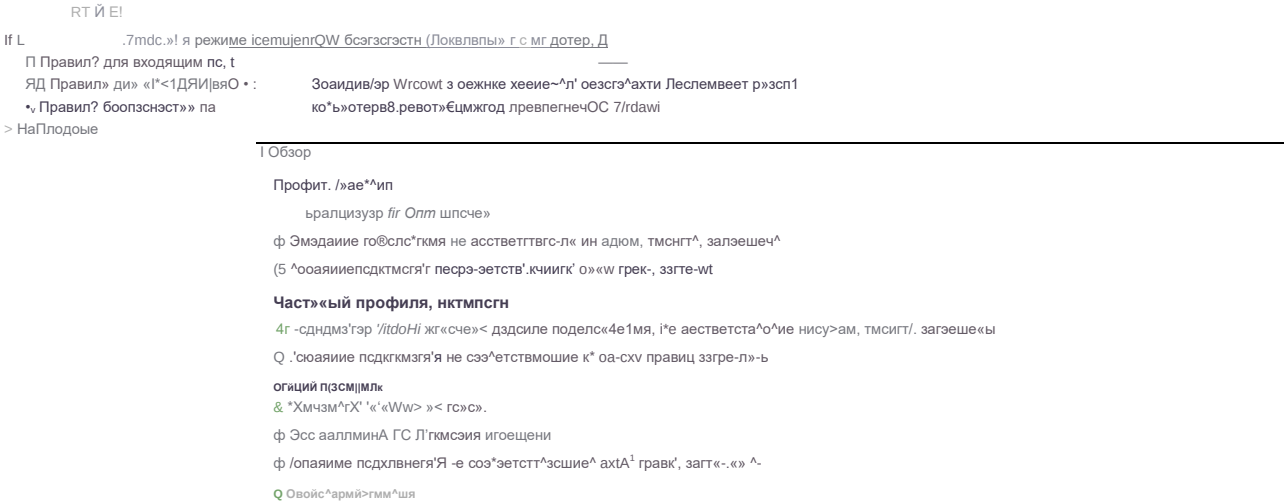
В открывшемся окне есть три набора профилей (**Общий профиль, Профиль домена** и **Частный профиль**), а также параметры **IPSec**.




Здесь для **каждого** из профилей нужно включить брандмауэр **Windows** (первый выпадающий список), включить блокировку всех входящих подключений (второй выпадающий список) и блокировать исходящие подключения (третий список).

Результатом должно стать:



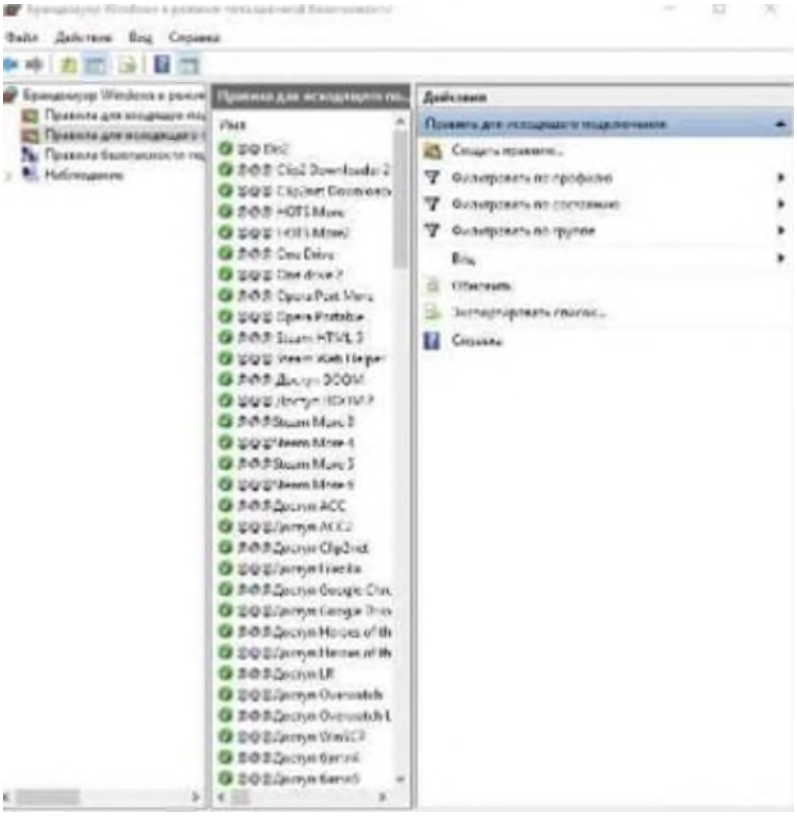



В данный момент запрещены **все** входящие подключения и **все** исходящие, кроме тех правил, что заданы изначально приложениями или самой системой.

Правила для исходящих соединений

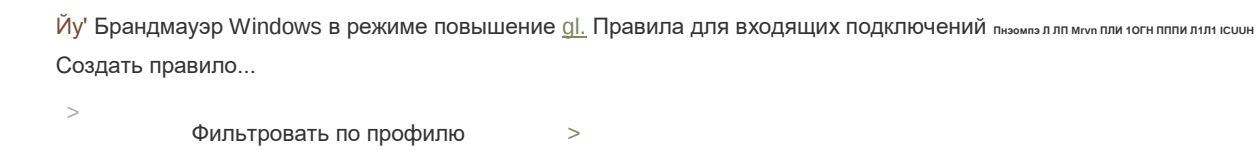
В большинстве случаев для входящих соединений ничего настраивать **не** нужно и их стоит держать заблокированными (за исключением требуемых и установленных по умолчанию).

Настройки правила для исходящих соединений, выполняется в окне:



Для этого перейдите на вкладку "**Правила для исходящего подключения**", где существующие (все) и активные (зеленая галочка), правила, которые есть в системе.

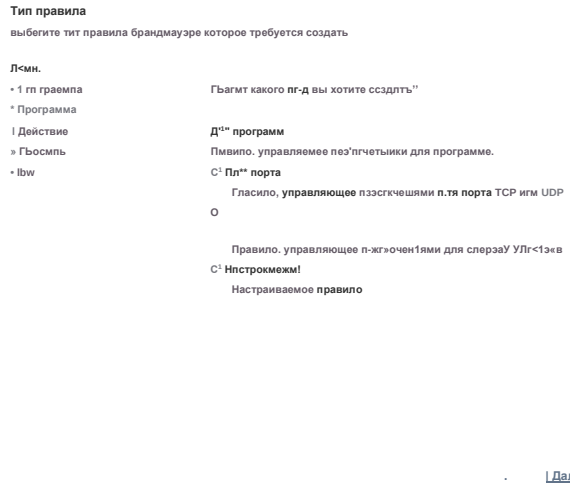
Чаще всего здесь **стоит оставить всё** как есть изначально, либо удалить все правила, **кроме** отмеченных зелёной галочкой, т.е включенных самой системой (и приложениями) в данный момент.




Для вызова контекстного меню кликаем правой кнопкой по «Правилам исходящих подключением» В правой колонке вы найдите кнопку "**Создать правило**", которая так же доступна при клике правой кнопкой мышки на пункте "**Правила для исходящего подключения**".

С помощью этой самой кнопки необходимо создать правила для **всех** приложений, которые, по Вашему мнению, должны иметь доступ в интернет.

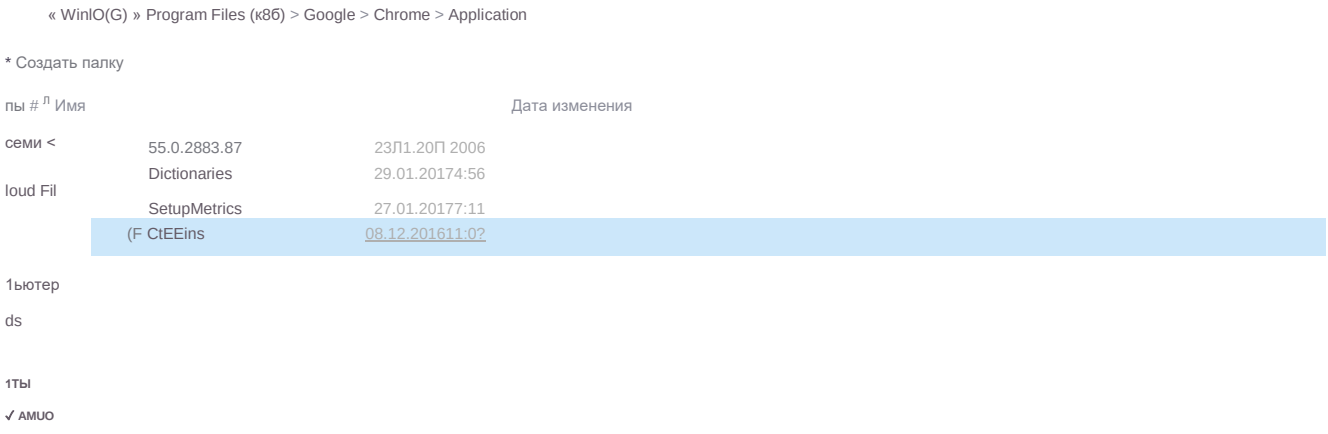
Создание правил работы брандмауэра




. | Далде > ~|

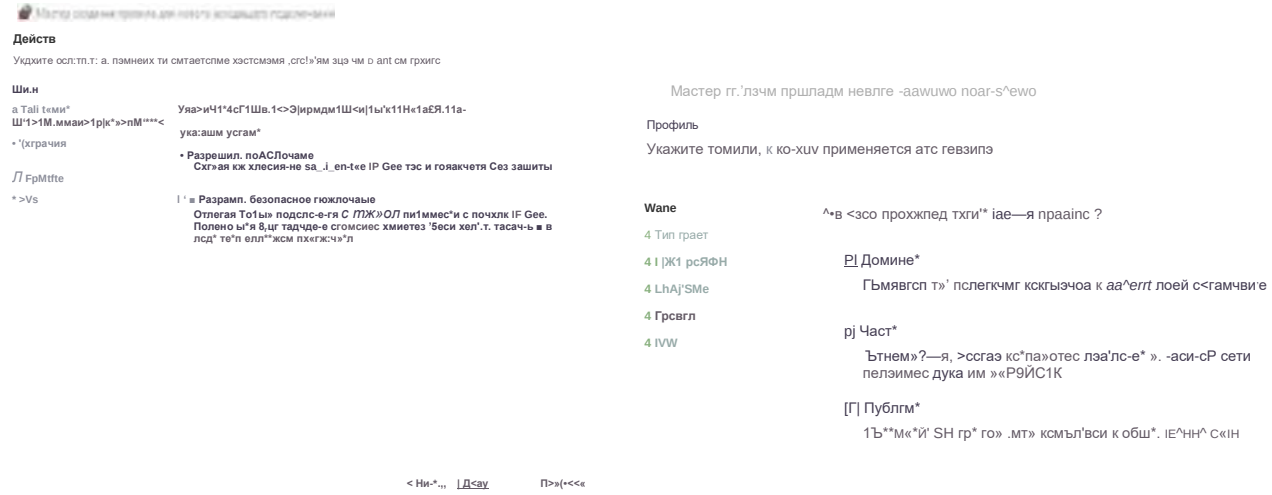
Например, давайте сделаем правило для браузера:

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



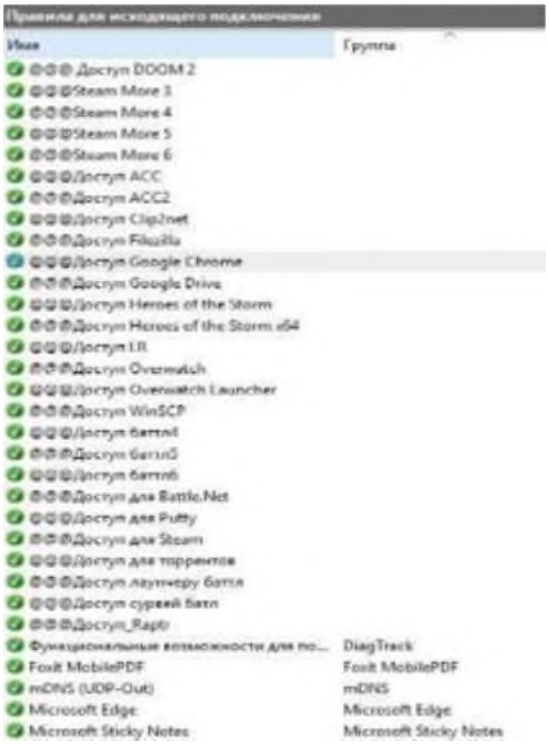

На следующей вкладке выбираем пункт "**Действие**" как "**Разрешить подключение**".

Профилирование




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

И на вкладке "**Имя**" мы задаём имя для своего профиля (рекомендуется начинать имя с




Имя:

@@@ Доступ для Google Chrome

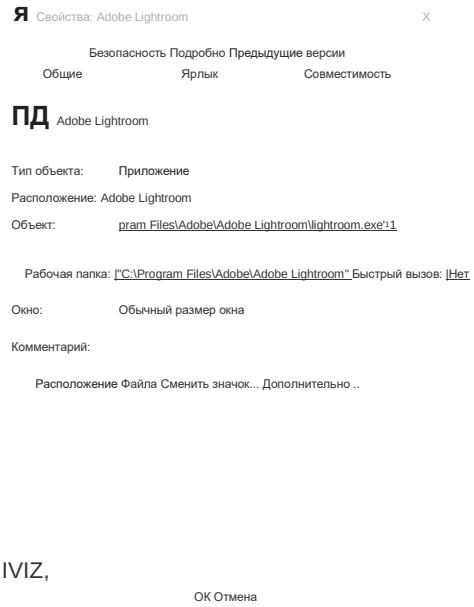
Описание (необязательно):

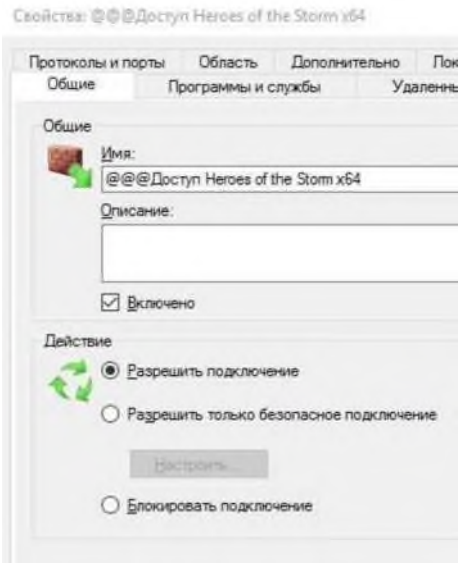
Исходящее правило для доступа браузера в интернет

одной и той же буквы или **символа**, что позволит быстро находить свои правила в списке):

По этому правилу браузер должен успешно соединятся с интернетом.

По тому же принципу добавляете правила, для всех приложений, которым, нужен доступ в интернет.




Г IIVIZ,

<!> @© Dis2

Q @@@ Clip2 Downloader 2 © ©©@ Clip2net Downloader O ©©© HOTS More o ©©@ HOTS More2 O @@© One Drive O @©@ One drive 2

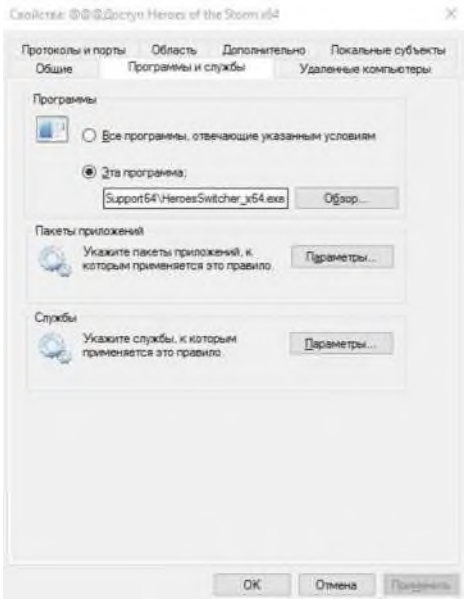
@©@ Opera Port More O @©@ Opera Portable O ©@@ Steam HTML 5 & ©©© Steam Web Helper © ©©©Steam правило 1 йй @©@ Доступ DOOM O @@@ Доступ DOOM 2

@@©Steam правило 3

©©©Steam правило 4

© ©©@Steam правило 5

@@@Steam правило 6 O ©©©Доступ ДСС ЙЛ ©©©Доступ ACC2 O ©©©Доступ Clip2net C/ ©©©Доступ Filezilla




Для определения полного пути к файлу для запуска нажмите правой кнопкой мышки по ярлыку и выберите пункт "**Свойства**", где в строке "**Объект**" будет указан полный путь до рабочего файла, а на строке "**Рабочая папка**", собственно, указана рабочая папка с программой.

Следует помнить, что для разных разрядностей есть разные версии программы, т.е порой необходимо **разрешать** доступ и **x86 (x32)** и **x64**-версии программы, в зависимости от того, какая используется система.

Для "сложносоставных" программ требуется много разрешений, например для **Steam^**

нужно где-то **6-8** правил для полностью рабочего функционала (т.к у них одно приложение отвечает за браузерную часть, второе за запуск клиента, третье за трансляции, четвертое за магазин, пятое за что-либо еще):

- **Steam\Steam.exe;**
- **Steam\bin\steamservice.exe;**
- **Steam\bin\x86launcher.exe;**
- **Steam\bin\x64launcher.exe;**
- **Steam\bin\steam_monitor.exe;**
- **Steam\bin\GameOverlayUI.exe;**
- И тд.

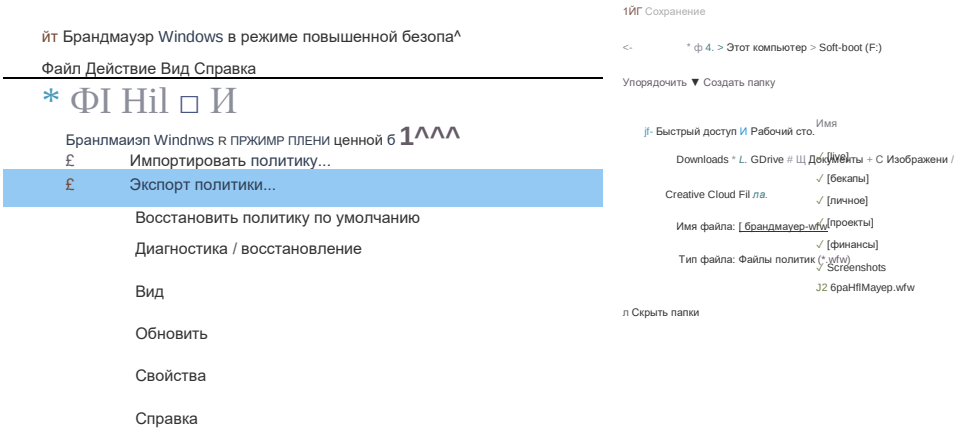
Такое встречается у достаточно большого количества программ, т.е, если дали доступ одному, основному **exe**-файлу, но приложение всё еще не может выйти в интернет, то стоит поискать другие файлы **exe** в папке с программой и задать разрешения для них до тех пор, пока весь нужный функционал не заработает должным образом.

Исключения, работа с проблемами, изоляция

Опять же, если после всех настроек работа нормализовалась, но не полностью то возможно есть смысл настроить разрешение для входящих соединений брандмауэра для конкретно этой программы на вкладке "**Правила для входящих подключений**".

