МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Колледж экономики, управления и права

Методические указания

по организации практических занятий

ОП 15 Информационная безопасность

Специальность

09.02.05 Прикладная информатика (по отраслям)

Ростов-на-Дону
2017

Методические указания по организации практической и самостоятельной работы студентов по дисциплине «Информационная безопасность» разработаны с учетом ФГОС среднего профессионального образования по специальности:

09.02.05 Прикладная информатика (по отраслям).

Методические указания содержат перечень практических работ, рекомендации по выполнению практической или самостоятельной работы, вопросы для самоконтроля.

Методические указания предназначены для обучающихся и преподавателей колледжа.

Автор - составитель: С.В. Шигаева преподаватель колледжа ЭУП

Одобрены на заседании предметной (цикловой) комиссии специальности Прикладная информатика (по отраслям).

Протокол № 1 от «31» августа 2017 г

Председатель предметной (цикловой) комиссии _____ Л.А. Белас
личная подпись

и одобрены решением учебно-методического совета колледжа.

Протокол № 1 от «31» августа 2017 г

Председатель учебно-методического совета колледжа
комиссии _____ С.В.Шинакова
личная подпись

Рекомендованы к практическому применению в образовательном процессе

Рецензенты:

Практическая работа №1-2
«Кодирование и подсчет количества информации»

Цель работы:

1. Изучить основные виды и свойства информации. Научиться определять количество представленной информации в ЭВМ.

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: 2i = 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 = 2i, 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: N = 1/p

Единицы измерения информации

1 байт = 8 бит

1 Кбайт = 210 байт=1024 байт

1 Мбайт = 210 Кбайт=1024 Кбайт

1 Гбайт = 210 Мбайт=1024 Мбайт

1 Тбайт = 210 Гбайт=1024 Гбайт

1 Пбайт = 210 Тбайт=1024 Тбайт

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

$$I = \log_2 N$$

Отсюда:

$$N = 2^I,$$

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:

V=I/t

Где I – количество информации в сообщении

t – время передачи сообщения

Примеры решения:

1 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

Задания к практической работе:

- **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 ПО ПРАКТИЧЕСКОЙ РАБОТЕ №1-2:

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

Практическая работа №3-4
«Настройка параметров безопасности в ОС Windows»

Цель работы:

1. Ознакомиться с механизмами аутентификации и идентификации, локальными политиками безопасности, встроенными в ОС Windows.

Краткие теоретические сведения:

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации. Идентификация и аутентификация применяются для ограничения доступа случайных 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 7 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 7 и Windows Server 2008 R2.

Задание

1 Настроить параметры локальной политики безопасности операционной системы Windows;

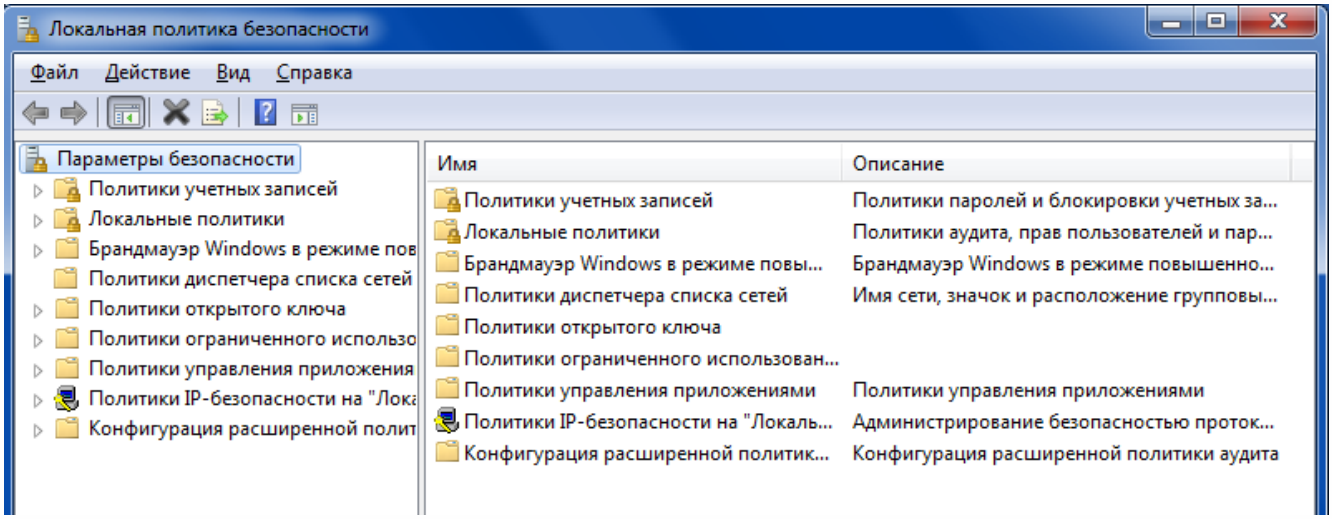
Алгоритм выполнения работы:

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку Пуск на панели задач.

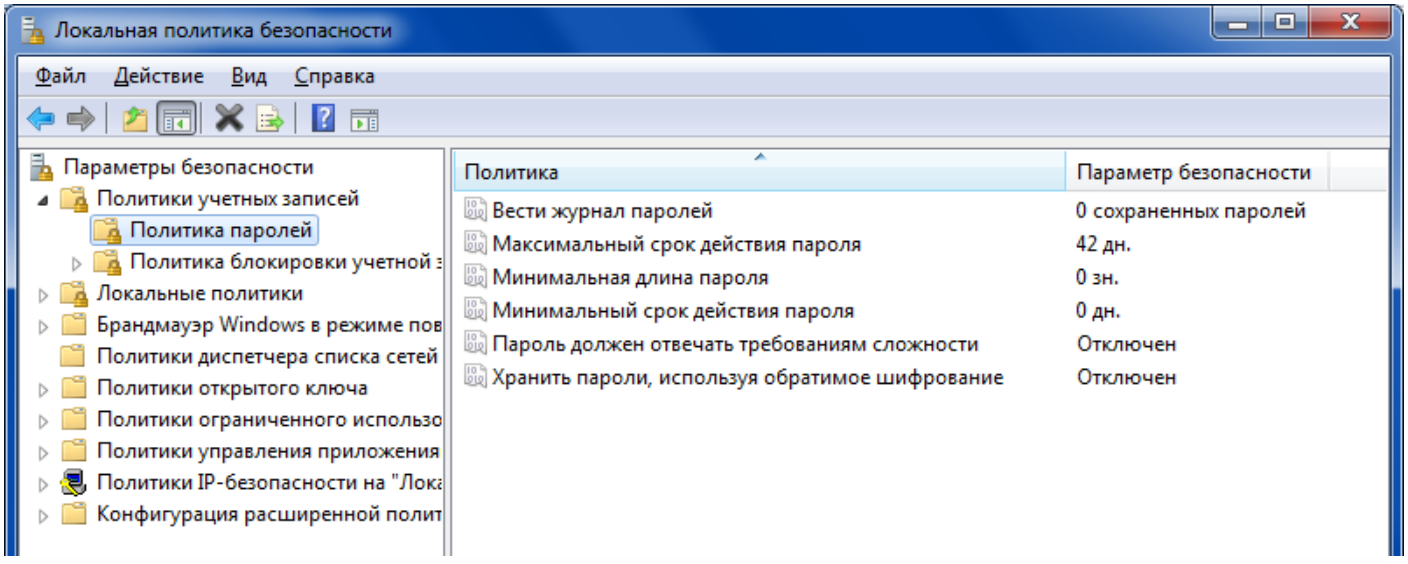
2. Откройте меню Настроить – Панель управления.

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.

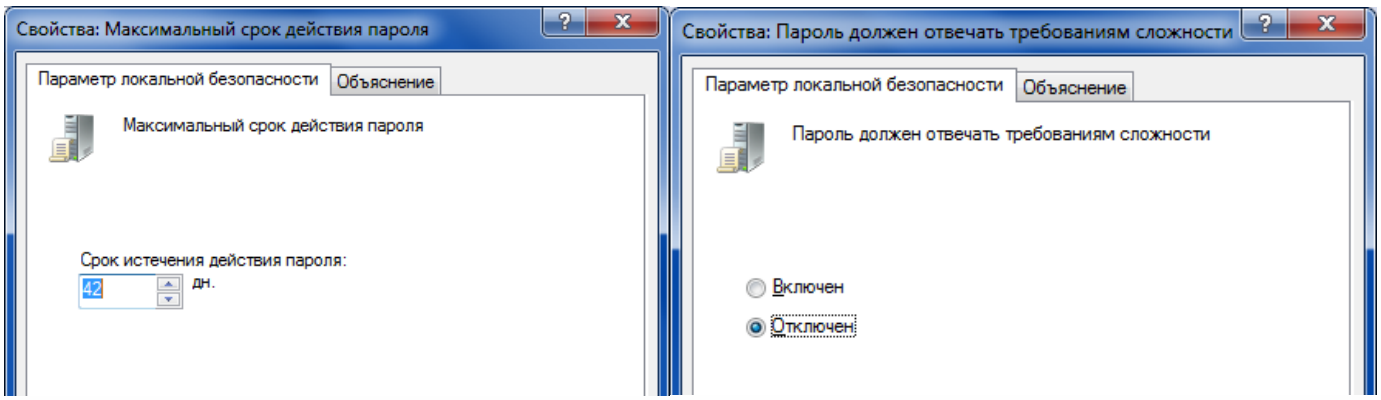
Таблица №1 - Значения параметров Политики паролей

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. Ø Пароль не может содержать имя учетной записи пользователя или какую-либо его часть; Ø Пароль должен состоять не менее чем из 6 символов; Ø В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1. Прописные буквы английского алфавита от A до Z; 2. Строчные буквы английского алфавита от A до Z; 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.



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.

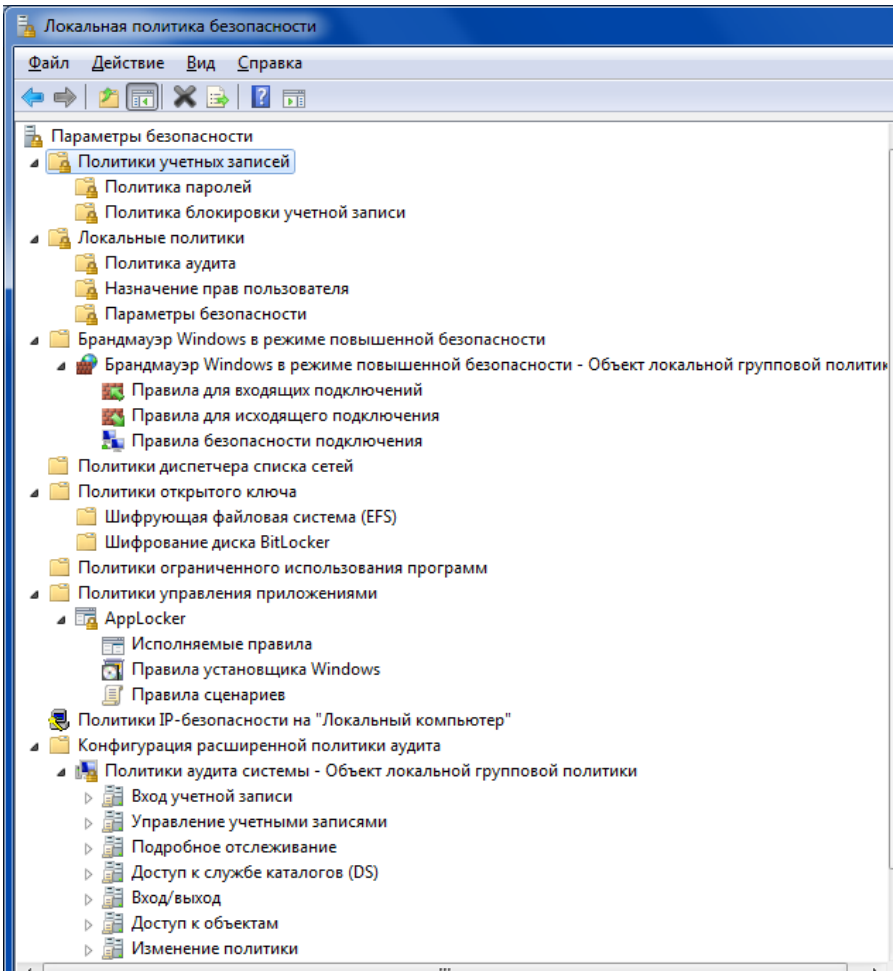
13. Значения параметров данного подпункта Политики учетной записи приведены в таблице №2.

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:

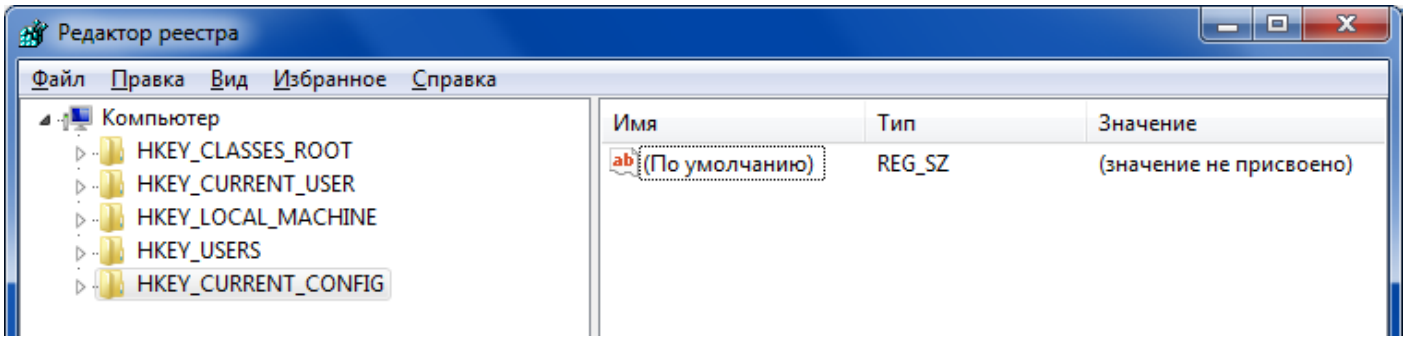
1. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего 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.



4.1 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**

4.2 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**

4.3 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

4.4 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

4.5 Отключить просмотр общих ресурсов анонимным пользователям

В разделе

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

измените значение параметра**restrictanonymous** на **1**

4.6 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.

4.7 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

4.8 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

4.9 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.

4.10Запрет 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 имнем **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.

4.11Отключение автоматического обновления Internet Explorer

Откройте раздел

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

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

4.12Запретить 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**

4.13Запрет 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

4.14Отключение 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 Manager**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.

4.15Запрет на установку простого пароля

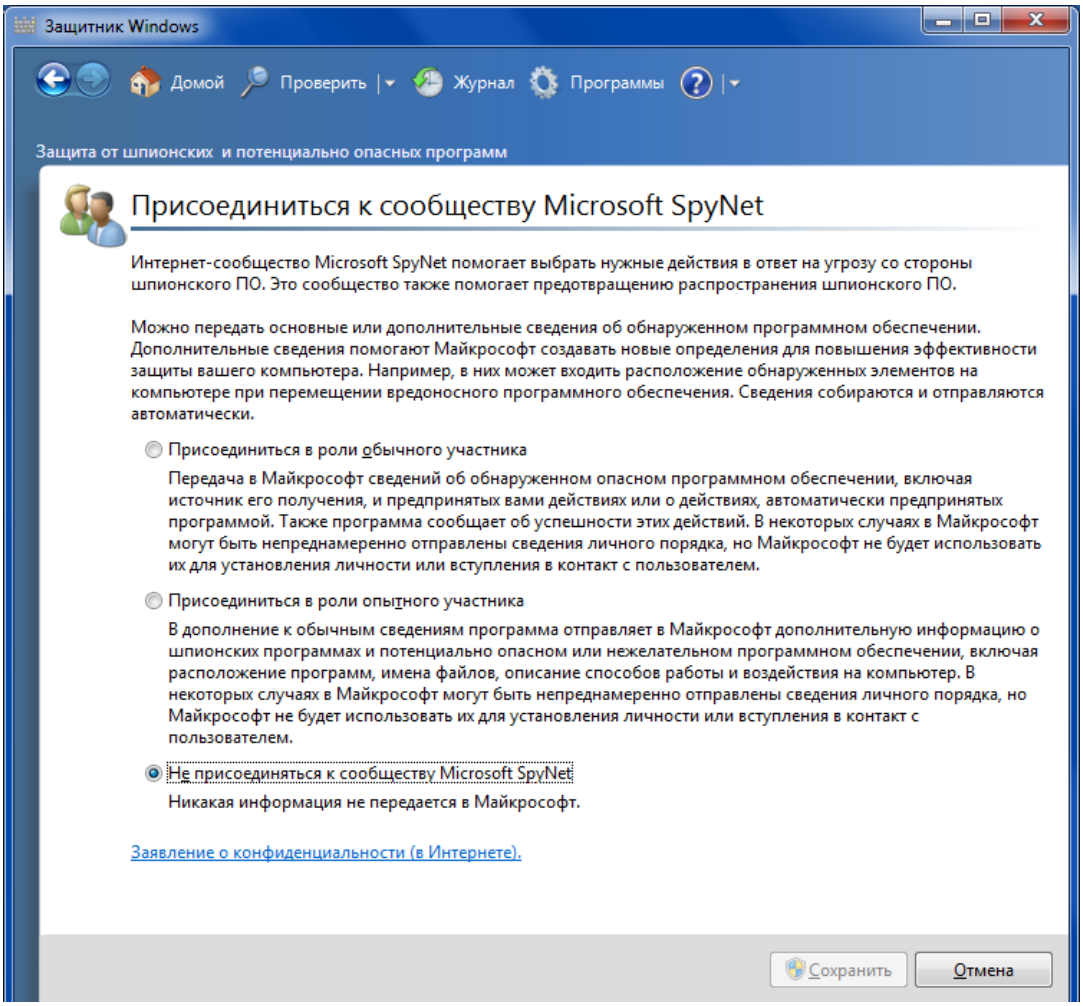
Дополнительная функция для усложнения пароля. По мимо установки минимальной длины, это параметр задает еще и буквенно-цифровой пароль. Откройте раздел

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies,

создайте подраздел **Network**и в этом подразделе создайте параметр типа DWORD с именем **AlphanumPwds** и значение параметра установите **1**

Запретить отсылать данные в Microsoft SpyNet

Если вы используете «Защитник Windows», встроенный в Windows 7 по умолчанию, то Microsoft собирает информацию не только об ошибках в программах, но и о вашей ОС. Чтобы отключить оправку данных: Пуск - Панель управления - Защитник Windows. В открывшемся окне нажмите на иконку «Программы» в верхнем меню, затем перейдите по ссылке «Microsoft SpyNet». В диалоговом окне выберите опцию «Не присоединяться к сообществу Microsoft SpyNet» и сохраните изменения.



КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №3-4:

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?

Практическая работа №5-6
«Создание и управление учетными записями в ОС Windows»

Цель работы:

1. Изучить методы создания учетных записей пользователей в ОС Windows 7, научиться создавать и работать с учетными записями
2. Научиться проводить настройку параметров аутентификации Windows
3. Научиться управлять доступом в Windows. Освоить возможности режима защиты экрана.

Учётная запись пользователя – это запись, которая содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации — например, биометрические характеристики). Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде (в целях его безопасности).

Для повышения надёжности могут быть, наряду с паролем, предусмотрены альтернативные средства аутентификации — например, специальный секретный вопрос (или несколько вопросов) такого содержания, что ответ может быть известен только пользователю. Такие вопросы и ответы также хранятся в учётной записи.

Создание учетных записей пользователей

В операционной системе **Windows 7** учетные записи можно создавать следующими способами:

1. Создание учетной записи с помощью Панели управления (средство **Управление учетными записями пользователей**)

Для того чтобы создать учетную запись при помощи средства **Учетные записи пользователей**, нужно сделать следующее:

– Выполните команду **Пуск - Панель управления** и из списка компонентов панели управления выберите **Учетные записи пользователей;**

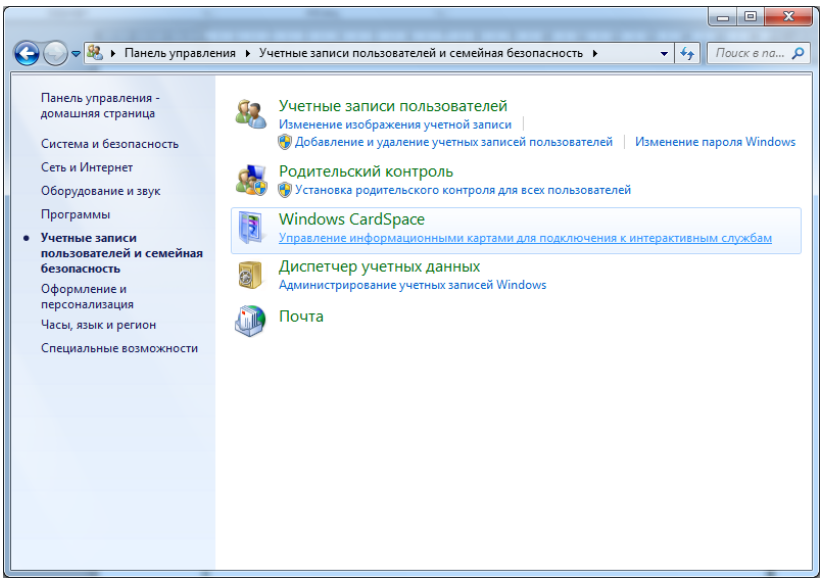


Рис. 1. Панель управления. Учетные записи пользователей

– В диалоговом окне **Учетные записи пользователей** перейдите по ссылке **Управление другой учетной записью,** а затем нажмите на **Создание учетной записи**;

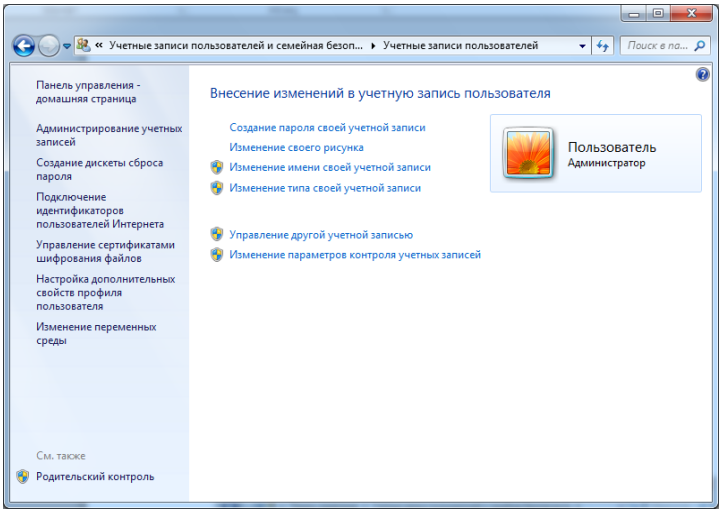


Рис. 2. Учетные записи пользователей. Управление другой учетной записью

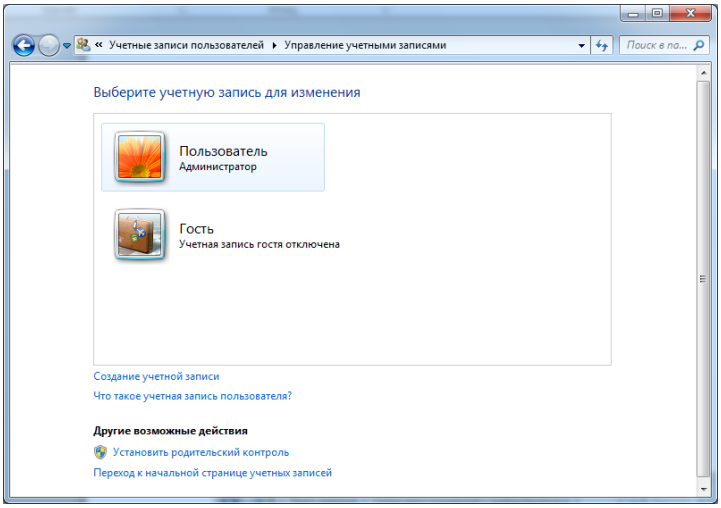


Рис. 3. Создание новой учетной записи

– Далее нужно ввести имя для учетной записи, выбрать тип учетной записи и нажать на кнопку **Создание учетной записи** (следующие шаги на рис. 4, 5).

Имя пользователя не должно совпадать с любым другим именем пользователя или группы на данном компьютере. Оно может содержать до 20 символов верхнего или нижнего регистров, за исключением следующих: « / \ [ ] : ; | = , + * ? <> @, а также имя пользователя не может состоять только из точек и пробелов.

В этом окне можно выбрать один из двух типов учетных записей:

– **Обычный доступ** - обычные учетные записи пользователей, которые предназначены для повседневной работы,

– **Администратор** - учетные записи администратора, которые предоставляют полный контроль над компьютером и применяются только в необходимых случаях.

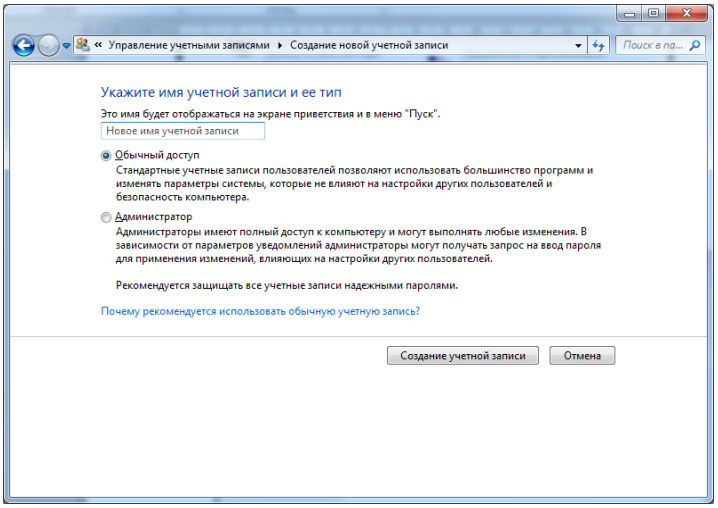


Рис. 4. Задание имени учетной записи

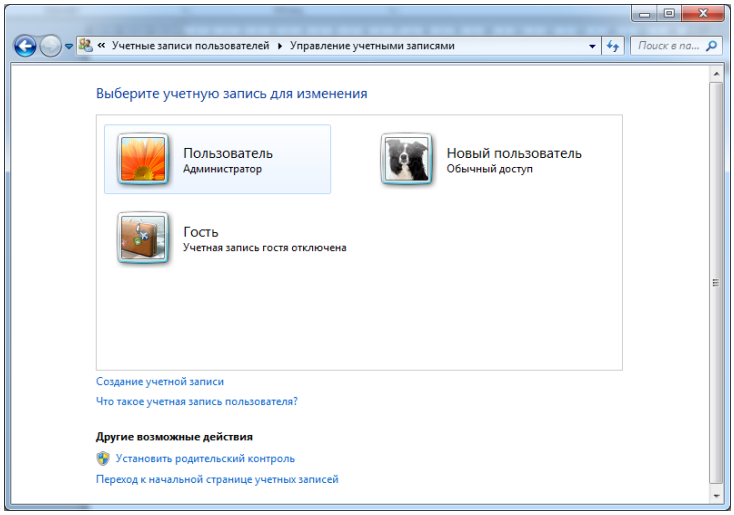


Рис. 5. Создана учетная запись Новый пользователь

При помощи диалогового окна **Управление учетными записями пользователей** можно не только создавать учетные записи, но и выполнять с ними **простейшие действия:**

– изменение имени;
– создание пароля;
– изменение пароля;
– удаление пароля;
– изменение рисунка;

– установка родительского контроля;
– изменение типа учетной записи;
– удаление учетной записи;
– включение и отключение гостевой учетной записи.

Чтобы внести изменения в созданную учетную запись, нужно выбрать ее из списка (рис. 5) и открыть окно учетной записи и выбрать соответствующую команду (рис. 6), далее следовать указаниям в диалоговых окнах.

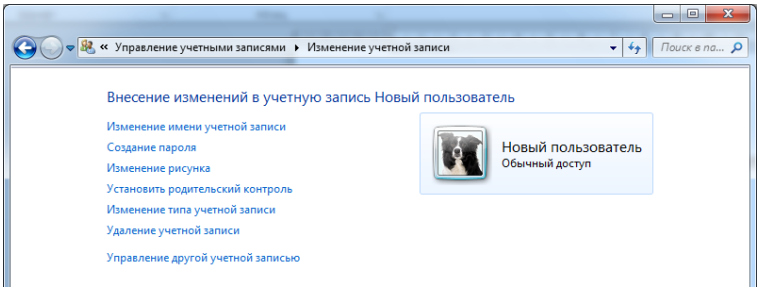


Рис. 6. Диалоговое окно учетной записи Новый пользователь

Рассмотрим алгоритм создания пароля для учетной записи Новый пользователь.

– Выберите учетную запись, для которой нужно создать пароль (в данном случае **Новый пользователь**, рис. 5) и перейдите по ссылке **Создание пароля**. Эта ссылка будет отображаться только в том случае, если у пользователя этой текущей записи нет пароля.

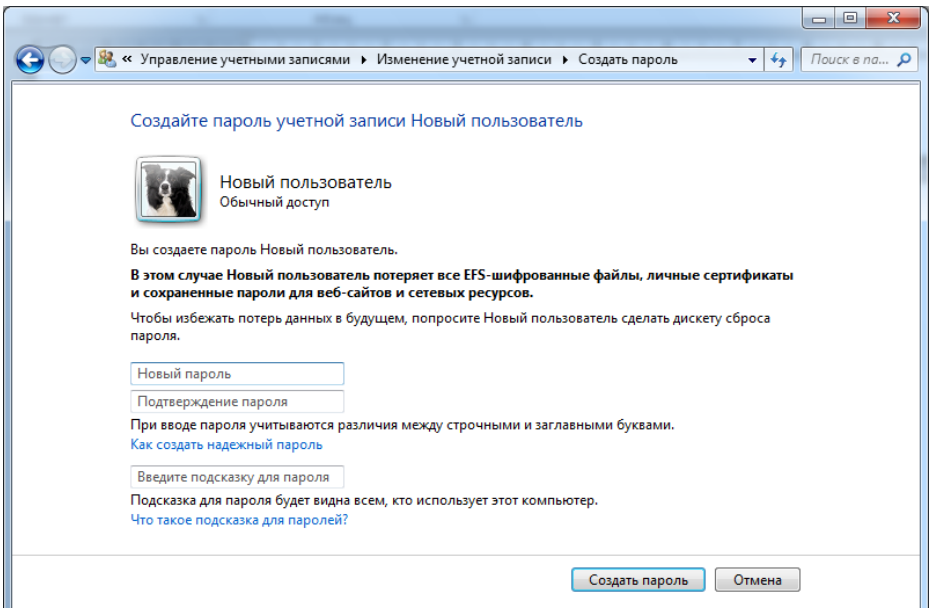


Рис. 7. Создание пароля для Новый пользователь

В диалоговом окне **Создание пароля** введите пароль для данной учетной записи, а затем повторите его в поле **Подтверждение пароля** и еще можно ввести подсказку в поле **Введите подсказку для пароля. Подсказка** – это текст, который операционная система отображает на экране приветствия. В связи с тем, что подсказку может увидеть любой пользователь, который попытается войти в вашу систему, она должна быть менее очевидной, но при этом понятной для того, кто ее создал в том случае, если он забудет пароль. После ввода пароля, подтверждения пароля и подсказки для создания пароля учетной записи нажмите на кнопку **Создать.**

Изменение пароля

– Если у учетной записи пользователя уже имеется пароль, но его нужно сменить, необходимо выполнить следующее:

– Выполните команду **Пуск - Панель управления** и из списка компонентов панели управления выберите **Учетные записи пользователей**;

– Выберите свою учетную запись и перейдите по ссылке **Изменение пароля**.

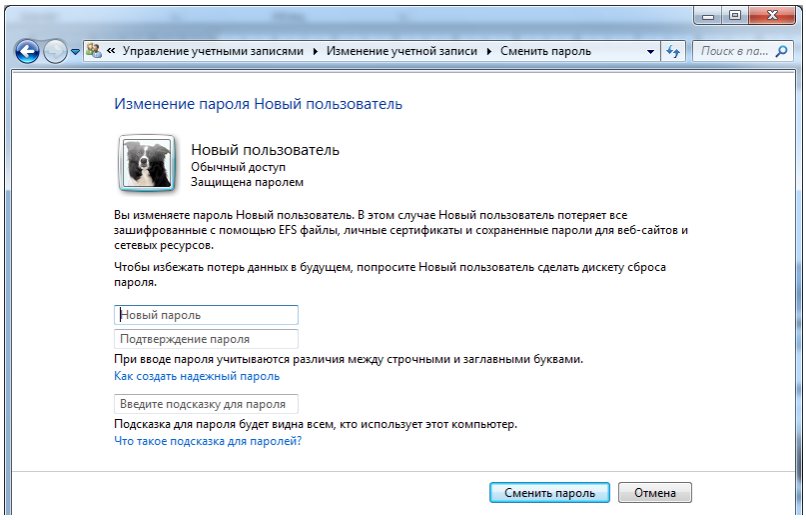


Рис. 8. Изменение пароля для учетной записи Новый пользователь

– Находясь в окне **Изменение пароля**, в поля **Новый пароль** и **Подтверждение пароля** введите и подтвердите новый пароль для учетной записи. В поле **Введите подсказку для пароля** введите подсказку.

Удаление пароля

В том случае, если у пользователя есть пароль и этот пароль для работы за компьютером ему не нужен, выполним следующие действия:

– Выполните команду **Пуск - Панель управления** и из списка компонентов панели управления выберите **Учетные записи пользователей**;

– Выберите свою учетную запись и нажмите на ссылку **Удаление пароля**;

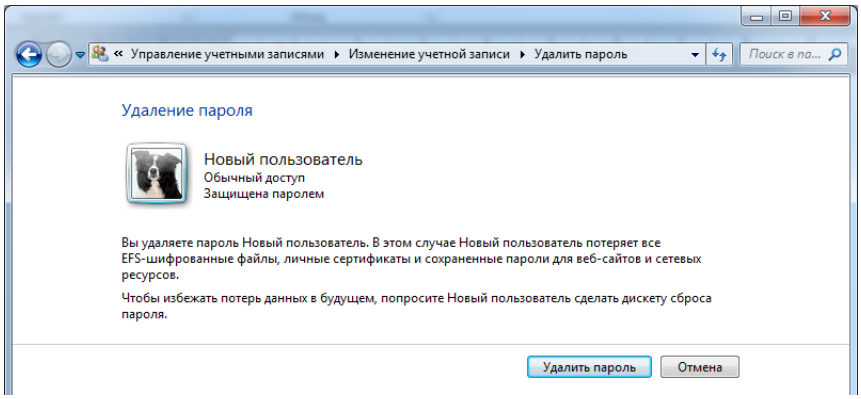


Рис. 9. Удаление пароля учетной записи

– В диалоговом окне **Удаление пароля** подтвердите удаление пароля, нажав на кнопку **Удалить пароль.**

2. Создание учетной записи при помощи средства «Учетные записи пользователей» (диалоговое окно **Выполнить**)

Доступный через панель управления диалог **Управление учетными записями пользователей** имеет очень серьезное ограничение: оно предлагает на выбор только учетные записи типа **Обычный доступ** или **Администратор**.