Экспорт и импорт готовых настроек

Если есть несколько компьютеров схожей конфигурации, то можно экспортировать уже настроенные параметры через **Экспорт политики**"(правая кнопка мышки по пункту "**Брандмауэр Windows в режиме повышенной безопасности**). Здесь можно во-первых экспортировать

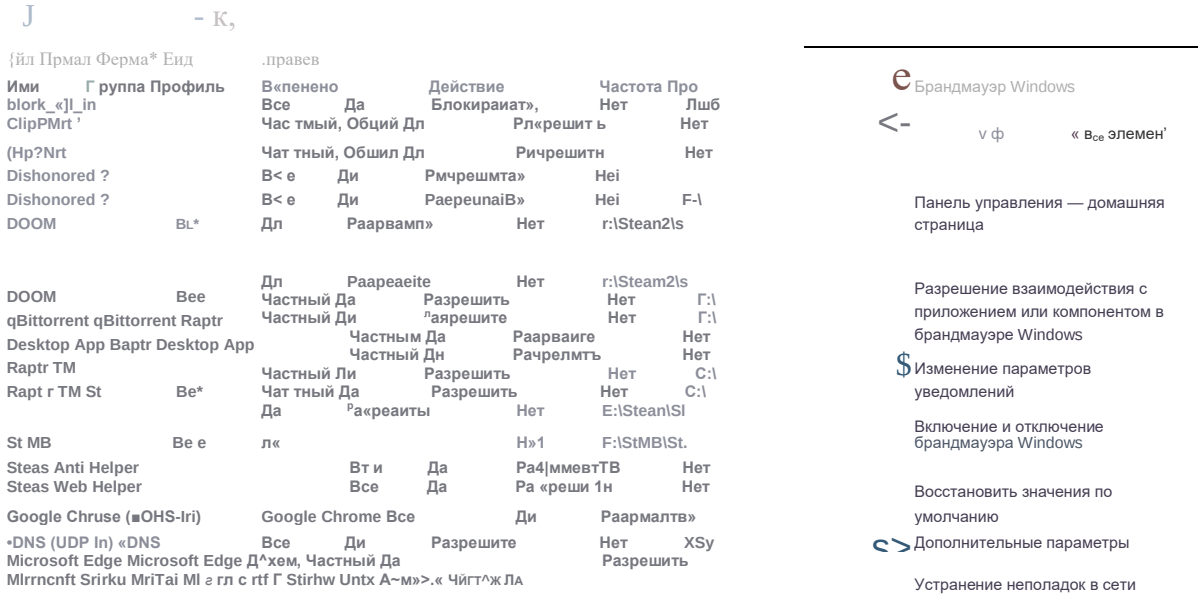



политики:

А, во-вторых, предусмотрена выгрузка списков правил (входящих и исходящих отдельно) в

виде **txt**, что делается в меню справа, где Вы создавали, собственно, правила:

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




Если при настройках что-то пойдет не так всегда можете включить-или выключить брандмауэр **Windows**, используя соответствующий пункт "**Включение и отключение брандмауэра Windows**", или сбросить все настройки, "**Восстановить значения по умолчанию**":

**Задание на самостоятельную работу**

1. Изучите возможные варианты включения и отключения брандмауэра в ОС Windows .
2. Процесс разрешения программе Write работать через брандмауэр в ОС Windows .
3. Как блокировать все исходящие и входящие подключения через брандмауэр в ОС Windows .
4. Действия при создании правила, разрешающие исходящего подключения к браузеру Internet Explorer.
5. Как исключить программу из разрешенных для связи через брандмауэр в ОС Windows

## Контрольные вопросы

1. Дайте определение брандмауэра.
2. В чем заключается основная функция брандмауэра в понятии ОС?
3. В чем связана необходимость блокирования исходящего трафика?
4. От чего не может защитить ПК брандмауэр в ОС Windows

**Лабораторная работа №6 «Шифрование методом Цезаря и Виженера»**

**Цель работы:** Знакомство с простейшими приемами шифрования и дешифрования текстовой информации. Изучить методы шифрования многоалфавитной замены.
Время 2 часа

**Теоретическая часть**

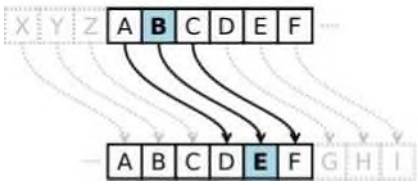
**Симметричное** шифрование (шифрованием с закрытым ключом), при котором ключ для шифрования и дешифрования представляет собой один и тот же ключ (на обыденном уровне - просто пароль).

В методе шифрования с секретным или *симметричным ключом* имеется один *ключ*, который используется как для шифрования, так и для расшифровки сообщения. Такой *ключ* нужно хранить в секрете. Это затрудняет использование системы шифрования, поскольку ключи должны регулярно меняться, для чего требуется их секретное распространение. Наиболее популярные *алгоритмы шифрования* с секретным ключом

Крайне простой пример **симметричного шифрования** - это подстановочный шифр. Подстановочный шифр заменяет каждую часть информации другой информацией. Чаще всего это достигается смещением букв алфавита. Алгоритм состоит в том, чтобы сдвинуть алфавит, а ключ - это число букв, на которое произведено смещение.

- **Шифр Цезаря**, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования

**Шаг шифрования или сдвиг** — это число, которое указывает на сколько позиций мы будем смещаться влево или вправо по алфавиту. Часто сдвиг называют ключом.
Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.




Шифр Цезаря со сдвигом на 3:

- A заменяется на D
- B заменяется на E
- Z заменяется на C и так далее

Шифрование с использованием ключа k = 3. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее: Оригинальный текст:

Исходный алфавит:АББГДЕ = ЖЗИй КЛМНОПРСТ
УФХЦЧШЩЪЬ ЬЭЮЯ
Ыифрованный: ГДЕЁЖЗИЙКЛМ НОПРСТУФХ
ЫЧиЩЬЫЬ ЭЮЯАБВ

Съешь же ещё этих мягких французских булок,, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

□эзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн,, жг еитвм ъгб.

**Шифр Цезаря.** В I в. н.э. **Юлий** Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвёртую (D). вторую (B) - на пятую (E), наконец последнюю – на третью:

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

Сообщение об одержанной им победе выглядело так:

YHQL YLGL YLFL

**«Veni, vidi, vici» – лат. «Пришёл, увидел, победил»**

Очевидно, что по сегодняшним меркам это чрезвычайно слабый алгоритм, тем не менее, даже он помогал Цезарю. И прекрасно демонстрирует, как действует симметричное шифрование.

## Шифр Виженера

Таблица ВИЖЕНЕРА

Буквы исходного текста

А Б В ГДЕЖЗИЙКЛМНОП РСТУФХЦЧШЩЪЫ ЬЭЮЯ

| | |
|---|---|
| А | Б В ГДЕЖЗИЙК В ГДЕЖЗИЙКЛ Л М Н О П РС М Н О П Р ТУФХЦЧШЩЪЫ ЬЭЮЯА УФХЦЧШЩЪЫ ЬЭЮЯА Б |
| Б | ГДЕЖЗИЙКЛМ ДЕЖЗИЙКЛМН Е ЖЗ С Т И О П Р С Т У О П Р С ФХ ЦЧШЩЪЫ Ь Э Ю Я А Б В ХЦЧШЩЪЫ ЬЭЮЯАБВ |
| в г | ИЙКЛМНО жзийклмноп Т У Ф Г Р С Т У Ф Х Р С Т Г ЦЧШЩЪЫ ЬЭЮЯАБВ ГД ЧШЩЪЫ ЬЭЮЯА Б В |
| д | ЗИЙКЛМНОПР У Ф Х Ц (I Т У Ф Х ц ч Т У ГДЕ ШЩЪЫ ЬЭЮЯА БВ ГДЕЖ ЩЪЫБЭЮЯАБВ |
| Е | -И—Й К Л М И О П—Р— Ф Х Ц ч ш У Ф Х Ц ч ш щ ГДЕЖЗ ЪЫ ЬЭЮЯАБВ ГДЕЖЗИ Ы ЬЭЮЯАБВ |
| ж | Й КЛМНОПРСТ КЛМНОПРСТУ Ф Х Ц ч ш щ ъ Х Ц ч ш щ ГДЕЖЗИЙ ЬЭЮЯАБВ ГДЕЖЗИЙК ЭЮЯАБВ |
| З и | ЛМНОПРСТУФ МНОПРСТУФХ ъ ы цчшщъы ь ч ш щ ъ ГДЕЖЗИЙКЛ ЮЯАБВ ГДЕЖЗИЙКЛМ |
| й к | НОПРСТУФХЦ ОПРСТУФХЦЧ Пы ь э Ш Щ Ъ Ы Б ЭЮ щ ЯАБВГДЕЖЗИЙКЛМН АБВ ГДЕЖЗИЙКЛМНО ББВ |
| л | РСТУФХЦЧШ Р СТУФХЦЧШЩъ ы ь э ю я Ъ Ы Ь Э Ю Я ГДЕЖЗИЙКЛМНОП ВГДЕЖЗИЙКЛМНОПР |
| м | СТУФХЦЧШЩЪ Т УФХЦЧШЩЪЫ А ГДЕЖЗИЙКЛМНОПРС ДЕЖЗИЙКЛМНОПРСТ |
| н о | УФХЦЧШЩЪЫЬ Ф Х ЦЧШЩЪЫ ЬЭЫ Ь Э Ю Я А Б Ь Э Ю Я ЕЖЗИЙКЛМНОПРСТУ ЖЗИЙКЛМНОПРСТУФ |
| п р | Х цчшщъы ьэю ЦЧШЩЪЫ ЬЭЮЯ А Б В Э Ю Я А Б В Г Ю Я ЗИЙКЛМНОПРСТУФХ ИЙКЛМНОПРСТУФХЦ |
| с т | ЧШЩЪЫ ЬЭЮЯА А Б В Г Д Я А Б В Г Д Е А ЙКЛМНОПРСТУФХЦЧ КЛМНОП РСТУФХЦЧШ |
| га т 2 § у | ШЩЪЫЬЭЮЯАБ ЩЪЫ ЬЭЮЯАБВ Б В Г Д Е Ж Б В Г Д Е Ж ЛМНОП РСТУФХЦЧШЩ МНОПРСТУФХЦЧШЩЪ |
| ф | ЪЫ ЬЭЮЯАБВ Г Ы ЬЭЮЯАБВ ГДЗ В Г Д Е Ж З И Г Д Е Ж З НОП РСТУФХЦЧШЩЪЫ ОП РСТУФХЦЧШЩЪЫ ь |
| Х | ЬЭЮЯАБВГДЕ ЭЮЯАБВГДЕЖ И Й Д Е Ж З И Й К Е Ж З ПРСТУФХЦЧШЩЪЫЬЭ РСТУФХЦЧШЩЪЫ ьэю |
| ц ч | ЮЯАБВГДЕЖЗ ЯАБВГДЕЖЗИ И Й К Л Ж З И Й К Л М З СТУФХЦЧШЩЪ ыьэюя |
| ш | АБВГДЕЖЗИЙ И Й К Л м н ИЙКЛМНО й |
| щ | к л м н о п к л м н О П Р |
| ъ | |
| ы | |
| ь э | |
| ю | |
| я | |

| | | в | C | D | E | F | G | H | | I | K | L | M | N | 0 | P | Q | R | 5 | т | и | V | W | к | | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | в | C | O | E | F | G | H | I | J | к | L | м | N | O | P | a | R | 5 | т | и | V | W | X | Y | Z |
| B | B | c | □ | E | F | G | H | I | J | K | L | M | N | O | P | a | R | S | T | и | V | W | X | Y | Z | A |
| C | C | o | E | F | G | H | I | J | к | L | M | N | 0 | P | a | R | 5 | T | и | V | W | X | ¥ | Z | A | B |
| O | D | E | F | G | H | I | J | K | L | M | N | 0 | P | 0 | R | 5 | T | и | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | E | 3 | K | L | M | N | 0 | P | Q | R | 5 | т | и | V | W | X | Y | Z | A | B | C | □ |
| p | F | G | H | E | J | K | L | м | м | 0 | P | a | R | S | т | и | V | W | X | Y | Z | A | B | C | □ | E |
| G | G | H | I | J | K | L | M | N | 0 | P | Q | R | S | т | и | V | W | X | Y | Z | A | B | C | □ | E | F |
| H | H | I | J | K | L | M | N | 0 | p | Q | R | S | T | и | V | W | X | Y | Z | A | B | C | D | E | F | G |
| | E | J | K | L | M | N | 0 | P | a | R | S | т | и | V | W | X | Y | Z | A | B | C | □ | E | F | G | H |
| | J | K | L | м | N | O | P | a | R | S | T | и | V | W | X | ¥ | Z | A | B | C | o | E | F | G | H | I |
| K | K | L | M | N | 0 | p | a | R | S | т | и | V | W | X | Y | Z | A | B | C | □ | E | F | G | H | E | J |
| L | L | M | N | O | P | a | R | S | T | и | V | W | X | Y | Z | A | B | C | o | E | F | G | H | I | J | K |
| M | м | N | 0 | P | Q | R | S | т | и | V | W | X | Y | Z | A | B | C | □ | E | F | G | H | I | J | K | L |
| N | N | O | P | O. | R | 5 | т | и | V | W | X | Y | Z | A | B | C | D | E | F | G | H | E | J | K | L | M |

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | P | a | R | 5 | т | и | V | W | X | Y | Z | A | B | C | 0 | E | F | G | H | E | J | K | L | | M | N |
| P | P | a | R | 5 | T | и | V | W | X | ¥ | Z | A | B | C | □ | E | F | G | H | I | J | K | L | M | N | | O |
| Q | Q | P | S | T | и | V | W | X | Y | Z | A | B | C | o | E | F | G | | H | ! | J | K | L | M | N | 0 | | P |
| R | R | 5 | т | и | V | W | X | Y | Z | A | B | C | □ | E | F | G | H | I | | J | K | L | M | N | 0 | P | | a |
| W | S | T | и | V | W | X | Y | Z | A | B | C | □ | E | F | G | H | I | J | | K | L | M | N | 0 | P | a | | R |
| T | т | и | V | W | X | Y | Z | A | B | C | o | E | F | G | H | I | J | K | | L | M | N | 0 | P | 0 | R | | S |
| и | и | V | W | X | ¥ | Z | A | B | C | D | E | F | G | H | E | J | K | L | | M | N | O | P | a | R | S | | т |
| V | V | W | X | Y | Z | A | B | C | O | E | F | G | H | I | J | K | L | M | | N | 0 | P | a | R | S | т | | и |
| W | W | X | Y | Z | A | B | C | □ | E | F | G | H | ! | J | K | L | | M | N | a | P | a | R | S | т | и | | V |
| к | X | V | Z | A | B | C | o | E | F | G | H | E | J | K | L | M | N | 0 | | p | | Q | R | 5 | т | и | V | W |
| Y | ¥ | Z | A | B | C | D | E | F | G | H | I | J | | K | L | M | M | 0 | | P | a | | R | 5 | T | и | V | | W | X |
| Z | Z | A | B | C | □ | E | F | G | H | I | J | K | L | M | N | 0 | P | Q | | R | S | T | и | V | | W | X | | Y |

Метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

**Шифр Виженера,** В процессе шифрования (и дешифрования) используется таблица {«таблица Виженера»), которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная (таблица, число строк которой равно числу столбцов и равно числу букв в алфавите. Ниже представлена таблица, составленная из 31 буквы русского алфавита (без букв Ё и Ъ). Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом!. Выбирается слово - лозунг (например, «монастырь») и подписывается с повторением над буквами сообщения.

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном. В данном примере сначала находим столбец, отвечающий букве «м» лозунга, а затем строку, соответствующую букве **«р"** открытого текста. На пересечении выделенных столбца **и** строки находим букву «о». Так продолжая дальше, находим шифрованный текст полностью:

**монастырьмонастырьмон**
**раскинулось мореширок**
**эоя к щаг ы й ю й щ о в ч ф шл ь ш ы**

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера.

Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Например, предположим, что исходный текст имеет такой вид:

ATTACKATDANN

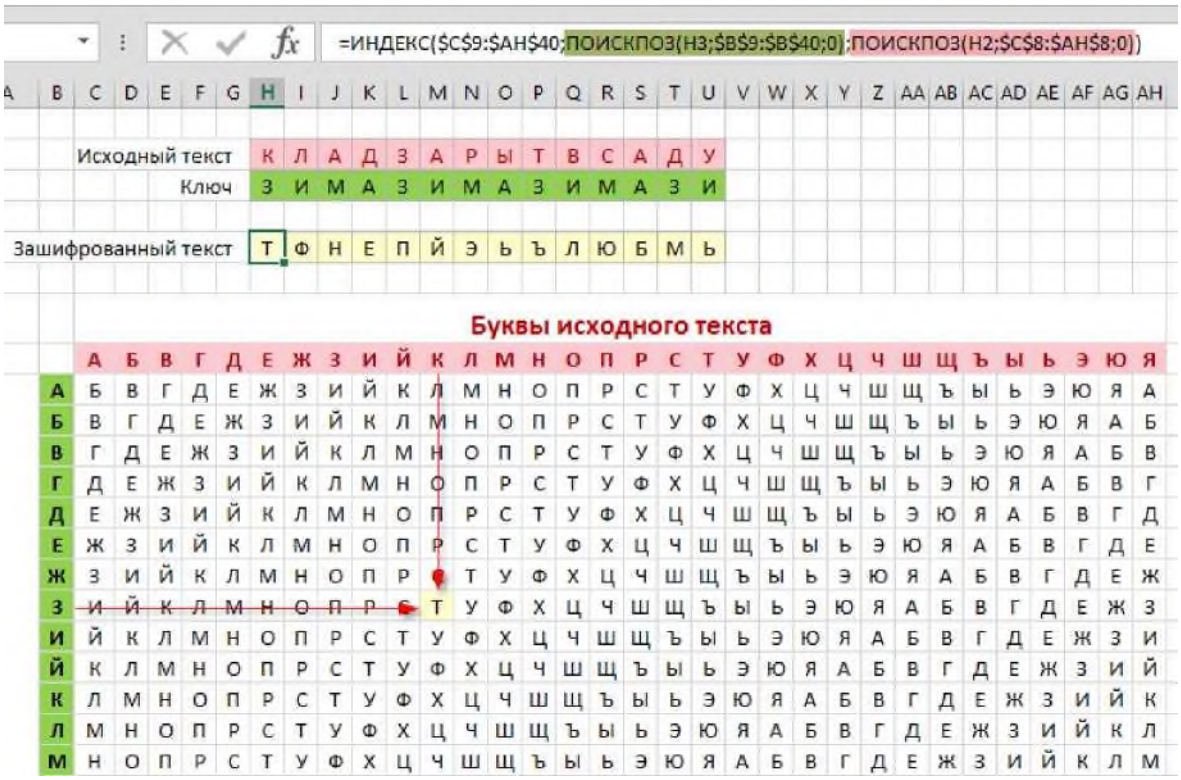
Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: ATTACKATDAWN
Ключ: LEMON LEMONLE
Зашифрованный текст: LXFOPVEFRNHR

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.




Квадрат Виженера, или таблица Виженера, также известная как tabula recta, может быть использована для шифрования и расшифровывания

**Практические задания №1:**

**1 Шифр Цезаря**. Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется следующей после нее буквой в алфавите, который считается написанным по кругу.

Используя шифр Цезаря, зашифровать следующие фразы:

а) Делу время - потехе час
б) С Новым годом
в) Первое сентября

**2** Используя шифр Цезаря, декодировать следующие фразы:

а) Лмбттоьк шбт

б) Вёмпё тпмочё рфтуьой

**2 Шифр Виженера**. Это шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста: 3 1 9 1 3 1 9 1 и т.д. Используя в качестве ключевого слово ЗИМА, закодировать слова:

a) АЛГОРИТМИЗАЦИЯ,
b) КОМПЬЮТЕР,
c) ИНТЕРНЕТ.

С помощью шифра Виженера с ключевым словом БАНК **расшифровать слово ЁПЯЪЕБ**.

**3** Используя в качестве ключа расположение букв на клавиатуре вашего компьютера, декодировать сообщение:

a) D ktce hjlbkfcm 'kjxrf?
b) D ktce jyf hjckf?

Используя в качестве ключа расположение букв на клавиатуре вашего компьютера, закодировать сообщение:

a) Москва - столица России.

**4.** Шифр перестановки. Кодирование осуществляется перестановкой букв в слове по одному и тому же правилу. Восстановить слова и определить правило перестановки:

НИМАРЕЛ, ЛЕТОФЕН, НИЛКЙЕА, НОМОТИР, РАКДНАША.

Используя приведенный выше шифр перестановки, закодировать следующие слова:

ГОРИЗОНТ, ТЕЛЕВИЗОР, МАГНИТОФОН.

Определить правило шифрования и расшифрования слова:

КЭРНОЦЛИТКЭЛУОНПИЕЖДАИФЯ

УКРОГРЕОШЛАЕКВИСЧТЕВМО

Придумать свой ключ шифрования и закодировать с помощью него сообщение:

БИТ - ЭТО МИНИМАЛЬНАЯ ЕДИНИЦА ИЗМЕРЕНИЯ ИНФОРМАЦИИ.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| АБВГДЕЁЖЗИЙ | | | | | | | | | 10 И | |
| 123456789 | | | | | | | | | | |
| КЛМНОПРСТУФ | | | | | | | | | | |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| ХЦЧШЩЪЫЬЭЮЯ | | | | | | | | | | |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |

**Задание на самостоятельную работу:**

- Зашифровать слово с помощью шифра Цезаря: ВЕРОЯТНОСТЬ
- Зашифровать слово с помощью шифра Виженера: ГИСТОГРАММА, ключевое слово - ДЕВА
- Зашифровать слово с помощью шифра Цезаря: ДОКУМЕНТАЦИЯ
- Зашифровать слово с помощью шифра Виженера: НАКОПИТЕЛЬ, ключевое слово - ЖАДИНА
- Зашифровать слово с помощью шифра Цезаря: ПОЛЬЗОВАТЕЛЬ
- Зашифровать слово с помощью шифра Виженера: АРХИТЕКТУРА, ключевое слово - ЗНАК
- Зашифровать слово с помощью шифра Цезаря: ГИПЕРССЫЛКА
- Зашифровать слово с помощью шифра Виженера: КОМПИЛЯТОР, ключевое слово - КАНАВА
- Зашифровать слово с помощью шифра Цезаря: ТАЙМЕР
- Зашифровать слово с помощью шифра Виженера: КЛАВИАТУРА, ключевое слово - ДРОЗД

- Зашифровать слово с помощью шифра Цезаря: ВЫСКАЗЫВАНИЕ
- Зашифровать слово с помощью шифра Виженера: КИБЕРНЕТИКА, ключевое слово - ЖАДИНА
- Зашифровать слово с помощью шифра Цезаря: ДИСКРЕТИЗАЦИЯ
- Зашифровать слово с помощью шифра Виженера: КОНФИГУРАЦИЯ, ключевое слово - КАНАВА
- Зашифровать слово с помощью шифра Цезаря: АВТОМАТИЗАЦИЯ
- Зашифровать слово с помощью шифра Виженера: ЭКСПЕРИМЕНТ, ключевое слово - ДРОЗД

**Контрольные вопросы***:*

1. Какой текст называется открытым?
2. Какой текст называется закрытым?
3. Что такое ключ?
4. Как осуществляется процесс шифрования в методе Цезаря?
5. Что такое «шифрование методом перестановки»?
6. Оценить надежность шифрования по таблице Виженера.
7. Какова частотность появления комбинаций по таблице Виженера.
8. Как осуществляется процесс шифрования в методе Виженера?
9. . Понятие криптостойкости.
10. Условия, предъявляемые к криптостойкости.

**Лабораторная работа № 7 «Шифрование методом Полибия»**

**Цель работы:** Ознакомиться с древнейшим шифром - шифром Полибия.
Время 2 часа
**Теоретическая часть**

В криптографии квадрат Полибия (англ. Polybius square), также известный как шахматная доска Полибия — оригинальный код простой замены

| **Квадрат Полибия.** E | | | | |
|---|---|---|---|---|
| Д | B | C | D | E |
| F | G | H | I.J | К |
| L | M | N | 0 | P |
| Q | R | S | T | LI |
| V | W | X | Y | Z |

Древней Греции был известен шифр, называемый «квадрат Полибия».

Это устройство представляла собой квадрат 5*5, столбць и строки «порого нумеровали цифрами **от** 1 до 5. В каждую клетку этого квадрата записывалась одна буква. В греческом варианте одна клетка оставалась пустой, в латинском - в одну клетку помещали **две** буквь и **j.** В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел. Например:

**13 34 22 24 44 34 15 42 22 34 43 45 32**

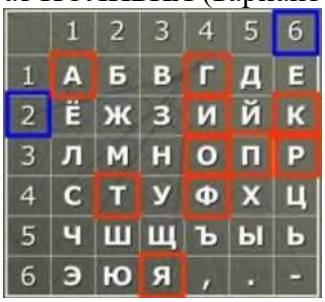
**«Cogito, ergo sum» - лат. «Я мыслю, следовательно, существую»** Это сообщение записано три использовании латинского варианта «квадрата Полибия», в котором буквы расположены в алфавитном порядке.

**Квадрат ПОЛИБИЯ**

| | | | | | |
|---|---|---|---|---|---|
| A | B | C | D | E | |
| F | G | H | | К | |
| L | M | N | O | P | |
| Q | R | S | T | И | |
| "У | W | X | Y | Z | |

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | А | Б | в | г | А |
| 2 | Е/Э | Ж | з | и/й | к |
| 3 | л | М | Н | о | П |
| 4 | Р/С | т | У | ф/Х | Ц |
| 5 | ч | ш/щ | э | ю | Я |

Квадрат ПОЛИБИЯ (вариант 2 для русского алфавита)




p' MyS|

| | | | | | | |
|---|---|---|---|---|---|---|
| ABODE F G H I, J K L | | | | | | M |
| | N | O | P | | | |
| Q | R S | | T | U | | |
| | | | | | | |
| V | W X | | Y | Z | | |

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | А | Б | в | Г | Д | Е |
| 2 | Ж | З | и | к | Л | м |
| 3 | н | О | п | р | с | т |
| 4 | У | ф | Х | Ц | ч | ш |
| 5 | щ | ы | ь | э | ю | я |

**Практическое задание**

Несмотря на то, что квадрат изначально создавался для кодирования, с его помощью можно успешно шифровать. Для того, чтобы зашифровать текст квадратом Полибия, нужно сделать несколько шагов:

**Шаг 1: Формирование таблицы шифрования**

К каждому языку отдельно составляется таблица шифрования с одинаковым (не обязательно) количеством пронумерованных строк и столбцов, параметры которой зависят от его мощности (количества букв в алфавите). Берутся два целых числа, произведение которых ближе всего к количеству букв в языке — получаем нужное число строк и столбцов. Затем вписываем в таблицу все буквы алфавита подряд — по одной в каждую клетку. При нехватке клеток можно вписать в одну две буквы (редко употребляющиеся или схожие по употреблению).

**Латинский алфавит**

В современном латинском алфавите 26 букв, следовательно, таблица должна состоять из 5 строк и 5 столбцов, так как 25=5*5 наиболее близкое к 26 число. При этом буквы I, J не различаются (J отождествляется с буквой I), так как не хватает 1 ячейки:

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

**Русский алфавит**

Идею формирования таблицы шифрования проиллюстрируем для русского языка. Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому размер таблицы выбран другой (квадрат 6*6=36, поскольку 36 наиболее близкое число к 33):

Используя подобный алгоритм, таблицу шифрования можно задать для любого языка. Чтобы расшифровать закрытый текст, необходимо знать, таблицей шифрования какого алфавита он зашифрован.

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

«Квадрат Полибия» представляет собой квадрат 5х5, столбцы и строки которого нумеруются цифрами от 1 до 5.

| | | 2 | | 4 | 5 |
|---|---|---|---|---|---|
| 1 | | Б | | Г | Д |
| 2 | | ж | | и/й | к |
| 3 | л | М | | о | П |
| 4 | р/с | | | Ф/Х | Ц |
| 5 | ч | | bl | ю | я |

В каждую клетку этого квадрата записывается одна буква (в нашем алфавите 31 буква, Ъ и Ё исключены, кроме того в одну клетку поместите буквы е-э, и-й, ж-з, р-с, ф-х, ш-щ). Буквы расположены в алфавитном порядке.

В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путём нахождения буквы, стоящей на пересечении строки и столбца.

**Шаг 2: Принцип шифрования**

Существует несколько методов шифрования с помощью квадрата Полибия. Ниже приведены три из них.

**Метод 1**

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

**Таблица координат**

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

Таким образом после шифрования получаем:

**Результат**

| До шифрования: | SOMETE |
|---|---|
| После | XTRKYK |

**Метод 2**

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

**Таблица координат**

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

Затем координаты считывают по строкам:

*34 25 45 34 43* 31 41 54

■ (*)

Далее координаты преобразуются в буквы поэтому же квадрату:

**Таблица координат**

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

Таким образом после шифрования получаем:

**Результат**

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

**Метод 3**

Усложнённый вариант, который заключается в следующем: полученный первичный

шифротекст (*) шифруется вторично. При этом он выписывается без разбиения на пары:

3425453443314154

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

4254534433141543

Эта последовательность вновь разбивается в группы по два:

42 54 53 44 33 14 15 43

и по таблице заменяется на окончательный шифротекст:

Таблица координат

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

Таким образом после шифрования получаем:

**Результат**

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

**Самостоятельное задание**

Зашифровать слово с помощью шифра Полибия: ВЕРОЯТНОСТЬ Расшифровать слово с помощью шифра Полибия: АБГБГГААВДАЕВЕГА Зашифровать слово с помощью шифра Полибия: ДОКУМЕНТАЦИЯ Расшифровать слово с помощью шифра Полибия: АГААВААБГБВДАГ 3. Зашифровать слово с помощью шифра Полибия: ПОЛЬЗОВАТЕЛЬ 4. Расшифровать слово с помощью шифра Полибия: ВАААВДВЕАЕБЕДД 3. Зашифровать слово с помощью шифра Полибия: ГИПЕРССЫЛКА 4. Расшифровать слово с помощью шифра Полибия: ВЕГАААВААБГББЕ 3. Зашифровать слово с помощью шифра Полибия: ДИДЖИТАЙЗЕР 4. Расшифровать слово с помощью шифра Полибия: АБГБГГААВДАЕВЕГА 3. Зашифровать слово с помощью шифра Полибия: ВЫСКАЗЫВАНИЕ 4. Расшифровать слово с помощью шифра Полибия: АГААВААБГБВДАГ 3. Зашифровать слово с помощью шифра Полибия: ДИСКРЕТИЗАЦИЯ 4. Расшифровать слово с помощью шифра Полибия: ВАААВДВЕАЕБЕДД 3. Зашифровать слово с помощью шифра Полибия: АВТОМАТИЗАЦИЯ 4. Расшифровать слово с помощью шифра Полибия: ВЕГАААВААБГББЕ

**Контрольные вопросы**

1. Что такое симметричные криптоалгоритмы?
2. Классификация симметричных криптоалгоритмов.
3. Какие методы подстановки, используемые для шифрования, вы знаете? 4. Какие методы перестановки, используемые для шифрования, вы знаете? 5. Что понимается под шифрованием информации методом гаммирования? 6. Что называется, ключом в криптосистеме?

**Лабораторная работа №8: Анализ защищенности компьютерных систем на основе ОС Windows**

**Цель** работы: изучить возможности анализа защищенности компьютерных систем на основе ОС Windows

**Время 2 часа**

**Теоретическая часть**

Одними из главных элементов информационной безопасности сетевой инфраструктуры являются операционные системы компьютеров, так как в них аккумулируется подавляющая часть используемых механизмов защиты: средства разграничения доступа к ресурсам, аутентификация пользователей, аудит событий и др. От эффективности защиты операционных систем напрямую зависит уровень безопасности сетевой инфраструктуры организации в целом.

**Принципы работы систем анализа защищенности**

Для понимания принципов работы систем анализа защищенности, необходимо обозначить некоторые термины и определения. Ключевое понятие данного занятия - это «**уязвимость»**. Под уязвимостью защиты ОС понимается такое ее свойство (недостаток), которое может быть использовано злоумышленником для осуществления несанкционированного доступа (НСД) к информации. Системы анализа защищенности способны обнаруживать уязвимости в сетевой инфраструктуре, анализировать и выдавать рекомендации по их устранению, а также создавать различного рода отчеты.

**К типичным уязвимостям можно отнести:**

- отсутствие обновлений системы безопасности ОС;
- неправильные настройки систем безопасности ОС;
- несоответствующие пароли;
- восприимчивость к проникновению из внешних систем;
- программные закладки;
- неправильные настройки системного и прикладного ПО, установленного на ОС.

Большинство систем анализа защищенности (XSpider, Internet Scanner, LanGuard, Nessus) обнаруживают уязвимости не только в операционных системах, но и в наиболее распространенном прикладном ПО. Существуют два основных подхода, при помощи которых системы анализа защищенности обнаруживают уязвимости: сканирование и зондирование.

Из-за первого подхода системы анализа защищенности еще называют «**сканерами безопасности**» или просто «сканерами».

При сканировании система анализа защищенности пытается определить наличие уязвимости по косвенным признакам, т.е. без фактического подтверждения ее наличия - это пассивный анализ. Данный подход является наиболее быстрым и простым в реализации. При зондировании система анализа защищенности имитирует ту атаку, которая использует проверяемую уязвимость, т.е. происходит активный анализ.

Данный подход медленнее сканирования, но позволяет убедиться, присутствует или нет на анализируемом компьютере уязвимость.

На практике эти два подхода реализуются в сканерах безопасности через следующие методы проверки:

1) Проверка заголовков (Banner check);
2) Активные зондирующие проверки (Active probing check);
3) Имитация атак (Exploit check).

Первый метод основан на подходе «сканирование» и позволяет делать вывод об уязвимостях, опираясь на информацию в заголовке ответа на запрос сканера безопасности. Примером такой проверки может быть анализ заголовков почтовой программы Sendmail, в результате которого можно узнать её версию и сделать вывод о наличии в ней уязвимости.

Активные зондирующие проверки также основаны на подходе «сканирование». Данный метод сравнивает фрагменты сканируемого программного обеспечения с сигнатурой известной уязвимости, хранящейся в базе данных системы анализа защищенности. Разновидностями этого метода являются, например, проверки контрольных сумм или даты сканируемого программного обеспечения.

Метод имитации атак основан на использовании различных дефектов в программном обеспечении, и реализует подход зондирования. Существуют уязвимости, которые не могут быть обнаружены без блокирования или нарушения функционирования сервисов операционной системы в процессе сканирования.

При сканировании критичных серверов корпоративной сети нежелательно использование данного метода, т.к. он может вывести их из строя. И в таком случае сканер безопасности успешно реализует атаку «Denial of service» (отказ в обслуживании). Поэтому в большинстве систем анализа защищенности по умолчанию такие проверки, основанные на имитации атак, выключены. При их включении в процесс сканирования обычно выдается предупредительное сообщение (рис. 8.1).

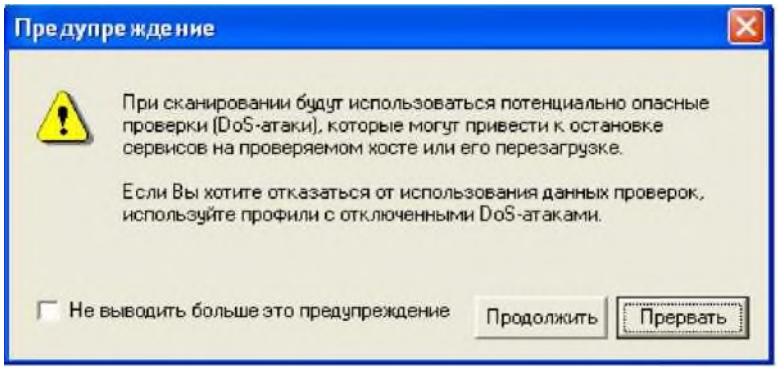



Рис. 1.1. Предупредительное сообщение сканера безопасности XSpider 7.0 о включении опасных проверок в процесс сканирования.

**Microsoft Baseline Security Analyzer**

Microsoft Baseline Security Analyzer (MBSA) - свободно распространяемое средство анализа защищенности операционных систем Windows и ряда программных продуктов компании Microsoft (Internet Information Services, SQL Server, Internet Explorer и др.).

Термин «**Baseline**» в названии MBSA следует понимать, как некоторый эталонный уровень, при котором безопасность ОС можно считать удовлетворительной. MBSA позволяет сканировать компьютеры под управлением операционных систем Windows на предмет обнаружения основных уязвимостей и наличия рекомендованных к установке обновлений системы безопасности. Критически важно знать, какие обновления установлены, а какие еще следует установить на вашей ОС. MBSA обеспечивает подобную проверку, обращаясь к постоянно пополняемой Microsoft базе данных в формате XML, содержащую информацию об обновлениях, выпущенных для каждого из программных продуктов Microsoft.

Работать с программой MBSA можно через графический интерфейс и командную строку. На данном занятии будет рассмотрен только первый вариант работы.

Интерфейс MBSA выполнен на основе браузера Internet Explorer.


Рис. 1.2. Главное окно программы Microsoft Baseline Security Analyzer 2.0 Главное окно программы разбито на две области.

Так как сеанс работы с MBSA настраивается с помощью мастера, то в левой области представлены шаги мастера, а в правой - основное окно с описанием действий каждого шага. На первом шаге «Welcome» необходимо выбрать одно из действий (см.рис. 1.2):

- Сканировать данный компьютер (Scan a computer);
- Сканировать несколько компьютеров (Scan more than one computer);
- Просмотреть существующие отчеты, сделанные MBSA ранее (View existing security

reports).

При первом запуске MBSA необходимо выбрать первый или второй вариант. На следующем шаге мастера в основном окне нужно задать параметры сканирования компьютера(ов) под управлением ОС Windows (см. рис. 1.3).

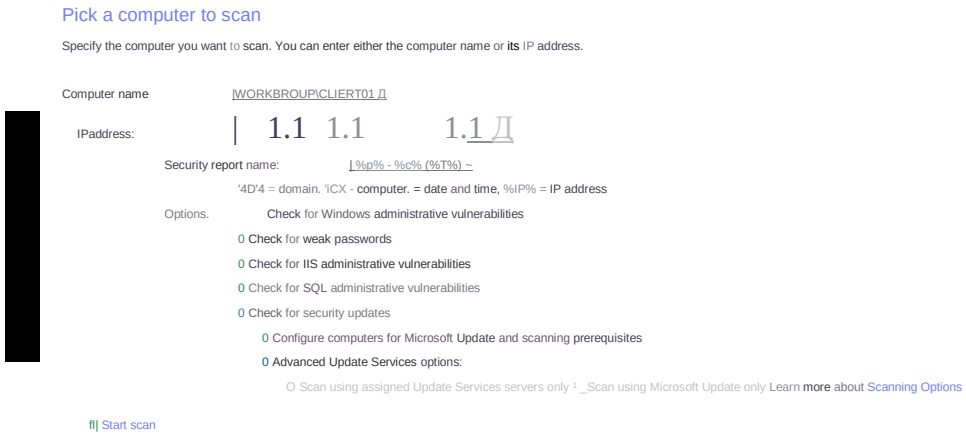



Рис. 8.3. Выбор компьютера и опций сканирования в программе MBSA 2.0

Можно ввести имя или IP-адрес сканируемого компьютера (по умолчанию выбирается компьютер, на котором был запущен MBSA).