Для того чтобы при создании нового пользователя его можно было поместить в какую-либо определенную группу, нужно сделать следующее:

– Выполните команду **Пуск – Все программы – Стандартные – Выполнить** (или комбинация клавиш **+R**) для открытия диалогового окна **Выполнить**;

– В диалоговом окне **Выполнить** в поле **Открыть** введите **control userpasswords2** и нажмите **ОК**;

– В диалоговом окне **Учетные записи пользователей** нажмите на кнопку **Добавить** для запуска мастера добавления нового пользователя;

– В появившемся диалоговом окне **Добавление нового пользователя** введите имя пользователя. Поля **Полное имя** и **Описание** не являются обязательными, то есть их можно заполнять при желании. Нажмите **Далее**;

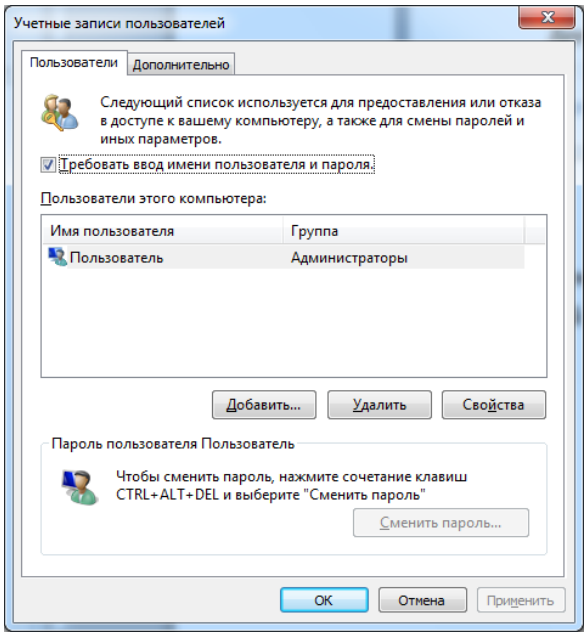


Рис. 10. Диалоговое окно Учетные записи пользователей

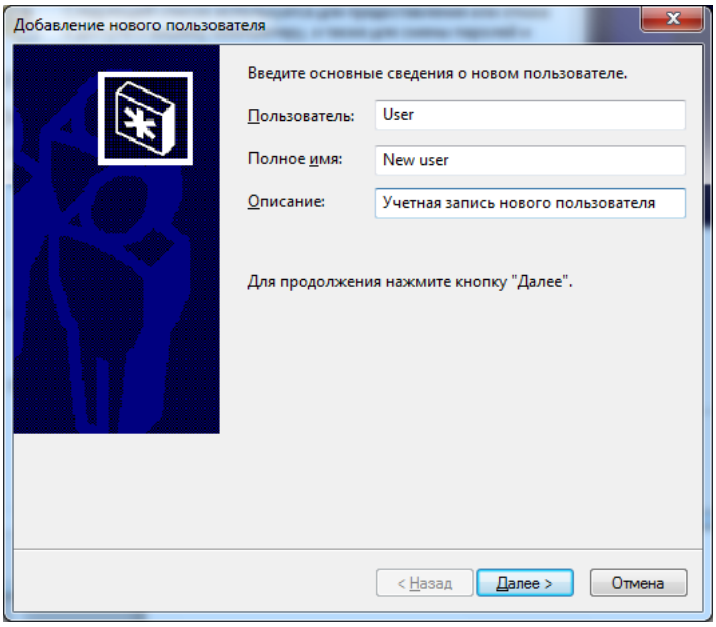


Рис. 11. Окно мастера добавления нового пользователя

– В окне **Введите и подтвердите пароль этого пользователя** введите пароль для данной учетной записи, а затем продублируйте его в поле **Подтверждение**, после чего нажмите **Далее** (рис. 12);

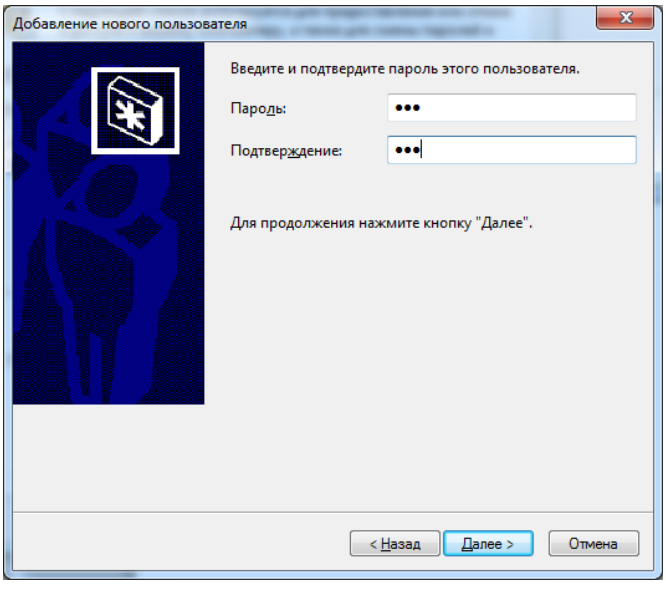


Рис. 12. Следующий шаг мастера

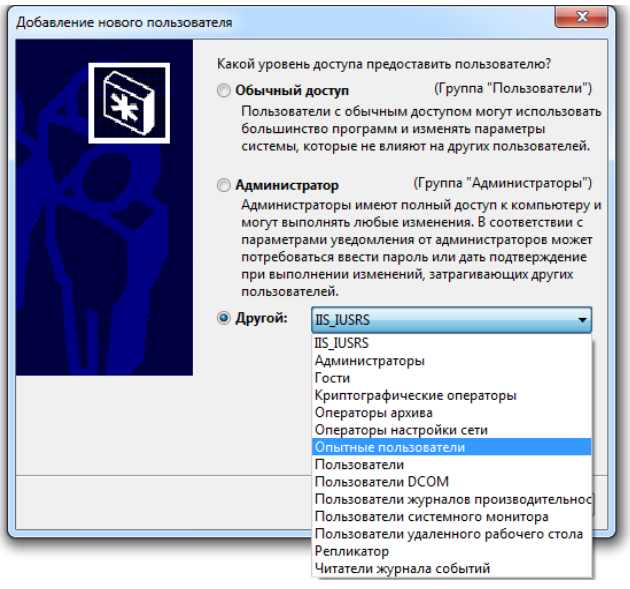


Рис.13. Выбор группы безопасности

На последнем шаге мастера необходимо установить переключатель, определяющий группу безопасности, к которой должна относиться данная учетная запись пользователя (рис. 13). Можно выбрать одну из следующих групп: **Обычный доступ, Администратор** или **Другой**. Последний переключатель стоит использовать в том случае, если нужно отнести пользователя к какой-то другой группе, созданной по умолчанию в операционной системе **Windows 7.**

В следующем списке перечислены 15 встроенных групп операционной системы Windows 7. Эти права назначаются в рамках локальных политик безопасности:

1. **Administrators (Администраторы).** Пользователи, входящие в эту группу, имеют полный доступ на управление компьютером и могут при необходимости назначать пользователям права пользователей и разрешения на управление доступом. По умолчанию членом этой группы является учетная запись администратора. Если компьютер подключен к домену, группа «Администраторы домена» автоматически добавляется в группу «Администраторы». Эта группа имеет полный доступ к управлению компьютером, поэтому необходимо проявлять осторожность при добавлении пользователей в данную группу;
2. **Backup Operators (Операторы архива).** Пользователи, входящие в эту группу, могут архивировать и восстанавливать файлы на компьютере независимо от любых разрешений, которыми защищены эти файлы. Это обусловлено тем, что право выполнения архивации получает приоритет над всеми разрешениями. Члены этой группы не могут изменять параметры безопасности.
3. **Cryptographic Operators (Операторы криптографии).** Членам этой группы разрешено выполнение операций криптографии.
4. **Debugger Users (Группа удаленных помощников).** Члены этой группы могут предлагать удаленную помощь пользователям данного компьютера.
5. **Distributed COM Users (Пользователи DCOM).** Членам этой группы разрешено запускать, активировать и использовать объекты DCOM на компьютере.
6. **Event Log Readers (Читатели журнала событий).** Членам этой группы разрешается запускать журнал событий Windows.
7. **Guests (Гости).** Пользователи, входящие в эту группу, получают временный профиль, который создается при входе пользователя в систему и удаляется при выходе из нее. Учетная запись «Гость» (отключенная по умолчанию) также является членом данной встроенной группы.
8. **IIS_IUSRS.** Это встроенная группа, используемая службами IIS.
9. **Network Configuration Operators (Операторы настройки сети).** Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP. Эта группа не имеет членов по умолчанию.
10. **Performance Log Users (Пользователи журналов производительности).** Пользователи, входящие в эту группу, могут управлять счетчиками производительности, журналами и оповещениями на локальном или удаленном компьютере, не являясь при этом членами группы «Администраторы».
11. **Performance Monitor Users (Пользователи системного монитора).** Пользователи, входящие в эту группу, могут наблюдать за счетчиками производительности на локальном или удаленном компьютере, не являясь при этом участниками групп «Администраторы» или «Пользователи журналов производительности».
12. **Power Users (Опытные пользователи).** По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учетные записи обычных пользователей. В предыдущих версиях операционной системы Windows эта группа была создана для того, чтобы назначать пользователям особые административные права и разрешения для выполнения распространенных системных задач. В этой версии операционной системы Windows учетные записи обычных пользователей предусматривают возможность выполнения большинства типовых задач настройки, таких как смена часовых поясов. Для старых приложений, требующих тех же прав опытных пользователей, которые имелись в предыдущих версиях операционной системы Windows,

администраторы могут применять шаблон безопасности, который позволяет группе «Опытные пользователи» присваивать эти права и разрешения, как это было в предыдущих версиях операционной системы Windows.

13. **Remote Desktop Users (Пользователи удаленного рабочего стола).** Пользователи, входящие в эту группу, имеют право удаленного входа на компьютер.

14. **Replicator (Репликатор).** Эта группа поддерживает функции репликации. Единственный член этой группы должен иметь учетную запись пользователя домена, которая используется для входа в систему службы репликации контроллера домена. Не добавляйте в эту группу учетные записи реальных пользователей.

15. **Users (Пользователи).** Пользователи, входящие в эту группу, могут выполнять типовые задачи, такие как запуск приложений, использование локальных и сетевых принтеров и блокировку компьютера. Члены этой группы не могут предоставлять общий доступ к папкам или создавать локальные принтеры. По умолчанию членами этой группы являются группы «Пользователи домена», «Проверенные пользователи» и «Интерактивные». Таким образом, любая учетная запись пользователя, созданная в домене, становится членом этой группы.

3. Создание учетной записи при помощи утилиты Локальные пользователи и группы (использование возможно в ОС **Windows 7 Максимальная (Ultimate)**)

Утилита **Локальные пользователи и группы** расположена в компоненте **Управление компьютером**, представляющем собой набор средств администрирования, с помощью которых можно управлять одним компьютером, локальным или удаленным. Утилита **Локальные пользователи и группы** служит для защиты и управления учетными записями пользователей и групп, размещенных локально на компьютере. Можно назначать разрешения и права для учетной записи локального пользователя или группы на определенном компьютере (и только на этом компьютере).

Использование утилиты **Локальные пользователи и группы** позволяет ограничить возможные действия пользователей и групп путем назначения им **прав и разрешений**.

Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера.

Разрешение представляет собой правило, связанное с объектом (обычно с файлом, папкой или принтером), которое определяет, каким пользователям и какой доступ к объекту разрешен.

Для того чтобы создать локальную учетную запись пользователя при помощи утилиты Локальные пользователи и группы, нужно сделать следующее:

Откройте утилиту **Локальные пользователи и группы одним из следующих способов:**

– Выполните команду **Пуск - Панель управления** и из списка компонентов панели управления выберите **Администрирование**, затем откройте компонент **Управление компьютером**. В **Управлении компьютером** откройте **Локальные пользователи и группы**;

– Выполните команду **Пуск – Все программы – Стандартные – Выполнить** (или комбинация клавиш **+R**) для открытия диалогового окна **Выполнить**;

– В диалоговом окне **Выполнить** в поле **Открыть** введите **lusrmgr.msc** и нажмите **ОК**;

– Откройте узел **Пользователи** и либо в меню **Действие**, либо из контекстного меню выбрать команду **Новый пользователь**;

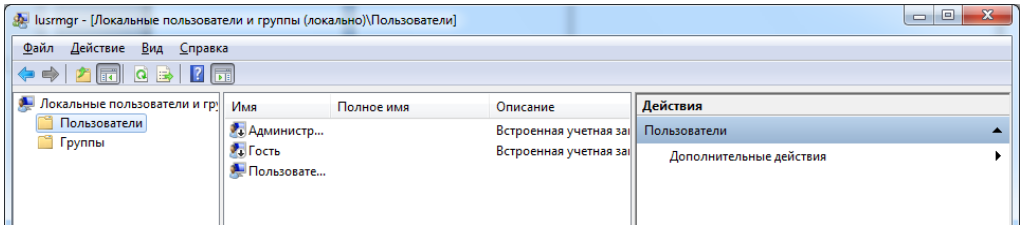


Рис. 14. Диалоговое окно Локальные пользователи и группы

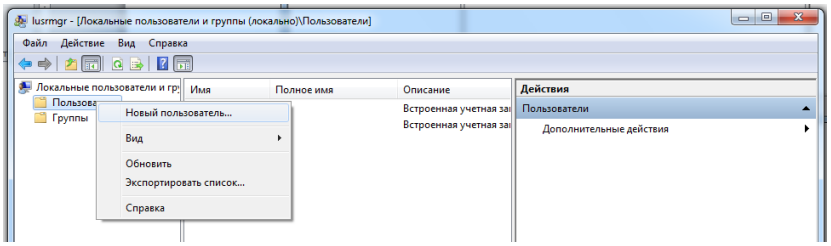


Рис. 15. Добавление нового пользователя

– В диалоговом окне **Новый пользователь** введите соответствующие сведения. Помимо указанных данных, можно воспользоваться следующими флажками: **Требовать смену пароля при следующем входе в систему, Запретить смену пароля пользователем, Срок действия пароля не ограничен, Отключить учетную запись** и нажать на кнопку **Создать**, а затем **Закрыть**.

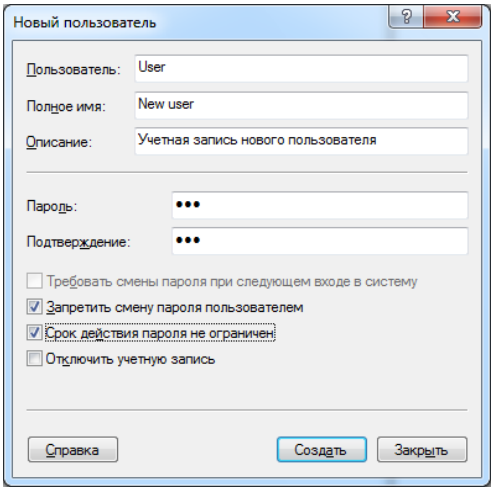


Рис. 16. Создание нового пользователя

– Для того чтобы добавить пользователя в группу, дважды щелкните имя пользователя для получения доступа к странице свойств пользователя (рис. 17).

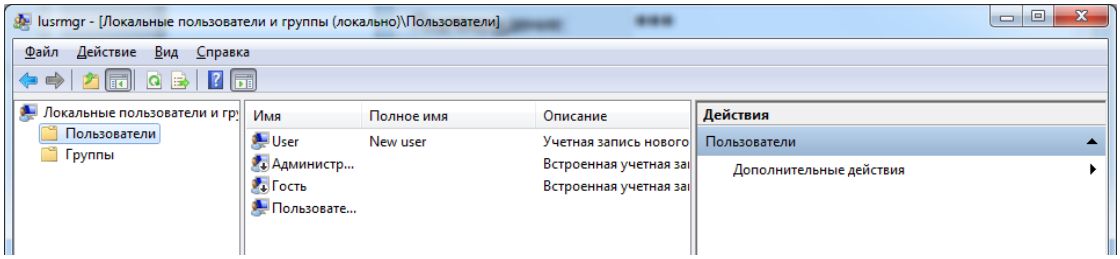


Рис. 17. Список пользователей

– На вкладке **Членство в группах** нажмите на кнопку **Добавить** (рис. 19).

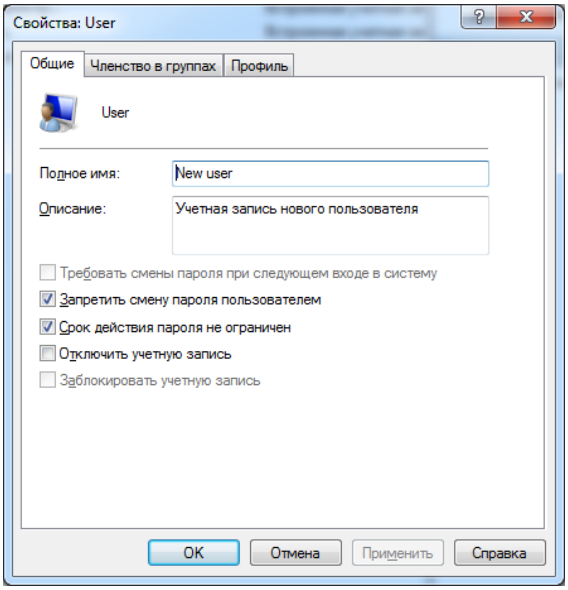


Рис. 18. Диалоговое окно свойств пользователя

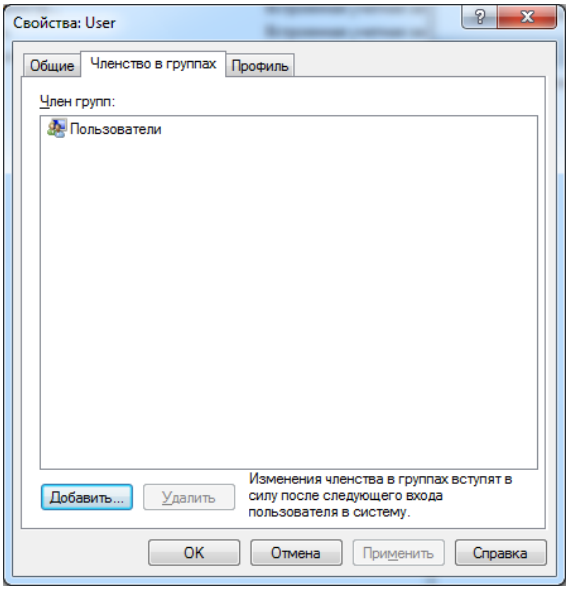


Рис. 19. Вкладка Членство в группах

– В окне **Выбор группы** можно выбрать группу для пользователя двумя способами:

1 В поле **Введите имена выбираемых объектов** введите имя группы и нажмите на кнопку **Проверить имена** (рис. 20)

2 Или в окне **Выбор группы** нажмите на кнопку **Дополнительно**, чтобы открыть диалоговое окно **Выбор группы**. В этом окне нажмите на кнопку **Поиск**, чтобы отобразить список всех доступных групп, выберите подходящую группу и нажмите два раза **ОК** (рис. 21).

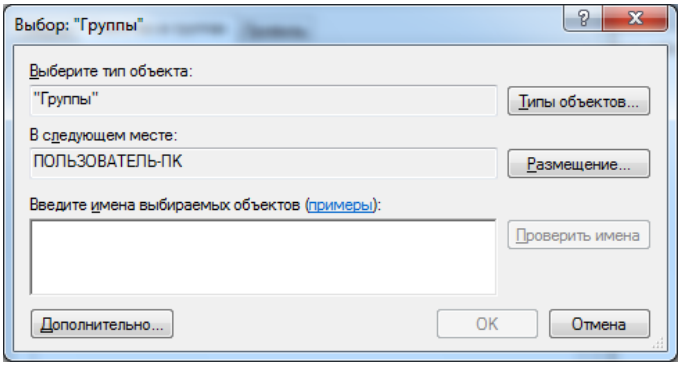


Рис. 20. Окно Выбор: Группы

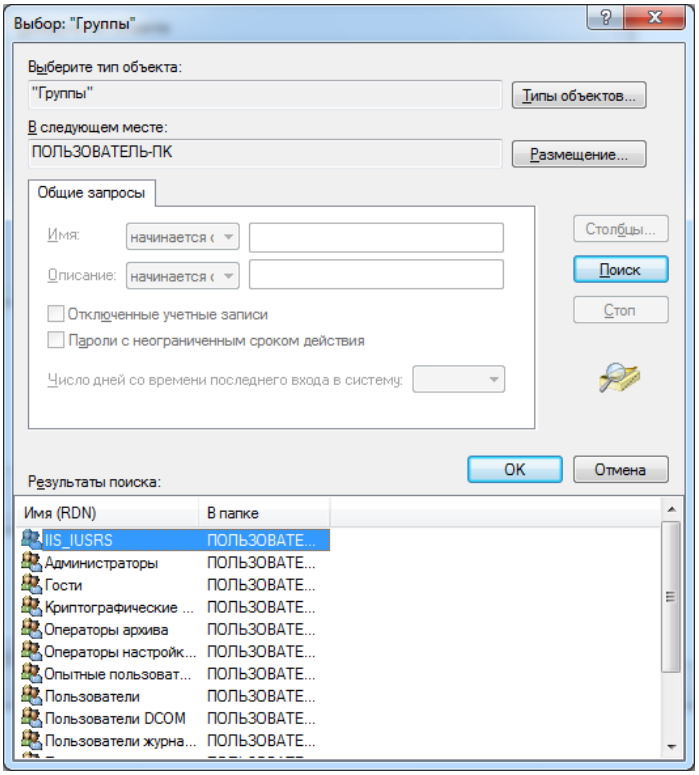


Рис. 21. Окно Выбор: Группы. Дополнительно

4. Создание учетной записи при помощи командной строки

Помимо вышеперечисленных способов, учетные записи пользователей можно создавать, изменять и удалять при помощи командной строки.

– Запустите **Command Prompt (**выполните команду **Пуск – Все программы – Стандартные – Выполнить** (или комбинация клавиш **+R**) для открытия диалогового окна **Выполнить** или воспользуйтесь режимом командной строки);

– В окне **Выполнить** введите **cmd**

– Изучите пример создания учетной записи в режиме командной строки, для этого наберите предложенные команды, просмотрите результаты их выполнения, выпишите в тетрадь (рис. 22)

Команда **net user** используется для добавления пользователей, установки паролей, отключения учетных записей, установки параметров и удаления учетных записей. При выполнении команды без параметров командной строки отображается список учетных записей пользователей, присутствующих на компьютере. Информация об учетных записях пользователей хранится в базе данных учетных записей пользователей.

Указание: по умолчанию учетная запись добавится в группу **Пользователи.** Проверьте это, введя последнюю команду **net user ivan** (просмотр свойств учетной записи).

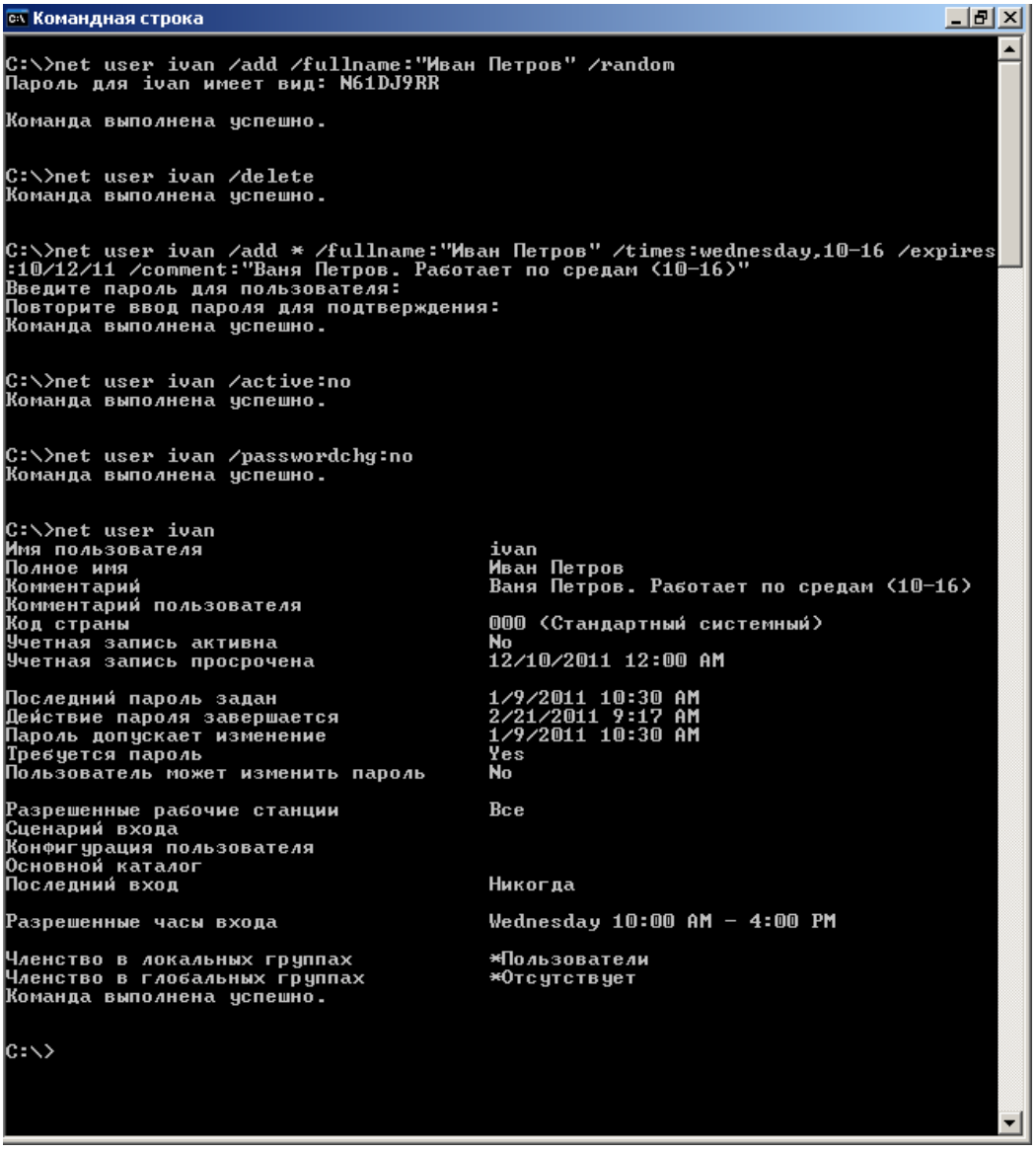


Рис. 22. Создание учетной записи и работа с нею в режиме командной строки

– Изучите параметры команды **Net User, выпишите в тетрадь.** (Дополнительную информацию можно получить, набрав net help user или net user /?)

Параметр	Описание
/Add	Создание новой учётной записи. Имя пользователя может содержать максимум 20 символов и не допускает применения следующих знаков: «//[]=,+*?<>
/Delete	Удаление учётной записи.
пароль или /Random	Установка пароля. Если указать звёздочку (*), отобразится запрос на ввод пользовательского пароля. Это удобно, если пользователь хочет ввести свой пароль сам. При выборе переключателя /Random случайным образом генерируется пароль, состоящий из 8 символов.
/Fullname:»имя»	Указание полного имени пользователя
/Comment:»текст»	Указание комментария (до 40 символов)
/Passwordchg:yes или /Passwordchg:no	Возможность изменения пароля пользователем. По умолчанию пользователь может менять пароль.
/Active:yes или /Active:no	Активизация/блокирование учётной записи. (Если учётная запись заблокирована, пользователь не может зарегистрироваться)
/Expires:*дата* или /Expires:never	Установка даты устаревания учётной записи. В случае указания параметра *дата* воспользуйтесь настройками сокращённого формата даты. Срок действия учётной записи завершается в начале указанного дня; после наступления этого события пользователь не может зарегистрироваться до тез пор, пока администратор не укажет новую дату устаревания
/Passwordreq:yes или /Passwordreq:no	Определяет можно ли использовать учётную запись без пароля.
/Times:время или /Times:all	Установка часов регистрации пользователя. Например: M-F,8am-6pm;Sa,9am-1pm. Что означает, регистрация разрешена в понедельник-пятницу с 8 до 18, в субботу с 9 до 13. Опция All разрешает регистрацию в любое время. Пустое значение блокирует регистрацию.

5. Включение скрытой учетной записи администратора

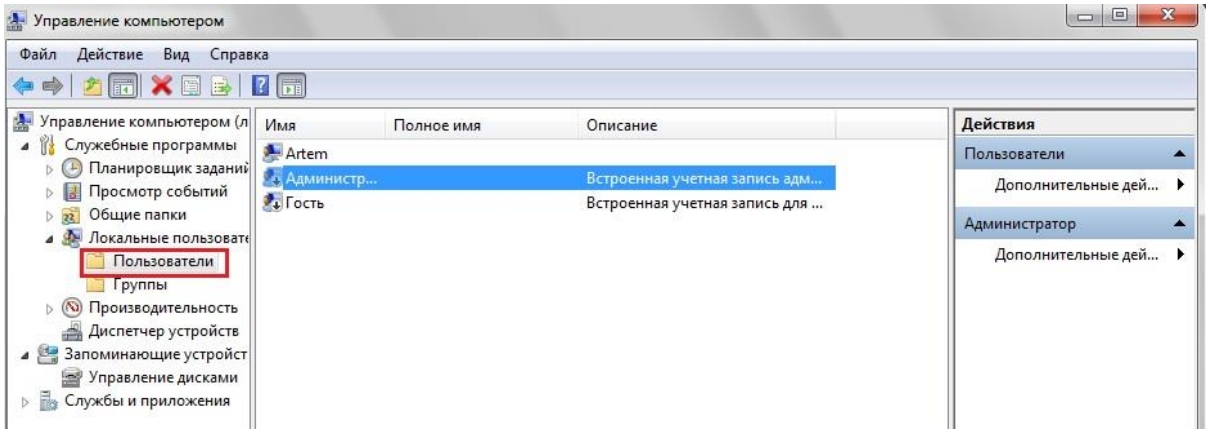
Вероятно, вам доводилось сталкиваться с тем, что в Windows 7 некоторые программы и приложения требуют для совершения определенных действий учетную запись администратора - и это несмотря на то, что работа ведется из-под учетной записи, в статусе которой значится «Администратор».

Дело в том, что в ОС Windows есть два типа учетных записей администратора, и тот, из-под которого работает большинство пользователей не предоставляет полного контроля над системой.

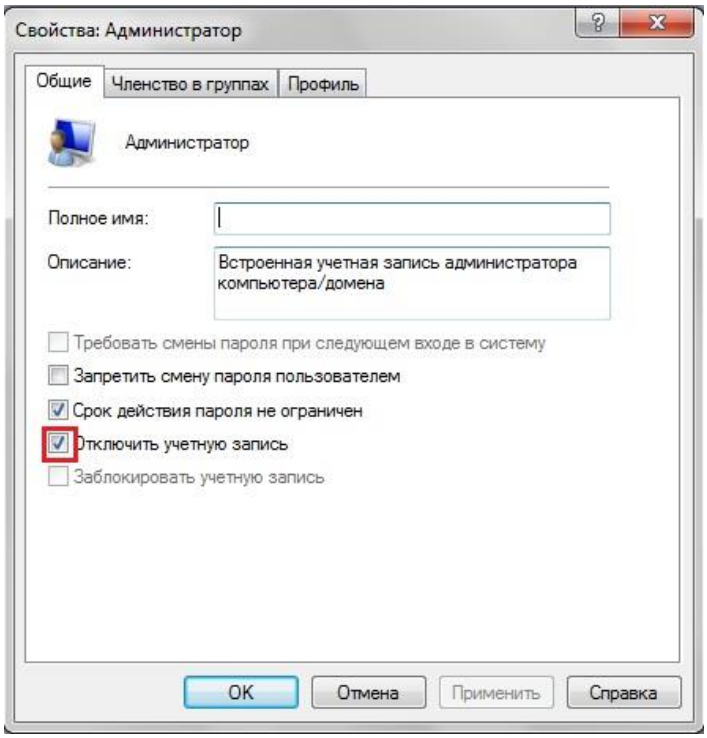
Другой тип учетной записи администратора, или, как его еще называют «СуперАдминистратор», позволяет производить абсолютно любые действия с системой, без каких бы то ни было ограничений, его-то обычно и требуют некоторые программы. Однако в целях безопасности в Windows 7 данная учетная запись по умолчанию отключена.

Для ее включения необходимо проделать следующие действия.

Щелкните правой кнопкой мышки по значку **Мой компьютер** и выберите из контекстного меню пункт **Управление**. В окне **Управление компьютером**перейдите к разделу **Локальные пользователи** и откройте папку **Пользователи**.



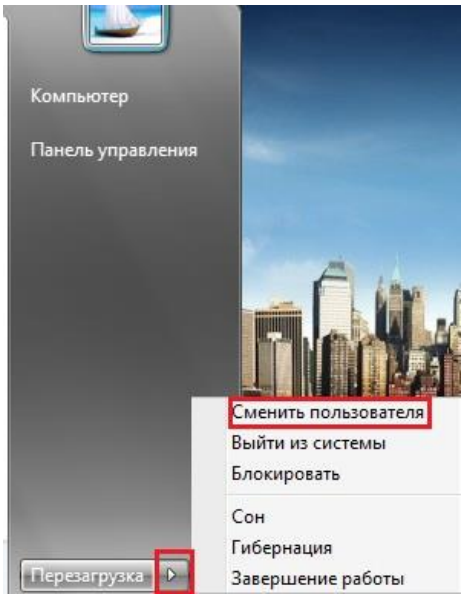
Щелкните дважды мышкой по учетной записи в описании которой значится «Встроенная учетная запись администратора» и уберите галочку с пункта **Отключить учетную запись**.



Выполнив необходимые действия в системе из под встроенной учетной записи администратора, не забудьте перейти к обычной учетной записи. Не следует все время работать на компьютере с правами администратора, так как в случае заражения вирусом вредоносная программа сможет получить полный доступ над системой.

Для того, чтобы сменить пользователя, нажмите на клавиатуре сочетание клавиш **Ctrl+Alt+Del** и на экране выберите пункт **Выйти из системы**. Затем щелкните по картинке нужной учетной записи и войдите под своим паролем.

В случае, если вам просто нужно переключаться между учетными записями двух пользователей (не администраторов), вы можете это сделать, зайдя в меню **Пуск**, нажав на стрелку справа и выбрав пункт **Сменить пользователя**.



КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №5-6:

1. Какие методы управления доступом вам известны?
2. Как создать новую учетную запись пользователя в Windows?
3. Чем характеризуется тип учетной записи Администратор компьютера?
4. Опишите алгоритм установки пароля на заставку.
5. Какие существуют рекомендации обеспечения достаточного уровня безопасности используемого пароля?
6. Перечислите способы создания учетных записей пользователей на ПК
7. Укажите возможности членов группы Администраторы
8. Укажите возможности членов группы Опытные пользователи
9. Укажите возможности членов группы Пользователи
10. Укажите возможности членов группы Гости
11. Укажите возможности членов группы Операторы настройки сети
12. Опишите технологию создания учетной записи с помощью панели управления
13. Перечислите действия, которые можно выполнять с созданной учетной записью
14. Опишите технологию создания учетной записи с помощью утилиты Учетные записи пользователей (окно **Выполнить**)
15. Опишите технологию создания учетной записи с помощью утилиты Локальные пользователи и группы
16. Как установить членство в группе?
17. Укажите команду создания учетной записи с помощью утилиты Net User: краткая форма команды, поясните операторы
18. Укажите команду создания учетной записи с помощью утилиты Net User: развернутая форма команды, поясните операторы
19. Укажите команду удаления учетной записи в режиме командной строки
20. С помощью какой команды можно просмотреть все свойства учетной записи в режиме командной строки?

Практическая работа №7
«Методы криптографического преобразования данных»

Цель работы:

1. Исследование основных методов криптографической зашиты информации.

Краткие сведения из теории

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для

лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифрования. В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

– алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;

– алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;

– гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;

– аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для симметричной криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В асимметричных криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Общие сведения

Основные требования, которые предъявляются к методам защитного преобразования информации:

1. Сложность и трудоёмкость процедур прямого и обратного преобразования (т.е. закрытия и санкционированного раскрытия) должны определяться в зависимости от степени секретности защищаемых данных.
2. Надёжность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику известен способ закрытия.
3. Способ закрытия и набор используемых служебных данных (ключевых установок) не должны быть слишком сложными. Затраты на защитные преобразования должны быть приемлемые при заданном уровне сохранности информации.
4. Выполнение процедур прямого и обратного преобразования должно быть формальным и как можно проще.
5. Процедуры прямого и обратного преобразования не должны зависеть от длины сообщения.
6. Ошибки, возникающие в процессе преобразования, не должны распространяться по системе и вызывать потерю информации. Из-за появления ошибок передачи зашифрованного сообщения по каналам связи не должна исключаться возможность надёжной расшифровки текста на приёмном конце.
7. Избыточность сообщений, вносимая закрытием должна быть как можно меньшей. Или - длина зашифрованного текста не должна превышать длину исходного текста.
8. Объём ключа не должен затруднять его запоминание и пересылку.
9. Необходимые временные и стоимостные ресурсы на шифрование и дешифрование информации определяются требуемой степенью защиты информации.

Перечисленные требования характерны в основном для традиционных средств защитных преобразований. С развитием устройств памяти, позволяющих с большей плотностью записывать и надёжно хранить длительное время большие объёмы информации, ограничение на размер ключа

может быть значительно снижено. Появление и развитие электронных элементов позволили разработать недорогие устройства, обеспечивающие преобразование информации.

Задание

1 Зашифровать любыми пятью методами свои данные: Фамилию, Имя, Отчество.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №7:

1. Цель и задачи криптографии.
2. Какие вы знаете методы криптографической защиты файлов?
3. В чем преимущества и недостатки одноалфавитных методов?
4. Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод вы выберете?
5. Шифр многоалфавитной замены и алгоритм его реализации.
6. Дайте определение и раскройте принципы построения криптографических средств защиты
7. Приведите и объясните классификацию методов криптографического преобразования информации
8. Раскройте сущность и схему шифрования заменой по таблице Виженера
9. Раскройте сущность и схему шифрования перестановкой по таблице
10. Раскройте сущность и схему шифрования по маршрутам Гамильтона

Практическая работа №8
«Технические и программные средства защиты криптографии»

Цель работы:

1. Провести исследование и системную классификацию средств защиты информации.

Термин «криптография» происходит от древнегреческих слов «скрытый» и «пишу». Словосочетание выражает основное назначение криптографии – это защита и сохранение тайны переданной информации. Защита информации может происходить различными способами. Например, путем ограничения физического доступа к данным, скрытия канала передачи, создания физических трудностей подключения к линиям связи и т. д.

Цель криптографии

В отличие от традиционных способов тайнописи, криптография предполагает полную доступность канала передачи для злоумышленников и обеспечивает конфиденциальность и подлинность информации с помощью алгоритмов шифрования, делающих информацию недоступной для постороннего прочтения. Современная система криптографической защиты информации (СКЗИ) – это программно-аппаратный компьютерный комплекс, обеспечивающий защиту информации по следующим основным параметрам.

- *Конфиденциальность* – невозможность прочтения информации лицами, не имеющими соответствующих прав доступа. Главным компонентом обеспечения конфиденциальности в СКЗИ является ключ (key), представляющий собой уникальную буквенно-числовую комбинацию для доступа пользователя в определенный блок СКЗИ.
- Целостность – невозможность несанкционированных изменений, таких как редактирование и удаление информации. Для этого к исходной информации добавляется избыточность в виде проверочной комбинации, вычисляемой по криптографическому алгоритму и зависящая от ключа. Таким образом, без знания ключа добавление или изменение информации становится невозможным.
- *Аутентификация* – подтверждение подлинности информации и сторон, ее отправляющих и получающих. Передаваемая по каналам связи информация должна быть однозначно

аутентифицирована по содержанию, времени создания и передачи, источнику и получателю. Следует помнить, что источником угроз может быть не только злоумышленник, но и стороны, участвующие в обмене информацией при недостаточном взаимном доверии. Для предотвращения подобных ситуации СКЗИ использует систему меток времени для невозможности повторной или обратной отсылки информации и изменения порядка ее следования.

– Авторство – подтверждение и невозможность отказа от действий, совершенных пользователем информации. Самым распространенным способом подтверждения подлинности является электронная цифровая подпись (ЭЦП). Система ЭЦП состоит из двух алгоритмов: для создания подписи и для ее проверки. При интенсивной работе с ЭКЦ рекомендуется использование программных удостоверяющих центров для создания и управления подписями. Такие центры могут быть реализованы как полностью независимое от внутренней структуры средство СКЗИ. Что это означает для организации? Это означает, что все операции с электронными подписями обрабатываются независимыми сертифицированными организациями и подделка авторства практически невозможна.

Алгоритмы шифрования

На текущий момент среди СКЗИ преобладают открытые алгоритмы шифрования с использованием симметричных и асимметричных ключей с длиной, достаточной для обеспечения нужной криптографической сложности. Наиболее распространенные алгоритмы:

- симметричные ключи – российский Р-28147.89, AES, DES, RC4;
- асимметричные ключи – RSA;
- с использованием хеш-функций - Р-34.11.94, MD4/5/6, SHA-1/2.

Многие страны имеют свои национальные стандарты алгоритмов шифрования. В США используется модифицированный алгоритм AES с ключом длиной 128-256 бит, а в РФ алгоритм электронных подписей Р-34.10.2001 и блочный криптографический алгоритм Р-28147.89 с 256-битным ключом. Некоторые элементы национальных криптографических систем запрещены для экспорта за пределы страны, деятельность по разработке СКЗИ требует лицензирования.

Системы аппаратной криптозащиты

Аппаратные СКЗИ - это физические устройства, содержащие в себе программное обеспечение для шифрования, записи и передачи информации. Аппараты шифрации могут быть выполнены в виде

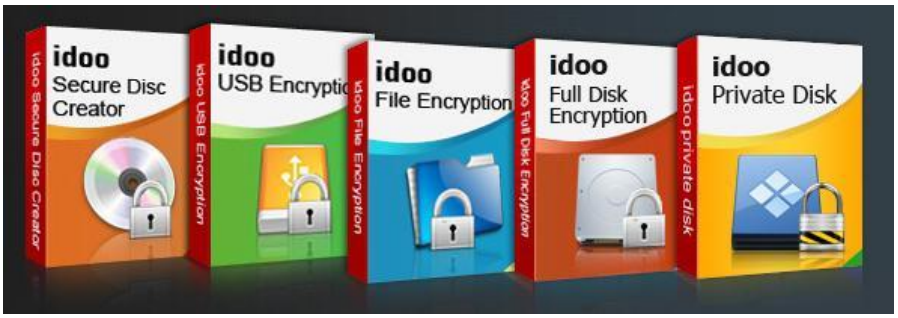
персональных устройств, таких как USB-шифраторы ruToken и флеш-диски IronKey, плат расширения для персональных компьютеров, специализированных сетевых коммутаторов и маршрутизаторов, на основе которых возможно построение полностью защищенных компьютерных сетей.

Аппаратные СКЗИ быстро устанавливаются и работают с высокой скоростью. Недостатки – высокая, по сравнению с программными и программно-аппаратными СКЗИ, стоимость и ограниченные возможности модернизации.

Также к аппаратным можно отнести блоки СКЗИ, встроенные в различные устройства регистрации и передачи данных, где требуется шифрование и ограничение доступа к информации. К таким устройствам относятся автомобильные тахометры, фиксирующие параметры автотранспорта, некоторые типы медицинского оборудования и т.д. Для полноценной работы таким систем требуется отдельная активация СКЗИ модуля специалистами поставщика.

Системы программной криптозащиты

Программные СКЗИ - это специальный программный комплекс для шифрования данных на носителях информации (жесткие и флеш-диски, карты памяти, CD/DVD) и при передаче через Интернет (электронные письма, файлы во вложениях, защищенные чаты и т.д.). Программ существует достаточно много, в т. ч. бесплатных, например, DiskCryptor. К программным СКЗИ можно также отнести защищенные виртуальные сети обмена информацией, работающие «поверх Интернет»(VPN), расширение Интернет протокола HTTP с поддержкой шифрования HTTPS и SSL – криптографический протокол передачи информации, широко использующийся в системах IP-телефонии и интернет-приложениях.



Программные СКЗИ в основном используются в сети Интернет, на домашних компьютерах и в других сферах, где требования к функциональности и стойкости системы не очень высоки. Или как в случае с Интернетом, когда приходится одновременно создавать множество разнообразных защищенных соединений.

Программно-аппаратная криптозащита

Сочетает в себе лучшие качества аппаратных и программных систем СКЗИ. Это самый надежный и функциональный способ создания защищенных систем и сетей передачи данных. Поддерживаются все варианты идентификации пользователей, как аппаратные (USB-накопитель или

смарт-карта), так и «традиционные» - логин и пароль. Программно-аппаратные СКЗИ поддерживают все современные алгоритмы шифрования, обладают большим набором функций по созданию защищенного документооборота на основе ЭЦП, всеми требуемыми государственными сертификатами. Установка СКЗИ производится квалифицированным персоналом разработчика.

Компания «КРИПТО-ПРО»

Один из лидеров российского криптографического рынка. Компания разрабатывает весь спектр программ по защите информации с использованием ЭЦП на основе международных и российских криптографических алгоритмов.

Программы компании используются в электронном документообороте коммерческих и государственных организаций, для сдачи бухгалтерской и налоговой отчетности, в различных городских и бюджетных программах и т. д. Компанией выдано более 3 млн. лицензий для программы КриптоПРО CSP и 700 лицензий для удостоверяющих центров. «Крипто-ПРО» предоставляет разработчикам интерфейсы для встраивания элементов криптографической защиты в свои программные продукты и оказывает весь спектр консалтинговых услуг по созданию СКЗИ.

Криптопровайдер КриптоПро

При разработке СКЗИ КриптоПро CSP использовалась встроенная в операционную систему Windows криптографическая архитектура Cryptographic Service Providers. Архитектура позволяет подключать дополнительные независимые модули, реализующие требуемые алгоритмы шифрования. С помощью модулей, работающих через функции CryptoAPI, криптографическую защиту могут осуществлять как программные, так и аппаратные СКЗИ.

Носители ключей

В качестве личных ключей могут использоваться различные аппаратные средства, такие как:

– смарт-карты и считыватели;

– электронные замки и считыватели, работающие с устройствами Touch Memory;
– различные USB-ключи и сменные USB-накопители;
– файлы системного реестра Windows, Solaris, Linux.

Функции криптопровайдера

СКЗИ КриптоПро CSP полностью сертифицирована ФАПСИ и может использоваться для:

1. Обеспечения юридической силы и авторизации электронных документов с помощью создания и проверки ЭЦП в соответствии с российскими стандартами шифрования.

2. Полной конфиденциальности, аутентичности и целостности данных с помощью шифрования и имитационной защиты согласно российским стандартам шифрования и протокола TLS.

3. Проверки и контроля целостности программного кода для предотвращения несанкционированного изменения, и доступа.

4. Создания регламента защиты системы.

Обзор программы Folder Lock

Основные возможности программы Folder Lock следующие:

– AES-шифрование, длина ключа 256 бит.
– Сокрытие файлов и папок.
– Шифрование файлов (посредством создания виртуальных дисков — сейфов) «на лету».
– Резервное копирование онлайн.
– Создание защищенных USB/CD/DVD-дисков.
– Шифрование вложений электронной почты.
– Создание зашифрованных «бумажников», хранящих информацию о кредитных картах, счетах и т.д.

Преимущества программы Folder Lock:

– Привлекательный и понятный интерфейс, который понравится начинающим пользователям, владеющим английским языком.
– Прозрачное шифрование «на лету», создание виртуальных зашифрованных дисков, с которыми можно работать, как с обычными дисками.
– Возможность резервного онлайн-копирования и синхронизации зашифрованных контейнеров (сейфов).
– Возможность создания саморасшифровывающихся контейнеров на USB/CD/DVD-дисках.

Недостатки программы:

– Нет поддержки русского языка, что усложнит работу с программой пользователей, не знакомых с английским языком.

– Сомнительные функции Lock Files (которая просто скрывает, а не «запирает» файлы) и Make Wallets (малоэффективна без экспорта информации). Честно говоря, думал, что функция Lock Files будет обеспечивать прозрачное шифрование папки/файла на диске, как это делает программа CyberSafe Top Secret или файловая система EFS.

– Отсутствие возможности подписания файлов, проверки цифровой подписи.

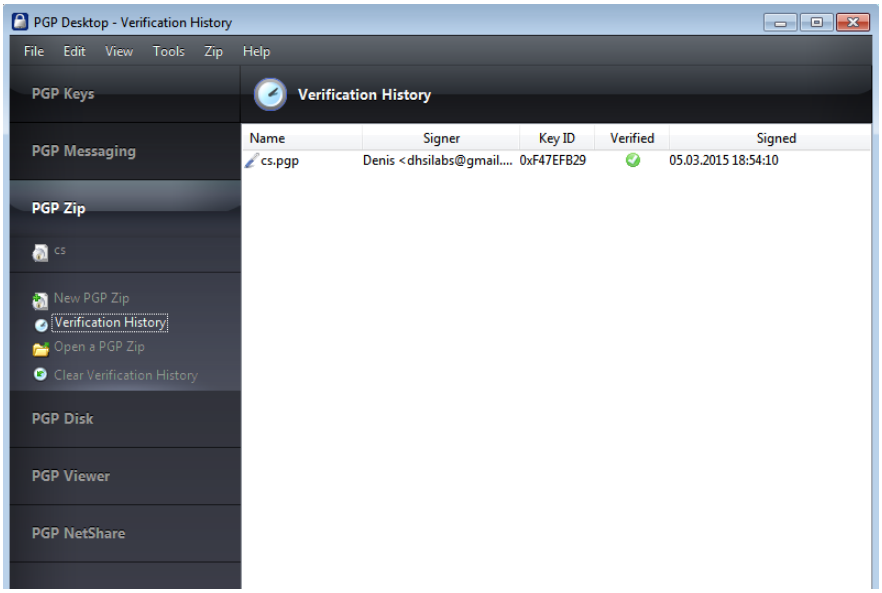
– При открытии сейфа не позволяет выбрать букву диска, которая будет назначена виртуальному диску, который соответствует сейфу. В настройках программы можно выбрать только порядок, в котором программа будет назначать букву диска — по возрастанию (от A до Z) или по убыванию (от Z до A).

– Нет интеграции с почтовыми клиентами, есть только возможность зашифровать вложение.

– Высокая стоимость облачного резервного копирования.

PGP Desktop

Программа PGP Desktop от Symantec — это комплекс программ для шифрования, обеспечивающий гибкое многоуровневое шифрование. Программа отличается от CyberSafe TopSecret и Folder Lock тесной интеграцией в системную оболочку. Программа встраивается в оболочку (Проводник), а доступ к ее функциям осуществляется через контекстное меню Проводника (рис. 14). Как видите, в контекстном меню есть функции шифрования, подписи файла и т.д. Довольно интересной является функция создания саморасшифровывающегося архива — по принципу самораспаковывающегося архива, только вместо распаковки архив также еще и расшифровывается.



Преимущества программы PGP Desktop:

– Полноценная программа, использующаяся для шифрования файлов, подписания файлов и проверки электронной подписи, прозрачного шифрования (виртуальные диски и шифрование всего раздела), шифрования электронной почты.

– Поддержка сервера ключей keyserver.pgp.com.

– Возможность создания саморасшифровывающихся архивов.

– Возможность шифрования системного жесткого диска.

– Функция PGP NetShare.

– Возможность затирания свободного места.

– Тесная интеграция с Проводником.

Недостатки программы:

– Отсутствие поддержки русского языка, что усложнит работу с программой пользователям, которые не знают английский язык.

– Нестабильная работа программы.

– Низкая производительность программы.

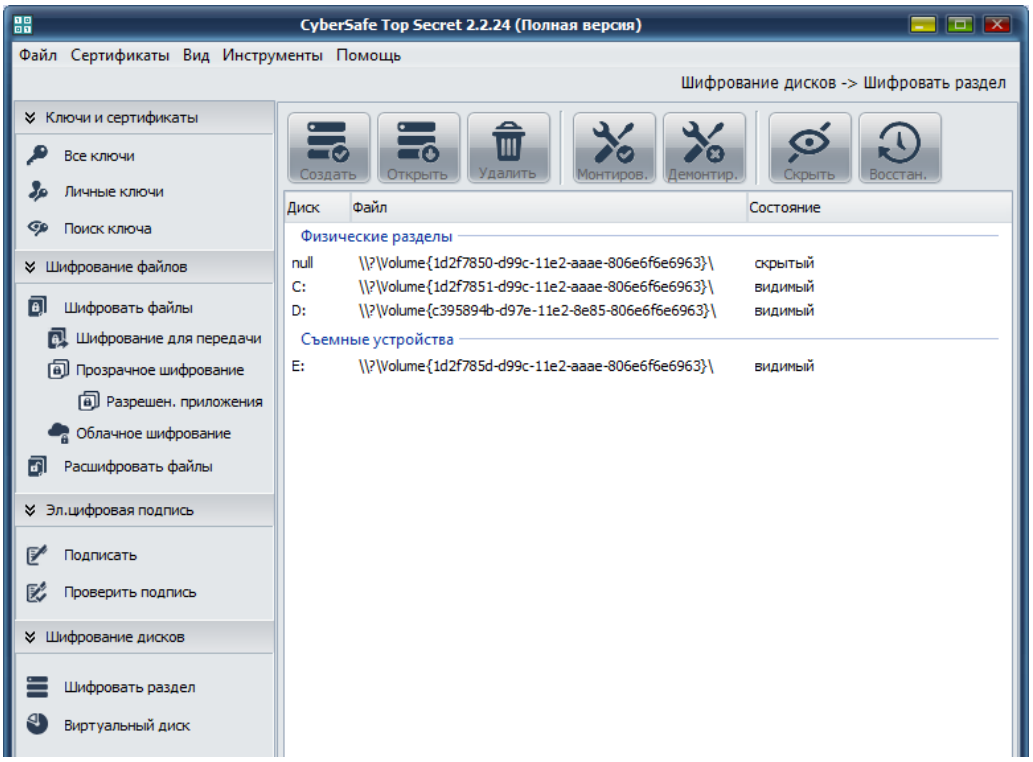
– Есть поддержка AOL IM, но нет поддержки Skype и Viber.

– Уже расшифрованные письма остаются незащищенными на клиенте.

– Защита почты работает только в режиме перехвата, который быстро вам надоест, поскольку окно защиты почты будет появляться каждый раз для каждого нового сервера.

CyberSafe Top Secret

Программа содержит средства управления ключами и сертификатами, а наличие в CyberSafe собственного сервера ключей позволяет пользователю опубликовать на нем свой открытый ключ, а также получить открытые ключи других сотрудников компании



Преимущества программы CyberSafe Top Secret:

– Поддержка алгоритмов шифрования ГОСТ и сертифицированного криптопровайдера КриптоПро, что позволяет использовать программу не только частным лицам и коммерческим организациям, но и государственным учреждениям.

– Поддержка прозрачного шифрования папки, что позволяет использовать программу в качестве замены EFS. Учитывая, что программа обеспечивает лучший уровень производительности и безопасности, такая замена более чем оправдана.

– Возможность подписания файлов электронной цифровой подписью и возможность проверки подписи файла.

– Встроенный сервер ключей, позволяющий публиковать ключи и получать доступ к другим ключам, которые были опубликованы другими сотрудниками компании.

– Возможность создания виртуального зашифрованного диска и возможность шифрования всего раздела.

– Возможность создания саморасшифровывающихся архивов.

– Возможность бесплатного облачного резервного копирования, которое работает с любым сервисом — как платным, так и бесплатным.

– Двухфакторная аутентификация пользователя.

– Система доверенных приложений, позволяющая разрешить доступ к зашифрованным файлам только определенным приложениям.

– Приложение CyberSafe поддерживает набор инструкций AES-NI, что положительно сказывается на производительности программы (этот факт будет продемонстрирован далее).

– Драйвер программы CyberSafe позволяет работать по сети, что дает возможность организовать корпоративное шифрование.

– Русскоязычный интерфейс программы. Для англоязычных пользователей имеется возможность переключения на английский язык.

Теперь о недостатках программы.

– Особых недостатков у программы нет, но поскольку была поставлена задача честно сравнить программы, то недостатки все же придется найти. Если совсем уж придираться, иногда в программе (очень-очень редко) «проскакивают» нелокализированные сообщения вроде «Password is weak». Также пока программа не умеет шифровать системный диск, но такое шифрование не всегда и не всем необходимо. Но все это мелочи по сравнению с зависанием PGP Desktop и ее стоимостью (но об этом вы еще не знаете).

Задание 1

1 Провести анализ предоставленных программ и сделать вывод о эффективности программ;

Таблица 1. Программы и функции

Функция	Folder Lock	PGP Desktop	CyberSafe Top Secret
Виртуальные зашифрованные диски			
Шифрование всего раздела			
Шифрование системного диска			
Удобная интеграция с почтовыми клиентами			
Шифрование сообщений электронной почты			
Шифрование файлов			
ЭЦП, подписание			
ЭЦП, проверка			
Прозрачное шифрование папки			
Самораспифровывающиеся архивы			
Облачное резервное копирование			
Система доверенных приложений			
Поддержка сертифицированного криптопровайдера			
Поддержка токенов			
Собственный сервер ключей			
Двухфакторная аутентификация			
Сокрытие отдельных файлов			
Сокрытие разделов жесткого диска			
Бумажники для хранения платежной информации			
Поддержка шифрования ГОСТ			
Русский интерфейс			
Последовательная чтение/ запись (DiskMark), Мб/с			
Стоимость			

Задание 2

1. Провести анализ производительности компьютера, с помощью CrystalDiskMark, во время работы данных программ

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №8:

1. Назовите основные цели криптографии;
2. Что такое конфиденциальность, Целостность, Аутентификация и Авторство?
3. Чем Системы программной криптозащиты отличаются от Программно-аппаратной криптозащиты
4. Назовите функции криптопровайдера.
5. Какие методы и средства защиты применяются на физическом, аппаратном, программном, организационном уровнях?
6. Какие основные задачи решаются на программно-аппаратном уровне защиты?
7. Какие средства защиты используют от НСД, НСИ?
8. Как произвести защиту от некорректного использования ресурсов?
9. Перечислите средства защиты БД: основные и дополнительные.

Практическая работа №9
«Шифрование методом Цезаря и Виженера»

Цель работы:

1 Знакомство с простейшими приемами шифрования и дешифрования текстовой информации;

2 Изучить методы шифрования многоалфавитной замены.

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).

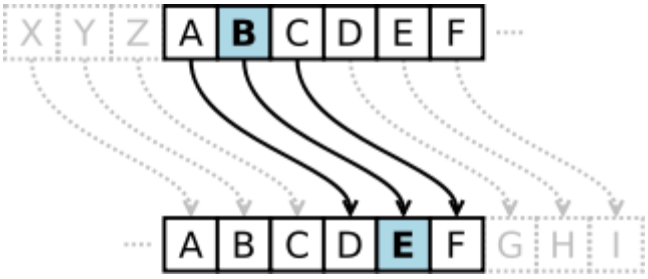
В методе шифрования с секретным или *симметричным ключом* имеется один *ключ*, который используется как для шифрования, так и для расшифровки сообщения. Такой *ключ* нужно хранить в секрете. Это затрудняет использование системы шифрования, поскольку ключи должны регулярно меняться, для чего требуется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

и так далее

- Z заменяется на C

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:

```
Исходный алфавит: А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т
У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Шифрованный:      Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х
Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В
```

Оригинальный текст:

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

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

```
Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм 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

Буквы ключа

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

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

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 «э». Так продолжая дальше, находим шифрованный текст полностью:

м о н а с т ы р ь м о н а с т ы р ь м о н
р а с к и н у л о с ь м о р е ш и р о к о
э о я к щ а п ы й ю й щ о в ч ф ш л 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:

```
ATTACKATDAWN
```

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

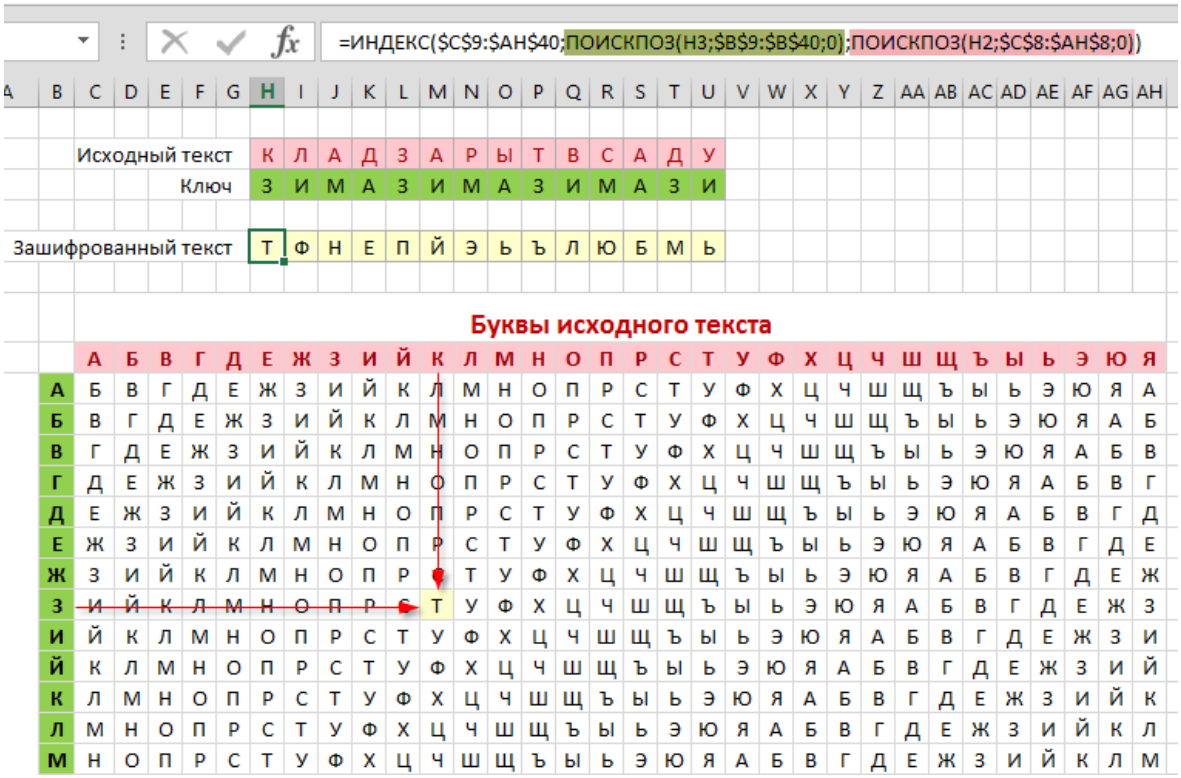
```
LEMONLEMONLE
```

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:                 LEMONLEMONLE
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

I. Задание:

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

3 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: АЛГОРИТМИЗАЦИЯ, КОМПЬЮТЕР, ИНТЕРНЕТ.

4 Слово ЁПЯЪЕБ получено с помощью шифра Виженера с ключевым словом БАНК. Восстановить исходное слово.

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

D ktce hjlbkfcm `kjxrf?

D ktce jyf hjckf?

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

Москва - столица России.

7 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.

8 Используя приведенный выше шифр перестановки, закодировать следующие слова:

ГОРИЗОНТ, ТЕЛЕВИЗОР, МАГНИТОФОН.

9 Определить правило шифрования и расшифрования слова:

КЭРНОЦЛИТКЭЛУОНПИЕЖДАИФЯ

УКРОГРЕОШЛАЕКВИСЧТЕВМО

10* Придумать свой ключ шифрования и закодировать с помощью него сообщение:

Бит - это минимальная единица измерения информации.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

II. Задание:

- 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
- ПРОГРАММА
- ПАМЯТЬ – ГВОЗДЬ
- ЖЕЛЕЗО

- МОНИТОР – АКУЛА
- МЫШКА
- КОЛОНКИ – МОРЕ
- СТУЛ
- НОУТБУК – ТАЧПАД
- ЗАРЯДКА
- КАБЕЛЬ – КОГТИ
- ИГРА
- БРАУЗЕР – МАШИНА
- ХОЛОДИЛЬНИК
- ВОДА – ЭНЕРГИЯ
- ГОРОД
- РАБОТА – СНЕГ
- СТУДЕНТ
- ПАНЕЛЬ – ЗАРЯДКА
- ЧАЙНИК
- НАУШНИКИ – СКЛАД
- ДВИГАТЕЛЬ
- МОДЕРНИЗАЦИЯ – ШИФР

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №9:

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.
11. Понятие полиалфавитной замены.
12. Понятие замены с помощью матрицы Виженера.
13. Перечислите достоинства и недостатки полиалфавитной замены.

Практическая работа №10
«Шифрование методом Полибия»

Цель работы:

1. Ознакомиться с древнейшим шифром – шифром Полибия.

– **Шифр Полибия**

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

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

Это устройство представляло собой квадрат 5×5, столбцы и строки которого 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 буквы i 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 при использовании латинского варианта «квадрата Полибия», в котором буквы расположены в алфавитном порядке.

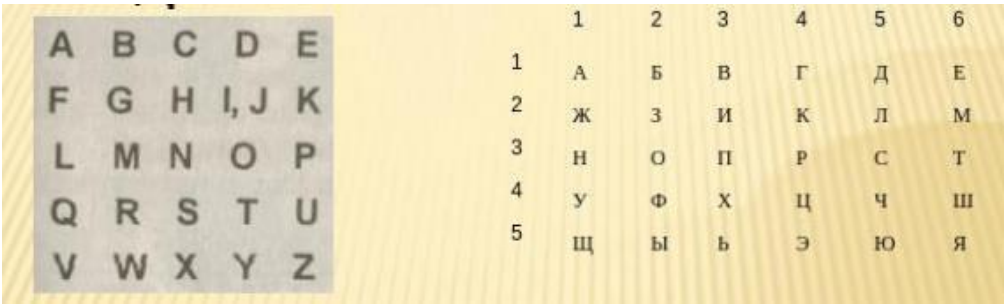
Квадрат ПОЛИБИЯ

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

	1	2	3	4	5
1	А	Б	В	Г	Д
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)

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



	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

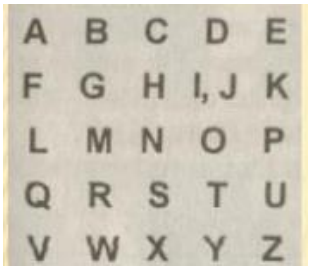
Несмотря на то, что квадрат изначально создавался для кодирования, с его помощью можно успешно шифровать. Для того, чтобы зашифровать текст квадратом Полибия, нужно сделать несколько шагов:

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

Или есть такой вариант: Шифр «Квадрат Полибия».

«Квадрат Полибия» представляет собой квадрат 5x5, столбцы и строки которого нумеруются цифрами от 1 до 5.

	1	2	3	4	5
1	А	Б	В	Г	Д
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	Ы	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:	SOMETEXT
После шифрования:	XTRKYKCY

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	U

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 шифрования:	**IUPTNQVO**

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 ПО ПРАКТИЧЕСКОЙ РАБОТЕ №10:

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?
7. Что такое криптостойкость системы?
8. Правила использования ключа.

Практическая работа №11
«Мероприятия по защите информации от вредоносных программ»

Цель работы:

1. Изучение вредоносных программ и антивирусного программного обеспечения
2. Выработать практические навыки работы с антивирусными программами.

1. Краткие теоретические сведения.

Вирусы. Антивирусное программное обеспечение

Компьютерный вирус - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере. Признаки заражения:

- прекращение работы или неправильная работа ранее функционировавших программ
- медленная работа компьютера

– невозможность загрузки ОС
– исчезновение файлов и каталогов или искажение их содержимого
– изменение размеров файлов и их времени модификации
– уменьшение размера оперативной памяти
– непредусмотренные сообщения, изображения и звуковые сигналы
– частые сбои и зависания компьютера и др.

Классификация компьютерных вирусов

По среде обитания:

– Сетевые - распространяются по различным компьютерным сетям
– Файловые - внедряются в исполняемые модули (COM, EXE)
– Загрузочные - внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
– Фалово-загрузочные - внедряются и в загрузочные сектора, и в исполняемые модули

По способу заражения:

– Резидентные - при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
– Нерезидентные - не заражают оперативную память и активны ограниченное время

По воздействию:

– Неопасные- не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
– Опасные - приводят к различным нарушениям в работе компьютера
– Очень опасные - могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

– Паразиты - изменяют содержимое файлов и секторов, легко обнаруживаются
– Черви- вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
– Степсы - перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
– Мутанты - содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
– Трояны - не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

Основные меры по защите от вирусов

– оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, A VP
– постоянно обновляйте антивирусные базы
– делайте архивные копии ценной для Вас информации (гибкие диски, CD)

Классификация антивирусного программного обеспечения

– Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти, и поиске в них известных и новых (неизвестных сканеру) вирусов.
– Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.
– Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре

каталогов, иногда -объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят

Хакерские утилиты и прочие вредоносные программы.

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Руткит (Rootkit) - программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы.

В системе Windows под термином руткит принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).

В последнее время угроза руткитов становится все более актуальной, т.к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер (Интернет, локальная сеть, электронная почта, съемные носители информации). Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Межсетевой экран — это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файервол от английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана. Межсетевой экран позволяет:

- Блокировать хакерские атаки;
- Не допускать проникновение сетевых червей;
- Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Защитные технологии Windows 7

ОС Windows 7 содержит следующие новые и усовершенствованные технологии, обеспечивающие повышенную защиту от вредоносных программ:

- центр поддержки;
- контроль учетных записей (UAC);
- средства биометрической защиты;
- защитник Windows;
- средство удаления вредоносных программ (MSRT);
- брандмауэр Windows;
- технология AppLocker.

Необходимо также помнить, что вход в систему в качестве обычного пользователя по-прежнему является настоятельно рекомендуемой мерой обеспечения безопасности.

Настоятельно рекомендуется также установить антивирусное решение, обеспечивающее защиту в реальном времени, например Forefront Client Security. Это позволит защитить компьютер от новых угроз по мере их появления. Если на предприятии используется стратегия глубокой обороны (defense-in-depth), возможно также использование других средств сканирования, доступных либо как часть Windows 7, либо в виде отдельных загрузок.

Следует помнить, что если возможность получения административных привилегий не оберегается должным образом, то даже при использовании всех этих технологий все компьютеры сети оказываются под угрозой.

Центр поддержки

В ОС Windows Vista параметры безопасности собраны в центре обеспечения безопасности, расположенном в панели управления. В Windows 7 центр обеспечения безопасности стал частью нового центра поддержки (Action Center). В нем сведены как параметры безопасности, так и настройки других административных задач, например резервного копирования, разрешения проблем, диагностики и обновления Windows Update. Категории уведомлений, которые можно включить или выключить в центре поддержки, перечислены в диалоговом окне **Change Action Center settings** (настройка центра поддержки), показанном на рис. 2.1.

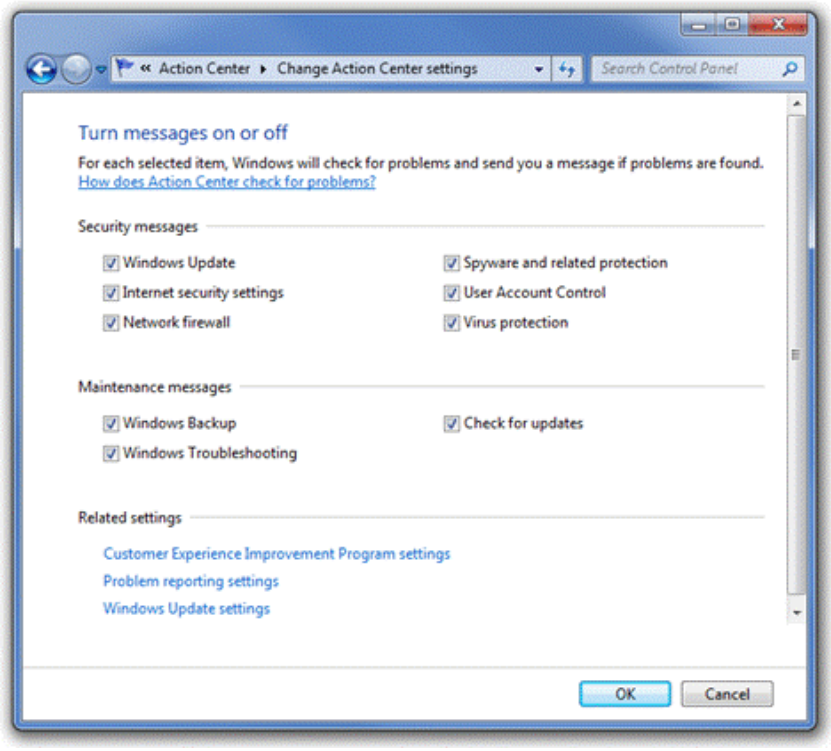


Рисунок 2.1 Диалоговое окно настройки центра поддержки

Помимо выдачи пользователю уведомлений о возможных проблемах, центр поддержки также контролирует способ передачи этой информации в Майкрософт для поиска решений. Возможные варианты показаны на рис. 2.2.

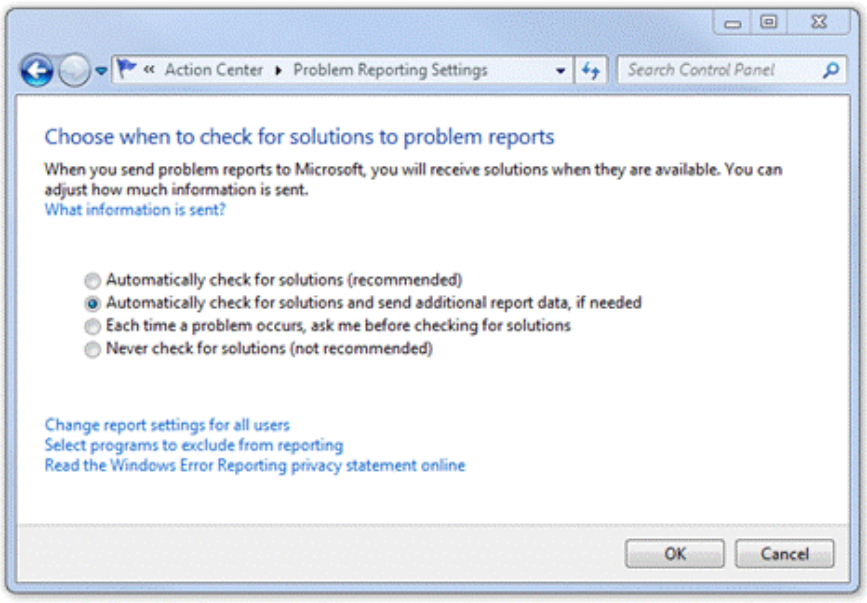


Рисунок 2.2 Диалоговое окно параметров отчетов о проблемах центра поддержки

Информацию, отправляемую при этом в Майкрософт, можно просмотреть следующим образом.

1. Откройте главное окно **Центра поддержки**.
2. Нажмите кнопку **Maintenance** (обслуживание).
3. В разделе **Check for solutions to problem reports** (поиск решений для указанных в отчетах проблем) щелкните **View reliability history**(показать журнал стабильности работы).
4. Дважды щелкните любую запись журнала, чтобы просмотреть технические подробности.

Записи категории **Informational events** (информационные события) обычно описывают изменения в программной и аппаратной конфигурации компьютера.

Подробнее об отправлении информации и обеспечении конфиденциальности см. Заявление о конфиденциальности службы отчетов об ошибках.

Использование групповой политики для снижения рисков, связанных с центром поддержки

Доступные в этой категории параметры находятся в двух расположениях редактора объектов GPO:

Computer Configuration\Windows Components\Windows Error Reporting (Конфигурация компьютера\Компоненты Windows\Отчеты об ошибках Windows)

В следующей таблице приведены параметры этой технологии, применимые к Windows 7.

Таблица 2.1 Параметры центра поддержки Windows

Объект политики	Описание	По умолчанию в Windows 7
Disable Windows Error Reporting (отключить отчеты об ошибках Windows)	Если включить этот параметр, служба отчетов об ошибках не станет отправлять в Майкрософт никакой информации. Кроме того, не будет доступа к информации о возможных решениях проблем в панели управления центра поддержки.	Не задано

User Configuration\Start Menu and Taskbar (Конфигурация пользователя\Меню «Пуск» и панель задач\)

В следующей таблице приведены параметры этой технологии, применимые к Windows 7.

Таблица 2.2 Параметры центра поддержки Windows

Объект политики	Описание	По умолчанию в Windows 7
Remove the Action Center icon (удалить значок центра поддержки)	Удаляет значок центра поддержки из области уведомлений. Если включить этот параметр, значок центра поддержки не будет отображаться в системной области уведомлений. Если отключить этот параметр или не настраивать его, значок центра поддержки будет отображаться.	Не задано

Контроль учетных записей

Контроль учетных записей (UAC) появился в ОС Windows Vista с целью упрощения использования учетных записей, не обладающих административными привилегиями. В состав UAC входят несколько технологий: учетная запись защищенного администратора (PA), запросы на повышение прав, виртуализация реестра, виртуализация файловой системы и уровни целостности Windows. Хотя использование защищенной учетной записи администратора более безопасно, чем использование незащищенной, все же безопаснее всего для повседневных задач выбирать учетную запись обычного пользователя. Многое из того, что в предыдущих версиях Windows требовало административных привилегий, в Windows Vista доступно обычным пользователям. Благодаря использованию для повседневных задач учетной записи со стандартными правами снижается риск, что вредоносное ПО установит нежелательную программу или внесет опасные изменения в систему.

В ОС Windows 7 можно выбрать тип уведомлений UAC и частоту их появления. Имеется четыре основных уровня, настроить которые можно в соответствующем разделе центра поддержки.

– **Always notify me when:** (всегда уведомлять в следующих случаях). При выборе этого варианта UAC будет запрашивать подтверждение при установке программ и внесении любых изменений в параметры Windows.

– **Default – Notify me only when programs try to make changes to my computer** (По умолчанию — уведомлять только при попытках программ внести изменения в компьютер). В этом случае UAC выдает предупреждения, только когда программы вносят изменения в компьютер, но не когда это делает пользователь. Этот уровень в Windows 7 используется по умолчанию.

– **Notify me only when programs try to make changes to my computer (do not dim my desktop)** (Уведомлять только при попытках программ внести изменения в компьютер (не затемнять рабочий стол). На этом уровне подтверждение запрашивается только при внесении изменений программами, но безопасный рабочий стол для этого не используется, так что текущий рабочий стол не затемняется при выдаче запроса.

– **Never notify me when:** (никогда не уведомлять в следующих случаях:). При этом значении UAC не выдает никаких запросов, когда программы устанавливают ПО или вносят изменения в систему, а также когда пользователь пытается внести в параметры Windows изменения административного уровня. Использовать его не рекомендуется.

Когда технология UAC только появилась, частая выдача запросов приводила к тому, что ее отключали. В Windows 7 количество запросов на повышение прав сократилось, поскольку обычным пользователям разрешено выполнять больший круг действий. А при использовании учетной записи защищенного администратора некоторые программы из состава Windows 7 самостоятельно могут выполнить повышение, не выдавая запроса.

Мы рекомендуем как минимум оставить значение по умолчанию — **Уведомлять только при попытках программ внести изменения в компьютер**, а также рассмотреть вопрос о его повышении до **Всегда уведомлять** в тех средах, где клиентские компьютеры часто подключаются к публичным

сетям или где безопасность имеет высокий приоритет. Меньшая частота выдачи запросов повышает шансы вредоносного ПО внести нежелательные изменения в компьютер.

Режим одобрения администратором в UAC обеспечивает ограниченную защиту компьютеров с ОС Windows 7 и Windows Vista с пакетом обновления 1 (SP1) от некоторых типов вредоносных программ. Большинство программ и задач из состава Windows 7 работают как должно со стандартными правами пользователя. Когда пользователь пытается выполнить административную задачу, например установить новую программу или изменить некоторые параметры системы, сначала производится запрос подтверждения этого действия. Однако, этот режим не обеспечивает того же уровня защиты, что работа со стандартными правами. Он не гарантирует, что вредоносное ПО, уже проникшее на клиентский компьютер, не сможет внедриться в программу, работающую с повышенными правами. Он также не гарантирует, что программа с повышенными правами не попытается совершить вредоносных действий после повышения.

Оценка рисков

Пользователи с правами администратора при входе в систему обладают административными привилегиями. Это позволяет им случайно выполнить или неосознанно разрешить выполнение какой-либо административной задачи, как в следующих примерах.

- Пользователь, не сознавая того, загружает и устанавливает вредоносную программу с зараженного или специально сфабрикованного веб-сайта.
- Пользователя хитростью убеждают открыть приложение к электронному письму. Вирус, содержащийся в нем, запускается и, возможно, внедряется на компьютер.
- В компьютер вставляется съемный диск. Функция автозапуска немедленно запускает программу с него, которая оказывается вредоносной.
- Пользователь устанавливает неподдерживаемое приложение, что отражается на производительности или стабильности работы.

Снижение риска

Для выполнения повседневных задач пользователям рекомендуется использовать учетную запись со стандартными правами. Хотя контроль учетных записей и может использоваться для повышения прав путем запроса учетных данных администратора, нужно вместо этого начать новый сеанс с правами администратора, используя быстрое переключение пользователей. Следует также убедиться, что контроль учетных записей запрашивает подтверждение при выполнении задачи, требующей административных привилегий.

Анализ мер по снижению риска

Риски, описанные в предыдущем разделе, «Оценка рисков», могут быть снижены благодаря использованию UAC. При этом, однако, необходимо учитывать следующее.

- Если на предприятии есть собственные разработчики, им рекомендуется изучить статью «Требования к разработке приложений для Windows Vista, совместимых с контролем учетных записей«. В этом документе описывается проектирование и разработка UAC-совместимых приложений.
- Приложения, не соответствующие требованиям UAC, могут вызывать проблемы на уровнях защиты по умолчанию. По этой причине перед развертыванием необходимо тестировать приложения на совместимость с UAC. Подробнее о тестировании совместимости приложений см. главу 4, «Совместимость приложений с Windows 7».
- Запросы UAC на ввод учетных данных администратора и повышение прав увеличивают число шагов, необходимых для выполнения многих административных задач. Необходимо установить, представляет ли это проблему для штата администраторов. Если дополнительные запросы UAC существенно сказываются на них, можно установить для параметра политики **Behavior of the elevation prompt for administrators in Admin Approval Mode** (поведение запроса на повышение прав для администраторов в режиме одобрения администратором) значение **Elevate without prompting**

(повышать без запроса). Это, однако, ослабит степень защищенности компьютера и повысит риск, исходящий от более старых вредоносных программ.

– Пользователь, обладающий административными привилегиями и работающий от имени учетной записи защищенного администратора (PA), может отключить режим одобрения администратором, запретить выдачу запросов учетных данных администратора при установке приложений и изменить способ выдачи запросов на повышение прав. Поэтому, если пользователи обладают правами администратора, то нельзя гарантировать, что политики UAC выполняются.

– Администраторам предприятия рекомендуется иметь две учетные записи. Для повседневных задач следует использовать учетную запись обычного пользователя. При необходимости выполнить административное действие следует войти в систему от имени учетной записи с правами администратора, выполнить это действие, выйти из системы и вернуться к работе от имени обычного пользователя.

– Параметры групповой политики, рекомендуемые в этом руководстве, отключают возможность обычных пользователей повышать права. Обратите внимание, что это поведение по умолчанию для компьютеров, входящих в домен Active Directory. Это рекомендуемый подход, поскольку так административные задачи могут выполняться только пользователями, чьи учетные записи были специально отнесены к группе администраторов.

– Если приложение неверно отнесено к группе административных или пользовательских, Windows может запустить его в неверном контексте безопасности, например с маркером «администратор» или «обычный пользователь».

Процесс снижения рисков

Процесс снижения рисков начинается с изучения всех возможностей контроля учетных записей. Подробнее об этом см. Контроль учетных записей в Windows Vista: общие сведения и настройка и Введение в контроль учетных записей Windows Vista.

Ход процесса снижения рисков

1. Определить количество пользователей, способных выполнять административные задачи.
2. Определить, насколько часто административные задачи требуется выполнять.
3. Установить, могут ли администраторы выполнять административные задачи, просто соглашаясь с запросом UAC, или для этого им необходимо вводить учетные данные.
4. Определить, следует ли обычным пользователям иметь возможность повышать права для выполнения административных задач. Параметры политики, рекомендуемые в рамках этого руководства, блокируют эту возможность для обычных пользователей.
5. Определить, как часто требуется устанавливать приложения.
6. Настроить групповую политику UAC в соответствии с вашими требованиями.

Использование групповой политики для снижения рисков, связанных с UAC

Доступные в этой категории параметры находятся в следующем расположении редактора объектов GPO:

Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options\ (Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности\)

В следующей таблице приведены параметры этой технологии, применимые к Windows 7.

Таблица 2.3 Параметры контроля учетных записей Windows

Объект политики	Описание	По умолчанию в Windows 7
User Account Control: Admin Approval Mode for the built-in Administrator account (Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора)	Этот параметр политики контролирует поведение режима одобрения администратором для встроенной учетной записи администратора.	Отключено
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop (Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол)	Этот параметр определяет, могут ли UIAccess-приложения, или UIA-приложения, автоматически отключать безопасный рабочий стол при выдаче обычному пользователю запросов на повышение прав.	Отключено
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode (Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором)	Этот параметр политики определяет поведение запроса на повышение прав для администраторов.	Запрос для исполняемых файлов не из состава Windows