Пользователь, запустивший MBSA, должен обладать правами администратора данного компьютера или входить в группу администраторов системы. В случае сканирования нескольких компьютеров пользователь дол-жен обладать правами администратора на каждом из компьютеров, а лучше - правами администратора домена.

Выбрав компьютер(ы) для сканирования, необходимо задать опции сканирования:

- проверкаОС Windows;
- проверкапаролей;
- проверкаслужб IIS;
- проверкасервера SQL;
- проверкаустановленных обновлений безопасности.

Более подробную информацию о проверках MBSA можно получить на официальном сайте Microsoft.

Например, задав опцию «проверка паролей» MBSA проверяет на компьютере учетные записи локальных пользователей, которые используют пустые или простые пароли (эта проверка не выполняется на серверах, выступающих в роли контроллеров домена) из следующих комбинаций: • пароль пустой;

- пароль совпадает с именем учетной записи пользователя;
- пароль совпадает с именем компьютера;
- паролем служит слово «password»;
- паролем служат слова «admin» или «administrator».

Данная проверка также выводит сообщения о заблокированных учетных записях. После того как все опции будут заданы необходимо нажать на ссылку внизу «Start scan» (см. рис. 8.3 **Сканер безопасности XSpider**

В последнее время в России все большую популярность среди специалистов по защите информации набирает сканер безопасности XSpider версии 7.0, выпускаемый отечественной компанией Positive Technologies.

Есть ряд особенностей, которые дают преимущества сканеру XSpider как системе анализа защищенности, над другими продуктами данного класса. Как подчеркивают сами разработчики, главная особенность

XSpider 7 - это его сканирующее ядро, которое способно имитировать сценарий поведения потенциального злоумышленника. Также следует отметить мощную «интеллектуальную начинку» XSpider 7, которая реализуется во встроенных эвристических алгоритмах, позволяющих надежно идентифицировать еще неопубликованные новые уязвимости.

Надежные и исчерпывающие проверки XSpider 7 базируются, в частности, на следующих

интеллектуальных подходах:

- полная идентификация сервисов на случайных портах;
- эвристический метод определения типов и имен серверов (HTTP,FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы;
- обработка RPC-сервисов с их полной идентификацией;
- проведение проверок на нестандартные DoS-атаки.

**Практическая часть**

**Упражнение 1. Создание профиля для сканирования уязвимостей ОС Windows XP Professional**

Упражнение выполняется на виртуальной машине с ОС Windows XP Professional с предустановленным ПО

1. Запустите виртуальную машину с ОС Windows XP Professional.
2. Зарегистрируйтесь в системе как пользователь с правами администратора.
3. Запустите программу XSpider 7.0.
4. В меню «Профиль» выберите пункт «Редактировать текущий». Откроется окно для настройки профиля Default (базовый профиль).
5. Слева, в дереве настроек выберите пункт «Сканер портов» и в правой области окна появятся соответствующие настройки. По умолчанию выбран файл портов default.prt
6. Нажимаем кнопку . Откроется окно со списком файлов портов.
7. В верхней части открывшегося окна, на панели инструментов нажмите кнопку «Новый».
8. В появившемся окне оставьте вариант «Пустой файл» и нажмите кнопку «Выбрать».
9. Откроется окно «Новый файл портов». В области для комментария напишите «LabWork ports».
10. В нижней части окна в строке для ввода «Добавить порт(ы)» введите следующие значения портов: 80, 123, 135, 137, 139, 3306. После ввода каждого номера порта нажимайте кнопку справа «Добавить».
11. Нажмите кнопку «Сохранить как» и назовите файл LabWork.prt.
12. В окне со списком файлов портов выберите только что созданный файл портов.
13. Далее в дереве настроек выберите «Определение уязвимостей». В правой области настроек отметьте самый нижний флажок «проверять на новые Dos-атаки (эвристический метод)».
14. Найдите в дереве настроек пункт «Анализатор скриптов». Выбрав эту настройку отметьте в ней флажок «Сложная проверка прикладных скриптов».
15. Далее нажмите кнопку «Сохранить как» и назовите файл LabWork.prf. Таким образом, вы создали профиль для последующего сканирования.

**Упражнение 2. Поиск уязвимостей ОС Windows XP Professional**

В этом упражнении с помощью XSpider 7.0 вы выполните сканирование хоста с ОС Windows XP Professional для обнаружения имеющихся уязвимостей.

1. Запустите программу XSpider 7.0.
2. Находясь на вкладке «Сканирование», добавьте хост для сканирования.

Для этого в панели инструментов нажмите соответствующую графическую кнопку «Добавить хост».

3. В появившемся окне введите IP-адрес или DNS-имя компьютера, на котором вы работаете, например: Client01.
4. С помощью меню «Профиль» / «Выбрать существующий» откройте окно выбора профиля для сканирования.
5. Пользовательские профили отображаются синим цветом. Щелкните два раза левой кнопкой мыши на профиль LabWork.prf.
6. В панели инструментов нажмите соответствующую графическую кнопку «Начать сканирование выделенных хостов».
7. Появится окно с предупреждением об использовании проверок DoS атаками. Нажмите кнопку «Продолжить»
8. Начнется процесс сканирования. В правой области главного окна программы XSpider 7.0

содержится информация о сканируемом хосте. Убедитесь, что имя хоста, полученное при обратном DNS-запросе такое же, как вы указали на шаге 3 этого упражнения, а также, что в параметрах сканирования используется ваш профиль LabWork.prf.

9. Внизу, в строке статуса синей полосой отображается степень общей завершенности процесса. Дождитесь окончания сканирования.

**Упражнение 3. Просмотр и исправление обнаруженных уязвимостей**

В этом упражнении вы просмотрите результаты сканирования хоста программой XSpider 7.0 и исправите некоторые обнаруженные уязвимости.

1. Перейдите на вкладку «Уязвимости» главного окна программы XSPider 7.0. Вы увидите, что по умолчанию обнаруженные уязвимости упорядочены по степени их опасности. Серьезные уязвимости находятся вверху списка (красные), предупреждения - внизу (зеленые). Рассмотрим и примем меры к устранению некоторых обнаруженных уязвимостей.

2. Нажмите на заголовок столбца «Порт», чтобы упорядочить соответствующим образом все найденные уязвимости. Рассмотрим уязвимости сервиса NetBIOS, который работает через порт 139 / TCP.

3. Найдите в списке уязвимость (оранжевая) «Неочищаемая виртуальная память». Щелкните два раза левой кнопкой мыши на нее.

4. Откроется окно с описанием уязвимости. Выполните действия по устранению данной уязвимости, описанные в области «Решение».

5. Повторите шаги 3, 4 для уязвимости «Слабое шифрование» (оранжевая) и «Scheduler Service» (зеленая).

6. Далее найдите в списке уязвимость (красная) «Обновления Windows». Щелкните по ней два раза левой кнопкой мыши.

7. Откроется окно с описанием уязвимости. Вы увидите список обновлений, которые следует установить на данный компьютер. Если какие-то обновления из списка вам доступны для установки, то выйдите из программы XSpider 7.0 и установите их.

8. После установки некоторых обновлений компьютер требует перезагрузки. Установив обновления, снова запустите программу XSpider 7.0.

9. Повторите операцию сканирования хоста с использованием профиля LabWork.prf.

10. Убедитесь, что исправленные вами уязвимости более не присутствуют в списке обнаруженных.

**Контрольные вопросы.**

1. Перечислите сканеры уязвимостей ПО
2. Достоинство XSPider 7.0

**Лабораторная работа №9: Алгоритм шифрования RSA**

**Цель работы:** изучение возможности Алгоритм шифрования RSA
Время 2 часа

**Теоретическая часть**

Алгоритм RSA был предложен в 1977 году и стал первым полноценным алгоритмом асимметричного шифрования и электронной цифровой подписи. Алгоритм назван по первым буквам фамилий авторов - Рональд Райвест (Ronald Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman).

Стойкость алгоритма основывается на вычислительной сложности задачи факторизации (разложения на множители) больших чисел и задачи дискретного логарифмирования.

**Практическая часть**

Для пересылки сообщения в зашифрованном виде с использованием алгоритма RSA необходимо выполнить пошаговые операции по шифрованию.

Вычисление открытого и закрытого ключа:

Возьмем два больших простых числа p и q.

Определим n, как результат умножения p на q (n= p*q).

Выберем случайное число d. Это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме 1) с результатом умножения (p-1)*(q-1).

Определим такое число e, для которого является истинным следующее соотношение (e*d) mod ((p-1)*(q-1))=1.

Открытым ключом будет числа (e;n), а секретным - (d;n).

Передача открытого ключа (пары чисел) отправителю шифрограммы по незащищенному каналу связи, для зашифровки сообщения (e;n).

Шифрование сообщения «M» полученным открытым ключом для этого: .

разбить исходный открытый текст *M* на блоки,

присвоение каждому блоку цифровое значение, например, в виде:

$M_i = 0, 1, 2, ..., N — 1.$

шифруем каждый блок последовательности чисел $M_i$ по формуле:

$C_i = M_i \pmod N$,

соединить зашифрованные блоки и отправить криптограмму $C_1, C_2, ., C_i$ . .

Выполнить операции по расшифровки для этого:

разбить криптограмму $C_1, C_2, ., C_i$ ., на блоки

находит значение первого блока сообщения «M» из шифрованного значения $C_1$ используя секретный ключ **d** по формуле:

$M_i = C_i \pmod N$

последовательно расшифровываем каждый блок шифрограммы.

соединяем полученные значения блоков сообщения «M» вместе.

При реализации алгоритма на практике, можно использовать не большие простые числа, для быстрого нахождения значения ключей и расшифровки сообщения.

**Пример: шифрование сообщения**

***Действия объекта B:***

- Берем p = 3, q = 11.
- Вычисляем модуль $n = p \times q = 3 \times 11 = 33$.
- Вычисляем значение функции Эйлера для n = 33:

$$\phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20.$$

- Берет в качестве закрытого ключа d простое число из всего диапазона простых чисел до числа 20 (1,3,5,7,11,13,17,19), с учетом условия что оно взаимно простое с ф(Ы), то есть не иметь ни одного общего делителя, кроме
- допустим d= 3.

- Вычисляем значение открытый ключ $e_3$ используя алгоритм Евклида

$$(e*3) \bmod 20=1.$$

Например, e=7,

- Передаем объекту А пару чисел (n = 33, e = 7).

***Действия объекта А:***

- Возьмем сообщение М это «САВ»
- Представим сообщение как последовательность целых чисел в диапазоне 0.. .32.
- Допустим буква А представляется как число 1, буква В это 2 и С = 3.
- Заменим в сообщении буквы «САВ» последовательностью их числового значения т.е. получим 321,
- Разобьем сообщения на блоки, то есть $M_1 = 3$, $M_2 = 1$, $M_3 = 2$.
- Шифрует блок сообщение $M_1$ используя значения открытого ключа e = 7 и n = 33 по формуле: $C_i = (Mi^A e) \bmod n$
- Получим:
  - $C_i = (3^Л 7) \bmod 33 = 2187 \bmod 33 = 9$;
  - $C_2 = (1Л7) \bmod 33 = 1 \bmod 33 = 1$;
  - $C_3 = (2Л7) \bmod 33 = 128 \bmod 33 = 29$;
- Получаем зашифрованное сообщение $C_1$; $C_2$; $C_3$; = 9; 1; 29;
- Передает объекту «В» криптограмму: 9; 1; 29. (Важно четко разделить цифры в криптограмме)

***Действия объекта В:***

- Расшифровываем принятую криптограмму 9;1;29.
- Разбиваем криптограмму 9;1;29 на три блока С; С; С; соответственно.
  - $M_1=(9^A 3) \bmod 33 =729 \bmod 33 = 3$(С);
  - $M_?=(1^A 3) \bmod 33 =1 \bmod 33 = 1$(А);
  - $M_э=(29Л3) \bmod 33 = 24389 \bmod 33 = 2$(В);

Объект «В» получил исходное сообщение, которое послал объект «А».

**Самостоятельное задание**

Используя алгоритм шифрования RSA зашифровать следующие слова из варианта с номером по списку

| | | |
|---|---|---|
| 1. ТАРА | 13 РОЛЬ | 25 РОГА |
| 2. МОСТ | 14 РОТА | 26 КОСА |
| 3. ТОРС | 15 РЕКА | 27 КОРТ |
| 4. ТОРТ | 16 ЗАЛА | 28. ЛАДА |
| 5. ТЕЛО | 17 СЕЛО | 29 ЛАПА |
| 6. ЛОТО | 18 РУКА | 30 СОРТ |
| 7. ЛЕТО | 19 САЛО | 31 СМАК |
| 8. ЗИМА | 20 ГОРА | 32. ХОДЫ |
| 9. СОРТ | 21 ГЕРБ | 33 ПОРТ |
| 10 РОСТ | 22 ГНОМ | 34 МЕРА |
| 11. РЕЙС | 23 НЕБО | 35 СОЛЬ |
| 12 ЛОСЬ | 24 РЕПА | 36 ОМУТ |
| 37 | | |

В качестве кода каждой буквы используйте ее номер в алфавите без учета «ё» и «й». В отчете указать подробный подробным образом вычисления всех компонентов, а также процесса шифрования и расшифровки. Пара простых чисел3, 7

Алфавит для кодировки

1. А,
2. Б,
3. В,
4. Г,
5. Д,
6. Е,
7. Ж,
8. З,
9. И,
10. К,
11. Л,
12. М,
13. Н,
14. О,
15. П,
16. Р,
17. С,
18. Т,
19. У,
20. Ф,
21. Х,
22. Ц,
23. Ч,
24. Ш,
25. Щ,
26. Ъ,
27. Ы,
28. Ь,
29. Э,
30
31. Ю,

**Контрольные вопросы**

1. Что такое функцию Эйлера
2. Порядок генерации ключей в алгоритме RSA
3. Что значит модуль числа

**Лабораторная работа №10 «Шифрование с использованием сети Фейстеля»**

**Цель работы:** изучение метода блочного шифрования, разработанный

Время 2 часа

**Теоретическая часть**

Сеть Фейстеля — это метод блочного шифрования, разработанный Хорстом Фейстелем в лаборатории IBM в 1971 году.

Сегодня сеть Фейстеля лежит в основе большого количества криптографических протоколов. Сеть Фейстеля оперирует блоками открытого текста. Рассмотрим механизм работы на одном из блоков. С остальными блоками действия будут аналогичны.

**Практическая часть**

**Алгоритм работы сети Фестеля при шифровании одного блока**

1. Блок разбивается на две равные части — левую (L) и правую (R).
2. После разбиения левый подблок изменяется функцией f с использованием ключа K:

   **x = f(L, K).**

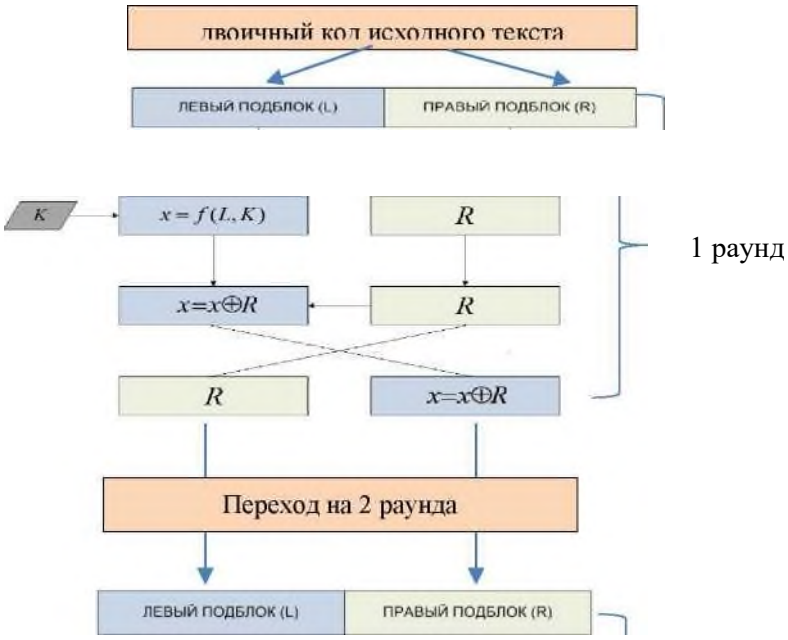
   В качестве функции можно представить себе какое угодно преобразование — например, старый добрый шифр сдвига с на величину ключа K.
3. Полученный подблок складывается по модулю 2 с правым подблоком R, который не менялся:

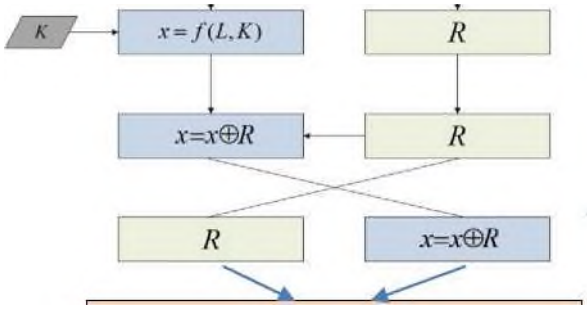
   **x = x©R.**

   Далее полученные части меняются местами и склеиваются

   Такая схема называется ***ячейкой Фейстеля***

   На рисунке представлена ячейки Фейстеля 1 и 2 раундов






Склеивание после 2 раунда для получения шифрограммы

Как видно из рисунка сама сеть Фейстеля состоит из нескольких ячеек. Полученные на выходе первой ячейки подблоки поступают на вход второй ячейки, результирующие подблоки из второй ячейки попадают на вход третьей ячейки и так далее в зависимости от количества *раундов* сети Фейстеля.

В каждом таком раунде применяется заранее определенный *раундовый* ключ. Чаще всего раундовые ключи выработаны из основного секретного ключа K.

Когда все раунды будут пройдены, подблоки текста склеиваются, и получается нормальный такой шифротекст.

Пример шифрования сети Фейстеля на примере.

Возьмем слово **AVADAKEDAVRA** и разобьем его на два блока по шесть символов — *AVADAK* | *EDAVRA*.

За функцию возьмем шифр сдвига на число позиций, определенных раундовым ключом.

Пусть секретный ключ K = [1, 2].

В качестве раундовых ключей возьмем K[0] = 1, K[1] = 2.

Для сложения по модулю 2 переведем текст в двоичный код согласно телеграфному алфавиту, которым вряд ли кто-то еще пользуется вообще.