User Account Control: Behavior of the elevation prompt for standard users (Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей)	Этот параметр политики определяет поведение запроса на повышение прав для обычных пользователей.	Запрос учетных данных на безопасном рабочем столе
User Account Control: Detect application installations and prompt for elevation (Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав)	Этот параметр политики определяет, следует ли пытаться распознать факт установки приложения.	Включено
User Account Control: Only elevate executable that are signed and validated (Контроль учетных записей: повышать права только для подписанных и проверенных исполняемых файлов)	Этот параметр политики вводит принудительную проверку подписей инфраструктуры открытых ключей (PKI) для любых интерактивных приложений, требующих повышения прав. Добавляя сертификаты в хранилище доверенных издателей на локальных компьютерах, можно контролировать, какие приложения разрешено запускать.	Отключено
User Account Control: Only elevate UIAccess applications that are installed in secure locations (Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах)	Этот параметр политики определяет, обязано ли приложение, запрашивающее уровень целостности UIAccess, находиться в безопасном расположении файловой системы.	Включено
User Account Control:Run all Administrators in Admin approval Mode (Контроль учетных записей: все администраторы работают в режиме одобрения администратором)	Этот параметр политики определяет поведение всех параметров политики UAC на компьютере. При его изменении компьютер нужно перезапустить.	Включено
User Account Control:Switch to the secure desktop when prompting for elevation (Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав)	Этот параметр политики определяет, на каком рабочем столе выдавать запрос — на безопасном или на текущем.	Включено
User Account Control: Virtualize file and registry write failures to per-user locations (Контроль учетных записей: при отказе в праве на запись использовать виртуализацию файловой системы и реестра для перенаправления в расположение пользователя)	Этот параметр политики определяет, следует ли при отказе в праве на запись перенаправлять вывод в определенные расположения реестра и файловой системы.	Включено

В этой таблице приведено лишь краткое описание каждого параметра. Более подробно о каждом из них см. вкладку **Explain** (объяснение) редактора объектов групповой политики.

Средства биометрической защиты

В состав Windows 7 входит биометрическая платформа Windows (Windows Biometric Framework), которая обеспечивает единообразное представление сканеров отпечатков пальцев и других биометрических устройств в форме, удобной высокоуровневым приложениям, а также позволяет в единой манере использовать приложения по анализу отпечатков пальцев. В предыдущих версиях Windows сканеры отпечатков пальцев поддерживались как средство входа в систему. Такими сканерами сейчас оборудованы многие переносные компьютеры, но для их работы требовались драйверы и специальное программное обеспечение. Теперь поддержка таких устройств является частью Windows 7, и для их работы ничего кроме драйвера не требуется.

Оценка рисков

Общепринятые методики проверки паролей имеют ряд недостатков, из которых произрастают риски для безопасности. Если вся система проверки подлинности построена исключительно на паролях, то их могут записывать на бумажках, подслушивать, забывать, а если пароль несложен, его можно просто подобрать.

Для усиления защиты паролей можно использовать многофакторную проверку подлинности, добавив в процесс проверки дополнительное устройство, например смарт-карту. Тогда пользователь должен будет и *доказать, что знает* (пароль), и *доказать, что обладает* (смарт-картой). По сравнению с проверкой только на основе пароля это шаг вперед. Однако, смарт-карты и устройства их чтения могут украсть, потерять и даже внести в них какие-то изменения.

Снижение риска

Появление в ОС Windows 7 поддержки биометрии позволяет создать дополнительный уровень проверки, в рамках которого пользователь должен предъявить *что-то, что является его частью*. Этот подход снижает риски, связанные с недостатками паролей и смарт-карт. Хотя Windows 7 поддерживает много различных способов биометрической проверки подлинности, распространенность и доступность сканеров отпечатков пальцев делает именно эту технологию наиболее часто встречающейся.

Проверка отпечатков пальцев обладает следующими преимуществами.

- Обычно отпечатки пальцев не меняются в течение всей жизни.
- За всю историю не было обнаружено ни одной пары одинаковых отпечатков (даже у однояйцевых близнецов).
- Сканеры отпечатков пальцев теперь более доступны.
- Процесс сканирования прост и занимает мало времени.
- Высокая надежность сканирования, т.е. более низкий коэффициент ложного пропуска по сравнению с другими формами биометрического анализа, например распознавания лица или голоса.
- У этой формы установления личности есть и следующие недостатки.
- При повреждении пальца становится невозможным пройти проверку.
- Исследования показали, что некоторые системы распознавания отпечатков пальцев можно обойти, представив «обманку».
- Возраст или характер работы пользователя могут не позволить ему успешно проходить проверки.

Анализ мер по снижению риска

Если на предприятии вместе с Windows 7 планируется внедрение биометрического механизма проверки, например сканирования отпечатков пальцев, следует заранее учесть следующие соображения.

– Биометрические системы обычно требуют хранения на компьютере информации, которая может использоваться для установления личности. По этой причине предприятию придется заниматься обеспечением конфиденциальности.

– Многие современные переносные компьютеры обладают встроенными сканерами отпечатков пальцев, что может упростить внедрение биометрического решения, однако по функциональности и качеству распознавания такие встроенные устройства могут уступать специализированному оборудованию. Следует сравнить относительное качество по таким показателям, как коэффициент ложного пропуска, коэффициент ложного отказа, коэффициент ошибок кроссовера, коэффициент ошибок регистрации и пропускная способность.

– Если по характеру работы пользователи или компьютеры оказываются в загрязненных помещениях, где сложно поддерживать чистоту рук или требуются перчатки, сканеры отпечатков использовать не удастся. Эту проблему можно преодолеть за счет использования систем анализа других физиологических параметров, например геометрии лица, радужной оболочки глаза или ладони.

– Наряду с биометрическим подтверждением пользователю необходимо представлять какое-либо иное свидетельство, например ключевую фразу, ПИН-код или смарт-карту, поскольку биометрические устройства можно обмануть. Например, группа японских исследователей показала, как с помощью искусственных желатиновых пальцев обойти некоторые системы. Подробнее см. Результаты применения искусственных желатиновых пальцев в системах распознавания отпечатков.

Процесс снижения рисков

Особенности внедрения биометрических средств сильно разнятся от предприятия к предприятию. Однако, можно выделить ряд шагов, которые следует пройти для надлежащего его выполнения. Они приведены ниже.

Ход процесса снижения рисков

1. Установить, какие из имеющихся механизмов проверки биометрических данных больше подходят нуждам предприятия.
2. Проанализировать внутреннюю документацию по обеспечению конфиденциальности, чтобы убедиться в возможности управления конфиденциальными биометрическими данными.
3. Определить требования к оборудованию, используемому при биометрическом сканировании, и наметить сроки выполнения этих требований.
4. Определить элементы инфраструктуры, необходимые для биометрического сканирования, как то инфраструктура публичных ключей или требования к клиентскому программному обеспечению.
5. Установить, у каких сотрудников могут возникнуть проблемы с использованием биометрической системы, и подобрать для них альтернативные варианты, например проверку по имени пользователя и паролю или смарт-карте с ПИН-кодом.
6. Заранее обучить пользователей обращению с системой биометрической проверки подлинности, а тех, кто не сможет ею пользоваться, — альтернативным методам проверки.
7. Провести масштабный пилотный запуск в целях выявления и разрешения проблем до начала повсеместного внедрения.
8. Следуя инструкциям производителя по сканированию и проверке, ввести данные о пользователях в биометрическую систему.
9. Обучить пользователей обращению с системой, обеспечить помощь для тех, кто испытывает трудности.
10. Учесть, что некоторые пользователи могут категорически отказаться использовать биометрическую систему. Предусмотреть для таких пользователей альтернативный способ проверки подлинности.

Использование групповой политики для снижения рисков, связанных с биометрической проверкой

Доступные в этой категории параметры находятся в следующем расположении редактора объектов GPO:

Computer Configuration\Administrative Templates\Windows Components\Biometrics (Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Биометрия)

В следующей таблице приведены параметры этой технологии, применимые к Windows 7.

Таблица 2.4 Параметры биометрического контроля

Объект политики	Описание	По умолчанию в Windows 7
Allow the use of biometrics (Разрешить использование биометрии)	Если включить (или не задавать) этот параметр политики, разрешается запуск приложений, использующих средства Windows по проверке биометрии.	Не задано
Allow users to log on using biometrics (Разрешить пользователям выполнять вход в систему с использованием биометрии)	Этот параметр политики определяет, можно ли пользователям осуществлять вход в систему или производить повышение прав с помощью биометрии. По умолчанию локальным пользователям разрешен такой вход в систему локального компьютера.	Не задано
Allow domain users to log on using biometrics (Разрешить пользователям домена выполнять вход в систему с использованием биометрии)	Этот параметр политики определяет, можно ли пользователям домена осуществлять вход в систему или производить повышение прав с помощью биометрии. По умолчанию пользователи домена не могут использовать такой способ входа в систему.	Не задано
Timeout for fast user switching events (Время ожидания для событий функции быстрого переключения пользователей)	Этот параметр политики задает количество секунд, которое остается активным событие быстрого переключения пользователей перед тем, как переключение произойдет. По умолчанию событие быстрого переключения остается активным 10 секунд, затем переходит в неактивное состояние.	Не задано

В этой таблице приведено лишь краткое описание каждого параметра. Более подробно о каждом из них см. вкладку **Explain** (объяснение) редактора объектов групповой политики.

Защитник Windows

Защитник Windows — это служба защиты от шпионского ПО, впервые появившаяся в качестве необязательного загружаемого компонента Windows® XP. Теперь эта служба интегрирована в Windows® и по умолчанию запускается автоматически, помогая в защите от шпионских программ и другого нежелательного ПО. Шпионские программы могут незаметно попасть на компьютер в любой момент при подключении к Интернету, а также при установке какой-либо программы со съемного диска. Защитник Windows обеспечивает и защиту в реальном времени, и полное сканирование по расписанию.

Диалоговое окно, показанное на рис. 2.3, отображает рекомендуемые параметры защитника Windows для компьютера под управлением Windows 7.

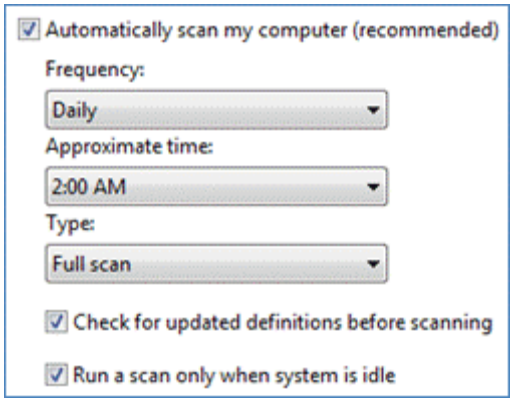


Рисунок 2.3 Диалоговое окно параметров отчетов о проблемах центра поддержки

Когда программа пытается внести изменения в защищенную часть Windows 7, защитник Windows запрашивает у пользователя согласие на эти изменения, чтобы предотвратить возможную установку шпионской программы.

Различные аспекты поведения защитника Windows контролируются параметрами групповой политики ОС Windows 7. Приведенные в следующих разделах значения этих параметров не изменяют поведения этой программы по умолчанию. Это сделано потому, что желательные значения сильно зависят от конкретных условий.

Сообщество Microsoft SpyNet

Microsoft® SpyNet — это сетевое сообщество, призванное научить пользователей адекватно реагировать на угрозы, исходящие от шпионских программ. Оно также борется с распространением новых видов этих программ.

Если защитник Windows обнаруживает программу или изменение, внесенное ею, которые еще не получили оценки степени опасности, можно просмотреть, как другие участники сообщества отреагировали на такое же предупреждение. И наоборот, действия, предпринимаемые вами, помогают другим пользователям определиться с решением. Они также позволяют корпорации Майкрософт выявить программы, степень риска использования которых следует проверить. Об обнаруженном ПО можно отправить как базовую, так и расширенную информацию. Расширенная информация используется для улучшения работы защитника Windows. Например, можно включить данные о расположении обнаруженных и удаленных компонентов вредоносного ПО, и эта информация будет автоматически отправлена сообществу. Подробнее о том, какая информация отправляется в рамках отчетов Microsoft SpyNet, см. Политика обеспечения конфиденциальности защитника Windows.

Оценка рисков

Шпионские программы представляют серьезную опасность для предприятия. Необходимо принять соответствующие меры защиты данных и компьютеров. Чаще всего риски, исходящие от такого ПО, сводятся к следующему.

- Несанкционированное разглашение конфиденциальной деловой информации.
- Несанкционированное разглашение личных данных о сотрудниках.
- Захват контроля над компьютерами со стороны неустановленных лиц.
- Потери производительности из-за негативного эффекта, оказываемого шпионским ПО на стабильность и скорость работы компьютеров.
- Рост стоимости поддержки, вызванный заражением.
- Потенциальный риск шантажа, связанного с попавшей не в те руки конфиденциальной информацией.

Снижение риска

Защитник Windows предназначен для снижения рисков, связанных со шпионским ПО. Эта технология постоянно обновляется через веб-сайт Windows Update или службы Microsoft Windows Server Update Services (WSUS).

В дополнение к защите от шпионских программ, обеспечиваемой защитником Windows, Майкрософт настоятельно рекомендует установить антивирусное решение, чтобы получить возможность обнаруживать вирусы, троянские программы и черви. Например, таким продуктом является Microsoft Forefront™ Client Security, обеспечивающий единообразную защиту настольных, переносных и серверных компьютеров.

Анализ мер по снижению риска

В ОС Windows 7 по умолчанию защитник Windows включен. Этот компонент спроектирован так, чтобы в нормальных условиях оказывать наименьшее влияние на работу пользователя. Несмотря на это, в рамках стратегии развертывания Windows 7 следует учитывать следующие рекомендации.

- Протестируйте совместимость помощника Windows с другими используемыми антивирусными программами, работающими в реальном времени.
- Если число компьютеров на предприятии велико, спроектируйте систему управления развертыванием обновлений сигнатур.
- Обучите пользователей распознавать типичные приемы социальной инженерии, с помощью которых людей убеждают запустить вредоносную программу.
- Задайте желаемое расписание сканирования. По умолчанию оно происходит в 2 часа ночи каждый день. Если компьютер в это время оказывается не в состоянии выполнить сканирование, позднее пользователю будет предложено запустить его вручную. Если в течение следующих двух дней сканирование так и не произойдет, оно автоматически будет запущено примерно через 10 минут после следующего запуска компьютера. В ОС Windows 7 процессу сканирования назначается низкий приоритет, чтобы его влияние на работу пользователя было минимальным. Степень такого влияния существенно ниже, чем было в ОС Windows XP.
- Защитник Windows не является антишпионским приложением корпоративного класса. Он не обеспечивает возможностей по централизованному мониторингу, созданию отчетности и контролю. Если подобные средства необходимы, следует обратить внимание на другие продукты, например Microsoft Forefront Client Security.
- Определитесь с политикой предприятия в части отправки отчетов о возможно шпионском ПО в сообщество Microsoft SpyNet.

Процесс снижения рисков

Защитник Windows изначально входит в состав ОС Windows 7, поэтому для его активации никаких дополнительных шагов не требуется. Однако, в целях обеспечения должной защиты рекомендуется предпринять следующие шаги.

Ход процесса снижения рисков

1. Изучите антишпионские возможности Windows 7 и защитника Windows.
2. Изучите параметры групповой политики, относящиеся к защитнику Windows.
3. Оцените дополнительные средства защиты от вирусов и установите, обеспечивают ли они также защиту от шпионских программ.
4. Составьте оптимальный план по обновлению компьютеров предприятия. Для переносных компьютеров могут потребоваться иные действия по обновлению, чем для настольных.
5. Обучите пользователей замечать подозрительное поведение компьютера.
6. Обучите сотрудников службы поддержки использовать средства защитника Windows для разрешения поступивших вопросов.

Использование групповой политики для снижения рисков, связанных с защитником Windows

Доступные в этой категории параметры находятся в следующем расположении редактора объектов GPO:

Computer Configuration\Administrative Templates\Windows Components\Windows Defender (Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Защитник Windows)

В следующей таблице приведены параметры этой технологии, применимые к Windows 7.

Таблица 2.5 Параметры защитника Windows

Объект политики	Описание	По умолчанию в Windows 7
Turn on definition updates through both WSUSand Windows Update (Включить обновление определений с помощью WSUS и Windows Update)	Этот параметр позволяет помощнику Windows проверять наличие обновленных определений и загружать их с веб-узла Windows Update, если локальный сервер служб WSUS оказывается недоступен.	Не задано
Turn on definition updates through both WSUS and the Microsoft Malware Protection Center (Включить обновление определений через WSUS и Центр Майкрософт по защите от вредоносных программ)	Этот параметр позволяет помощнику Windows проверять наличие обновленных определений и загружать их и с веб-узла Windows Update, и из центра Майкрософт по защите от вредоносных программ, если локальный сервер служб WSUS оказывается недоступен.	Не задано
Check for New Signatures Before Scheduled Scans (Проверять новые подписи перед запланированным сканированием)	Если этот параметр включен, перед сканированием по расписанию будет проверяться наличие обновленных сигнатур. Если параметру задано значение Disabled (отключено) или Not configured (не задано), перед сканированием по расписанию наличие обновлений проверяться не будет.	Не задано
Turn off Windows Defender (Отключить защитник Windows)	Если оставить этот параметр со значением по умолчанию, защита реального времени будет включена.	Не задано
Turn off Real-Time Monitoring (Отключить мониторинг в реальном времени)	Этот параметр отключает запросы защиты реального времени при обнаружении вредоносной программы.	Не задано
Turn off Routinely Taking Action (Отключить постоянные действия)	Этот параметр определяет, будет ли защитник Windows автоматически предпринимать действия при обнаружении угроз. Характер действия для каждой угрозы определяется индивидуально на основе того, что предписано политикой, пользовательскими настройками и базой сигнатур. Если включить этот параметр, защитник Windows не станет автоматически предпринимать действий при обнаружении угрозы, вместо этого предлагая пользователю выбрать один из возможных вариантов. Если отключить или не настраивать этот параметр, защитник Windows будет автоматически предпринимать действия в отношении всех обнаруженных угроз по истечении примерно 10 минут (эта задержка не настраивается),	Не задано
Configure Microsoft SpyNet Reporting (Настроить отчеты Microsoft SpyNet)	Этот параметр отвечает за участие в сетевом сообществе Microsoft SpyNet.	Не задано

В этой таблице приведено лишь краткое описание каждого параметра. Более подробно о каждом из них см. вкладку **Explain** (объяснение) редактора объектов групповой политики.

Средство удаления вредоносных программ

Средство удаления вредоносных программ (MSRT) — это небольшая исполняемая программа, разработанная для обнаружения и устранения отдельных особо опасных видов вредоносных программ с компьютеров под управлением Windows. Каждый месяц на веб-сайтах Microsoft Update, Windows Update, WSUS и центра загрузок Майкрософт появляется новая версия этого средства. Будучи запущенным, средство MSRT в фоновом режиме сканирует компьютер и создает отчет по обнаруженным заражениям. Эта программа не устанавливается в операционной системе и не имеет

параметров групповой политики. Журнал отчета MSRT хранится в папке %SystemRoot%\Debug\mrt.log.

Средство MSRT не является антивирусным приложением корпоративного класса. Оно не обеспечивает возможностей по централизованному мониторингу, созданию отчетности и контролю. Если подобные средства необходимы, следует обратить внимание на другие продукты, например Microsoft Forefront Client Security.

Оценка рисков

В дополнение к средствам защиты ОС Windows 7 рекомендуется использовать на всех компьютерах антивирусную защиту реального времени. Но даже это не позволит полностью избежать рисков, перечисленных ниже.

- Установленному средству обеспечения антивирусной защиты реального времени не удается распознать вредоносную программу.
- Вредоносной программе удается отключить используемую защиту реального времени.

В этих ситуациях средство MSRT может использоваться как дополнительный способ обнаружения и устранения часто встречающихся вредоносных программ. Полный список таких программ, распознаваемых этим средством, см. на странице Группы вредоносных программ, удаляемых средством MSRT.

Снижение риска

Для снижения перечисленных рисков рекомендуется включить на клиентских компьютерах автоматическое обновление, чтобы средство MSRT загружалось на них по мере выхода новых версий. Это средство предназначено для обнаружения угроз, исходящих от особенно часто встречающихся или особо опасных вредоносных программ.

Анализ мер по снижению риска

При рассмотрении вопроса об использовании средства MSRT на предприятии стоит учитывать следующие соображения.

- Средство удаления вредоносных программ (MSRT) имеет размер примерно 9 МБ. Если большое число клиентских компьютеров попытаются загрузить его в одно и то же время, пропускная способность подключения к Интернету может оказаться недостаточной.
- Средство MSRT в основном предназначено для некорпоративных пользователей, у которых не установлено актуальное антивирусное ПО. Однако, ничто не мешает развернуть это средство в корпоративной среде для усиления существующих мер защиты и в качестве составной части стратегии глубокой обороны. Для подобного развертывания можно использовать любые из следующих способов:
  - службы Windows Server Update Services;
  - программные пакеты SMS;
  - задаваемый групповой политикой сценарий запуска компьютера;
  - задаваемый групповой политикой сценарий входа в систему.

О развертывании в корпоративной среде можно подробнее узнать из статьи базы знаний номер 891716 «Развертывание средства удаления вредоносных программ для Microsoft Windows в среде организации«.

- Средство MSRT не обеспечивает никакой защиты реального времени, поэтому настоятельно рекомендуется использовать антивирусную программу, способную в реальном времени обнаруживать вирусы, троянские программы и черви. Например, таким продуктом является Microsoft Forefront Client Security, обеспечивающий единообразную защиту настольных, переносных и серверных компьютеров.
- Обычно при запуске средства удаления вредоносных программ для Windows в корне диска с наибольшим свободным местом создается временная папка со случайным именем. Обычно это оказывается корневой каталог системного диска. В эту папку помещается несколько файлов, среди которых есть файл Mrtstub.exe. Чаще всего папка автоматически удаляется по завершении работы

средства или при следующем перезапуске компьютера. Но иногда удаления не происходит. В этом случае папку можно удалить вручную. Это никак не скажется на работе компьютера.

Процесс снижения рисков

Использовать средство MSRT более эффективно позволит следующий процесс.

Ход процесса снижения рисков

1. Изучить возможности средства удаления вредоносных программ. Подробнее см. Средство удаления вредоносных программ.
2. Определить степень необходимости средства MSRT в текущих условиях.
3. Выбрать наиболее подходящий метод развертывания средства MSRT в организации.
4. Выявить компьютеры, использование на которых средства MSRT является желательным.
5. Развернуть средство MSRT выбранным способом.

Брандмауэр Windows

Личный брандмауэр — это исключительно важная линия обороны от многих типов вредоносных программ. Как и брандмауэр, появившийся в ОС Windows XP Professional с пактом обновления 2 (SP2), брандмауэр ОС Windows 7 по умолчанию включен и обеспечивает защиту компьютера сразу после установки операционной системы.

Брандмауэр из состава Windows 7 использует тот же подход, что брандмауэр ОС Windows Vista, фильтруя как входящий, так и исходящий трафик, что обеспечивает защиту на случай непредвиденного поведения компонентов системы. Интерфейс консоли брандмауэра Windows в режиме повышенной безопасности также не изменился. В нем для упрощения настройки и уменьшения числа конфликтов с политиками сведены средства фильтровки входящего и исходящего трафика, а также параметры IPsec-сервера и изоляции домена.

Брандмауэр Windows в режиме повышенной безопасности поддерживает следующие профили.

- **Профиль домена.** Этот профиль вступает в силу, когда компьютер подключается к сети и проходит проверку подлинности на контроллере домена, которому принадлежит компьютер.
- **Общий профиль.** Этот профиль по умолчанию применяется для компьютера, не подключенного к домену. Его параметры должны накладывать самые сильные ограничения, поскольку компьютер подключается к публичной сети, где безопасность нельзя гарантировать в той степени, что в контролируемой ИТ-среде.
- **Частный профиль.** Этот профиль будет использоваться, только если пользователь с правами локального администратора назначит его сети, ранее использовавшей общий профиль. Делать это рекомендуется только для доверенных сетей.

В ОС Windows Vista в каждый момент времени может быть активным только один сетевой профиль. В Windows 7 же может быть несколько активных профилей, по одному на сетевой адаптер. Если разные сетевые адаптеры подключены к разным сетям, для каждого из них выбирается тип профиля, подходящий этой сети — частный, общий или доменный. Допустим, сидя в кафе, где есть беспроводная точка доступа, вы устанавливаете VPN-подключение к корпоративной сети. Тогда общий профиль будет продолжать защищать сетевой трафик, не относящийся к VPN-туннелю, а профиль домена — трафик, проходящий по нему. Это также позволяет разрешить проблему сетевых адаптеров, не подключенных к сетям — им будет назначаться общий профиль, поскольку сеть подключения неизвестна, а остальные сетевые адаптеры компьютера будут продолжать использовать тот профиль, который соответствует их сети.

Оценка рисков

Возможность работы в сети — непреложное условие успешности современного предприятия. И в то же время она — основная цель различных атак. В целях обеспечения сохранности компьютеров и данных необходимо использовать средства защиты от связанных с сетевой работой угроз. Наиболее часто встречающиеся из этих угроз перечислены ниже.

– Неизвестное лицо проводит успешную атаку на компьютер и получает административные привилегии на нем.

– Атакующий с помощью сканеров сети удаленно находит открытые порты и проводит атаку на них.

– Троянская программа устанавливает неразрешенное подключение к компьютеру атакующего и передает закрытую деловую информацию.

– Переносной компьютер подвергается сетевой атаке в то время, когда находится вне корпоративного брандмауэра.

– Компьютеры внутренней сети подвергаются сетевой атаке со стороны зараженного компьютера, у которого есть доступ ко внутренней сети.

– Потенциальный риск шантажа, связанного с успешным проникновением на внутренние компьютеры.

Снижение риска

Брандмауэр Windows 7 обеспечивает защиту клиентского компьютера сразу после установки ОС. Он блокирует большую часть незапрошенного сетевого трафика, пока иные правила не будут установлены администратором или групповой политикой.

Брандмауэр Windows также позволяет фильтровать исходящий трафик, причем по умолчанию весь такой трафик разрешен. Для обеспечения единообразия настроек соответствующие правила можно описать с помощью групповой политики.

Анализ мер по снижению риска

Планируя использование брандмауэра Windows 7, следует принимать во внимание следующие соображения.

– Необходимо убедиться в надлежащей работе бизнес-приложений. Для каждого из приложений нужно знать используемые им порты, чтобы только они оставались открытыми в брандмауэре.

– Как и в Windows Vista, брандмауэр Windows 7 поддерживает доменный, частный и общий профили, что обеспечивает точный контроль уровня защиты при работе вне средств сетевой защиты предприятия.

– Необходимо изучить возможности брандмауэра Windows по ведению журнала и рассмотреть способы включения их в корпоративные решения по отчетности и мониторингу.

– По умолчанию брандмауэр Windows блокирует удаленный контроль и удаленное управление компьютерами с ОС Windows 7. Для поддержки этих задач в брандмауэре имеется ряд правил. Те из них, что отвечают необходимым задачам, можно включить для каждого из требуемых профилей. Например, можно включить правило удаленного рабочего стола для профиля домена, чтобы в рамках сети предприятия можно было оказывать пользователям поддержку. А вот для общего и частного профиля это правило стоит оставить выключенным, поскольку так снижается контактная зона компьютеров, когда они не в сети.

Процесс снижения рисков

Параметры групповой политики Windows 7 и пользовательский интерфейс управления помогут настроить возможности брандмауэра Windows. Расширенные параметры безопасности ОС Windows 7 также действуют и для Windows Vista, но не действуют для компьютеров под управлением Windows XP или виртуальных машин в режиме Windows XP.

Если планируется вносить изменения в настройки брандмауэра по умолчанию, рекомендуется для клиентских компьютеров на основе Windows Vista или Windows 7 использовать параметры групповой политики брандмауэра Windows в режиме повышенной безопасности.

Новая оснастка брандмауэра Windows, содержащая средства управления и параметры групповой политики, расположена в редакторе объектов GPO по следующему пути:

Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security (Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Брандмауэр Windows в режиме повышенной безопасности)

Брандмауэр Windows в режиме повышенной безопасности рекомендуется включить для всех трех профилей. В дополнение к расширенным правилам, брандмауэр также поддерживает правила обеспечения безопасности подключений. В рамках этих правил перед началом коммуникации проводится проверка подлинности компьютеров, а передаваемая информация защищается. Для обмена ключами, проверки подлинности, обеспечения целостности данных и (необязательно) шифрования используется технология IPsec.

Подробнее см. раздел «IPsec« на веб-сайте Microsoft TechNet.

В файле «Windows 7 Security Baseline Settings.xls», который прилагается к настоящему руководству, объяснено рекомендуемое значение каждого параметра брандмауэра Windows в режиме повышенной безопасности, а также отмечено, где для выбора верного значения нужна дополнительная информация.

Технология AppLocker

Windows 7 включает в себя обновленную и улучшенную версию политик ограниченного использования программ — технологию AppLocker. Она проще в использовании, а ее новые возможности и расширяемость снижают затраты на управление и позволяют контролировать доступ к таким файлам, как сценарии, файлы установщика Windows, исполняемые файлы и файлы DLL. AppLocker настраивается в рамках домена с помощью групповой политики или на локальном компьютере в оснастке локальных политик безопасности.

Оценка рисков

Когда пользователь устанавливает неодобренное приложение на рабочий компьютер, он подвергает его определенным рискам. Как минимум, это изменяет контактную зону компьютера и создает вероятность запуска дополнительных служб или открытия портов брандмауэра. Но даже если ничего этого не происходит, все равно теперь на компьютере на одно приложение больше, и оно может сыграть на руку злоумышленнику, который обнаружит уязвимость, внесенную этим приложением.

Наконец, есть вероятность того, что приложение по сути своей вредоносно, и было установлено либо по ошибке, либо с умыслом провести атаку на другие компьютеры, как только этот компьютер подключится к корпоративной сети.

Снижение риска

Технология AppLocker позволяет задать набор политик контроля использования приложений, которые существенно сокращают риск подвергнуться атаке со стороны программ, установленных на компьютерах без разрешения. В этом помогают следующие возможности данной технологии.

- Определение правил, основанных на атрибутах файлов, получаемых из цифровых подписей, как то издатель, название продукта, имя файла и версия. Например, можно создать правило, проверяющее имя издателя, которое остается неизменным при выходе обновлений, а можно — правила, зависящие от конкретной версии файла.
- Назначение правил группам или отдельным пользователям.
- Возможность создавать исключения. Например, можно создать правило, разрешающее запуск любых процессов Windows, кроме редактора реестра (Regedit.exe).
- Режим «Только аудит», позволяющий развернуть политику и понять, что произойдет, когда запреты вступят в силу.
- Импорт и экспорт правил. Импортировать и экспортировать можно только политику целиком. Если политику экспортировать, будут экспортированы все правила из всех наборов, в том числе параметры введения политики в силу. Если импортировать политику, существующая политика будет полностью заменена.

– Простота создания и управления правилами AppLocker с помощью командлетов AppLocker оболочки PowerShell.

Анализ мер по снижению риска

При рассмотрении вопроса об использовании этого средства на предприятии стоит учитывать следующие соображения.

– Необходимо тщательно протестировать все политики контроля приложений до того, как развертывать их. Ошибки в проектировании или реализации могут серьезно сказаться на продуктивности труда.

– Отведите время на оценку модели использования приложений на предприятии с помощью режима «только аудит». Это позволит составить полный список необходимых программ, прежде чем вводить ограничения.

– Рассмотрите возможность поэтапного внедрения, начиная с пользователей, создающих наибольшие риски в связи с установками приложений, или компьютеров, содержащих закрытую информацию.

Процесс снижения рисков

Технология AppLocker представлена в узле «Политики управления приложениями» редактора групповой политики. Политики ограниченного использования программ в Windows 7 также поддерживаются, как и раньше.

Примечание. Технология AppLocker недоступна в потребительских редакциях Windows 7.

Использование групповой политики для снижения рисков, связанных с технологий AppLocker

Доступные в этой категории параметры находятся в следующем расположении редактора объектов GPO:

Computer Configuration\Windows Settings\Security Settings\Application Control Policies (Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики управления приложениями)

В этом руководстве нет рекомендаций блокировать те или иные приложения на клиентских компьютерах, поскольку это, со всей очевидностью, определяется конкретными условиями работы. Подробнее о планировании и развертывании политик AppLocker см. Техническую документацию технологии AppLocker для Windows 7 и Windows Server 2008 R2.

Политики ограниченного использования программ

Политики ограниченного использования программ, входящие в состав ОС Windows Vista, Windows XP, Windows Server 2003 и Windows Server 2008, доступны и поддерживаются и в Windows 7. Их по-прежнему можно использовать для обнаружения программ и управления возможностью запускать их на локальных компьютерах. Однако, поскольку технология AppLocker из состава Windows 7 значительно удобнее в использовании, рекомендуется заменить на нее эти политики. По этой причине в настоящем руководстве они не рассматриваются. Подробнее о проектировании и внедрении этих политик см. статью «Применение политик ограниченного использования программ для защиты от неразрешенного ПО« на веб-сайте TechNet.

Задание 1

1. Создайте резервную копию системы

Задание 2

1 Изменение настроек программы

2 Перейдите на вкладку «Параметры».

3 Выберите в списке слева «Действия по умолчанию».

4 Для критического уровня оповещения выберите «Удалить».

5 Выберите в списке слева «Подробно».
6 Отметьте параметр «Проверять съемные носители».

Задание 3

1 Выполнить несколько (2-3) защитных технологии Windows 7.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №11:

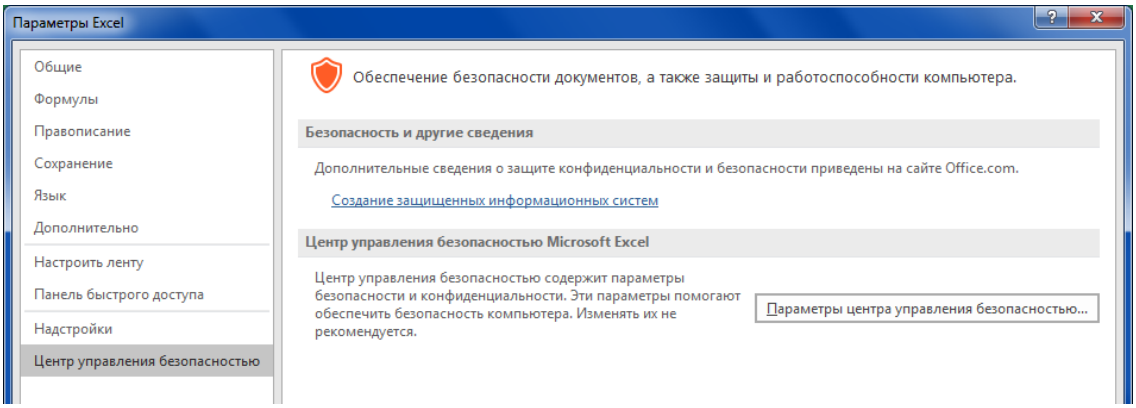
1. Дайте классификацию вирусов.
2. Дайте понятие компьютерного вируса.
3. Какие угрозы информации способны нанести вредоносные программы?
4. Для чего предназначены антивирусные программы?
5. Каковы функции брандмауэра?
6. В чем разница между антивирусными сканерами и мониторами?
7. Какие существуют признаки заражения компьютерным вирусом?
8. Что необходимо сделать в первую очередь в случае заражения компьютерным вирусом?
9. Каковы характерные особенности компьютерных вирусов как типа вредоносных программ?
10. Какие существуют типы компьютерных вирусов?
11. Как сетевые черви проникают на компьютер?
12. Какие вредоносные действия выполняют троянские программы?
13. Какие типы хакерских атак и методы защиты от них существуют?
14. К какому типу вредоносных программ относятся руткиты?
15. Приведите классификацию антивирусных программ. Приведите примеры.

Практическая работа №12
«Средства безопасности в MS Excel 2010»

Цель работы:

1 Изучение простейших методов зашиты информации и закрепление навыков работы в программной среде Microsoft Excel.

В категории Надстройки имеется одноименный список надстроек, активных и неактивных, установленных и доступных в данный момент в системе. Выбор группы надстроек, в которой вы хотели бы выбрать надстройку и сделать ее активной (или, наоборот, отключить), производится в раскрывающемся списке Управление. Щелчок на кнопке Перейти выводит на экран окно включения надстроек.



Окно центра управления безопасностью содержит группы параметров: Защита конфиденциальности, Безопасность и другие сведения и Центр управления безопасностью Microsoft Excel.

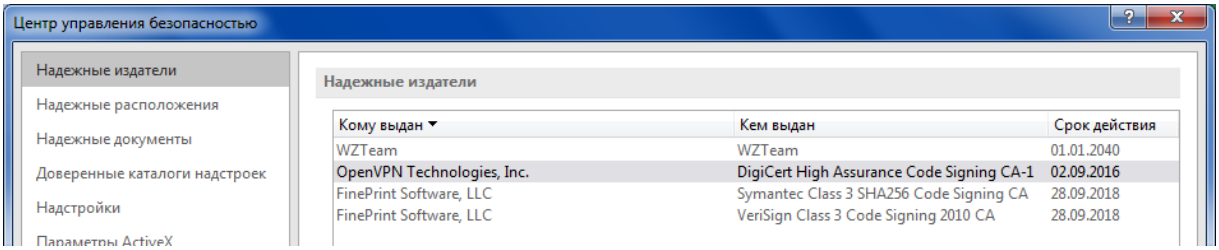
– Защита конфиденциальности — три ссылки на разные материалы, расположенные на сайте Microsoft. Перейдя по этим ссылкам, вы сможете узнать, как и зачем корпорация Microsoft при помощи своего программного обеспечения собирает личные сведения о пользователях программ, каким образом можно ограничить сбор этих сведений, а также помочь корпорации Microsoft повысить качество ее программного обеспечения.

– Безопасность и другие сведения — в этом разделе две ссылки. Первая, Центр управления безопасностью Microsoft Windows, выводит на экран окно настройки параметров безопасности операционной системы, вторая, Создание защищенных информационных систем, указывает на соответствующий информационный раздел на сайте Microsoft.

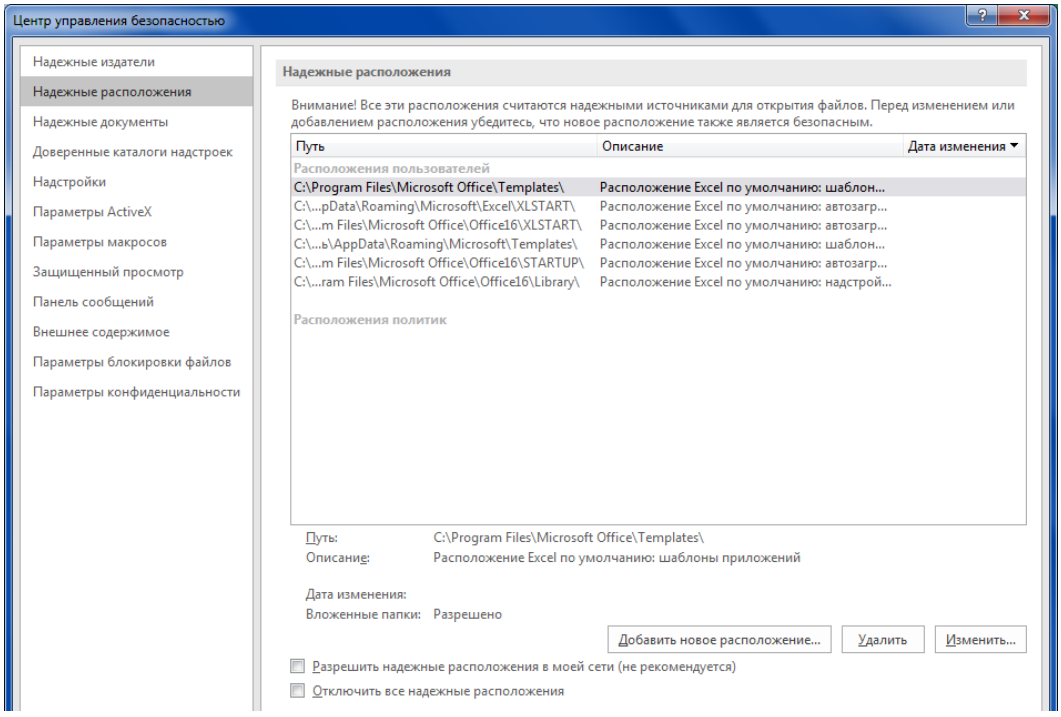
– Центр управления безопасностью Microsoft Excel — в этом разделе всего одна кнопка, Параметры центра управления безопасностью, зато эта кнопка выводит на экран окно настройки, в котором довольно много разделов.

Кратко рассмотрим назначение каждого из них:

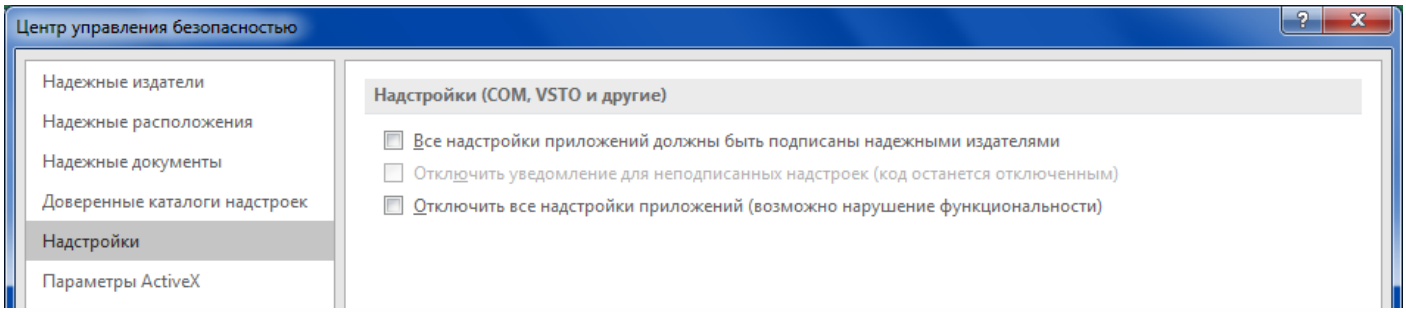
1 Надежные издатели — список сертификатов для открываемых файлов и дополнительных элементов управления, устанавливаемых в Excel. Список пополняется в момент установки элемента управления или открытия файла, а в данном окне вы можете просмотреть каждый из сертификатов или удалить те сертификаты, которые не вызывают вашего доверия.



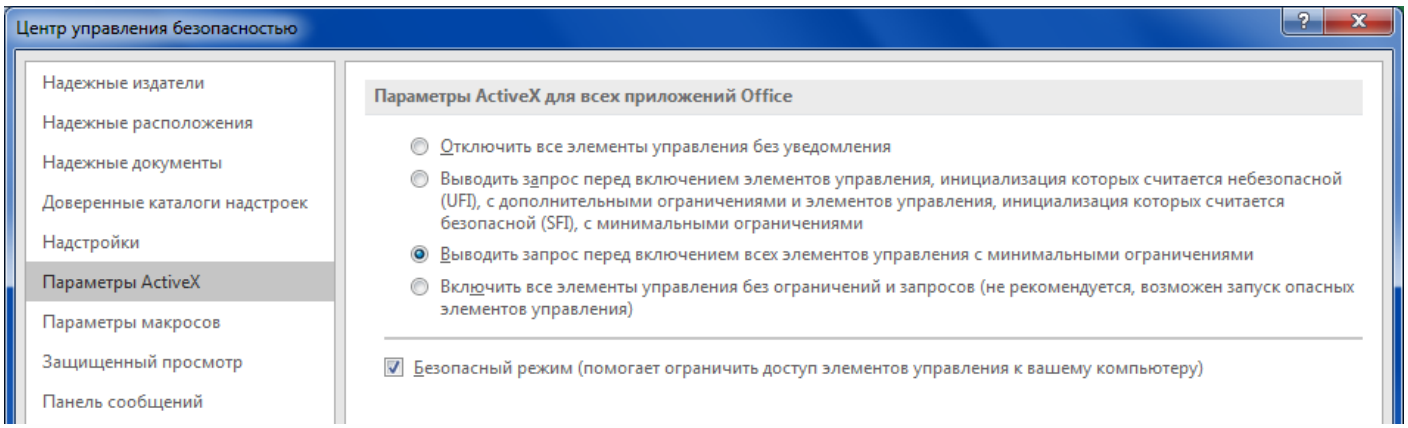
2 Надежные расположения — список мест, файлы из которых считаются надежными и не требуют дополнительных проверок и запросов при открытии.



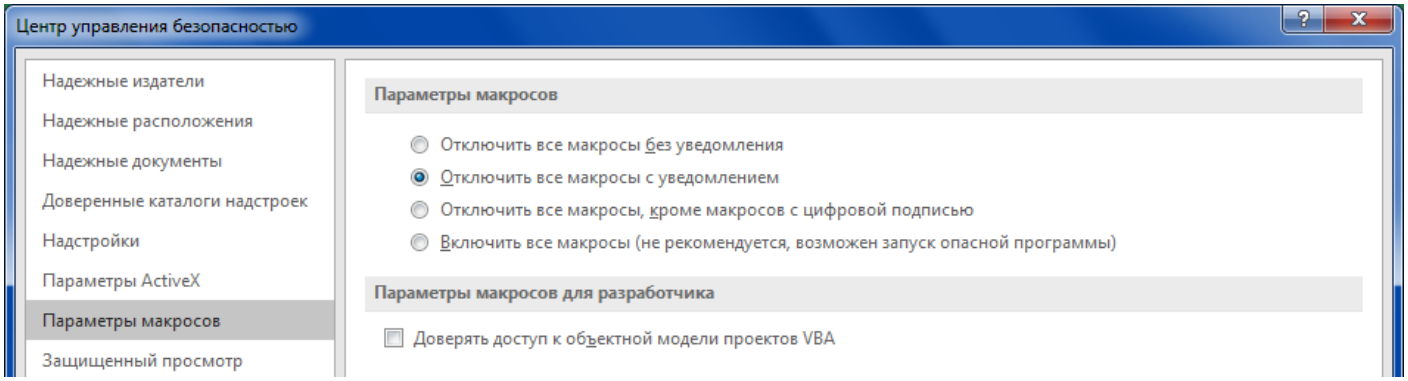
3 Надстройки — управление режимом безопасности открытия надстроек Excel. Вы можете разрешить или запретить Excel загружать неподписанные надстройки, а также надстройки, подписанные ненадежными издателями.



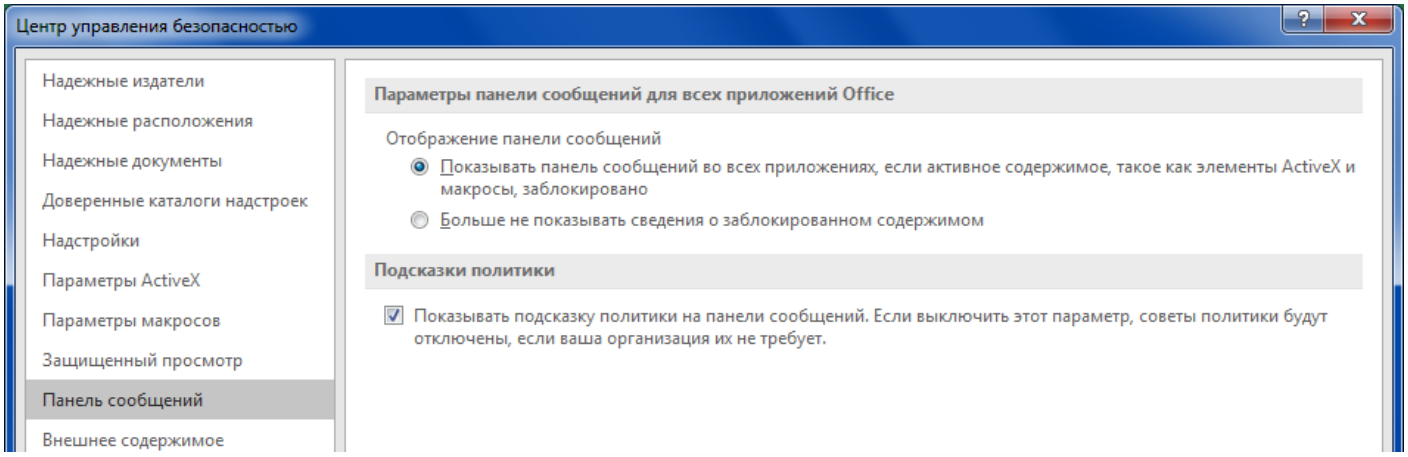
4 Параметры ActiveX — управление ограничениями, накладываемыми на запуск компонентов ActiveX. Компоненты ActiveX являются, по сути, полноценными Windows-программами и могут содержать вирусы. Поскольку диапазон действия компонента ActiveX функционально не ограничен (он может удалять файлы, изменять записи реестра и изменять параметры безопасности), внимательно отнеситесь к данному разделу.



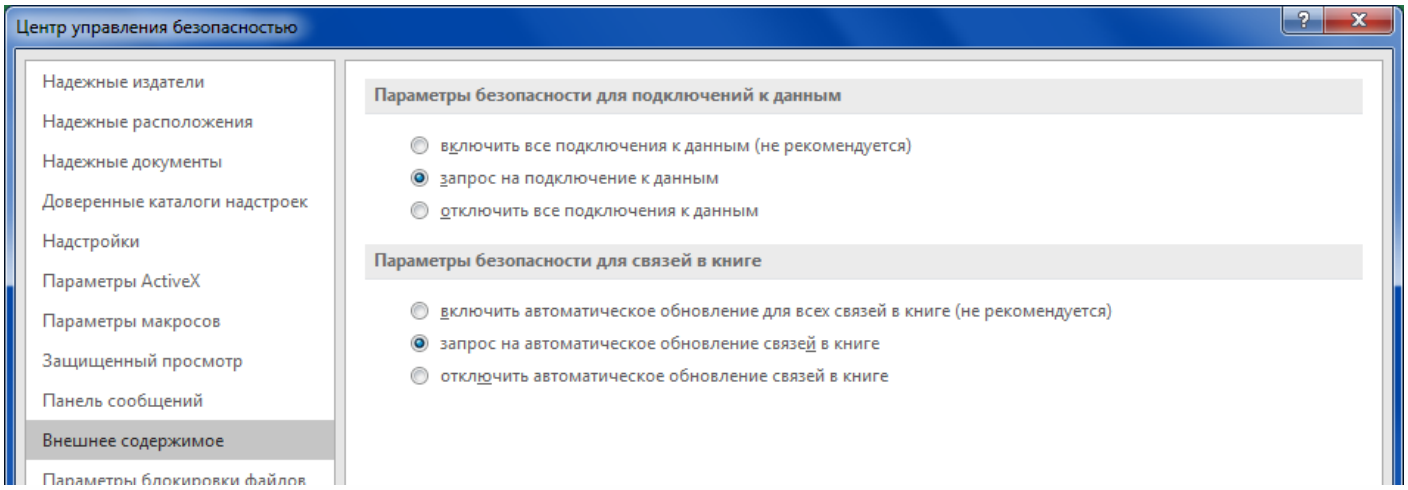
5 Параметры макросов — управление макросами. Этот раздел позволяет отключить макросы или ограничить их функциональность. Макросы являются одним из часто встречающихся путей распространения вирусов.



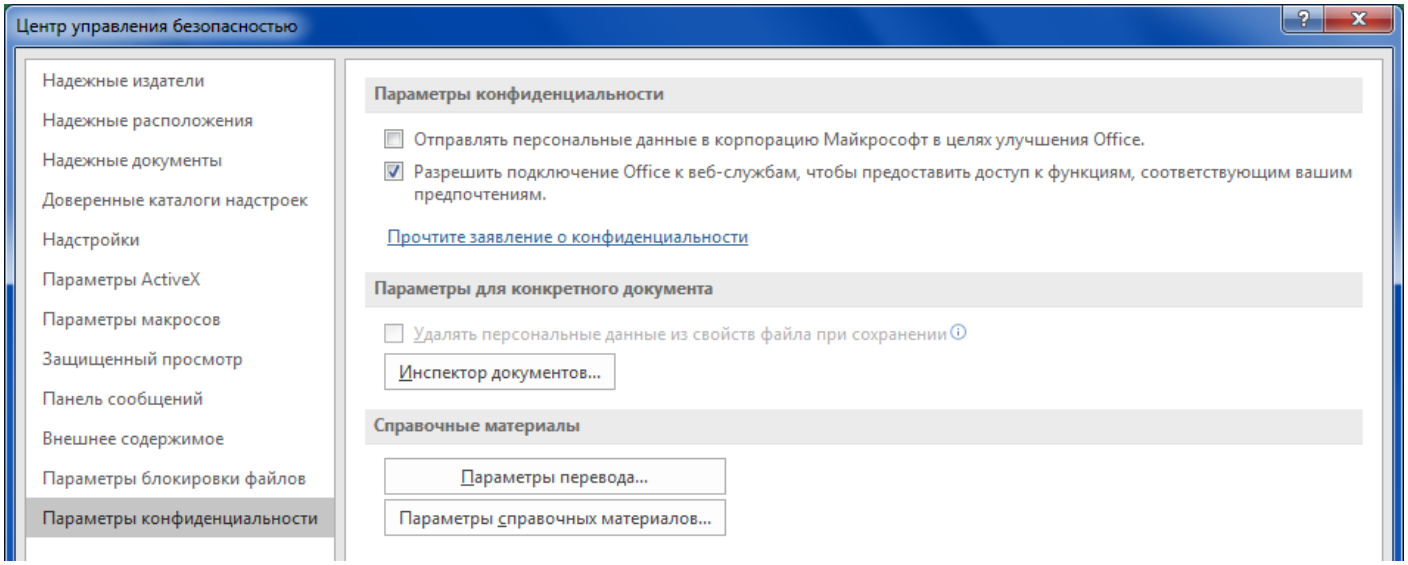
6 Панель сообщений — этот раздел позволяет показывать или нет сообщения о заблокированном содержимом документе.



7 Внешнее содержимое — настройка режима безопасности при получении внешних данных.



8 Параметры конфиденциальности — настройка объема и содержания сведений о вас и вашей операционной системе, передаваемых во внешний мир (в основном в Microsoft). Кроме того, в этом разделе можно настроить родительский контроль доступа программы к Интернету (Excel во множестве случаев, например при получении справочной информации или при необходимости перевода, обращается за такими функциями в Интернет).



Защита документов В Microsoft Excel предусмотрено несколько уровней защиты, позволяющих управлять доступом к документам Microsoft Excel:

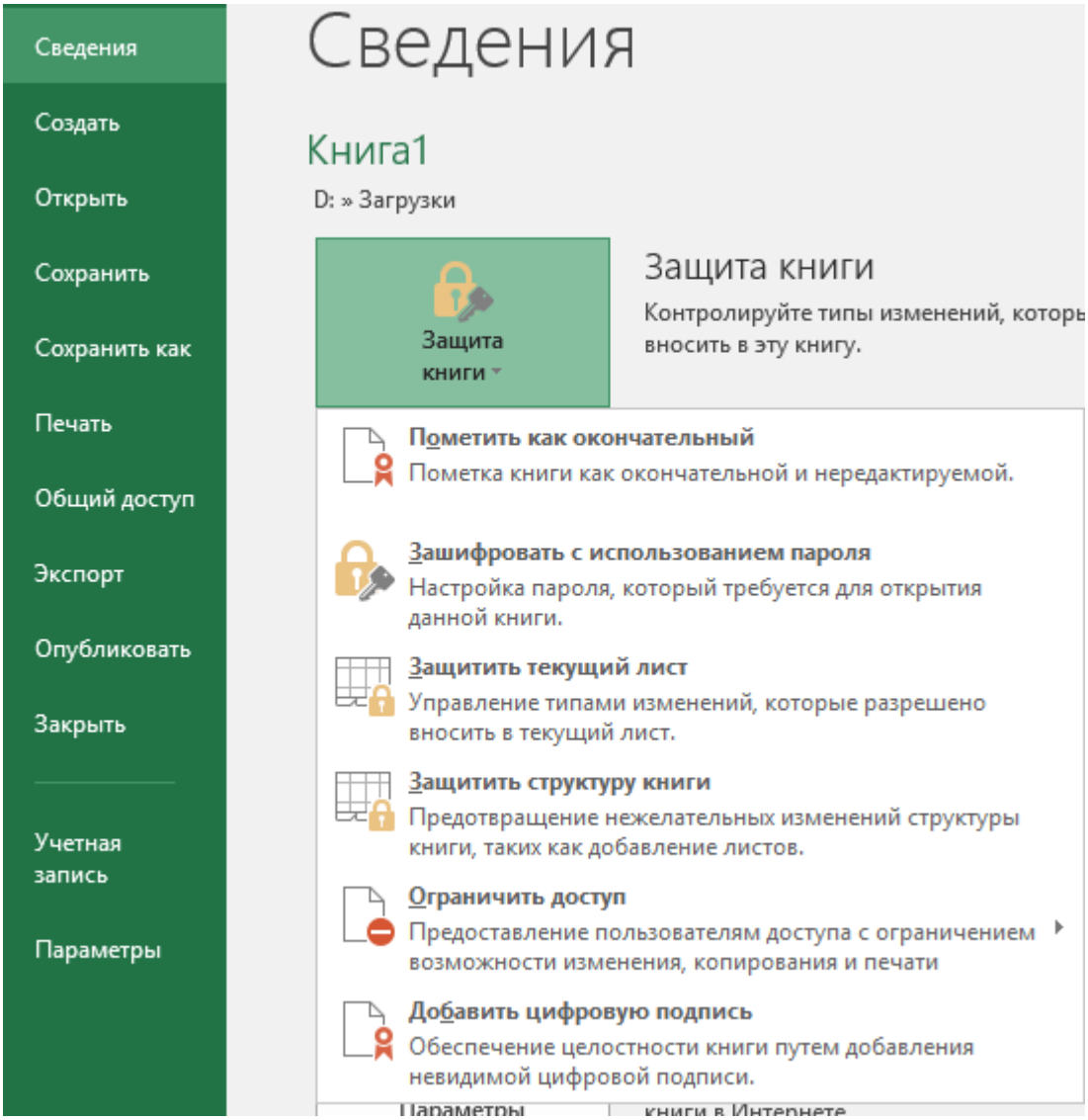
– Пометить как окончательный. Это помогает пользователю сообщить о том, что он предоставляет для совместного использования окончательную версию документа. Кроме того, это позволяет предотвратить внесение в документ случайных изменений рецензентами или читателями. • Зашифровать паролем. Это позволяет ограничить доступ к документу, предоставив его только «доверенным» пользователям.

– Защитить текущий лист. Это позволяет включить защиту паролем, чтобы разрешить или запретить пользователям выделять, форматировать, вставлять, удалять, сортировать и редактировать области таблицы.

– Защитить структуру книги. Это позволяет заблокировать структуру книги, чтобы пользователи не могли добавлять или удалять листы, или отображать скрытые листы. Это также позволяет запретить пользователям изменять размер или положение окон листа. Защита структуры и окна книги распространяется на всю книгу.

– Ограничить разрешения для пользователей. Для ограничения разрешений позволяет использовать идентификатор Windows Live ID или учетную запись Microsoft Windows.