**Вот что получилось**:

| A | V | A | D | A | K | E | D | A | V | R | A |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 00011 | 11110 | 00011 | 01001 | 00011 | 01111 | 00001 | 01001 | 00011 | 11110 | 01010 | 00011 |

Теперь прогоним через сеть Фейстеля из двух раундов первый блок:

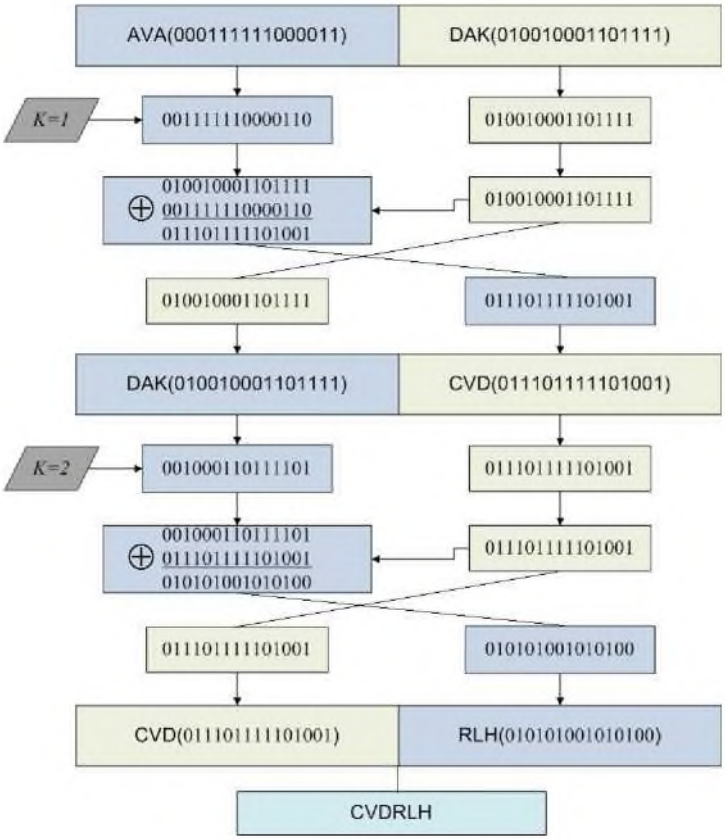



*Рис. 1 Прогон первого блока*

Второй блок зашифровать аналогичными образом и получится **MOSSTR.**

Соединим два блока получим **CVDRLHMOSSTR**

Расшифровка

Расшифрование осуществляется точно так же: шифротекст разбивается на блоки и затем подблоки, левый подблок поступает в функцию, складывается по модулю 2 с правым, и затем подблоки меняются местами.

Отличие заключается в том, что раундовые ключи подаются в обратном порядке, то есть в нашем случае в первом раунде применим ключ K=2, а затем во втором раунде K=1.

**Самостоятельное задание**

Используя сети Фейстеля зашифровать и расшифровать следующие слова:

Альбинос
Археолог
Аграрный
Алгоритм
Амнистия
Банкомат
Батареец
Безлюдье
Березняк
Бороться
Бригадир
Булочная
Верховье
Выполоть
Побороть
Взломать
Высотный

Геодезия
Глазомер
Государь
Гуманизм
Детектор
Дикобраз
Дискобол
Доверить
Доиграть
Дробовик
Криминал
Ласточка
Линолеум
Мудрость
Наркомат

Отчет по лабораторной работе должен включать подробный ход преобразования слов. Для кодирования слов в двоичный код использовать
Таблицу кодов символов Windows-1251 (cp1251).

| Dec | Hex | Символ | Dec | Hex | Символ | Dec | Hex | Символ | Dec | Hex | Символ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 000 | 00 | NOP | 064 | 40 | @ | 128 | 80 | Ъ | 192 | C0 | А |
| 001 | 01 | SOH | 065 | 41 | A | 129 | 81 | Г | 193 | C1 | Б |
| 002 | 02 | STX | 066 | 42 | B | 130 | 82 | , | 194 | C2 | В |
| 003 | 03 | ETX | 067 | 43 | C | 131 | 83 | г | 195 | C3 | Г |
| 004 | 04 | EOT | 068 | 44 | D | 132 | 84 | „ | 196 | C4 | Д |
| 005 | 05 | ENQ | 069 | 45 | E | 133 | 85 |  | 197 | C5 | Е |
| 006 | 06 | ACK | 070 | 46 | F | 134 | 86 | t | 198 | C6 | Ж |
| 007 | 07 | BEL | 071 | 47 | G | 135 | 87 | { | 199 | C7 | З |
| 008 | 08 | BS | 072 | 48 | H | 136 | 88 | € | 200 | C8 | И |
| 009 | 09 | TAB | 073 | 49 | I | 137 | 89 | %0 | 201 | C9 | Й |
| 010 | 0A | LF | 074 | 4A | J | 138 | 8A | Л | 202 | CA | К |
| 011 | 0B | VT | 075 | 4B | K | 139 | 8B | < | 203 | CB | Л |
| 012 | 0C | FF | 076 | 4C | L | 140 | 8C | а | 204 | CC | М |
| 013 | 0D | CR | 077 | 4D | M | 141 | 8D | к | 205 | CD | Н |
| 014 | 0E | SO | 078 | 4E | N | 142 | 8E | ъ | 206 | CE | О |
| 015 | 0F | SI | 079 | 4F | O | 143 | 8F | Ц | 207 | CF | П |
| 016 | 10 | DLE | 080 | 50 | P | 144 | 90 | 5 | 208 | D0 | Р |
| 017 | 11 | DC1 | 081 | 51 | Q | 145 | 91 | ‘ | 209 | D1 | С |
| 018 | 12 | DC2 | 082 | 52 | R | 146 | 92 | ’ | 210 | D2 | Т |
| 019 | 13 | DC3 | 083 | 53 | S | 147 | 93 | “ | 211 | D3 | У |
| 020 | 14 | DC4 | 084 | 54 | T | 148 | 94 | ” | 212 | D4 | Ф |
| 021 | 15 | NAK | 085 | 55 | U | 149 | 95 | • | 213 | D5 | Х |
| 022 | 16 | SYN | 086 | 56 | V | 150 | 96 | — | 214 | D6 | Ц |
| 023 | 17 | ETB | 087 | 57 | W | 151 | 97 | — | 215 | D7 | Ч |
| 024 | 18 | CAN | 088 | 58 | X | 152 | 98 |  | 216 | D8 | Ш |
| 025 | 19 | EM | 089 | 59 | Y | 153 | 99 | ™ | 217 | D9 | Щ |
| 026 | 1A | SUB | 090 | 5A | Z | 154 | 9A | л | 218 | DA | Ъ |
| 027 | 1B | ESC | 091 | 5B | [ | 155 | 9B | > | 219 | DB | Ы |
| 028 | 1C | FS | 092 | 5C | \ | 156 | 9C | ж | 220 | DC | Ь |
| 029 | 1D | GS | 093 | 5D | ] | 157 | 9D | к | 221 | DD | Э |
| 030 | 1E | RS | 094 | 5E | л | 158 | 9E | Ь | 222 | DE | Ю |
| 031 | 1F | US | 095 | 5F |  | 159 | 9F | Ц | 223 | DF | Я |
| 032 | 20 | SP | 096 | 60 | ' | 160 | A0 |  | 224 | E0 | а |
| 033 | 21 | ! | 097 | 61 | a | 161 | A1 | у | 225 | E1 | б |
| 034 | 22 | " | 098 | 62 | b | 162 | A2 | у | 226 | E2 | в |
| 035 | 23 | # | 099 | 63 | c | 163 | A3 | ъ | 227 | E3 | г |
| 036 | 24 | $ | 100 | 64 | d | 164 | A4 | о | 228 | E4 | д |
| 037 | 25 | % | 101 | 65 | e | 165 | A5 | Г | 229 | E5 | е |
| 038 | 26 | & | 102 | 66 | f | 166 | A6 | 1 | 230 | E6 | ж |
| 039 | 27 | ' | 103 | 67 | g | 167 | A7 | § | 231 | E7 | з |
| 040 | 28 | ( | 104 | 68 | h | 168 | A8 | Ё | 232 | E8 | и |
| 041 | 29 | ) | 105 | 69 | i | 169 | A9 | © | 233 | E9 | й |
| 042 | 2A | * | 106 | 6A | j | 170 | AA | е | 234 | EA | к |
| 043 | 2B | + | 107 | 6B | k | 171 | AB | « | 235 | EB | л |
| 044 | 2C | , | 108 | 6C | l | 172 | AC |  | 236 | EC | м |
| 045 | 2D | - | 109 | 6D | m | 173 | AD |  | 237 | ED | н |
| 046 | 2E | . | 110 | 6E | n | 174 | AE | ® | 238 | EE | о |
| 047 | 2F | / | 111 | 6F | o | 175 | AF | I | 239 | EF | п |
| 048 | 30 | 0 | 112 | 70 | p | 176 | B0 | ° | 240 | F0 | р |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 049 | 31 | 1 | 113 | 71 | q | 177 | B1 | ± | 241 | F1 | с |
| 050 | 32 | 2 | 114 | 72 | r | 178 | B2 | I | 242 | F2 | т |
| 051 | 33 | 3 | 115 | 73 | s | 179 | B3 | i | 243 | F3 | у |
| 052 | 34 | 4 | 116 | 74 | t | 180 | B4 | r | 244 | F4 | ф |
| 053 | 35 | 5 | 117 | 75 | u | 181 | B5 | Ц | 245 | F5 | х |
| 054 | 36 | 6 | 118 | 76 | v | 182 | B6 | Н | 246 | F6 | ц |
| 055 | 37 | 7 | 119 | 77 | w | 183 | B7 | • | 247 | F7 | ч |
| 056 | 38 | 8 | 120 | 78 | x | 184 | B8 | ё | 248 | F8 | |
| 057 | 39 | 9 | 121 | 79 | y | 185 | B9 | № | 249 | F9 | |
| 058 | 3A | | 122 | 7A | z | 186 | BA | е | 250 | FA | ъ |
| 059 | 3B | ; | 123 | 7B | { | 187 | BB | » | 251 | FB | ы |
| 060 | 3C | < | 124 | 7C | \| | 188 | BC | j | 252 | FC | ь |
| 061 | 3D | = | 125 | 7D | } | 189 | BD | S | 253 | FD | э |
| 062 | 3E | > | 126 | 7E | ~ | 190 | BE | s | 254 | FE | ю |
| 063 | 3F | ? | 127 | 7F | DEL | 191 | BF | i | 255 | FF | я |

# Лабораторная работа №11 Защита документов MS Office

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

Время 2 часа

**Теоретическая часть**

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

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

**Предполагаемое действие:**

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

**Практическая часть**

Шифрование документа и задание пароля для его открытия Чтобы зашифровать файл и задать пароль для его открытия, выполнитедействия:

. C -

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

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

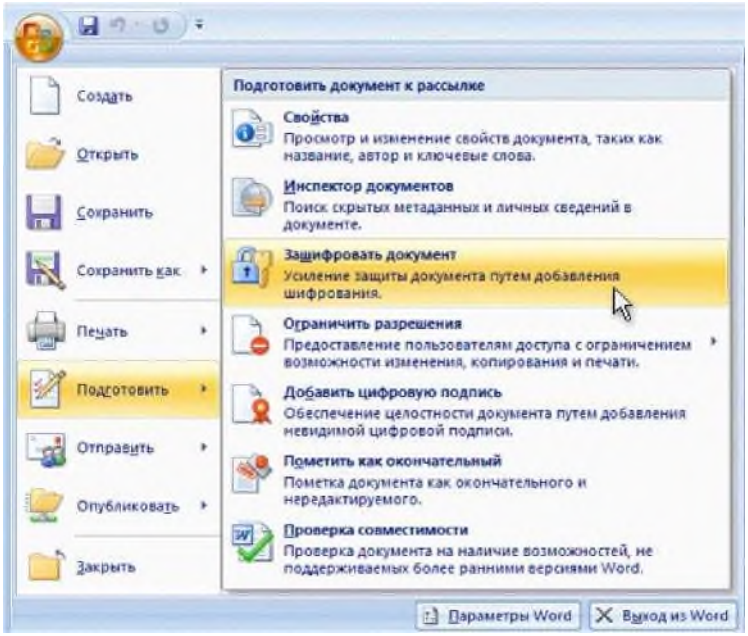



Рис. 1. Меню кнопки MS Office

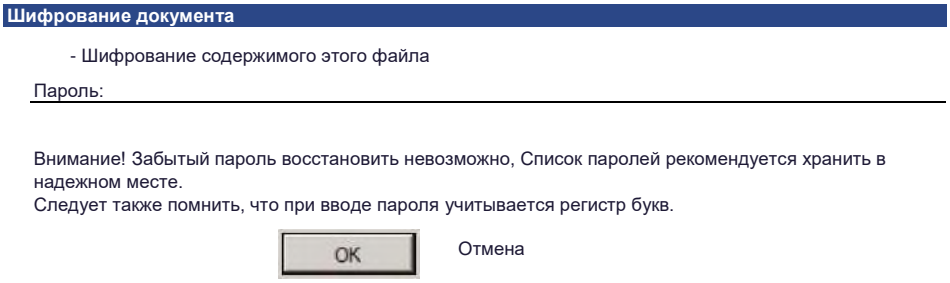



Рис. 2 Диалоговое окно Шифрование документа

**3.** В диалоговом окне **Подтверждение пароля** введите пароль еще раз в поле подтверждение и нажмите кнопку **ОК**. Чтобы сохранить пароль, сохраните файл**.**

Задание пароля для изменения документа

Чтобы обеспечить возможность изменения содержимого толькоавторизованными рецензентами, выполните действия:

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

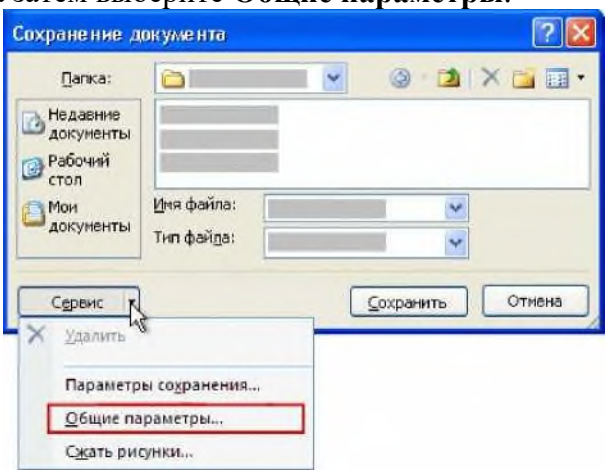



Рис. 3. Окно Сохранение документа

3. Выполните одно или оба следующих действия:

- Если нужно, чтобы рецензенты вводили пароль перед просмотром документа, введите пароль в поле **Пароль для открытия**. По умолчанию при этом используется расширенное шифрование, но в отличие от команды **Зашифровать документ**, описанной выше, в этом случае можно ввести только до 15 знаков.
- Если нужно, чтобы рецензенты вводили пароль перед сохранением внесенных в документ изменений, введите пароль в поле **Пароль разрешения записи**. При этом шифрование не используется. Эта функция предназначена для сотрудничества с рецензентами,которым вы доверяете, а не для защиты файлов.

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

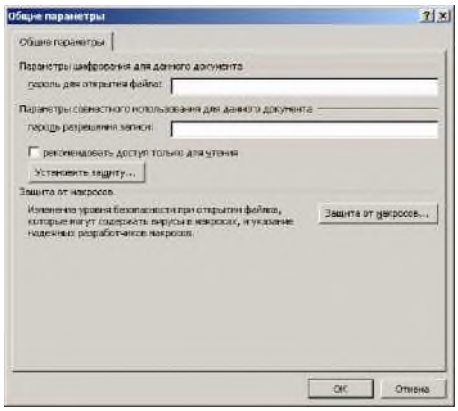



Рис. 4. Диалоговое окно задания пароля

4. Чтобы предотвратить случайное изменение файла рецензентами, установите флажок **рекомендовать доступ только для чтения**. При открытии файла рецензентам будет предложено открыть его в режиме «только для чтения».

5. Нажмите кнопку **ОК**.

6. При запросе подтвердите пароль введите его еще раз, а затем нажмите кнопку **ОК**.

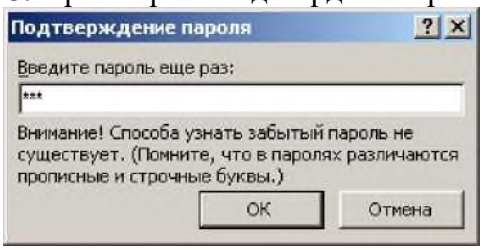



Рис. 5. Окно подтверждения пароля

7. В диалоговом окне **Сохранить как** нажмите кнопку **Сохранить**.

8. Если последует приглашение, нажмите кнопку **Да**, чтобы заменитьсу

**Практические задания**

**Задание 1**. Установка пароля в документе MS Word 2007

- Скопируйте любой файл MS Word 2007 на Рабочий стол.
- Установите пароль на открытие, проверьте его действие. Запишите пароль в тетрадь.
- Установите пароль на изменение, проверьте его действие. Запишит епароль в тетрадь.
- Изучите возможности кнопки **Установить защиту** диалогового окна Общие параметры

**Задание 2.** Установка пароля в документе MS Excel 2007 и MSPowerPoint 2007

- Самостоятельно изучите возможности установки паролей на документыМЗ Excel 2007 и MS PowerPoint 2007.
- Если на ПК установлен MS Office 2010, изучите возможности установки паролей на документы

**Задание 3** Изменение пароля

- Выполните одно или оба следующих действия:
- Откройте файл с использованием пароля для открытия в режимечтения и записи.
- Откройте файл с использованием пароля для изменения в режимечтения и записи.
- Нажмите кнопку **MS Office**, а затем выберите команду **Сохранить как**.
- Щелкните пункт **Сервис**, а затем выберите **Общие параметры** (рис. 3).
- Выберите существующий пароль, а затем введите новый пароль.
- Нажмите кнопку **ОК**.
- При запросе подтвердить пароль введите его еще раз, а затем нажмитекнопку **ОК**.
- Нажмите кнопку **Сохранить**.

- Если последует приглашение, нажмите кнопку **Да**, чтобы заменить существующий файл.

**Задание 4** Удаление пароля

- Выполните одно или оба следующие действия:
- Откройте файл с использованием пароля для открытия в режимечтения и записи.
- Откройте файл с использованием пароля для изменения в режимечтения и записи.
- Нажмите кнопку **MS Office**, а затем выберите команду **Сохранить как**.
- Щелкните пункт **Сервис**, а затем выберите **Общие параметры**.
- Выберите пароль, а затем нажмите клавишу **Del.**
- Нажмите кнопку **ОК**.
- Нажмите кнопку **Сохранить**.
- Если последует приглашение, нажмите кнопку **Да**, чтобы заменить существующий файл

**Задание 5.** Изменение пароля в документах

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

**Задание 6** Создание надёжных паролей

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

Надежный пароль должен отвечать следующим требованиям:

• пароль должен состоять не менее чем из восьми знаков

• должен содержать знаки, относящиеся к каждой из следующих трех групп:

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

**Лабораторная работа №12 Резервное копирование программ, системных параметров и файлов**

**Цель:** изучить возможности резервного копирования в ОС Windows

Время 2 часа

**Теоретическая часть**

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

**Контрольные вопросы**:

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

Компьютер ломается всегда в самый неподходящий момент. Потеря данных может стать не только неприятным событием, но и убыточным. Чтобы избавить себя от танцев с бубнами и сложнейших операций по восстановлению данных, рекомендуем регулярно делать бэкапы важной информации.

**Бэкап (backup) —** резервная копия каких-либо данных. Предположим, у вас на компьютере есть папка с любимыми фотографиями. Вы взяли и скопировали все снимки на отдельную флешку. Это и есть простейший бэкап.

Однако когда речь заходит о сотнях мегабайт информации, а также необходимости сделать образы операционной системы или всего жесткого диска, то взять и «перетянуть» нужные файлы просто так не получится. Намного удобнее и быстрее это делать с помощью специализированных программ.

Как часто делать бэкапы — зависит от важности информации и периодичности ее обновления.

Для каких-то домашних или рабочих файлов резервную копию можно создать всего один раз, а затем обновлять ее по мере того, как папки с документами будут пополняться. Бэкап файлов небольшого сайта стоит делать приблизительно раз в месяц, а для крупных ресурсов этот период может быть сокращен до недели.

Если говорить об ОС Windows, то все зависит от пользователя. Обычно достаточно делать резервную копию после успешной установки какого-либо софта, чтобы в случае повреждения системных файлов или потери данных восстановить копию уже со всеми необходимыми программами. Другой вариант — бэкап свежеустановленной Windows. При нестабильной работе ОС вы сможете быстро восстановить систему, но весь пользовательский софт придется инсталлировать заново.

Начиная с Windows 8, можно создать образ системы без помощи сторонних приложений. Образ — это все данные на вашем компьютере, скопированные в определенный момент времени. Они сохраняются в специальной структуре, из которой впоследствии можно все восстановить обратно той же утилитой.

Сохранять образ рекомендуется на внешний носитель — съемный HDD, флешку (носители должны обязательно быть отформатированы в NTFS) или компакт-диск. Утилита позволяет сделать бэкап системного логического диска на другой диск, например, сохранить все данные с «C» на «D», но делать это не стоит, поскольку «летят» обычно не логические диски, а весь физический, поэтому такой бэкап окажется бесполезным.

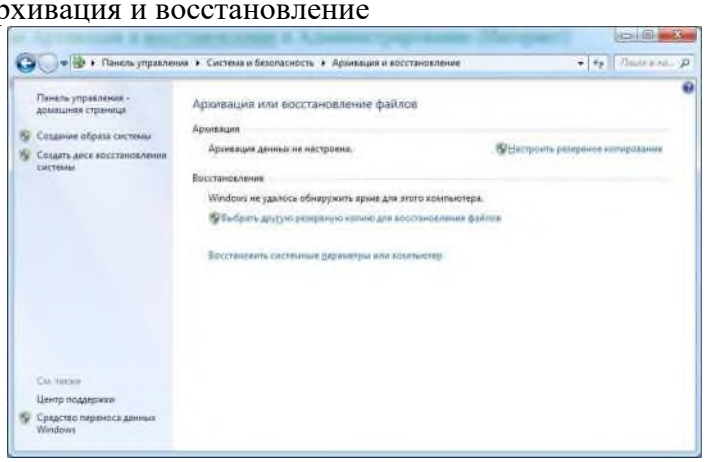
**Практическая часть**

**Задание №1**. Изучите теоретический материал темы, выполнитеконспект в тетради.

**С помощью элемента Архивация и восстановление на Панели управления можно:**

- Выполнять архивацию заданных папок по расписанию и восстанавливать их из резервной копии
- создать полный образ системы
- создать загрузочный диск для восстановления Windows

Рис. 1. Диалоговое окно Архивация и восстановление




Windows позволяет пользователю создавать как резервные копии папок,так и полный образ разделов жесткого диска.

| Тип архивации | Технология и возможности |
|---|---|
| Пользовательские файлы | • Архивация производится на уровне файлов.<br>• Сохранение резервных копий возможно на разделы NTFS и FAT32.<br>• Добавления к первоначальному архиву происходят инкрементно (т. е. добавляются только изменившиеся файлы).<br>• Для сжатия используется формат ZIP.<br>• Имеется возможность восстановления отдельных папок ибиблиотек. |
| Образ раздела | • Архивация производится на уровне блоков (в архив включаются только используемые блоки).<br>• Сохранение резервных копий возможно только на разделы NTFS.<br>• Полный образ сохраняется в формате VHD, при этом сжатия файлов не происходит. В дальнейшем образы создаются инкрементно, т. е. добавляются только изменившиеся блоки. Для этого используется функционал теневых копий. Последующее создание полных образов также возможно.<br>• Образы разделов дают возможность быстрого восстановления ОС и файлов в случае выхода из строя жесткого диска. |

Эти функции в совокупности с возможностью загрузки в среду восстановления без установочного диска способны удовлетворить запросы большинства пользователей. Теперь вполне можно обходиться без сторонних программ резервного копирования.

**Изменения в пользовательском интерфейсе**

Изменения в возможностях архивации Windows затронули не толькотехнологии, но и пользовательский интерфейс. В частности:

- переработан интерфейс главного окна элемента панели управления
- Архивация и восстановление
- Создан новый пользовательский интерфейс для управленияпространством, занятым под резервные копии
- упрощено восстановление файлов, выполняющееся с помощью мастера
- реализована интеграция с центром поддержки для своевременногоуведомления пользователей о необходимости создания резервной копии

**Задание №2**. **Настройка параметров регулярного резервного копирования**

По умолчанию резервное копирование не настроено. Щелкните ссылку **Настроить резервное копирование** в главном окне элемента **Панели управления**, чтобы задать параметры архивации.

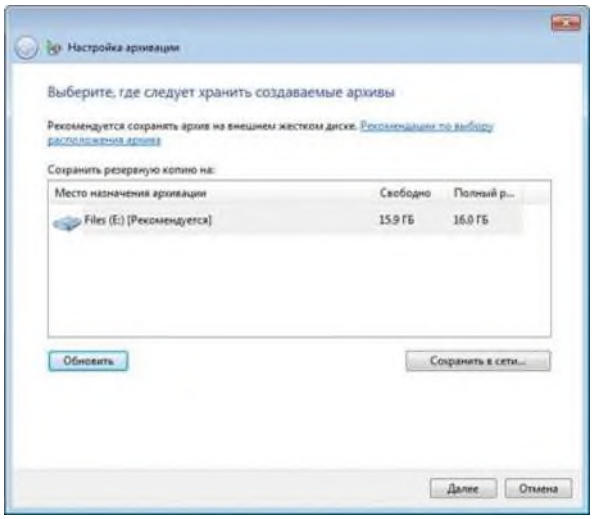



Рис. 2. Диалоговое окно Настройка архивации

**Варианты размещения резервной копии файлов**

| **Размещение** | **Комментарии** |
|---|---|
| Внутренний жесткий диск | Вы можете разместить архивные файлы на:<br>• несистемном разделе того же физического диска, на котором установлена ОС<br>• любом разделе другого физического диска<br>Рекомендуется второй вариант, ибо в случае выхода из строя системного диска вы потеряете как операционную систему, так и резервные копии. |
| Внешний жесткий диск | Если настроена архивация по расписанию, внешний жесткий диск должен быть подключен на момент создания резервной копии.<br>**Примечание:** Windows не поддерживает создание образов на USB дисках с флэш-памятью. |
| Локальная сеть | Поддерживается архивация только на компьютеры сети, работающие под управлением Windows. Пользователю потребуются учетные данные для доступа к компьютеру, на котором размещается резервная копия. |

Вы можете размещать архивы файлов на разделах, отформатированныхкак в файловую систему NTFS, так и в FAT32. При архивации на жесткий диск файлы размещаются в корневом каталоге раздела. Для архива нельзя задатьвложенную папку, но можно размещать на этом диске другие файлы и папки.

Определившись с размещением архива, необходимо задать параметры архивации. Можно предоставить это решение операционной системе, а можно выбрать папки самостоятельно.

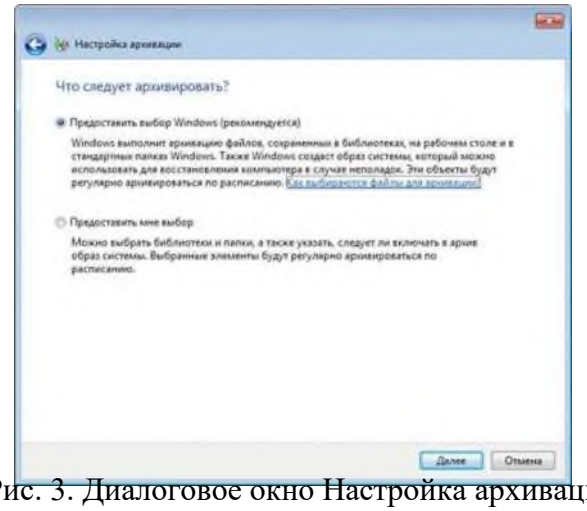



Рис. 3. Диалоговое окно Настройка архивации

При самостоятельном выборе можно создать резервные копии:

пользовательских файлов, включая библиотеки

папок локального диска


Рис. 4. Диалоговое окно Настройка архивации

В конце Windows выводит сводку параметров резервного копирования.

полного образа системы

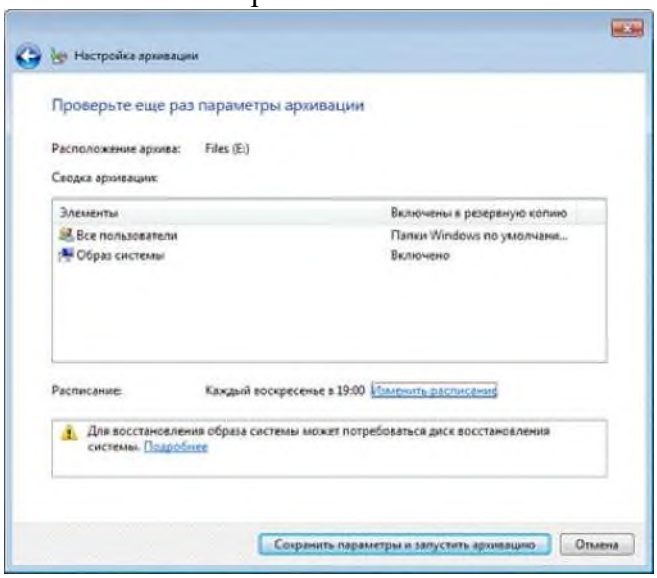



Рис. 5. Диалоговое окно Настройка архивации

Щелкните ссылку **Изменить расписание**, чтобы настроить резервное копирование по расписанию в удобное вам время.

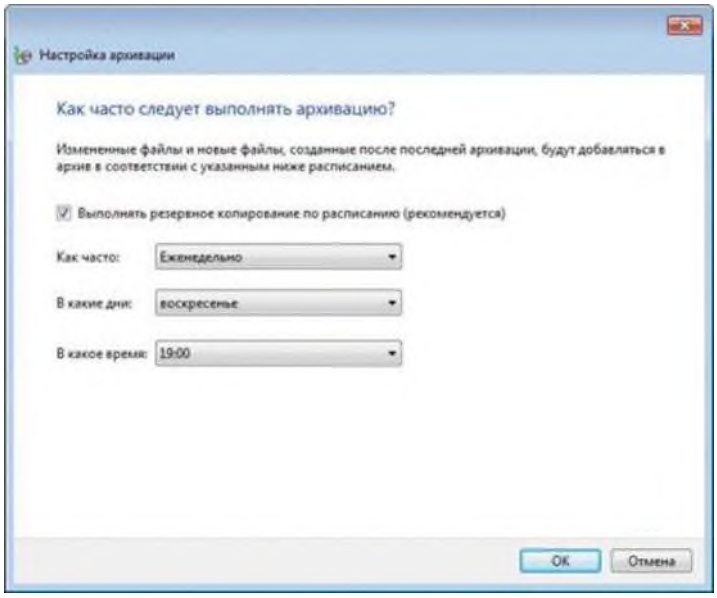



Рис. 6. Диалоговое окно Настройка архивации

Заданные параметры расписания сохраняются в **планировщике заданий**,который отвечает за своевременный запуск архивации.

По завершении настройки параметров архивации пользователь возвращается в главное окно элемента **Панели управления**.

**Задание №3 Создание резервной копии файлов**

Теперь в главном окне отображаются все параметры архивации. Нажмитекнопку **Архивировать**, чтобы начать процесс резервного копирования.

Ход архивации отображается с помощью полосы прогресса, но вы можетепосмотреть подробности, нажав кнопку **Просмотр сведений**.


Рис. 7. Диалоговое окно Архивация или восстановление файлов

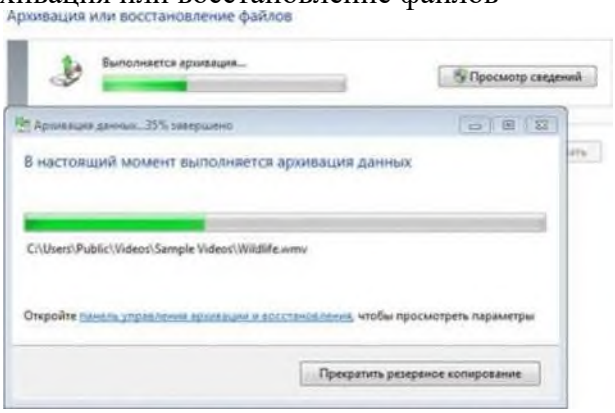



Рис. 8. Диалоговое окно выполнения архивации файлов

Завершив архивацию, можно посмотреть сведения об используемомдисковом пространстве и перейти к управлению архивами.

**Задание №4 Создание образа системы**

В отличие от файловых архивов, системный образ можно сохранить только на диске, отформатированном в файловую систему **NTFS**. Это обусловлено тем, что образы представляют собой файлы в формате **VHD**, размер которых может превышать 4 Гб (предельный размер файла для FAT32).

Первый системный образ представляет собой полный снимок раздела, а последующие являются инкрементными, т. е. включают в себя лишь изменения по сравнению с предыдущим образом. Эта возможность, позволяющая сэкономить дисковое пространство, реализована с помощью теневых копий.

Такой принцип создания образов применяется при их сохранении на внутренних,внешних и оптических дисках. Для внутренних и внешних дисков этот принцип действует до тех пор, пока на диске имеется достаточно места. Когда место заканчивается, создается полный образ, а все предыдущие удаляются. Что же касается сетевых дисков, то на них всегда создается полный образ, а старыйобраз при этом перезаписывается новым.

Рассмотрим создание первого образа.

- В левой панели элемента **Архивация и восстановление** нажмите ссылку **Создание образа системы**. Откроется окно с вариантами размещения образа.
- На следующем шаге вы сможете выбрать разделы для архивации.

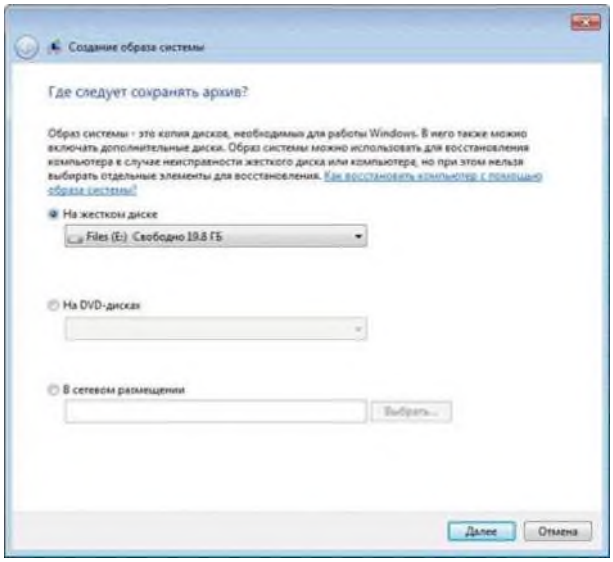



Рис. 9. Создание образа системы - шаг 1

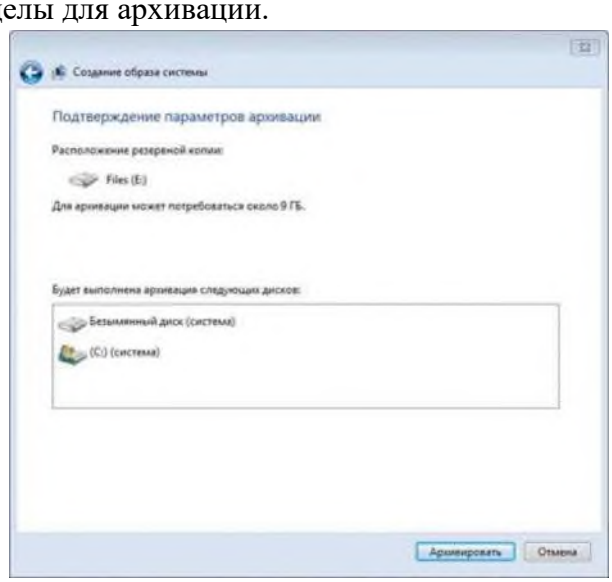



Рис. 10. Создание образа системы - шаг 2

- В образ автоматически включается **служебный раздел со средой восстановления (Windows RE)** и **системный раздел**. Исключить их из резервной копии нельзя. Если в системе имеются другие разделы, вы сможете выбрать их на этом шаге.
- Определившись с выбором разделов, нажмите кнопку **Архивировать**, чтобы начать процесс создания резервной копии.

Все следующие образы создаются точно так же. Они содержат толькоизменившиеся блоки. Для того чтобы снова создать полный образ системы, вам необходимо удалить существующие образы или перенести их на другой раздел. Вы также можете переместить их из корневого каталога диска во вложенные папки, однако примите к сведению, что в этом случае их не увидит программа восстановления системы из образа.

**Задание №5 Управление пространством**

В главном окне элемента панели управления **Архивация и восстановление** щелкните ссылку **Управление пространством**. Откроется окно, в котором выводится информация о расположении архива, сводка об использовании дискового пространства, а также ссылки и кнопки

для просмотра архивов и управления ими.

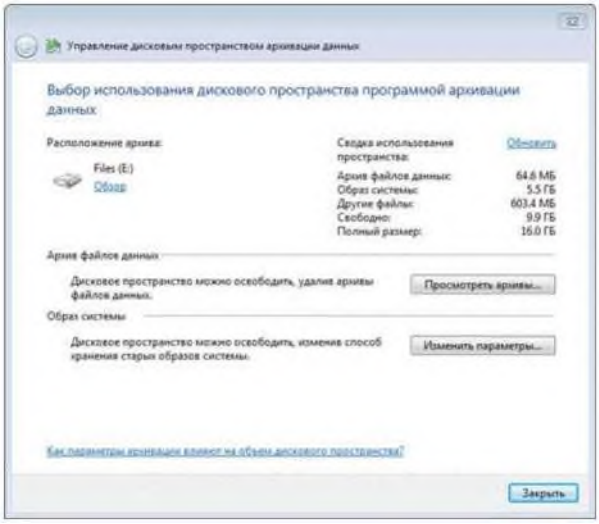



Рис. 11. Диалоговое окно Управление дисковым пространством архивации

**Расположение резервных копий**

Помимо просмотра подробных сведений об используемом пространстве, можно открыть место хранения резервной копии - нажмите ссылку **Обзор**, и файлы откроются в Проводнике. Windows распознает папку с архивом и предоставляет доступ к параметрам восстановления.

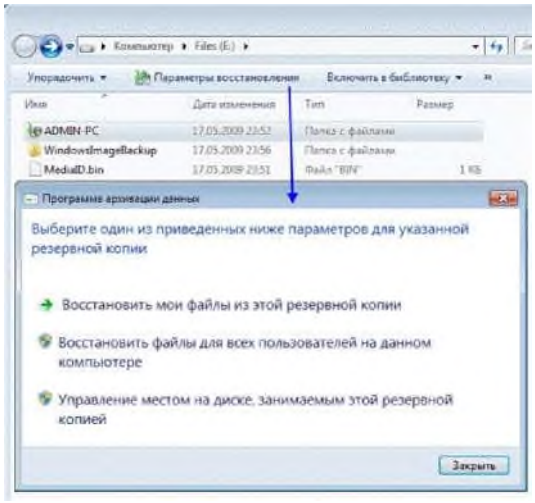



Рис. 12. Определение расположения резервных копий

Из списка папки: **%COMPUTERNAME%** (в данном случае **ADMIN-PC**) - архив файлов

**WindowsImageBackup -** папка с образом раздела

**Содержимое файлового архива**

Открыть папку с архивом можно с помощью контекстного меню. Содержимое архива прозрачно для пользователя - внутри ZIP-архивы, и при желании файлы можно оттуда извлечь непосредственно из Проводника.