– Добавление цифровой подписи. Цифровые подписи используются для проверки подлинности цифровых данных, например документов, сообщений электронной почты и макросов, с помощью криптографии. Они создаются путем ввода или на основе изображения и позволяют обеспечить подлинность, целостность и неотрекаемость. Все уровни защиты являются не взаимоисключающими, а скорее взаимодополняющими друг друга.



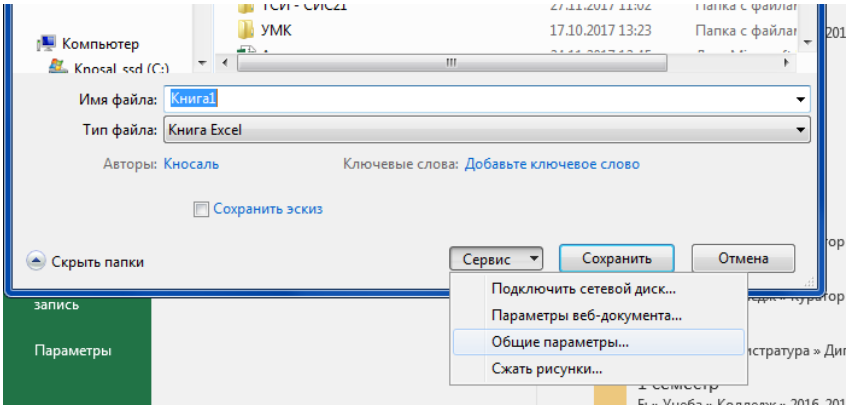
Рассмотрим эти возможности.

Назначение первых трех ограничений такое же, что и в MS Word. При установке пароля на открытие книга шифруется, однако стойкость алгоритма шифрования к взлому в MS Excel ниже по сравнению с алгоритмом в MS Word.

Установка этих ограничений в MS Excel производится не в диалоговом окне «Параметры», как в MS Word, а при сохранении файла в диалоговом окне «Сохранение документа» Общие параметры (в MS Excel — Параметры безопасности).

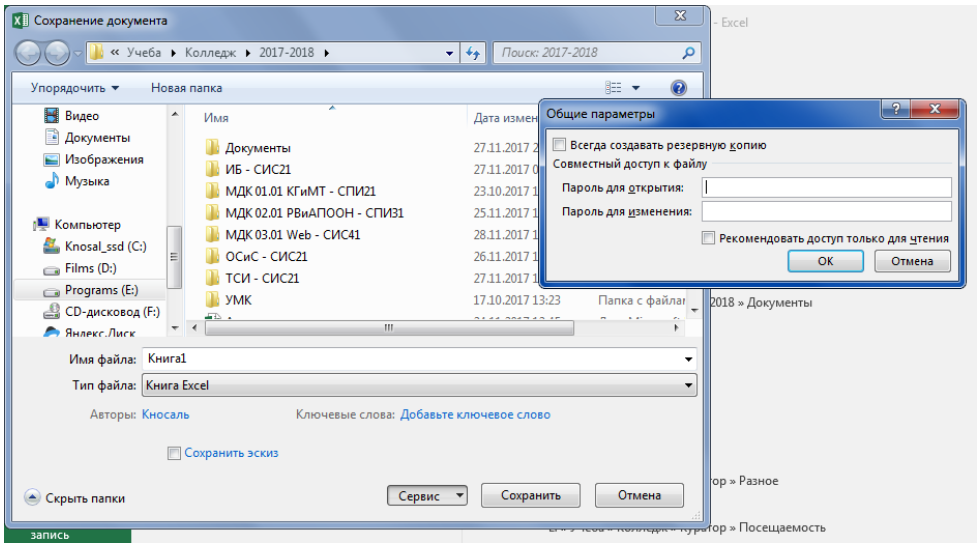
1 Рассмотрим, как установить защиту на открытие документа.

Для этого необходимо открыть защищаемый документ при Сохранении во вкладке Сервис указать на Общие параметры.



При вводе символы не отображаются — вместо них на экране появляются звездочки. Делается это для того, чтобы любопытный сосед не смог бы узнать пароль, подглядев его у вас через плечо. Поэтому прежде чем вводить пароль, необходимо переключиться на нужную раскладку клавиатуры и убедиться, что Caps Lock не включен. При вводе пароля строчные и прописные буквы различаются.

Нужно помнить, что вероятность взлома пароля в значительной мере зависит от самого пароля.



После нажатия кнопки OK появится окно «Подтверждение пароля», в котором необходимо повторно ввести тот же пароль. Это нужно для того, чтобы пользователь не смог ненароком «запереть» документ, введя случайную последовательность символов. После успешного подтверждения пароля необходимо сохранить документ, который при этом будет зашифрован.

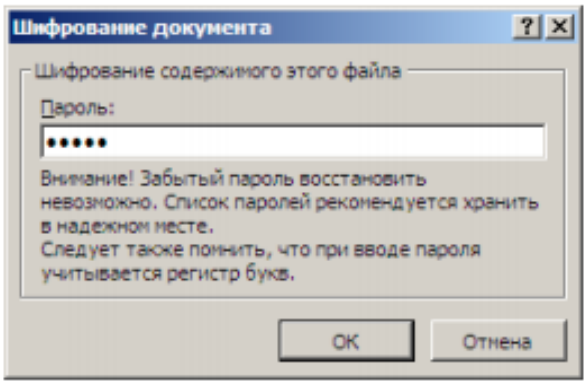
При открытии защищенного таким образом документа появляется диалоговое окно, в котором необходимо ввести пароль. Если введенные символы соответствуют паролю, то документ открывается, в противном случае выдается сообщение, что пароль указан неверно.

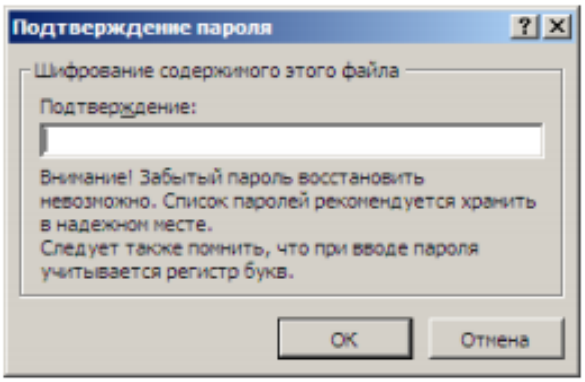
Установка пароля в представлении Backstage

Чтобы установить пароль на открытие файла выполните следующие действия:

1. В открытом документе выберите вкладку Файл. Откроется представление Backstage.
2. В представлении Backstage выберите команду Сведения.
3. В разделе Разрешения нажмите кнопку Защитить книгу (Рисунок 12.1).
4. Выберите команду Зашифровать паролем.
5. В окне Шифрование документа (Рисунок 12.2) введите пароль. Нажмите кнопку ОК. ! При вводе пароля следует строго следить за регистром и раскладкой клавиатуры. Нажатие на одни и те же клавиши клавиатуры в русской и английской раскладке вводит различные символы. Убедитесь в том, что при первом вводе пароля не нажата клавиша [CAPS LOCK].
6. В окне Подтверждение пароля (Рисунок 12.2) введите пароль еще раз и нажмите кнопку ОК.

Рисунок 12.2. Ввод и подтверждение пароля !





Пароль начнет действовать после сохранения и закрытия файла. ! В случае утраты пароля приложению Excel не удастся восстановить данные. При открытии защищенного файла или снятии защиты выводится окно для ввода пароля, в котором необходимо ввести пароль.

В случае неправильного ввода пароля выводится соответствующее сообщение. Следует нажать кнопку ОК и попытаться ввести правильный пароль.

2 Снятие пароля, установленного через Защиту документа

Снять пароль можно только после открытия файла.

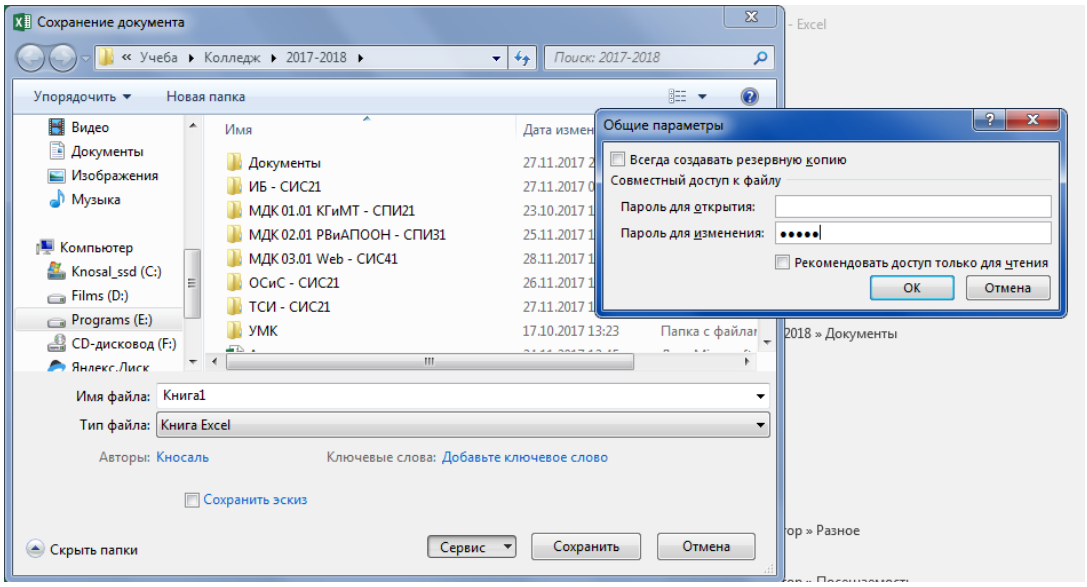
1. Перейдите на вкладку Файл.
2. В представлении Backstage выберите команду Сведения.
3. В разделе Разрешения нажмите кнопку Защитить книгу.
4. Выберите команду Зашифровать паролем.
5. В окне Шифрование документа очистите поле пароля. 6. Нажмите кнопку ОК. ! Отказ от пароля начнет действовать после сохранения и закрытия файла.

3 Парольная защита на запись файла

Цель данной защиты — не сокрытие содержимого документа, а предохранение его от нежелательных изменений. После ее установки при открытии документа появляется диалоговое окно, предлагающее ввести пароль. Если пользователь не знает пароля или по каким-то причинам не хочет

его вводить, он может нажать кнопку «Только чтение», и документ будет открыт. Однако при попытке сохранить сделанные в этом документе изменения появится диалоговое окно «Сохранение документа», как при первом сохранении, где пользователь должен будет указать либо новое имя файла, либо новый каталог, либо и то и другое. Таким образом, данная защита не дает возможности не знающим пароля пользователям испортить документ. Однако, например, брать его за основу и сохранять под другим именем не возбраняется.

Устанавливается данная защита аналогично предыдущей, только пароль следует вводить в поле «Пароль разрешения записи».



Вы можете ввести пароль и в оба поля. Таким образом одним пользователям можно вообще закрыть доступ к файлу, а другим — только запретить его перезаписывать.

К сожалению, алгоритм данной защиты является очень нестойким к взлому, поэтому доверять ему единственный экземпляр важного документа не стоит.

Рекомендация открытия файла в режиме «Только для чтения»

Данный вид защиты документа носит чисто рекомендательный характер. Пользователь, открывающий такой документ, может согласиться с рекомендацией и открыть документ в режиме «Только для чтения» без возможности его перезаписи, а может не согласиться.

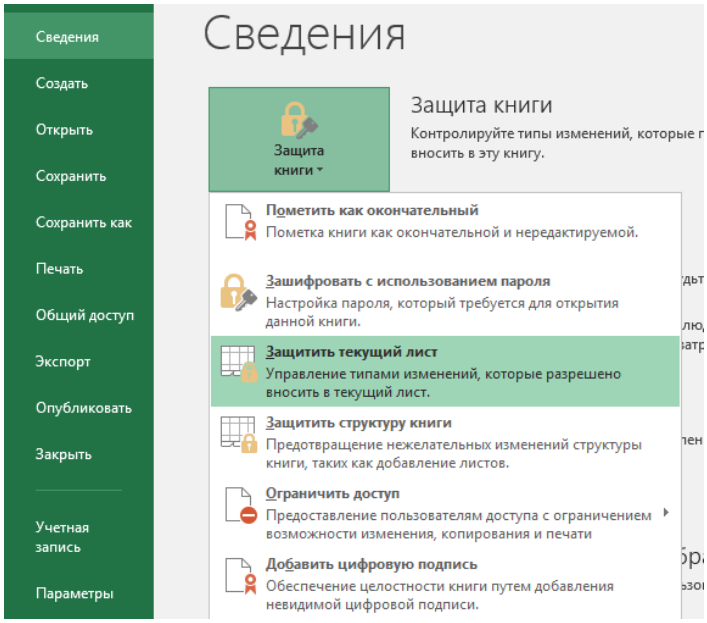
4 Парольная защита листа

MS Excel позволяет защищать отдельные листы рабочей книги от изменений. При этом защита может распространяться на содержимое ячеек, на графические объекты и диаграммы, а также на сценарии. MS Excel на защищенном листе также позволяет разрешать или запрещать форматирование, вставку и удаление строк и столбцов и пр. По вашему желанию запрет может носить рекомендательный характер, поскольку ввод пароля для защиты листа не является обязательным.

Под защитой содержимого понимается запрет любых изменений защищаемых ячеек (изменение значений, перемещение и удаление), а также запрет показа формул, содержащихся в ячейках, в строке формул.

Под защитой графических объектов и диаграмм понимается запрет их изменения, перемещения и удаления. Перестроение диаграмм при изменении исходных данных не блокируется.

Для того чтобы установить защиту активного листа, необходимо



В появившемся диалоговом окне «Защитить лист» необходимо выбрать защищаемые элементы листа, а также при необходимости ввести пароль.

Защита листа действует только на те ячейки и объекты, в свойствах которых включена их защита. Для ее включения или отключения необходимо открыть диалоговое окно настройки формата соответствующего элемента, выполнив команду меню Формат => Ячейки или Формат => Автофигура или Формат => Выделенная область диаграммы или т.п. и на вкладке «Защита» (или «Свойства» — для диаграммы) снять или установить флажок, отвечающий за защиту данного элемента.

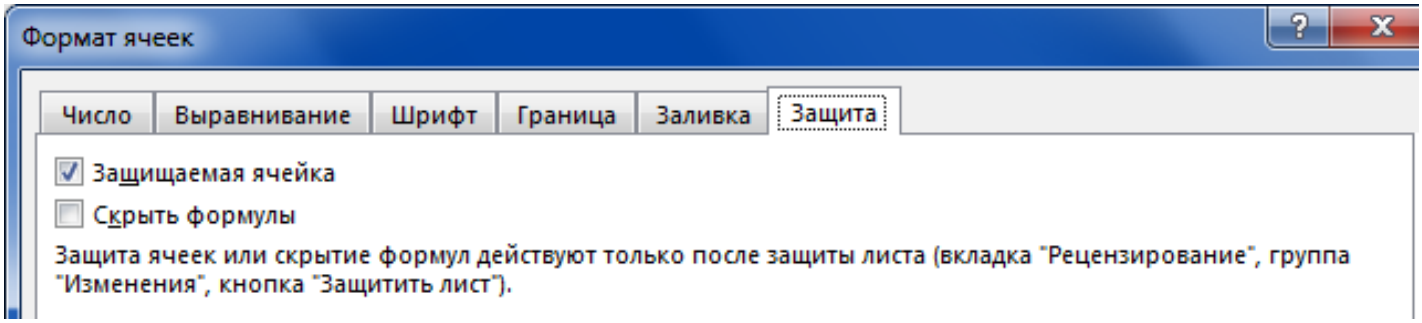
1. Выберите лист, который нужно защитить.

2. Чтобы разблокировать все ячейки или диапазоны, которые должны быть доступны другим пользователям для изменения, выполните указанные ниже действия:

a) Выберите ячейки или диапазоны, которые нужно разблокировать.

b) На вкладке Главная в группе Ячейки нажмите кнопку Формат, а затем выберите команду Формат ячеек.

c) На вкладке Защита снимите флажок Защищаемая ячейка, а затем нажмите кнопку ОК



При попытке изменить защищенные ячейки в том случае, если защита листа включена, появляется сообщение о том, что данная ячейка защищена от изменений. Защиту листа удобно, например, применять, когда лист содержит большое количество формул, которые могут быть потеряны в случае ошибочного ввода пользователем в эти ячейки значений. В этом случае на ячейки, содержащие формулы, устанавливается защита, а ячейки, содержащие изменяемые пользователем данные, остаются доступными.

Снятие защиты с листа производится командой меню Сервис => Защита => Снять защиту с листа.

3. Чтобы скрыть все формулы, которые не должны отображаться, выполните указанные ниже действия:

a) Выделите ячейки, содержащие формулы, которые необходимо скрыть.

b) На вкладке Главная в группе Ячейки нажмите кнопку Формат, а затем выберите команду Формат ячеек. ! Можно также нажать клавиши **[Ctrl]+[Shift]+[F]** или **[Ctrl]+[1].**

c) На вкладке Защита установите флажок Скрыть формулы, а затем нажмите кнопку ОК.

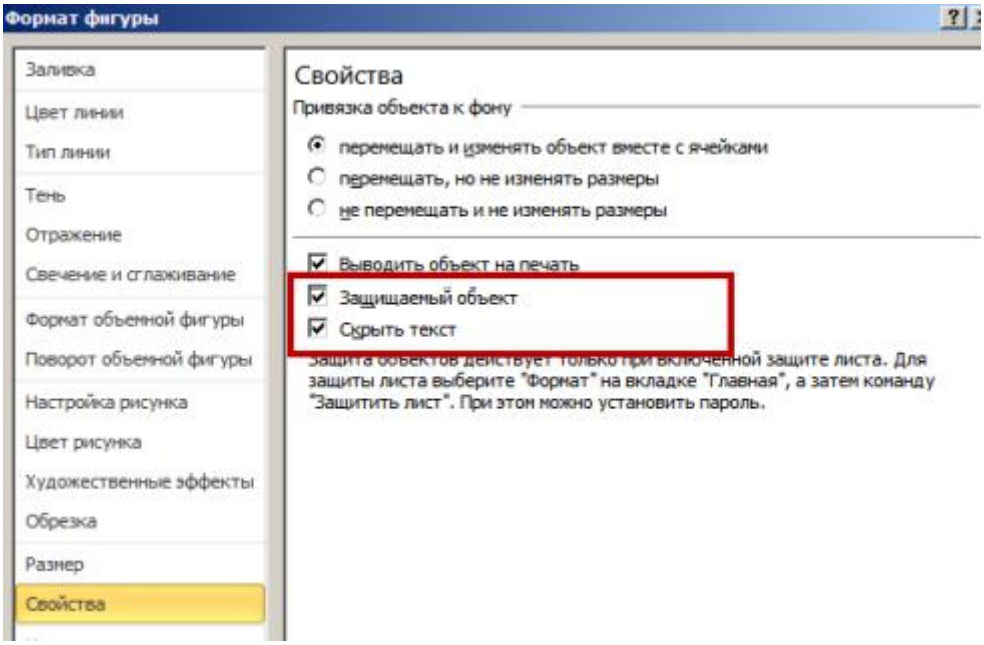
4. Чтобы разблокировать все графические объекты (например, рисунки, коллекции картинок, фигуры или графические объекты Smart Art), которые должны быть доступны пользователям для изменения, выполните указанные ниже действия:

d) Удерживая нажатой клавишу [Ctrl], выделите по очереди все графические объекты, которые требуется разблокировать.

e) На ленте появится вкладка Работа с рисунками или Средства рисования, содержащая вкладку Формат.

f) На вкладке Формат в группе Размер нажмите кнопку вызова диалогового окна рядом с кнопкой Размер.

g) На вкладке Свойства снимите флажок Защищаемый объект, а также флажок Скрыть текст (если он есть)

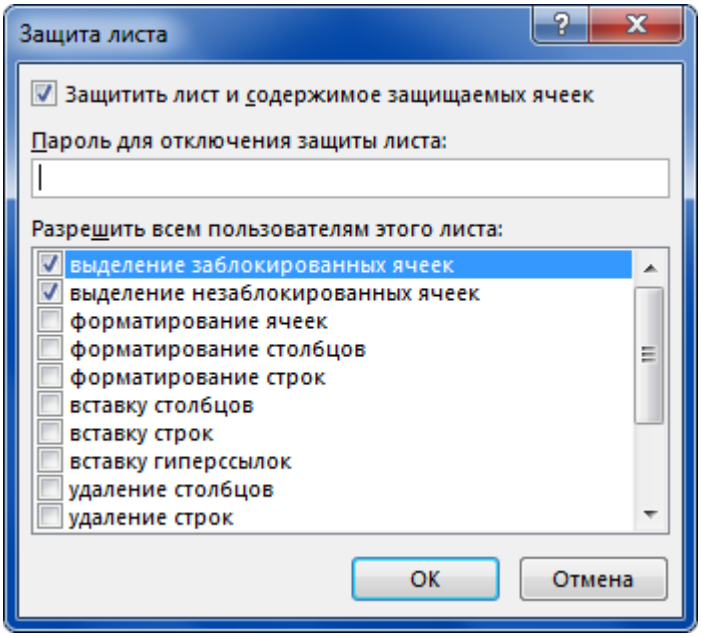


5. Выполните одно из следующих действий:

¬ На вкладке Файл в представлении Backstage выберите команду Сведения, нажмите кнопку Защитить книгу и выберите команду Защитить текущий лист.

¬ На вкладке Рецензирование в группе Изменения нажмите кнопку Защитить лист.

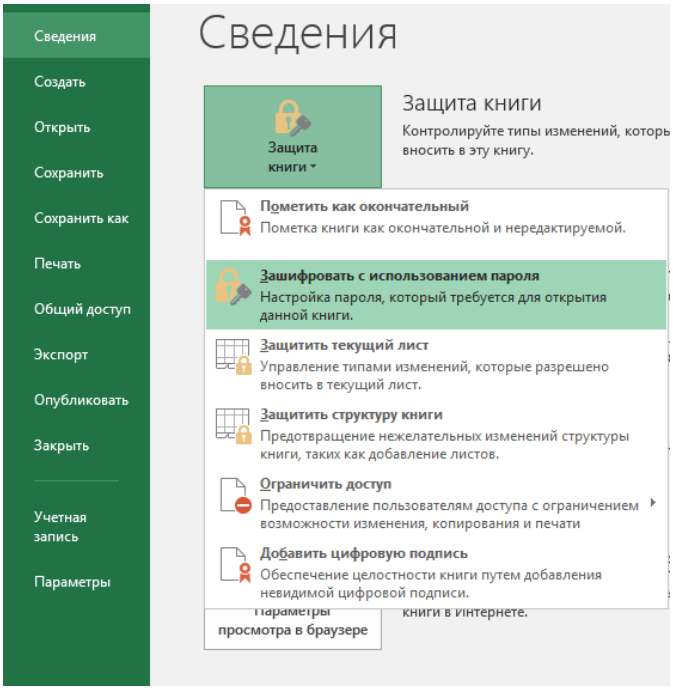
6. В окне диалога Защита листа в списке Разрешить всем пользователям этого листа отметьте флажками элементы, изменение которых должно быть доступно пользователям.



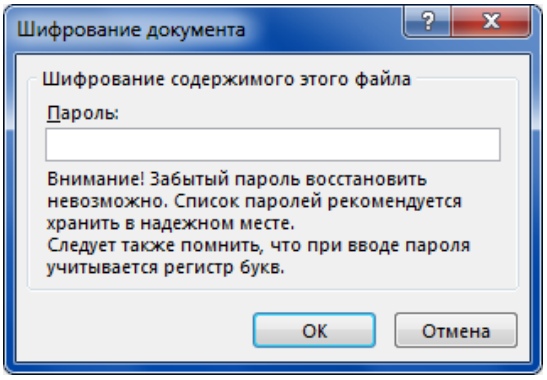
7. В поле Пароль для отключения защиты листа введите пароль для защиты листа, нажмите кнопку ОК, а затем еще раз введите пароль для его подтверждения. ! Пароль задавать необязательно. Однако если не задать пароль, любой пользователь сможет снять защиту с листа и изменить защищенные элементы. ! Убедитесь, что выбран пароль, который легко запомнить, поскольку если пароль будет утерян, получить доступ к защищенным элементам листа будет невозможно.

5 Парольная защита книги

MS Excel позволяет защищать рабочую книгу от изменений ее структуры (добавление, удаление, переименование, перемещение, копирование листов), а также от изменений окна книги внутри окна MS Excel (перемещение, изменение размеров, сворачивание/разворачивание и т.п.). По вашему желанию запрет может носить рекомендательный характер, так как ввод пароля для защиты книги не является обязательным.



Чтобы установить защиту книги, необходимо выполнить команду меню Сервис => Защита => Защитить книгу. В появившемся диалоговом окне «Защита книги» следует выбрать защищаемые элементы книги (структуру или окна), а также при необходимости ввести пароль.



6 Парольная защита общей книги

MS Excel позволяет защищать общую книгу от отключения режима записи исправлений. Под общей книгой в MS Excel понимается та, что одновременно может редактироваться несколькими пользователями по сети. При этом для того, чтобы было видно, какой пользователь внес какие изменения, все изменения помечаются разными цветами как исправления. В случае конфликта, то есть если в одну и ту же ячейку данные были введены разными пользователями, появляется диалоговое окно с вопросом о том, чьи данные оставлять.

Если книга уже является общей и ее нужно защитить паролем, необходимо закрыть совместный доступ к книге.

1. Попросите других пользователей сохранить и закрыть общую книгу, чтобы предотвратить потерю несохраненных данных.

2. Сохраните копию данных журнала изменений, которые будут утеряны при закрытии общего доступа к книге.

3. В общей книге на вкладке Рецензирование в группе Изменения нажмите кнопку Доступ к книге.

4. Убедитесь, что на вкладке Правка вы — единственный пользователь в списке Файл открыт следующими пользователями.

5. Снимите флажок Разрешить изменять файл нескольким пользователям одновременно (это также позволит объединять книги). ! Если этот флажок недоступен, необходимо сначала снять защиту с книги, а затем снять флажок.

6. Если появится сообщение о влиянии на других пользователей, нажмите кнопку Да.

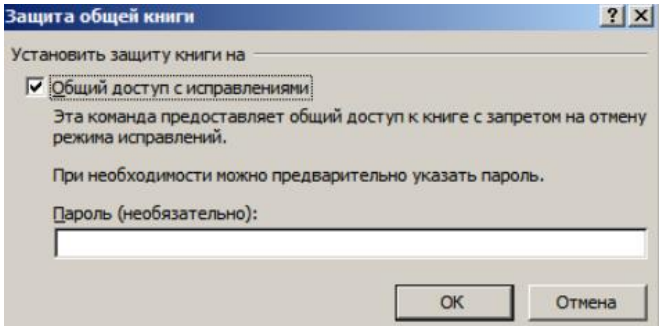
7. При необходимости предоставьте определенным пользователям доступ к диапазонам, защитите листы и элементы книги и задайте пароли для просмотра и изменения данных.

8. На вкладке Рецензирование в группе Изменения нажмите кнопку Защитить книгу и дать общий доступ.

9. В окне диалога Защита общей книги установите флажок Общий доступ с исправлениями.

10. Чтобы обязать других пользователей вводить пароль для отключения журнала изменений или удаления книги из общего пользования, введите пароль в поле Пароль (не обязателен), нажмите кнопку ОК, а затем введите пароль еще раз для его подтверждения.

11. Если будет предложено, сохраните книгу.



7 Добавление цифровой подписи к документу

Цифровая подпись — это электронная зашифрованная печать, удостоверяющая подлинность цифровых данных, таких как сообщения электронной почты, макросы или электронные документы. Подпись подтверждает, что сведения предоставлены подписавшим их создателем и не были изменены. Цифровые подписи помогают удостоверить следующее:

– Подлинность. Цифровая подпись подтверждает личность подписавшего.

– Целостность. Цифровая подпись гарантирует, что содержимое документа не было изменено или подделано с момента подписания.

– Неотрекаемость. Цифровая подпись подтверждает происхождение подписанного содержимого. Подписавший не сможет отрицать свою связь с подписанным содержимым.

– Нотариальное заверение. Подписи в файлах MS Excel 2010 с отметкой защищенного сервера времени при определенных обстоятельствах равносильны нотариальному заверению.

Для обеспечения этих гарантий создатель содержимого должен заверить его цифровой подписью, соответствующей указанным ниже требованиям.

– Цифровая подпись должна быть действительной.

– Сертификат, связанный с цифровой подписью, является действующим (не просрочен).

– Лицо или организация, поставившая цифровую подпись (издатель), является доверенной.

– Сертификат, связанный с цифровой подписью, выдан издателю компетентным центром сертификации.

Цифровыми подписями можно воспользоваться для подписи документов Office двумя различными способами:

– Добавить видимые строки подписи в документ для ввода одной или более цифровых подписей. Изображение этой подписи может быть напечатано вместе с документом;

– Добавить невидимую цифровую подпись в документ, чтобы гарантировать подлинность, целостность и происхождение документа. Невидимая цифровая подпись не видна в содержимом документа.

Добавление строк подписи в документ

Строка подписи напоминает обычное место для подписи в печатном документе, но работает иначе. Добавляя строку подписи в документ, автор может предоставить сведения о предполагаемом лице, которое будет подписывать документ, а также поместить инструкции для этого лица. При получении электронной копии файла пользователь, который будет ее подписывать, видит строку подписи и уведомление о том, что необходима его подпись. Он может:

– ввести подпись;

– выбрать изображение цифровой подписи;

– ввести подпись с помощью функции рукописного ввода на планшетном ПК.

! Одновременно с видимой подписью в документ добавляется и цифровая подпись для подтверждения личности подписавшего.

! Документ, подписанный цифровой подписью, становится доступен только для чтения.

7.1 Для создания строки подписи в документе

1. Поместите указатель мыши в то место документа, где необходимо создать строку подписи.

2. На вкладке Вставка в группе Текст раскройте список Строка подписи и выберите пункт Строка подписи Microsoft Office.

3. В информационном окне нажмите кнопку ОК. Для удобства работы можно установить флажок Больше не показывать это сообщение.

4. В диалоговом окне Настройка подписи (Рисунок 12.17) введите сведения, которые будут отображены под строкой подписи: полное имя подписывающего лица, его должность и адрес эл. почты, а также необходимые инструкции для подписывающего лица.

5. Чтобы разрешить подписывающему указать цель добавления подписи установите флажок Разрешить подписывающему добавлять примечания в окне подписи.

6. Для отображения даты подписи вместе с подписью установите флажок Показывать дату подписи в строке подписи.

7. Нажмите кнопку ОК.

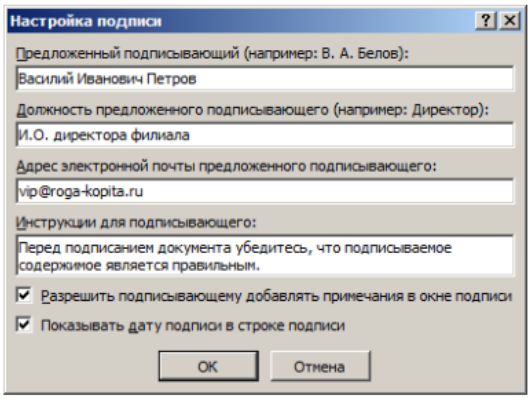


Рисунок 12.17. Настройка подписи

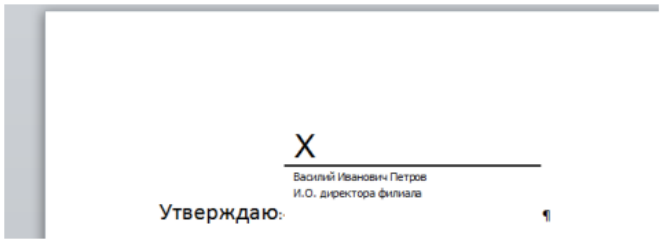


Рисунок 12.18. Строка подписи в документе

В документ будет добавлен графический объект, представляющий строку подписи (Рисунок 12.18).

7.2 Добавление подписи в строку подписи

При введении подписи в строку подписи в документе добавляется как видимая подпись, так и цифровая.

1. Дважды щелкните мышью в документе по строке подписи, в которую требуется ввести подпись.

2. В окне диалога Получение цифрового удостоверения (Рисунок 12.19) выберите переключатель Создать свое цифровое удостоверение и нажмите кнопку ОК.

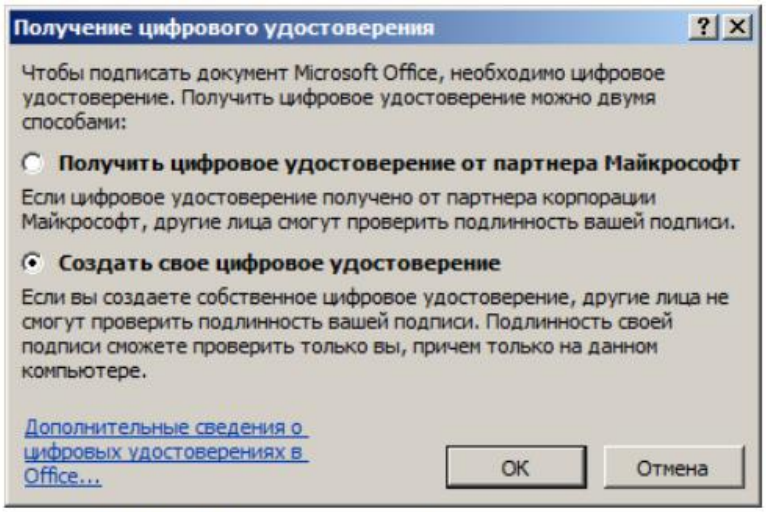


Рисунок 12.19. Получение цифрового удостоверения.

3. В окне диалога Подписание (Рисунок 12.20) нажмите ссылку Выбрать рисунок и откройте файл, содержащий изображение подписи.

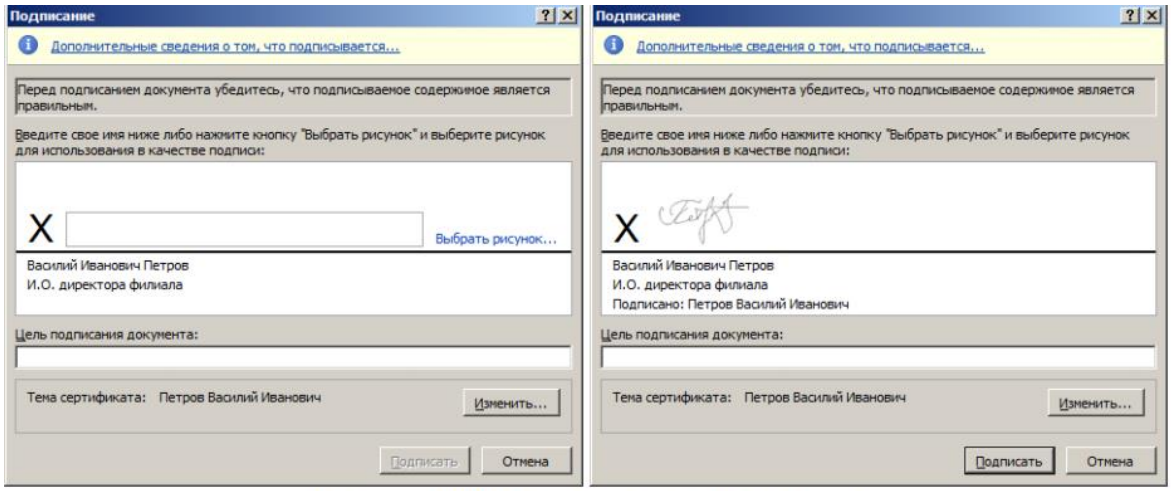


Рисунок 12.20. Окно диалога Подписание

4. В поле Цель подписания документа можно ввести информацию о назначении данной подписи.

5. При необходимости выбора другого цифрового сертификата для подписи нажмите кнопку Изменить и в окне Выбор сертификата выберите необходимый сертификат.

6. Нажмите кнопку Подписать.

7. В открывшемся информационном окне установите флажок Больше не показывать это сообщение и нажмите кнопку ОК

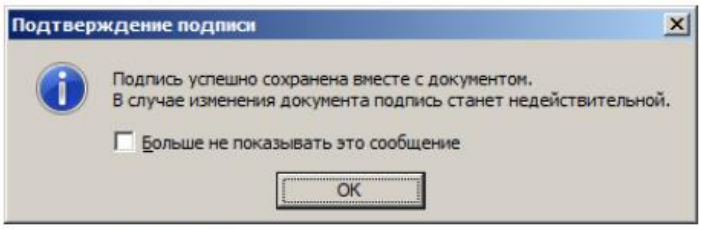


Рисунок 12.21. Отчет о подписании документа

В строке состояния отобразится кнопка Подписи, при нажатии на которую открывается область

задач Подписи, содержащая информацию об имеющихся в документе подписях (Рисунок 12.21). Созданная подпись будет находиться в разделе Действительные подписи. Незаполненная подпись - в разделе Требуемые подписи. ! Если книга содержит несколько строк подписей для нескольких лиц, книгу следует переслать этим лицам для подписания.

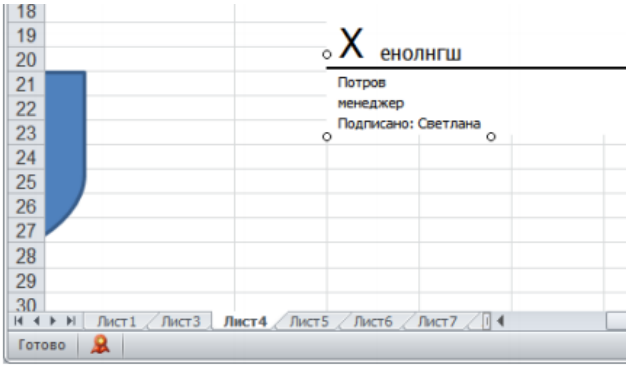


Рисунок 12.22. Пример документа

С книгой, содержащей цифровые подписи, можно работать в режиме «Только для чтения» - после того как в книге появилась цифровая подпись, она автоматически помечается как «Окончательная».

! При снятии отметки «Окончательная» с подписанной книги подписи удаляются!

! Подписи становятся недействительными и при попытке сохранить книгу под другим именем.

Задание

1 Выполнить защиту MS Excel документа, всеми рассматриваемыми способами.;

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №12:

1. Какие средства защиты использует MS Excel?
2. Что такое ЭЦП?
3. Как установить пароль на документ?
4. Как разрешить «только чтение»?
5. Как установить цифровую подпись в документе?

Практическая работа №13
«Способы атаки на пароль. Обеспечение безопасности пароля»

Цель работы:

1 реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют очень важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае,

информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя является, как правило, передним краем обороны СЗИ. В связи с этим, модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель злоумышленника в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя являются наиболее простыми методами аутентификации и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю

1. Минимальная длина пароля должна быть не менее 6 символов.
2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.).
3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации.

1. Администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, он должен быть сменен.
2. В подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля (как правило, не более 3).
3. В подсистеме парольной аутентификации должна быть установлена временная задержка при вводе неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы - автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации, единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то A=26).

L – длина пароля.

$S = A^L$ - число всевозможных паролей длины L, которые можно составить из символов алфавита A.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течении срока его действия V определяется по следующей формуле.

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$

Задание 1

1. Наберите предложенный текст.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.¶

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.¶

Использование электронной подписи позволяет осуществить:¶

– → контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему;¶

– → защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев;¶

– → невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом;¶

– → доказательное подтверждение авторства документа: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.¶

2. При помощи команд ***Сервис/Параметры/Безопасность*** отработайте различные варианты постановки пароля.
3. Запомните свой пароль (его указывать в отчете).
4. Рассчитать оценку стойкости парольной защиты по приведенной формуле с использованием таблицы, приведенной ниже, согласно своего варианта.

Вариант	***V***	***T***
1	15 паролей/мин	2 недели
2	3 паролей/мин	10 дней
3	10 паролей/мин	5 дней
4	11 паролей/мин	6 дней
5	100 паролей/день	12 дней
6	10 паролей/день	1 месяц
7	20 паролей/мин	3 недели
8	15 паролей/мин	20 дней
9	3 паролей/мин	15 дней
10	10 паролей/мин	1 неделя
11	11 паролей/мин	2 недели
12	100 паролей/день	10 дней
13	10 паролей/день	5 дней
14	20 паролей/мин	6 дней
15	15 паролей/мин	12 дней
16	3 паролей/мин	1 месяц
17	10 паролей/мин	3 недели
18	11 паролей/мин	20 дней
19	100 паролей/день	15 дней
20	10 паролей/день	1 неделя
21	20 паролей/мин	2 недели

22	15 паролей/мин	10 дней