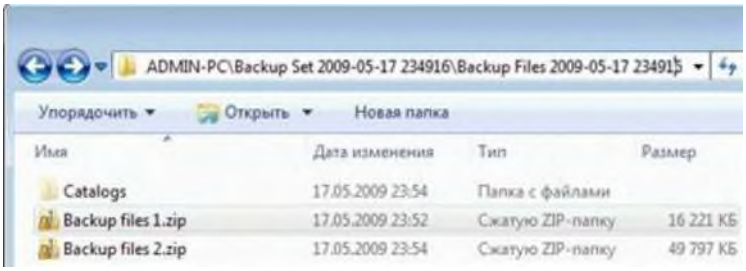



Рис. 13. Содержимое архива

Однако из **Панели управления** восстанавливать файлы удобнее,например, благодаря встроенному поиску.

**Содержимое образа**

Архивный образ системы создается в формате **VHD** и хранится в папке **WindowsImageBackup** наряду со вспомогательными файлами.

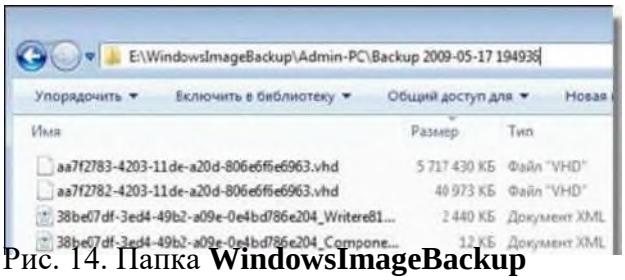



Рис. 14. Папка **WindowsImageBackup**

Увидеть его содержимое можно, воспользовавшись новой возможностью Windows - подключением виртуальных жестких дисков в утилите управления дисками (**Пуск - Поиск - diskmgmt.msc - Действие - Присоединить виртуальный жесткий диск**).

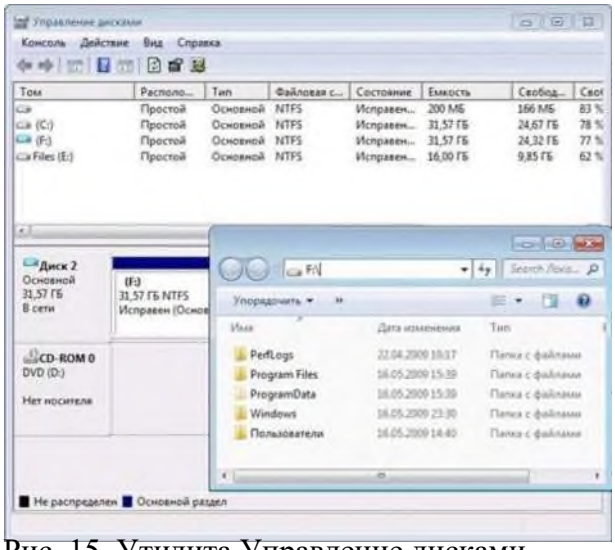



Рис. 15. Утилита Управление дисками

Возможно, вас заинтересует вопрос, можно ли добавить файлы на виртуальный жесткий диск. Технически это возможно, однако с точки зрения восстановления средствами Windows это ничего не даст. Лучше сделать новый образ - изменившиеся блоки добавляются инкрементно на основе теневых копий, что позволяет сэкономить дисковое пространство.

**Просмотр и удаление резервных копий**

Из окна управления пространством пользователь может удалять файловые архивы и резервные образы.

Нажмите кнопку **Просмотр архивов** в окне управления пространством, чтобы увидеть список архивов.

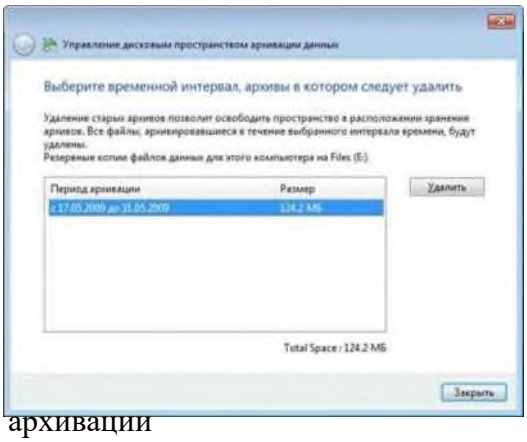



Рис. 16. Период архивации

Windows находит все архивы и отображает период архивации и занимаемое дисковое пространство. В этом окне можно удалить ненужные архивы.

Чтобы удалить резервные образы, нажмите кнопку **Изменить параметры** в окне управления пространством. Откроются параметры хранения образов.

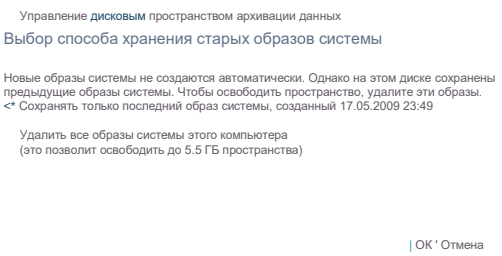



Рис. 17. Параметры удаления

Система предлагает пользователю удалить абсолютно все образы, либо все образы кроме последнего.

**Рекомендации по резервному копированию**

Все знают, что нужно регулярно выполнять резервное копирование, но приэтом далеко не все его делают. Учитывая широкие возможности резервного копирования в Windows , о потере важных данных вы будете сожалеть только в том случае, если не настроите регулярную архивацию.

Для хранения резервных копий подойдет отдельный жесткий диск - внутренний или внешний, подключаемый по USB или FireWire. Если в вашем распоряжении есть сетевой диск, его также можно задействовать. Хранение резервных копий на другом разделе того же диска, где установлена ОС, не является хорошей идеей. В случае выхода из строя диска вы потеряете как систему, так и резервные копии.

Общие рекомендации, которые нужно корректировать в зависимости от имеющегося свободного дискового пространства:**Образы системного раздела**

- **Первый образ.** Установите Windows , затем все обновления и драйверы. Убедившись в нормальной работе ОС и устройств, создайте первый резервный образ.
- **Второй образ.** Установите все приложения и настройте систему по своему желанию. Поскольку более тонкая настройка ОС, как правило, производится по ходу ее использования, поработайте в Windows пару недель. Убедившись в нормальной работе ОС, создайте второй резервный образ. Если перед этим вы удалите первый образ, у вас будет полный образ полностью обновленной и настроенной системы с любимым набором приложений.
- **Последующие образы.** В зависимости от имеющегося у вас свободного дискового пространства, создавайте последующие образы ежемесячно/ежеквартально. Если возникнет проблема, требующая восстановления из образа, вы сможете вернуться к относительно недавнему состоянию системы.

Архивы пользовательских файлов

- Частота архивации ваших файлов определяется тем, насколько они ценны для вас и как часто вы добавляете или создаете новые файлы. В общем случае рекомендуется выполнять архивацию еженедельно или два раза в месяц. В сочетании с ежемесячным созданием образов системы вручную у вас будет отличный резервный набор, позволяющийне только вернуть с систему к недавнему рабочему состоянию, но и восстановить все ваши данные и файлы. Вы всегда сможете освободить дисковое пространство, удалив старые архивы, если место на диске потребуется для других нужд.
- В графическом интерфейсе невозможно задать разные расписания для создания

образов и архивации данных. Поэтому, если вы хотите в разное время автоматически создавать образ и выполнять архивацию файлов, воспользуйтесь утилитой командной строки **wbadmin** и **планировщиком заданий**.

**Контрольные вопросы**:

1. Перечислите типы архивации и их возможности, которые можно выполнить с помощью элемента Панели управления Архивация и восстановление
2. Перечислите варианты размещения резервной копии файлов
3. Опишите алгоритм создания резервной копии файлов
4. Опишите алгоритм создания резервной копии образа системы
5. Опишите возможности использования диалогового окна Управление пространством
6. Перечислите рекомендации по резервному копированию

**Лабораторная работа №13 Методы сжатия. Алгоритм Хаффмена**

**Цель:** ознакомиться с общими принципами сжатия информации сиспользованием метода Хаффмена

Время 2 чвса

Исследование экономичных схем поиска привело к появлению метода сжатия информации, который был назван методом Хаффмена. Фактически Дэвид Хаффмен (19251999) просто нашел метод решения задачи для сокращения объемов передаваемой и хранимой информации, и построенные на его основе программы оказались настолько эффективны, что вызвали целый поток конкурентных исследований в этой области.

Первоначально речь шла о сжатии текстовой информации, но затем внимание стало обращаться к экономному хранению других типов данных: изображений, музыки, кинофильмов.

**Алгоритм Хаффмена**

Суть алгоритма Хаффмена сводится к следующему:

- буквы алфавита сообщений выписываются в основной столбец таблицы в порядке убывания вероятностей;
- две последние буквы объединяются в одну вспомогательную букву, которой приписывается суммарная вероятность;
- вероятности букв, не участвовавших в объединении, и полученная суммарная вероятность снова располагаются в порядке убывания вероятностей, а две последние объединяются до тех пор, пока не получают единственную вспомогательную букву с вероятностью единица;
- далее для построения кода используется бинарное дерево, в корне которого располагается буква с вероятностью единица, при ветвлении ветви с большей вероятностью присваивается код единица, а с меньшей — код ноль (возможно левой — единица, а правой — ноль).

**Пример 1.** Рассмотрим условный алфавит из восьми букв, каждой из которых приписана соответствующая вероятность ее появления в сообщении (табл. 1).

| Буква | Вероят-ность | Вспомогательные столбцы вероятностей | Кол Хаффмена |
|---|---|---|---|
| Z1 | 0,22 | 0,22 0,22 0,26 0.32 0,42 0.581 1 | 01 |
| Z2 | 0,20 | 0,20 0,20 0,22 0,26 0,32 0,42 J | 00 |
| Z3 | 0,16 | 0,16 0,16 0,20 0,2210,2б/ | 110 |
| Z4 | 0,16 | 0.16 0.16 0.16 j 0,20 | III |
| Z5 | 0,10 | 0.10 0J6 0.161 | 100 |
| Z6 | 0,10 | 0, 101 0,10 | 1011 |
| Z7 | 0,04 ’ | 0.06 1 | 10101 |
| Z8 | 0,02 | | 10100 |

L = 0,22 x 2 + 0,20 x 2 + 0.16 x 3 + 0.16 x 3 + 0,10 x 3 + 0,10 x 4 + 0.04 x 5 +-0.02 x 5 = 2.8;
И =2.76:
L - H = 0,04.

Таблица 1

Кодовое дерево представлено на рисунке 1.

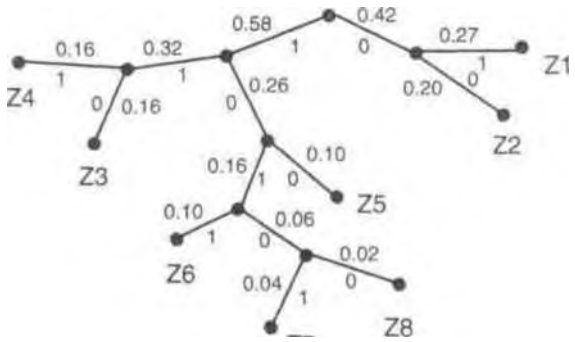



Рис. 1. Кодовое (бинарное) дерево для примера 1.

**Практические задания:**

**Задача 1.** Даны символы a, b, c, d с частотами $f_a = 0{,}5$; $f_b = 0{,}25$; $f_c = 0{,}125$; $f_d = 0{,}125$.

Построить эффективный код методом Хаффмена.

**Задача 2.** Построить код Хаффмена для алфавита, состоящего из пяти символов a, b, c, d, e с частотами (вероятностями появления в тексте) a - 0,37;b - 0,22; c - 0,16; d - 0,14; e — 0,11

1. на_дворе_трава_на_траве_дрова_не_руби_дрова_на траве_двора;
2. мороз_и_солнце_день_чудесный_еще_ты_дремлешь_друг_прелестный (А. Пушкин);
3. если_жизнь_тебя_обманет_не_печалься_не_сердись_в_день_уныния_с мирись_день_веселья_верь_настанет (А. Пушкин);
4. имеем_не_храним_потеряем_плачем;
5. в_горнице_моей_светло_это_от_ночной_звезды_матушка_возьмет_вед ро_молча_принесет_воды (Н. Рубцов);
6. выше_гор_могут_быть_только_горы_на_которых_еще_не_бывал (В.Высоцкий);
7. белеет_парус_одинокий_в_тумане_моря_голубом_что_ищет_он_в_стр ане_далекой_что_кинул_он_в_краю_родном (М. Лермонтов);
8. в_глубокой_теснине_Дарьяла_где_роется_Терек_во_мгле_стариннаябашня стояла_чернея на черной скале (М. Лермонтов);
9. не_презирай_совета_ничьего_но_прежде_рассмотри_его (И.А.Крылов);
10. образование_это_то_что_остается_когда_все_выученное_забыто;
11. математику_уже_за_то_любить_следует_что_она_ум_в_порядок_приводит (М.В. Ломоносов);
12. математика_это_язык_на_котором_написана_книга_природы (Галилео Галилей)
13. деньги_дороги_жизнь_человеческая_ещё_дороже_а_время_дороже_все го (А.В. Суворов);

15.легко в учении_тяжело_в_походе_тяжело_в_учении_легко_в_походе(А.В. Суворов)

Подсчитать частоты символов во фразе и по этим частотам построить код Хаффмена:

**Контрольные вопросы:**

1. Поясните алгоритм построения кода для сообщения с заданными вероятностями букв по алгоритму Хаффмена
2. Поясните алгоритм построения кода для произвольного сообщения по алгоритму Хаффмена

**Лабораторная работа№14 Обеспечение безопасности локальной сети. Настройка параметров безопасности браузера**

**Цель:** изучить возможности настройки безопасности локальной сети ибраузера
Время 2 часа

**Теоретическая часть**

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

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

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

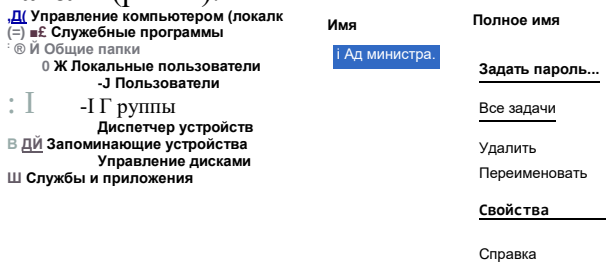



Рис. 1. Диалоговое окно Управление компьютером

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

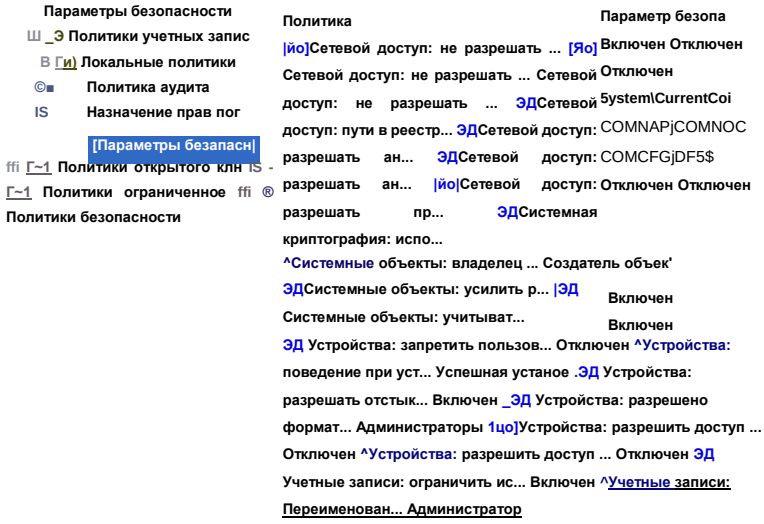



Рис. 2. Находим в системном реестре запись Переименование учетнойзаписи Администратор

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

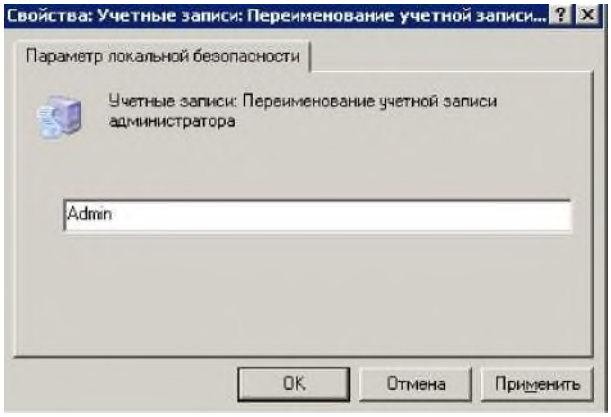



Рис. 3. Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий у нас получилась учетная ЗапucbAdmin с паролем 12345 и правами администратора (рис. 4).


Рис. 4. Окно входа в ОС Windows XP

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

**Примечание**

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, использовав окно **Учетные записи пользователей**, что гораздо проще (рис. 5).

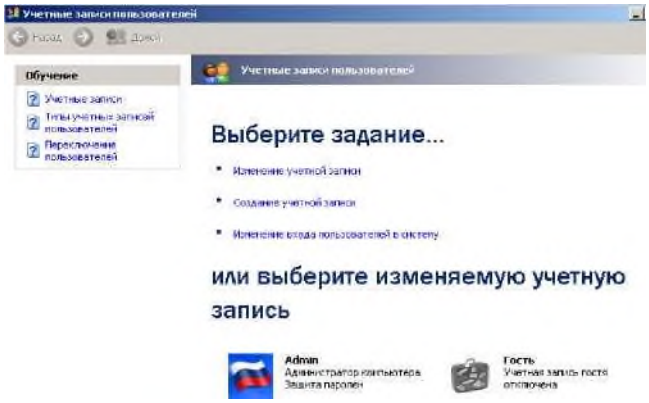



Рис. 5. Окно Учетные записи пользователей

**Примечание**

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

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

У нас окно входа в систему содержит подсказку Admin, давайте ее уберем, сделав окно пустым. Для начала в окне **Учетные записи пользователей** жмем на кнопку **Изменение входа пользователей в систему** и уберем флажок **Использовать страницу приветствия** (рис.6 и рис. 7).

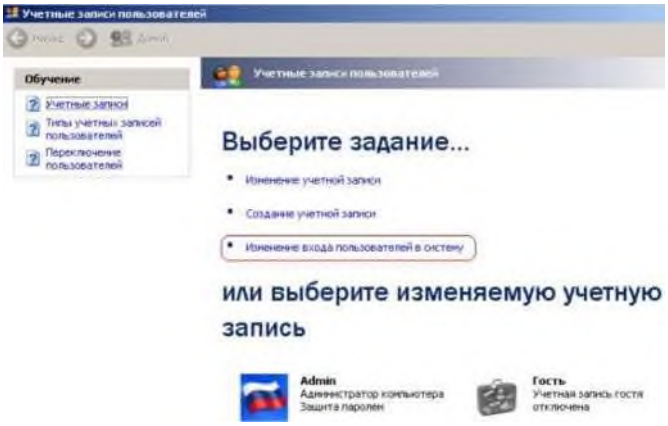



Рис. 6. Окно Учетные записи пользователей

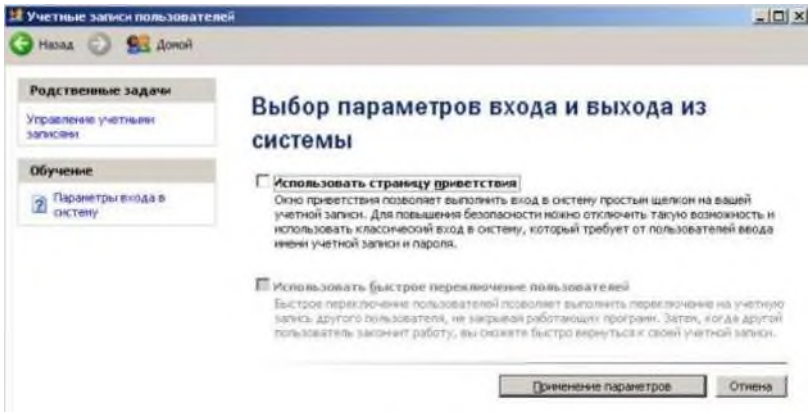



Рис. 7. Убираем флажок Использовать страницу приветствия

Теперь повысим безопасность сети еще на одну условную ступень,сделав оба поля окна приветствия пустыми (рис. 8).


Рис. 8. Обе строки данного окна сделаем пустыми

Выполним команду **Панель управления-Администрирование - Локальные политики безопасности- Локальные политики-Параметры безопасности—Интерактивный вход: не отображать последнего имени пользователя**. Эту запись необходимо включить (рис. 9).

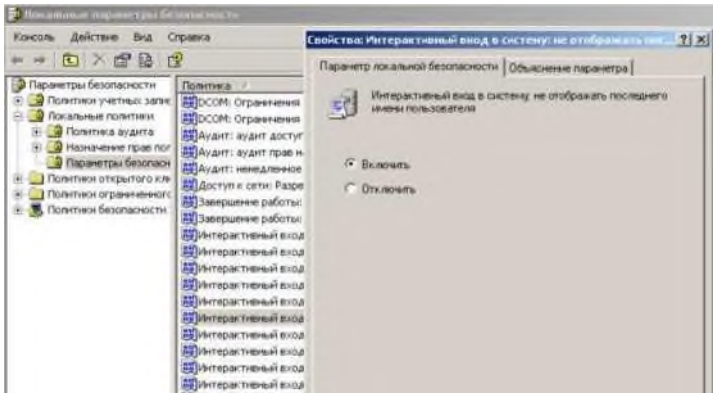



**Рис. 9.** Активируем переключатель Включить

Теперь после завершения сеанса пользователь должен угадать нетолько пароль, но и имя пользователя (рис. 10).


Рис. 10. Обе строки окна приветствия пусты

Выявление сетевых уязвимостей сканированием портов ПК

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

TCP/IP port — это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт — потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP(отправка почты) — 25 порт, WWW — 80 порт, FTP —21 порт.

Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютер.

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

finger — получение информации о пользователях

talk— возможность обмена данными по сети между пользователями

bootp — предоставление клиентам информации о сети

systat — получение информации о системе

netstat — получение информации о сети, такой как текущие соединения

rusersd — получение информации о пользователях,зарегистрированных в данный момент

Просмотр активных подключений утилитой Netstat

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

ссервером. **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются).

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

CLOSED — Закрыт. Сокет не используется.

LISTEN — Ожидает входящих соединений.

SYN_SENT — Активно пытается установить соединение.

SYN_RECEIVED — Идет начальная синхронизация соединения.

ESTABLISHED — Соединение установлено.

CLOSE_WAIT — Удаленная сторона отключилась; ожидание закрытиясокета.

FIN_WAIT_1 — Сокет закрыт; отключение соединения.

CLOSING — Сокет закрыт, затем удаленная сторона отключилась;ожидание подтверждения.

LAST_ACK — Удаленная сторона отключилась, затем сокет закрыт;ожидание подтверждения.

FIN_WAIT_2 — Сокет закрыт; ожидание отключения удаленнойстороны.

TIME_WAIT — Сокет закрыт, но ожидает пакеты, ещё находящиеся всети для обработки

Примечание

Что такое «сокет» поясняет рис. 11. Пример сокета - 194.86.6..54:21

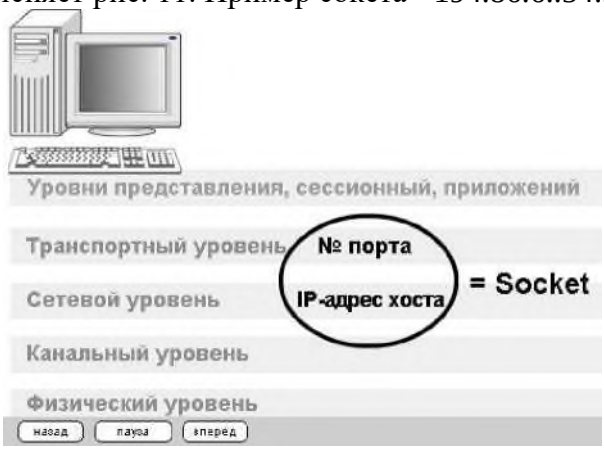



Рис. 11. Сокет это № порта + IP адрес хоста

**Выполните практическое задание:**

**Задание 1. Обнаружение открытых на ПК портов утилитой Netstat**

Для выполнения практического задания на компьютере необходимовыполнить команду **Пуск-Выполнить**. Откроется окно **Запуск программы**, в нем введите команду **cmd** (рис. 12).

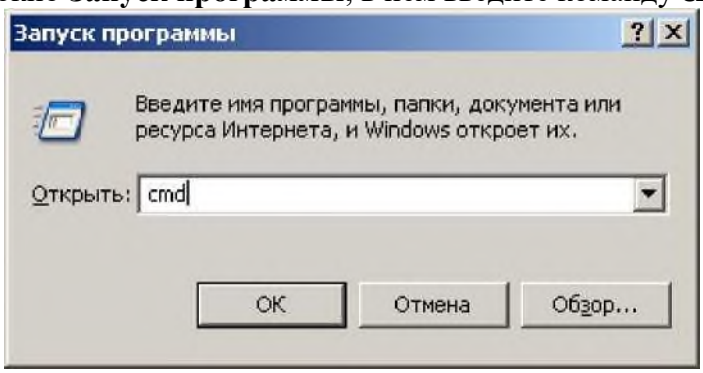



Рис. 12. Окно Запуск программы

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

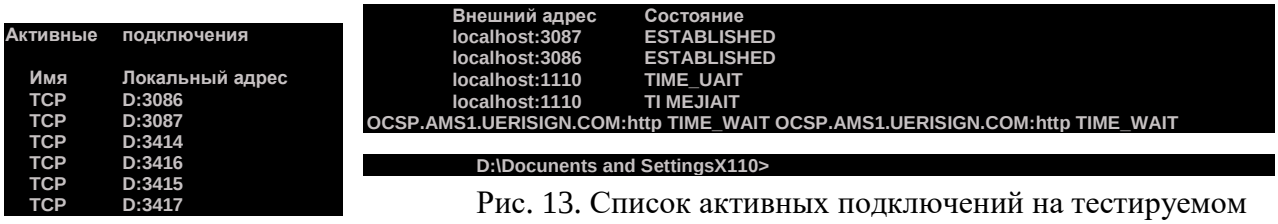



Рис. 13. Список активных подключений на тестируемом ПК

Запустите на вашем ПК Интернет и зайдите, например на **www.yandex.ru**. Снова выполните команду **netstat** (рис. 14). Как видим, добавилось несколько новых активных портов с их различными состояниями.

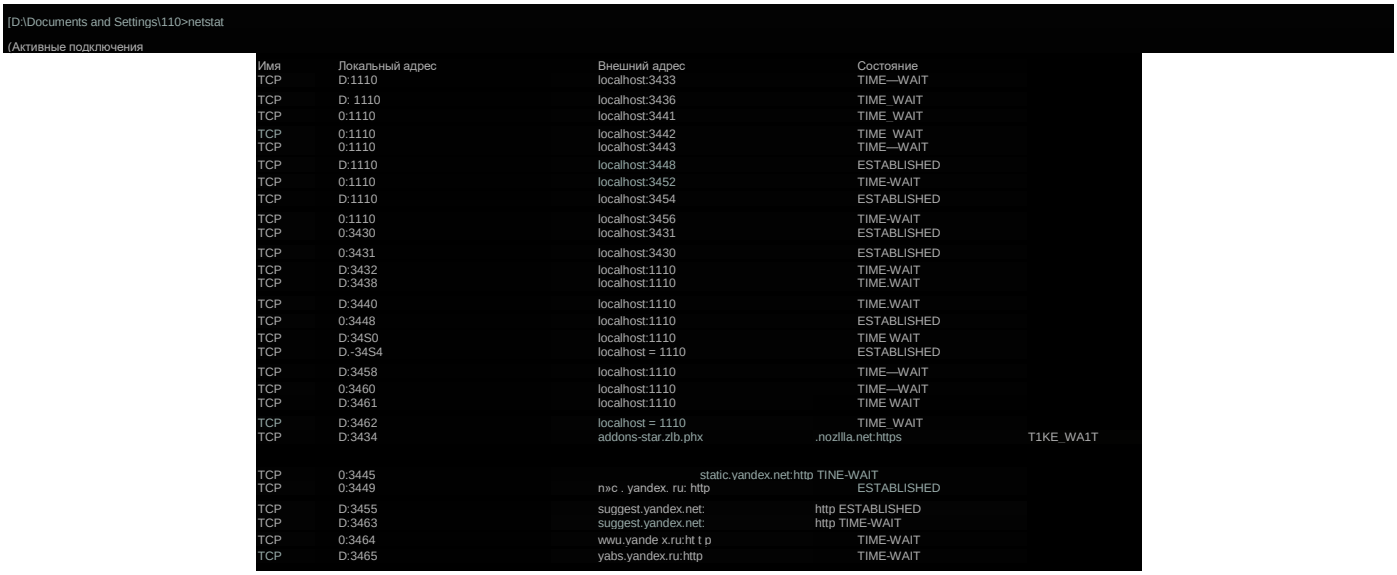



Рис. 14. Активные подключения при работе ПК в Интернет

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

| | |
|---|---|
| -i | Показывать состояние автоматически сконфигурированных (auto-configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но не найденные во время загрузки, не показываются. |
| -n | Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа. |
| -r | Показать таблицы маршрутизации. При использовании с опцией -s, показывает статистику маршрутизации. |
| -s | Показать статистическую информацию по протоколам .При использовании с опцией -r, показывает статистику маршрутизации. |
| -f семейство_адресов | Ограничить показ статистики или адресов управляющих блоков только указанным семейством_адресов, в качестве которого можно указывать: **inet** Для семейства адресов **A^ШЕТ**,или **unix** Для семейства адресов **AF_UNIX**. |

Таблица 1. Ключи для команды netstat

**Программа NetStat Agent**

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

Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера,

просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд **Ping** и**TraceRoute** (рис. 15).

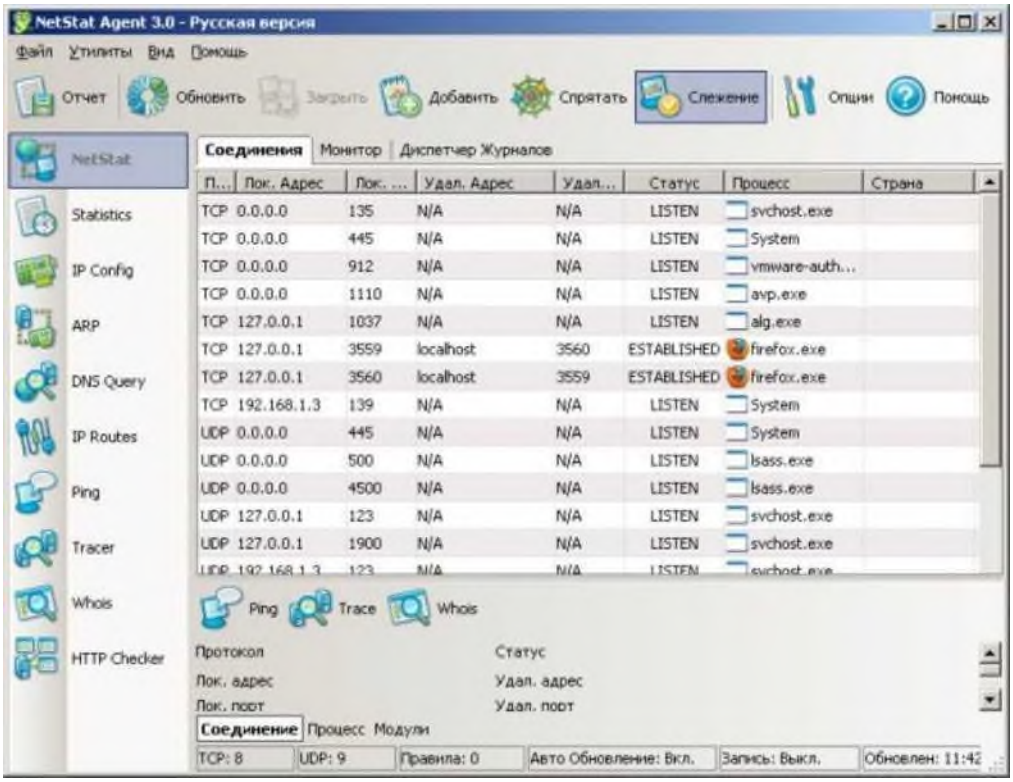



Рис. 15. Главное окно программы NetStat Agent

В состав программы NetStat Agent вошли следующие утилиты:

**NetStat** — отслеживает TCP и UDP соединения ПК (при этом отображается географическое местоположение удаленного сервера и имя хоста).

**IPConfig** — отображает свойства сетевых адаптеров и конфигурацию сети.

**Ping** — позволяет проверить доступность хоста в сети.

**TraceRoute** — определяет маршрут между вашим компьютером и конечным хостом, сообщая все IP-адреса маршрутизаторов.

**DNS Query** — подключается к DNS серверу и находит всю информацию о домене (IP адрес сервера, MX-записи (Mail Exchange) и др.).

**Route** — отображает и позволяет изменять IP маршруты на ПК.

**ARP** — отслеживает ARP изменения в локальной таблице.

**Whois** — позволяет получить всю доступную информацию об IP- адресе или домене.

**HTTP Checker** — помогает проверить, доступны ли Ваши веб-сайты.

**Statistics** — показывает статистику сетевых интерфейсов и TCP/IP протоколов.

Сканер портов Nmap (Zenmap)

**Nmap —** популярный сканер портов, который обследует сеть и проводит аудит защиты. Использовался в фильме «Матрица: Перезагрузка» при взломе компьютера. Наша задача не взломать, а защитить ПК, поскольку одно и то же оружие можно использовать как для защиты, так и для нападения. Иначе говоря, сканером портов **nmap** можно определить открытые порты компьютера, а для безопасности сети пользователямрекомендуется закрыть доступ к этим портам с помощью брандмауэра (рис. 16).

Обычно для того, чтобы просканировать все порты какого-либо компьютера в сети вводится команда **nmap -pl-65535 1P-адрес**_компьютера или **nmap -sV IP-адрес компьютера,** а для сканирования сайта — команда **nmap -sS -sV -O -P0 адрес сайта.**

Монитор портов TCPView

**TCPView** — показывает все процессы, использующие Интернет- соединения. Запустив **TCPView**, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорватьсоединение - рис. 17.

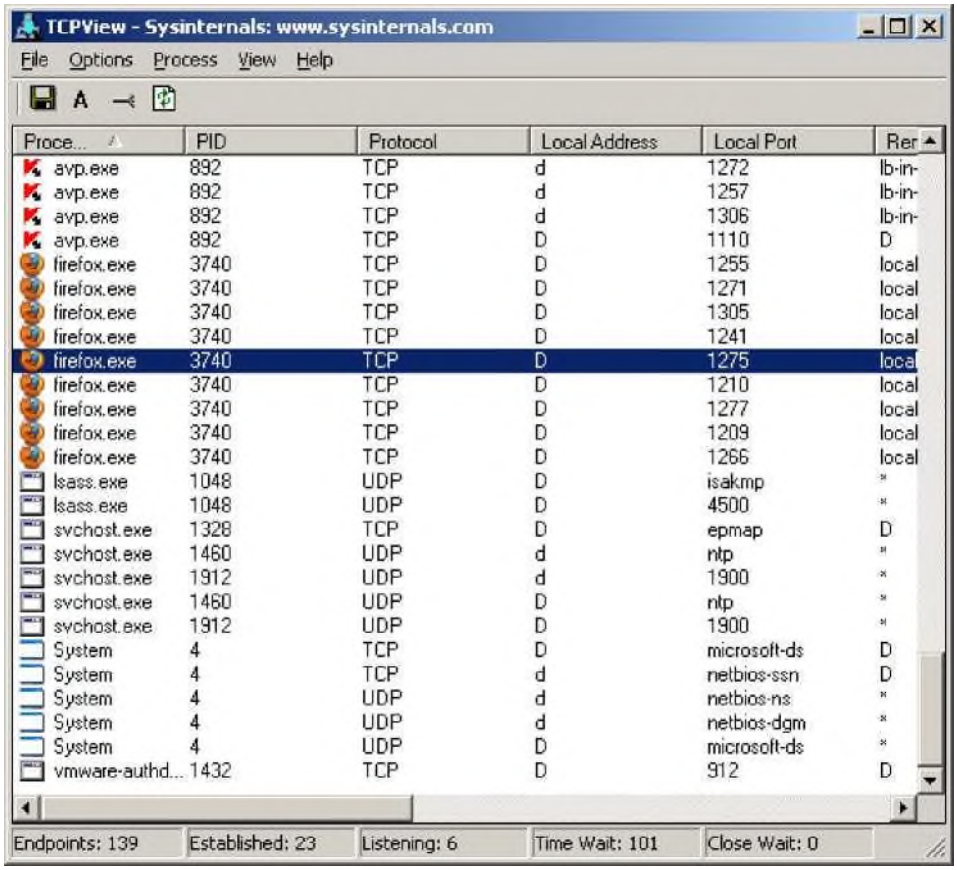



Рис. 17. Главное окно программы TCPView

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

**Контрольные вопросы:**

Какие уязвимости ОС Windows были устранены в данной практической работе и какими путями?

Для чего используется утилита Netstat?

Перечислите, какие утилиты вошли в состав программы NetStat Agent? Для чего используется каждая из утилит?

Для чего используется программа Nmap? TCPView?

**Используемая литература**

Основные источники:

1. Богомазова Г.Н. Обеспечение информационной безопасности компьютерных сетей : учеб. для студ. учреждений сред. проф. образования / Г.Н. Богомазова. - М. : Издательский центр «Академия», 2017. - 224 с.
2. Федорова Г.Н. Информационные системы : учеб. для студ. учреждений сред. проф. образования / Г.Н. Федорова. - 6-е изд., стер. - М. : Издательский центр «Академия», 2017. - 208 с.
3. Баранчиков А.И. Организация сетевого администрирования учебник для студ. учреждений сред. проф. образования / А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов. - М. : Издательский центр «Академия»,2017. - 320 с.
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html
5. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. доступа:
6. Алексеев А.П. Сборник лабораторных работ по дисциплине «Информатика». Часть 2 [Электронный ресурс] : учебное пособие по дисциплине «Информатика», для студентов первого курса специальностей 10.03.01 и 10.05.02 / А.П. Алексеев. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2017. — 256 с. — 978-5- 91359-220-0. —Режим доступа: http://www.iprbookshop.ru/65413.html

Дополнительные источники:

1. Мельников В.П. Информационная безопасность: учеб. пособие для студ. учреждений сред. проф. образования / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под редакцией С.А. Клейменова - 6-е изд., стер. М.: Издательский центр «Академия», 2011
2. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М. : КНОРУС, 2012
3. Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В. Операционные системы. Концепции построения и обеспечения безопасности. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2011

Интернет-ресурсы

1. Свободная общедоступная интернет - энциклопедия. [Электронныйресурс]. Режим доступа: http://ru.wikipedia.org
2. Национальный Открытый Университет [Электронный ресурс]. Режим доступа: http://intuit.ru

A
H
O
C

A
H
O
C