23	3 паролей/мин	5 дней
24	10 паролей/мин	6 дней
25	11 паролей/мин	12 дней
26	100 паролей/день	1 месяц
27	10 паролей/день	3 недели
28	20 паролей/мин	20 дней
29	15 паролей/мин	15 дней
30	3 паролей/мин	1 неделя

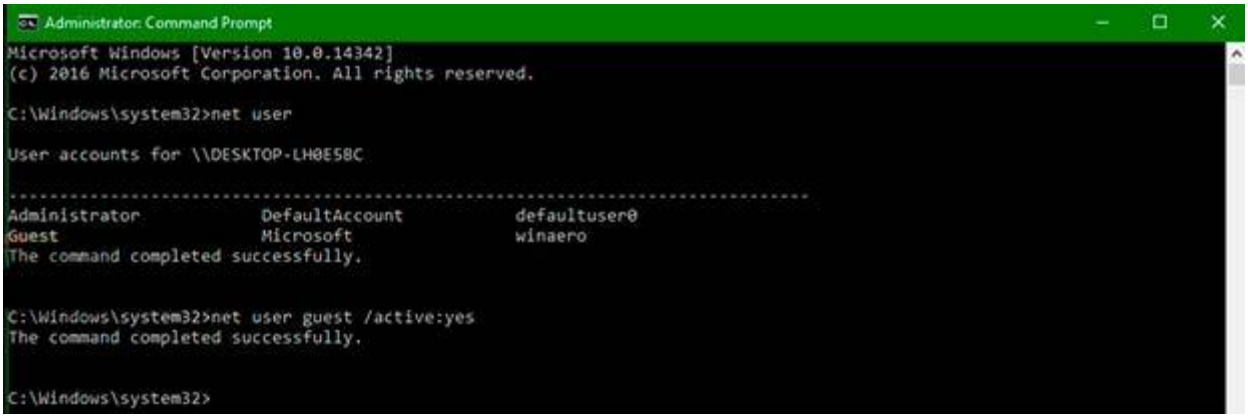
Задание 2. Обойти пароль Windows

Вы можете изменить пароль в Windows в безопасном режиме по следующим шагам:

– Шаг 1.Нажмите F8 перед экраном загрузки Windows.

– Шаг 2. Выберите безопасный режим Windows - «Безопасный режим с командной строкой» → Нажмите «Ввод» далее.

– Шаг 3. Введите net user и нажмите Enter, все учетные записи на ПК Windows будут отображаться.



– Шаг 4. Введите свою заблокированную учетную запись пользователя с новым паролем в командной строке, например, «Счастливый 123456» означает ваш новый пароль для пользователя сети «Счастливый».

Вводим команду: **net user Андрей 54321** и подтверждаем её нажатием enter.

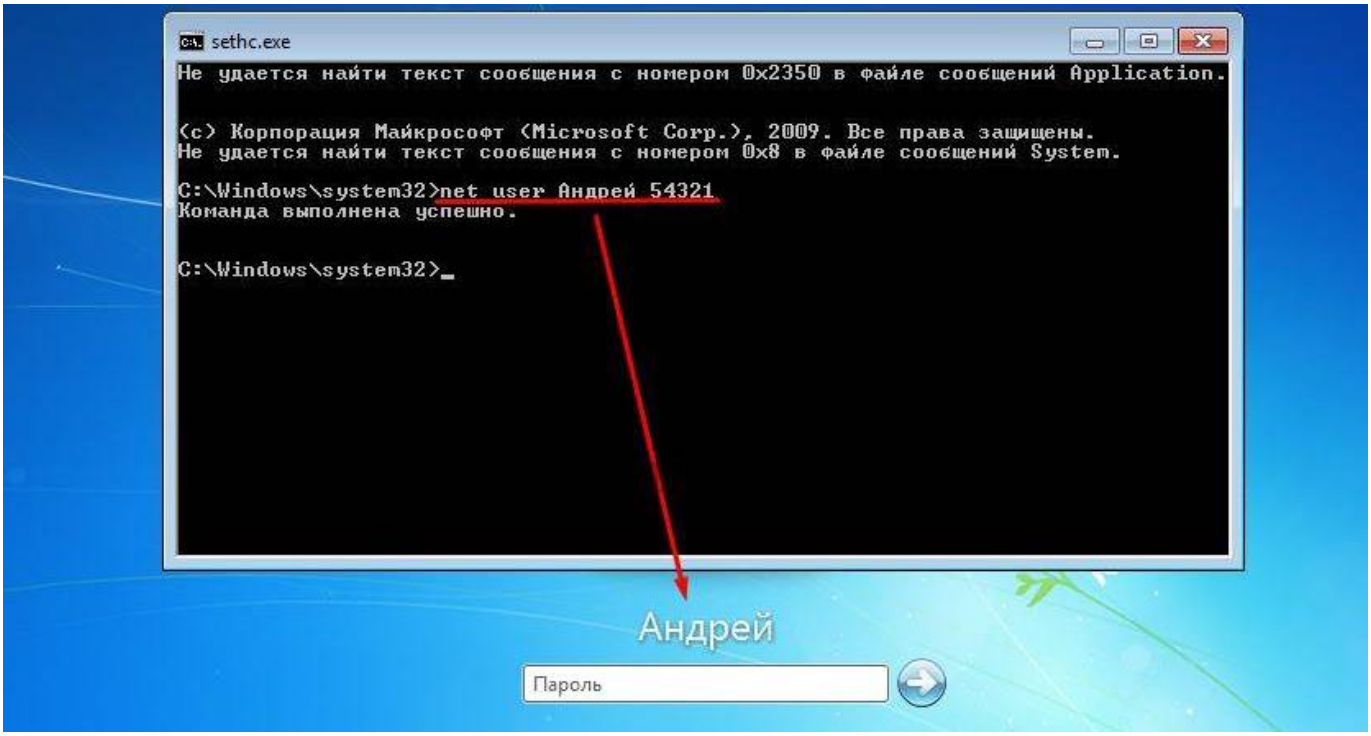
где,

1 net user - функция выбора пользователя.

2 Андрей - имя учетной записи(вводим свое).

3 54321 - новый пароль.

После успешного прохождения процедуры, вводим измененный пароль и радуемся.



– Шаг 5. После перезагрузки компьютера вы можете автоматически войти на свой компьютер с новым паролем.

(Примечание. Когда вы восстанавливаете пароль Windows из безопасного режима, необходима учетная запись администратора с известным паролем).

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №13:

1 Чем определяется стойкость подсистемы идентификации и аутентификации?

2 Перечислить минимальные требования к выбору пароля.

3 Перечислить минимальные требования к подсистеме парольной аутентификации.

4 Как определить вероятность подбора пароля злоумышленником в течении срока его действия?

5 Выбором каким параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Практическая работа №14
«Рассмотрение распространенных антивирусных программ»

Цель работы:

1. Познакомиться и научиться работать с современными антивирусными программами для защиты от вредоносного программного обеспечения.

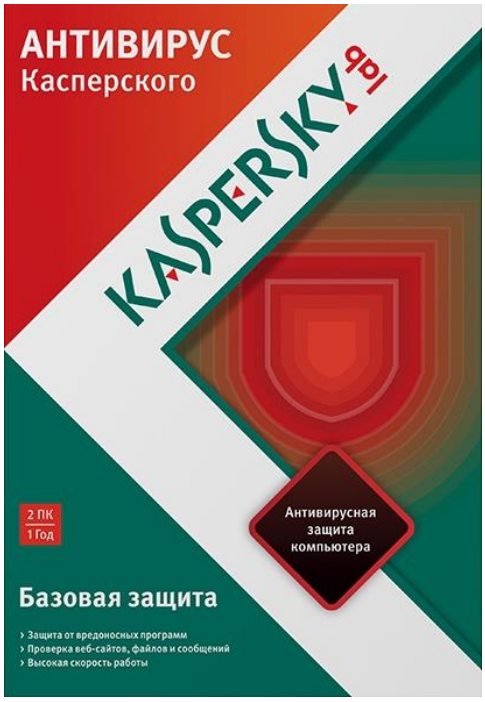
К антивирусному программному обеспечению предъявляются такие же требования, как и к остальным программным продуктам – удобство использования и широкие функциональные возможности, определяемые возможностью выбора различных режимов сканирования и высоким качеством детектирования вирусов. Несмотря на все разнообразие программных продуктов, принципы их работы одинаковы.

К основным функциям современных антивирусов относятся:

1. сканирование памяти и содержимого дисков по расписанию;
2. сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;
3. выборочное сканирование файлов с измененными атрибутами - размером, датой модификации, контрольной суммой и т.д.;
4. сканирование архивных файлов;
5. распознавание поведения, характерного для компьютерных вирусов;
6. удаленная установка, настройка и администрирование антивирусных программ с консоли системного администратора; оповещение системного администратора о событиях, связанных с вирусными атаками, по электронной почте, пейджеру и т. п.
7. принудительная проверка подключенных к корпоративной сети компьютеров, инициируемая системным администратором.
8. удаленное обновление антивирусного ПО и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам посредством Internet;
9. фильтрация трафика Internet на предмет выявления вирусов в программах и документах, передаваемых посредством протоколов SMTP, FTP, HTTP.
10. выявление потенциально опасных Java-апплетов и модулей ActiveX.
11. функционирование на различных серверных и клиентских платформах, а также в гетерогенных корпоративных сетях.
12. ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

Одной из основных характеристик современных вирусных атак является их высокая скорость распространения. Кроме того, можно отметить высокую частоту появления новых атак. Таким образом, в настоящее время к современному антивирусному программному обеспечению, можно предъявить требование частоты обновления продукта - чем чаще обновляется продукт, тем выше его качество, т.к. он учитывает все актуальные на текущий момент времени вирусные угрозы.

Необходимо отметить, что в нашей стране самым популярным антивирусным решением является семейство продуктов антивирусной лаборатории Касперского – AVP.



Среди пользователей бытует мнение, что для успешной защиты от вирусной угрозы достаточно иметь антивирусное средство. Однако, как сказал один автор, серебряных пуль не существует. Наличие антивирусного программного обеспечения является необходимым, но не достаточным условием для отражения антивирусной атаки (кроме наличия средства необходимо продумать методы его использования).

Таким образом, защита от вирусов в организации должна быть регламентирована некоторыми правилами, иначе говоря, быть элементом политики безопасности, которую должны понимать и соблюдать все пользователи системы (для разработки политики безопасности необходимо оценить риски, связанные с заражением вирусами, и разумные пути их минимизации).

Для того чтобы сформулировать основные принципы антивирусной политики безопасности необходимо вспомнить следующие основные моменты, относящиеся к вирусной атаке.

1. Вирусная атака состоит из двух фаз – фаза заражения и фаза распространения (и, возможно, выполнения деструктивных действий).

2. Современные вирусы часто распространяются не только с помощью исполняемых файлов, но и с помощью файлов-документов популярных программ.

3. Современные вирусы при атаке часто используют возможности сети Internet.

Рассмотрим, что можно порекомендовать пользователю с целью предотвращения заражения вирусами (очевидно, что лучший способ борьбы с атакой – ее предотвращение).

Итак, для предотвращения вирусных атак рекомендуется выполнить следующие действия:

1. Соответствующим образом сконфигурировать антивирусное программное обеспечение. Для этого необходимо произвести следующие установки:

– сканирование в режиме реального времени, в фоновом или аналогичном режиме должно быть разрешено;

– при старте системы должны сканироваться память, загрузочный сектор и системные файлы;

– своевременно обновлять вирусные базы данных;

– желательно сканировать все типы файлов или как минимум *.com, *.exe файлы, а также файлы типа *.vbs, *.shs, *.ocx;

– установить аудит всех действий антивирусных программ.

2. Использовать только лицензионное программное обеспечение. Программное обеспечение, полученное из неизвестного источника, может быть троянским или зараженным вирусом.

3. Ограничить набор программ, которые пользователь способен установить в системе (т.к. посторонние программы могут быть заражены вирусами или служить причиной успеха других атак). Особо следует обратить внимание на различные сервисы Internet и, в первую очередь, на программы передачи сообщений, такие как IRC, ICQ, Microsoft Chat (данные программы могут передавать файлы и служить источником заражения системы).

4. Кроме того, желательно устранить известные уязвимости в программном обеспечении (т.к. их наличие может служить причиной успеха вирусных атак). Известные уязвимости обычно публикуются в списках рассылки Internet, а также на специальных сайтах.

5. Контролировать использование накопителей гибких дисков и дисков CDROM. В идеале вся информация, содержащаяся на гибких дисках и дисках CDROM, должна быть проверена на наличие вирусов до того, как к ней будет осуществлен доступ со стороны пользователей вычислительной системы.

6. Разработать политику обработки электронной почты (как составной элемент политики безопасности). Сообщения электронной почты являются одним из самых популярных и самых быстрых способов распространения вирусов.

Для защиты от проникновения вирусов через сообщения электронной почты каждый пользователь системы должен:

– никогда не открывать сразу почтовое вложение в пришедшем ему почтовом сообщении;

– создать «карантинный» каталог - сохранять почтовые вложения в определенном «карантинном» каталоге;

– если отправитель сообщения неизвестен, то сообщение с вложением может быть даже удалено; если отправитель сообщения известен, то сообщение с вложением также может содержать вирус; общее правило может быть сформулировано следующим образом: никогда не открывать почтовых вложений, которые не были запрошены или о которых не было уведомления от отправителя.

– перед открытием вложения всегда проверить его с помощью антивирусного программного обеспечения;

– если после выполнения всех этих процедур остались сомнения в отсутствии вирусов в почтовом вложении, то можно связаться с отправителем и выяснить у него информацию о посланном вложении;

– устранить возможные уязвимости в клиентском почтовом программном обеспечении;

7. Разработать политику безопасности приложений (а особенно при использовании в организации семейства продуктов Microsoft Office), обрабатывающих документы с интерпретируемыми языками (как составной элемент политики безопасности).

Но, предположим, что заражение уже произошло. Рассмотрим, что пользователь должен делать в этом случае. Прежде всего, не надо ни в коем случае паниковать.

Первым шагом, который должен быть сделан при обнаружении атаки на систему, это ее идентификация. Для успешной идентификации атаки часто необходимо наличие загрузочного диска, создаваемого при установке системы и осуществление загрузки системы с его помощью.

Если атака идентифицируется антивирусом, то все очевидно. Но, если Вы имеете дело с некоторым неизвестным вирусом, во многих случаях, критичным является время, за которое была идентифицирована атака. В этой связи, большое значение имеет способность пользователя быстро обнаружить вирусную атаку (признаками могут служить массовая рассылка почты, уничтожение файлов и т.д.). Сложность идентификации атаки часто зависит от сложности самой атаки. На данном этапе желательно установить как минимум следующие признаки: сам факт атаки, типа атаки (сетевая или локальная) и источник происхождения атаки.

Вне зависимости от типа ОС необходимо обращать внимание на следующую активность в системе:

- · целостность ПО используемого для обнаружения нарушителя;
- · целостность критичных для безопасности системы программ и данных;
- · операции в системе и сетевой трафик.

Если Вы смогли определить факт вирусного заражения неизвестным вирусом (или у Вас есть такие небезосновательные подозрения), то желательно обратиться к производителю используемого Вами антивирусного программного обеспечения.

И, наконец, необходимо провести анализ последствий вирусной атаки. Если в Вашей системе обрабатывались какие-то ценные данные, то Вы, конечно, имеете их резервную копию. Для этого в организации должны быть разработаны правила резервного копирования. К сожалению, если резервная копия отсутствует, данные могут быть утеряны (это уже зависит не от Вас, а от злоумышленника, написавшего вирус, поразивший Вашу систему).

Итак, можно сделать следующий вывод: наличие адекватных средств защиты и дисциплины их применения позволяет если не избежать вирусной атаки, то, по крайней мере, минимизировать ее последствия.

Компьютерные вирусы

Это вид вредоносного программного обеспечения, способный создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера.

Компьютерный вирус - это небольшая программа, написанная программистом высокой квалификации, способная к саморазмножению и выполнению разных деструктивных действий.

Существует очень много разных вирусов. Условно их можно классифицировать следующим образом:

1) **загрузочные вирусы** или BOOT-вирусы заражают boot-секторы дисков. Очень опасные, могут привести к полной потере всей информации, хранящейся на диске;

2) **файловые вирусы** заражают файлы. Делятся на:

- вирусы, заражающие программы (файлы с расширением .EXE и .COM);
- макровирусы вирусы, заражающие файлы данных, например, документы Word или рабочие книгиExcel;
- вирусы-спутники используют имена других файлов;
- вирусы семейства DIR искажают системную информацию о файловых структурах;

3) **загрузочно-файловые вирусы** способные поражать как код boot-секторов, так и код файлов;

4) **вирусы-невидимки** или STEALTH-вирусы фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах;

5) **ретровирусы** заражают антивирусные программы, стараясь уничтожить их или сделать нетрудоспособными;

6) **вирусы-черви** снабжают небольшие сообщения электронной почты, так называемым заголовком, который по своей сути есть Web-адресом местонахождения самого вируса. При попытке прочитать такое сообщение вирус начинает считывать через глобальную сеть Internet свое 'тело' и после загрузки начинает деструктивное действие. Очень опасные, так как обнаружить их очень тяжело, в связи с тем, что зараженный файл фактически не содержит кода вируса.

7) **скрипт-вирусы** заражают локальный компьютер при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.

Практически все загрузочные и файловые вирусы резидентны, т.е. они находятся в оперативной памяти компьютера, и в процессе работы пользователя могут осуществлять опасные действия. Макровирусы являются ограниченно резидентными, т.е. они находятся в оперативной памяти и заражают документы, пока открыто приложение.

Если не принимать меры для защиты от компьютерных вирусов, то следствия заражения могут быть очень серьезными. В ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления, в том числе за внедрение вирусов. Для защиты информации от вирусов используются общие и программные средства.

Основные ранние признаки заражения компьютера вирусом:

- уменьшение объема свободной оперативной памяти;
- замедление загрузки и работы компьютера;
- непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

Различают такие типы антивирусных программ:

1) **программы-детекторы:** предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы. Существуют специализированные, то есть предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;

2) **программы-лекари:** предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса. Также могут быть как полифагами, так и специализированными;

3) **программы-ревизоры:** предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения;

4) **лекари-ревизоры:** предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.

5) **программы-фильтры:** предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.

6) **программы-вакцины:** используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).

Задание

С помощью антивирусной программы, установленной на вашем компьютере, проверить компьютер на наличие вирусов и при их обнаружении вылечить зараженные файлы.

Прежде всего, необходимо через Интернет обновить антивирусную программу и вирусную базу данных:

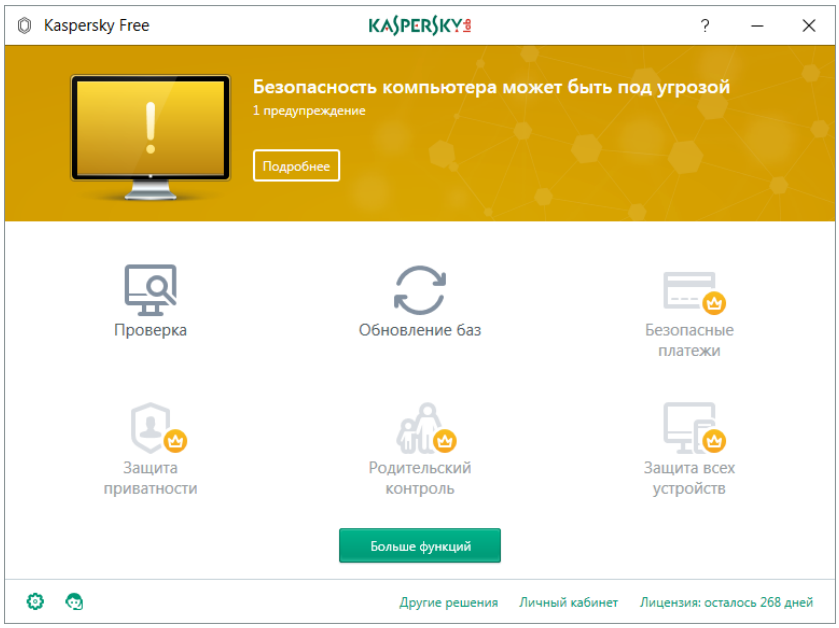
1 Выполните проверку папки «Мои документы» на вирусы. Дать характеристику этой программы.

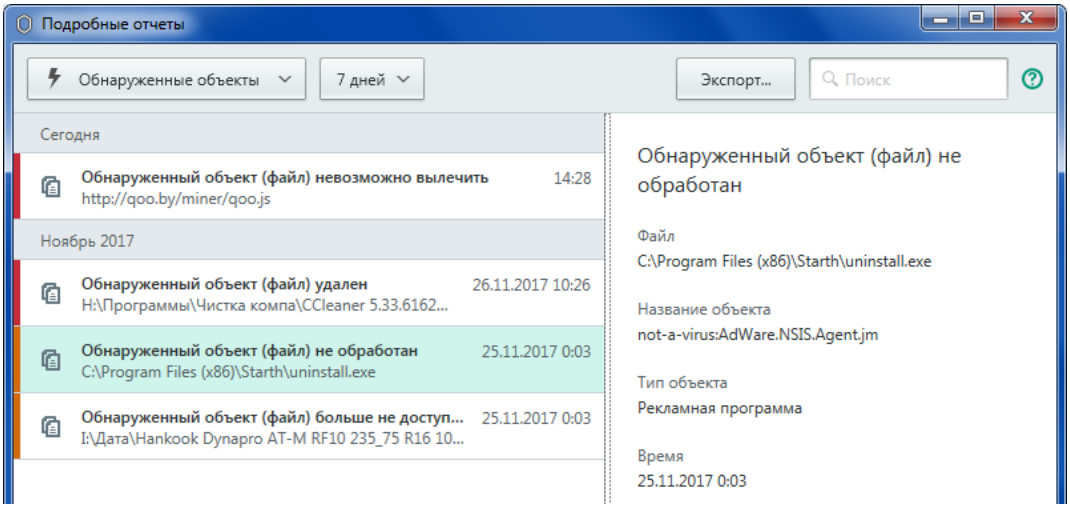
2 После окончания проверки в случае обнаружения угроз программа запросит вас, какое действие произвести над вредоносными объектами:

– **Лечить**. После лечения с объектом можно продолжить работу.

– **Поместить на Карантин**, если в результате проверки не удалось определить, заражен объект или нет. Если у вас установлена необходимая опция проверки файлов на карантине после каждого обновления баз, то после получения новой сигнатуры лечения объект на Карантине будет вылечен и вновь доступен для пользователя.

– **Удалить**. Если объекту присвоен статус вируса, но его лечение невозможно, вы можете удалить его. Информация об объекте сохранится в Рис.2 отчете об обнаруженных угрозах.





КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №14:

1. Функции современных антивирусных программ?
2. Что относится к вирусной атаке?
3. Рекомендации (действия), которые нужно выполнить с целью предотвращения заражения вирусами
4. Что должен сделать каждый пользователь для защиты от проникновения вирусов через сообщения электронной почты?
5. Расскажите о типах современных АП
6. Что такое вирус и их классификация.

Практическая работа №15
«Реализация отказоустойчивости на основе резервирования. Механизм и организация контроля доступа.»

Цель работы:

1. Приобрести практические навыки в реализации теоретических основ резервирования, проектирования систем контроля и управления доступом.

1. Резервирование и восстановление данных в Windows 7

Бэкап системы — гарантия стабильной работы компьютера

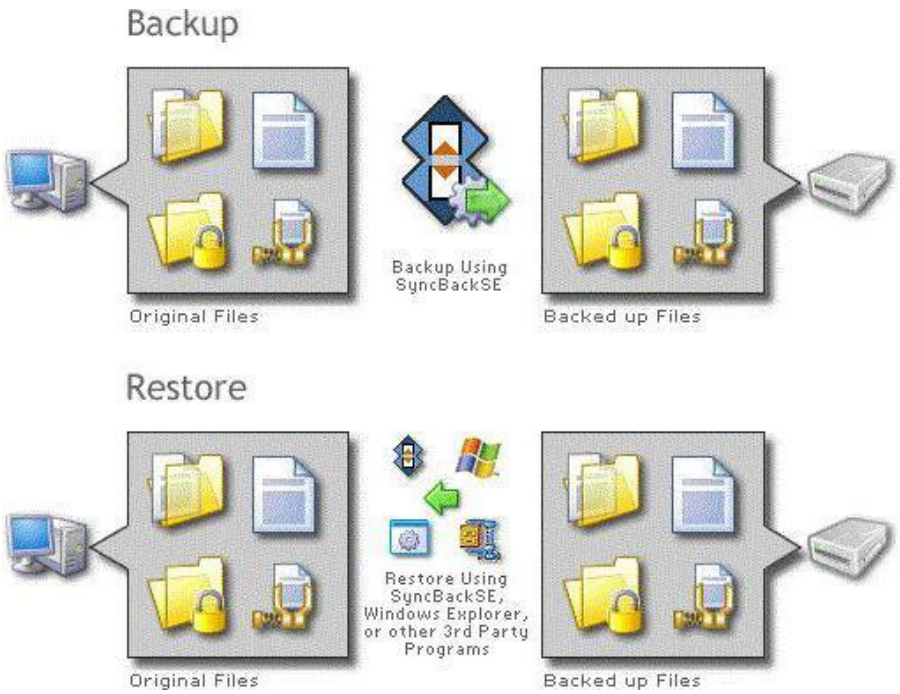
Можно по старинке документы для сохранности копировать на флешки или параллельные разделы жесткого диска, переживать за тьму настроек в операционной системы, трястись над каждым системным файлом во время установки сторонних тем оформления и иконок. Но ручной труд отныне в прошлом — в сети достаточно программного обеспечения, которое зарекомендовало себя как надежное средство для полного резервирования системы целиком. Чуть что не так после очередных

экспериментов — в любой момент можно вернуться к сохраненной версии.

Операционная система Windows 7 также имеет встроенную функцию создания копии самой себя, и о ней в данной статье мы тоже поговорим.

Основной принцип работы и варианты функционирования

Как правило, большинство сегодня известных и широко применяемых утилит в основном используют принципы создания образов и сжатия копируемых данных. При этом образы чаще всего применяются именно для создания копий операционной системы, что позволяет в дальнейшем восстановить ее после непредвиденного критического сбоя, а утилиты для копирования разделов или пользовательских файлов предполагают именно сжатие по типу архивирования.



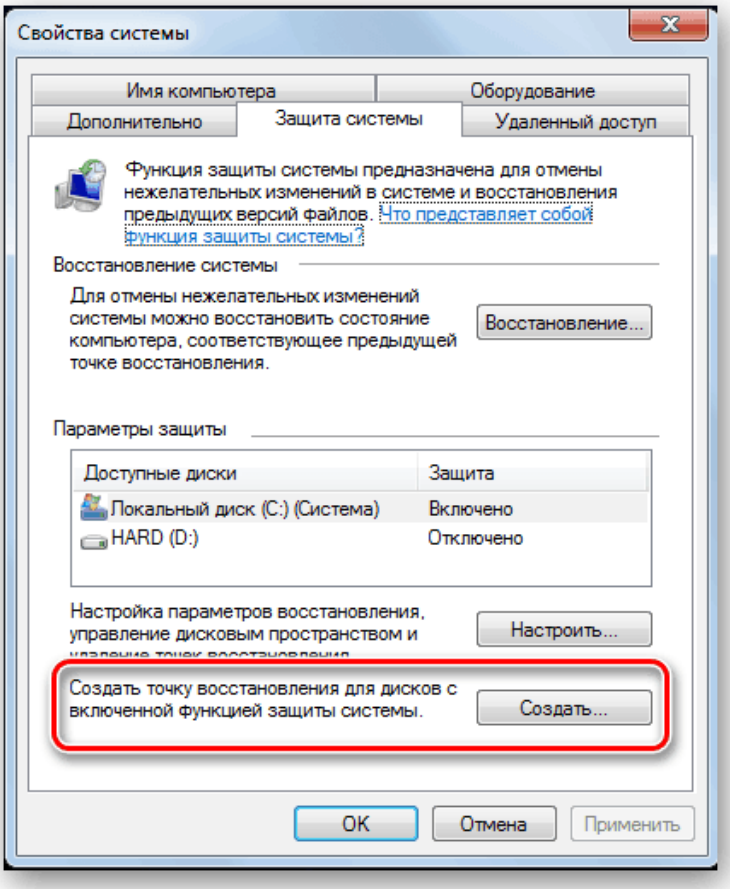
Что же касается вариантов резервирования, их может быть два. В принципе, практически любая программа для резервного копирования системы предлагает использовать внешний носитель (DVD-диск, флэшку и т. д.). Связано это только с тем, что при восстановлении системы придется загружаться не из системного раздела, а именно со съемного носителя. Образ в логическом разделе распознан не будет.

Другое дело – программы резервного копирования дисков. В них можно произвести сохранение нужной информации именно в других логических разделах или, опять же, использовать съемные носители. Но что делать, если используемый объем винчестера исчисляется сотнями гигабайт? Никакой оптический диск не позволит записать эту информацию даже в сжатом виде. Как вариант можно использовать внешний HDD, если он, конечно, имеется в наличии.

Что же касается выбора подходящей утилиты для сохранения пользовательских файлов, лучшее решение – программа резервного копирования файлов по расписанию. Такая утилита способна производить данную операцию без участия пользователя, сохраняя все сделанные за определенный промежуток времени изменения. В резервную копию могут добавляться новые данные, равно как и старые - удаляться из нее. И все это в автоматическом режиме! Преимущество налицо - ведь пользователю в настройках нужно только задать временной интервал между точками копирования, дальше все происходит без него.

Способ 1: точка восстановления

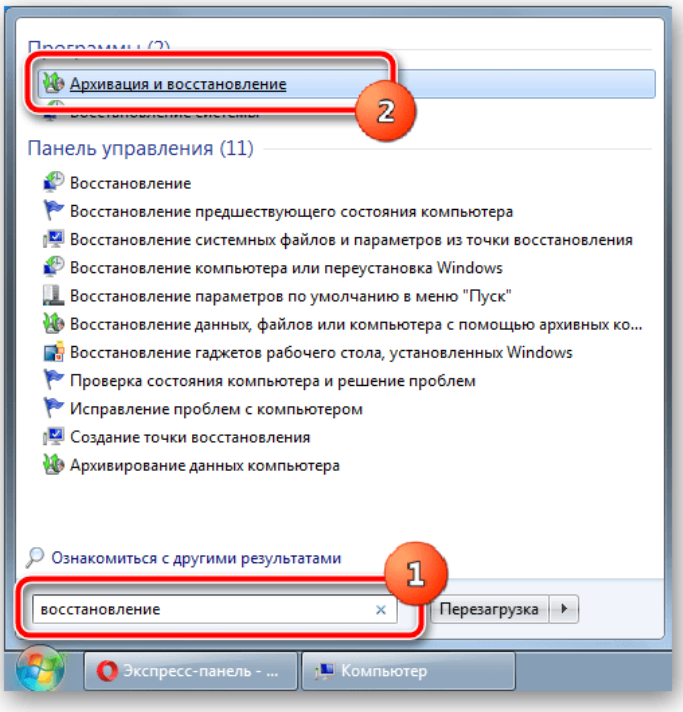
Самым популярным и быстрым способом создать резервную копию системы является точка восстановления. Она занимает сравнительно немного места, создается практически мгновенно. Точка восстановления имеет возможность вернуть компьютер к контрольной точке, восстановив критические системные файлы, не затрагивая данные пользователя.



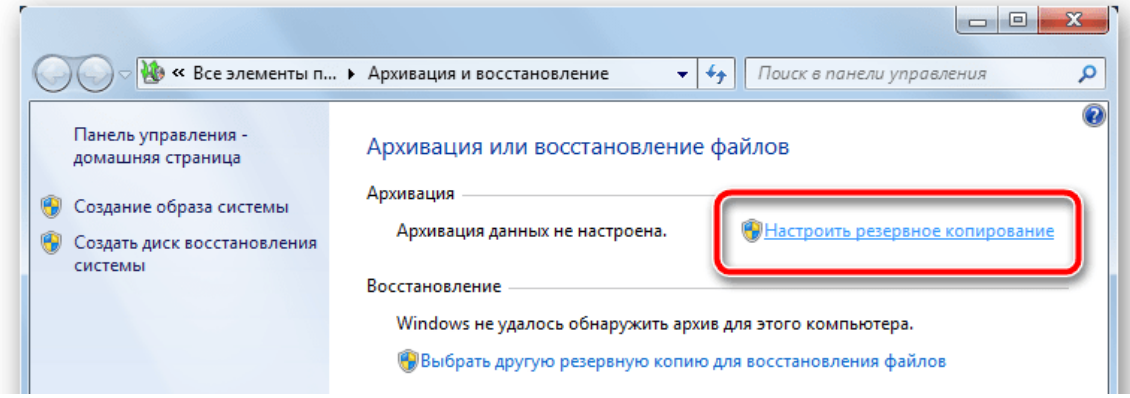
Способ 2: архивация данных

Windows 7 имеет еще один способ создания резервных копий данных с системного диска — архивация. При правильной настройке этот инструмент сохранит все файлы системы для их последующего восстановления. Имеется один глобальный недостаток — невозможно архивировать те исполняемые файлы и некоторые драйверы, которые в данный момент используются. Однако, это вариант от самих разработчиков, поэтому его тоже нужно учитывать.

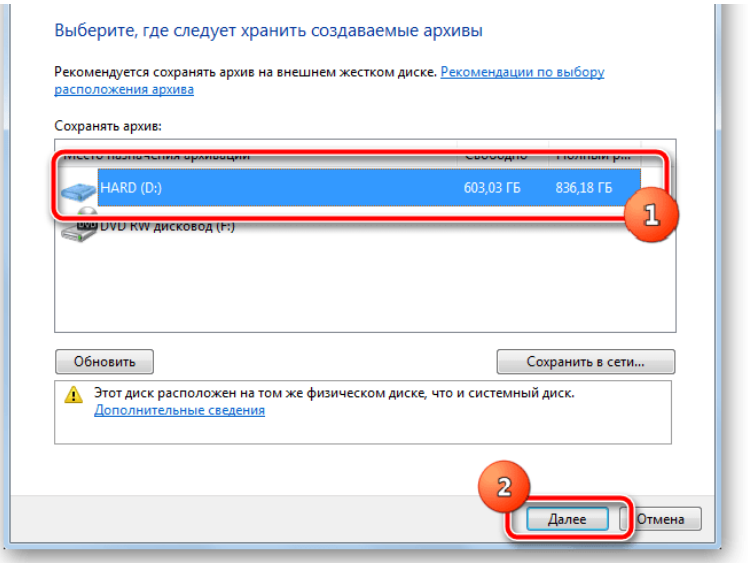
1. Откройте меню **»Пуск»**, впишите в поле поиска слово **восстановление**, выберите первый вариант из появившегося списка — **»Архивация и восстановление».**



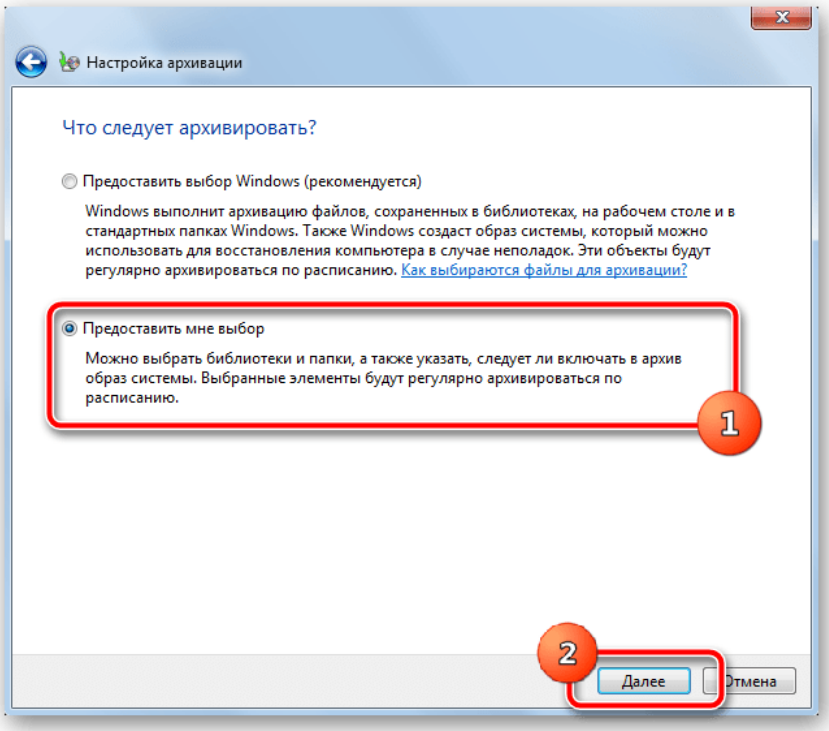
2. В открывшемся окне откройте параметры резервного копирования, нажав левой кнопкой мыши на соответствующую кнопку.



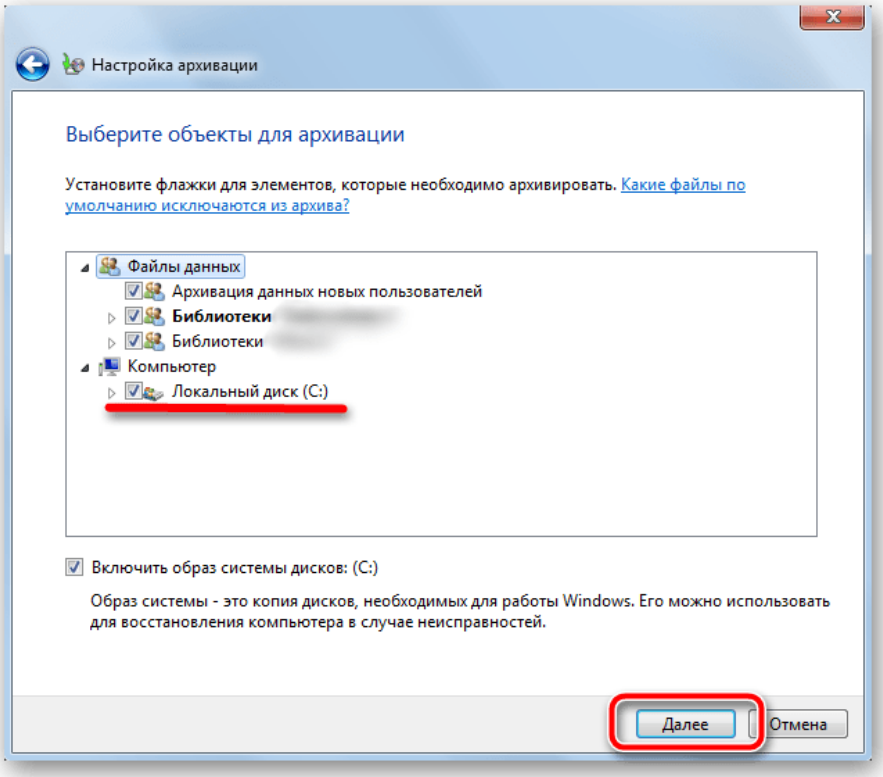
3. Выберите раздел, на который будет сохраняться резервная копия.



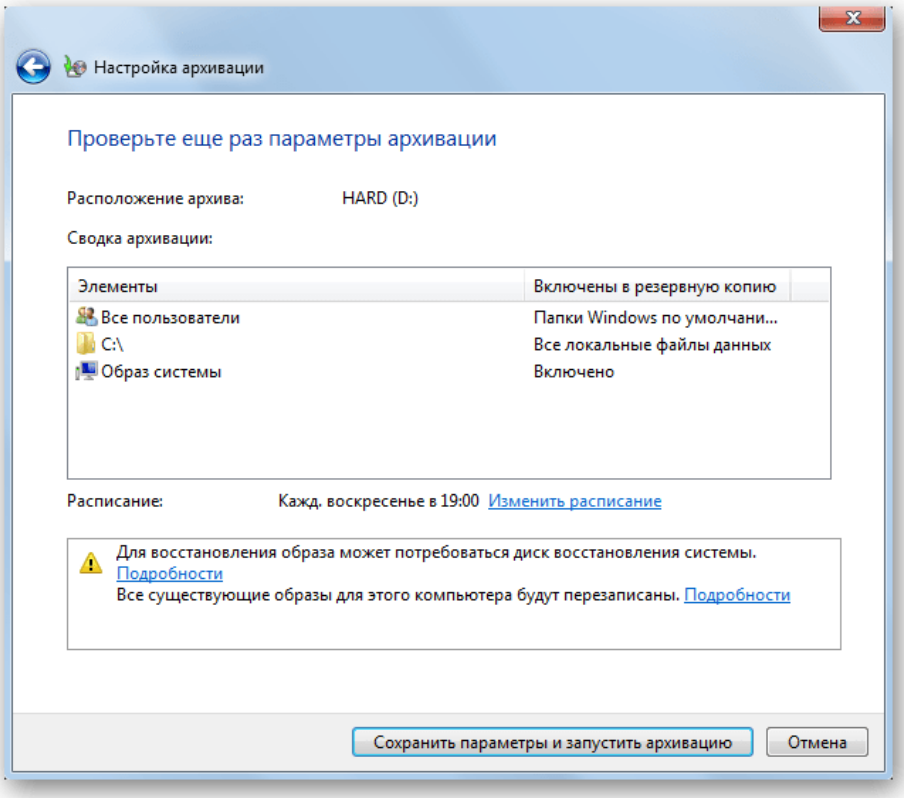
4. Укажите параметр, отвечающий за данные, которые будут сохранены. Первый пункт соберет в копию только данные пользователей, второй же даст нам выбрать весь системный раздел.



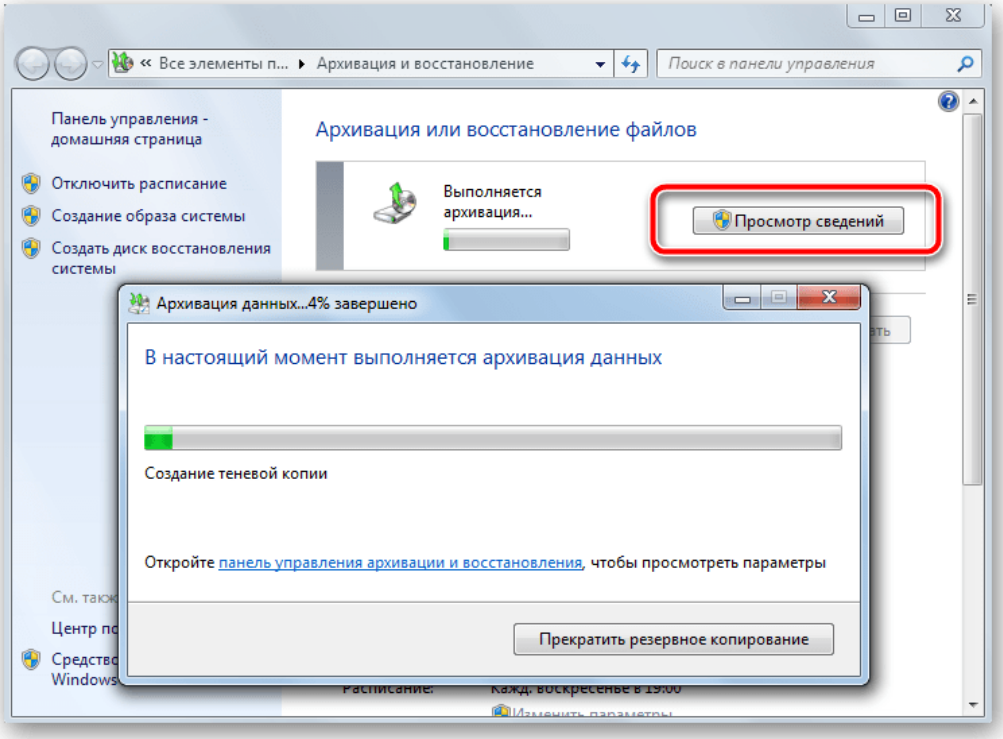
5. Укажите галочкой и диск (C:).



6. Последнее окно выводит всю настроенную информацию для проверки. Учтите, что автоматически будет создано задание для периодической архивации данных. Его можно отключить в этом же окне.

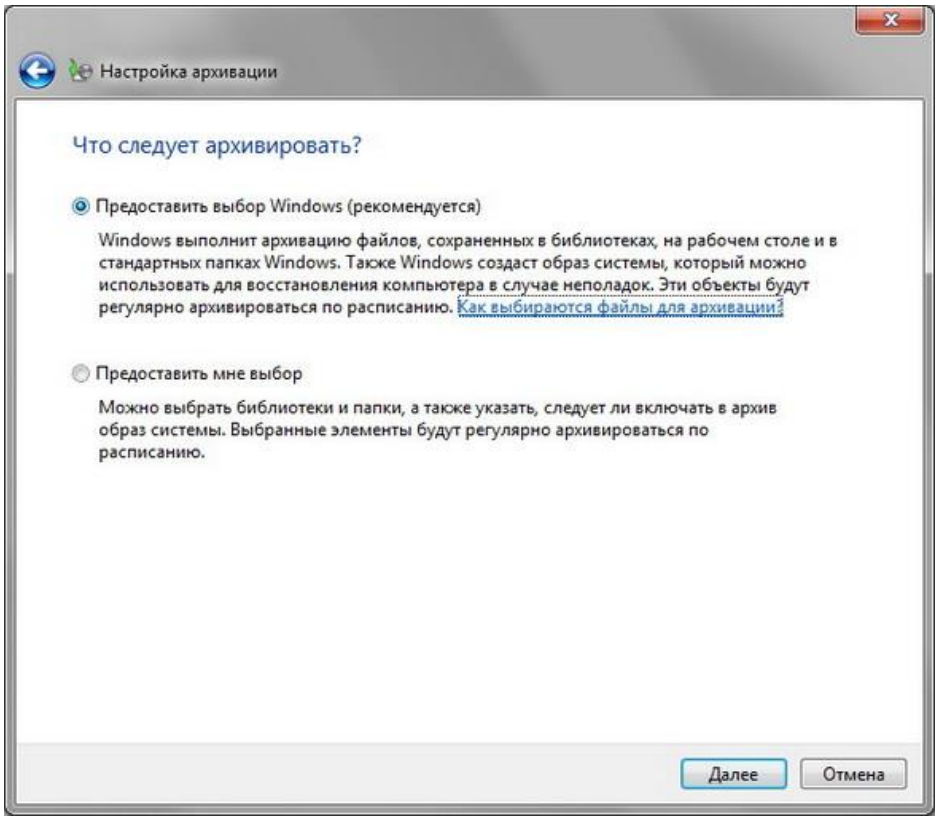


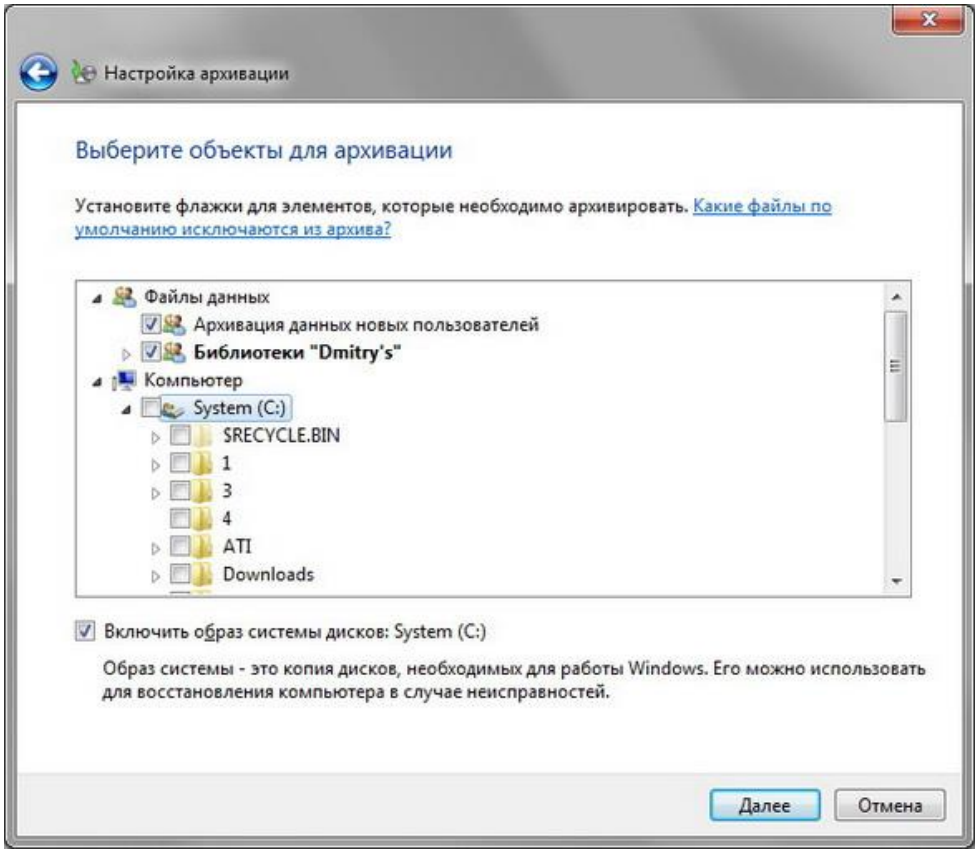
7. Инструмент начнет свою работу. Чтобы посмотреть прогресс копирования данных, нажмите на кнопку **»Просмотр сведений».**



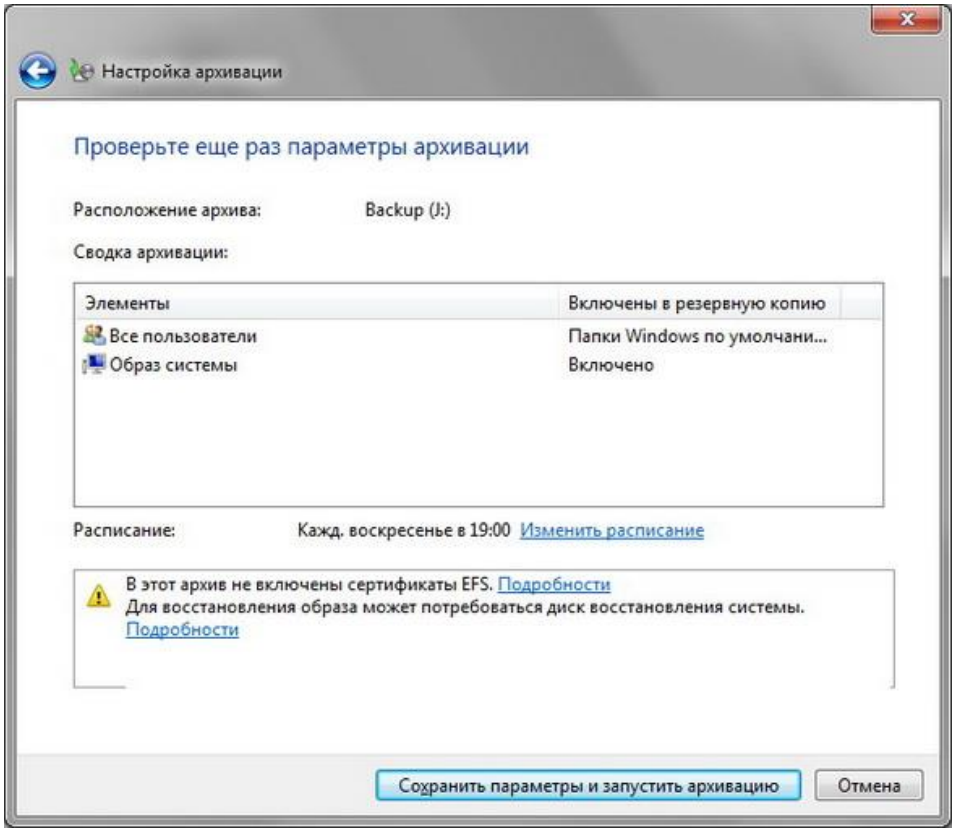
8. Операция займет некоторое время, компьютером будет пользоваться достаточно проблематично, потому как этот инструмент потребляет достаточно большое количество ресурсов.

5. Если выбрать первый вариант, тогда при выборе опции по умолчанию Windows включает в резервную копию все файлы. Сюда входят «Мои файлы/My Files» и рабочий стол («Мой компьютер/My Computer»). Данная опция создаёт также образ системы. Windows даже позаботится о подходящем расписании.

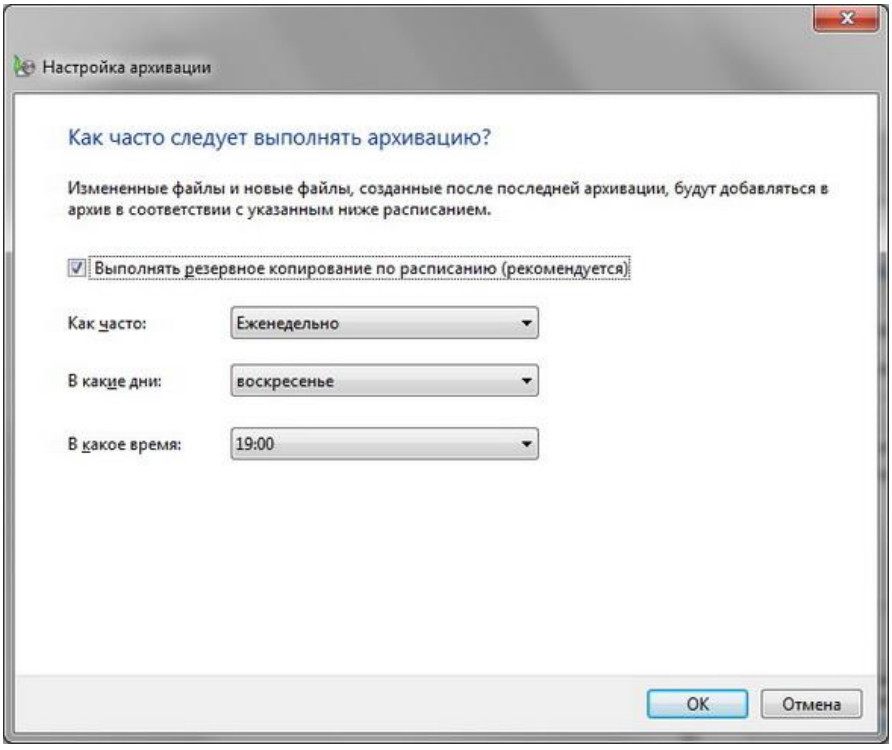




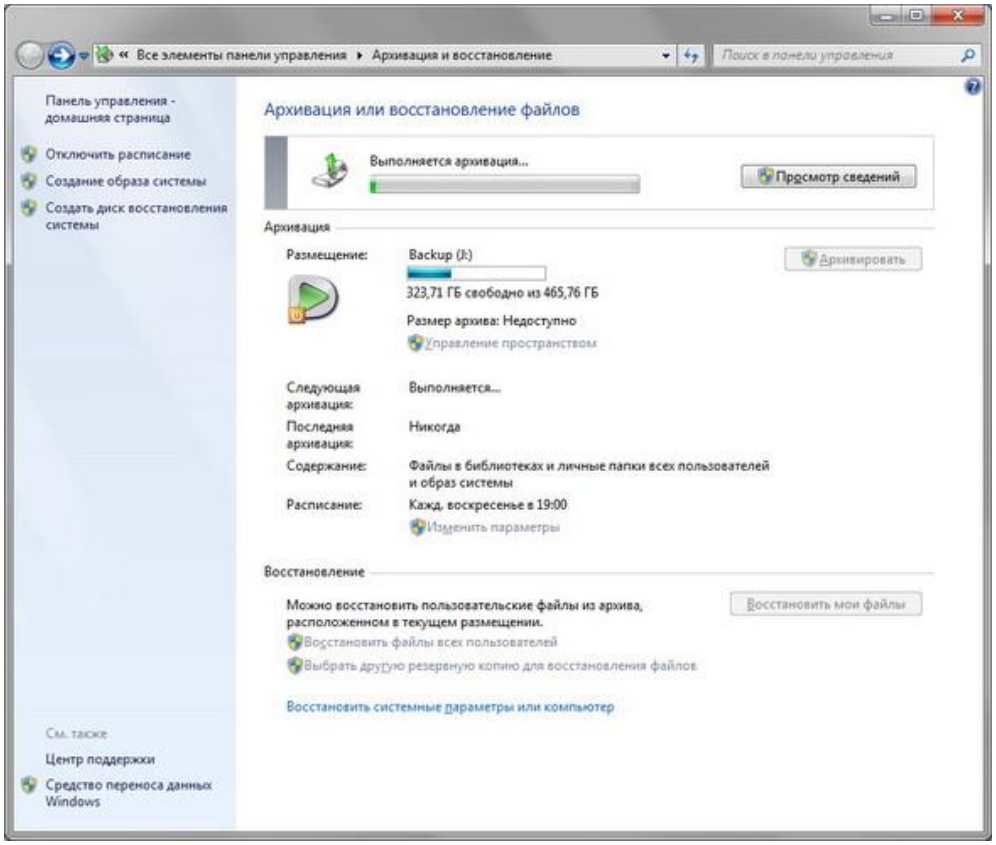
По умолчанию предлагается резервировать то, что считается файлами данных пользователя. Если вы выберете резервирование, настраиваемое пользователем (скриншот выше), то сможете добавить в копию больше файлов и дисков.



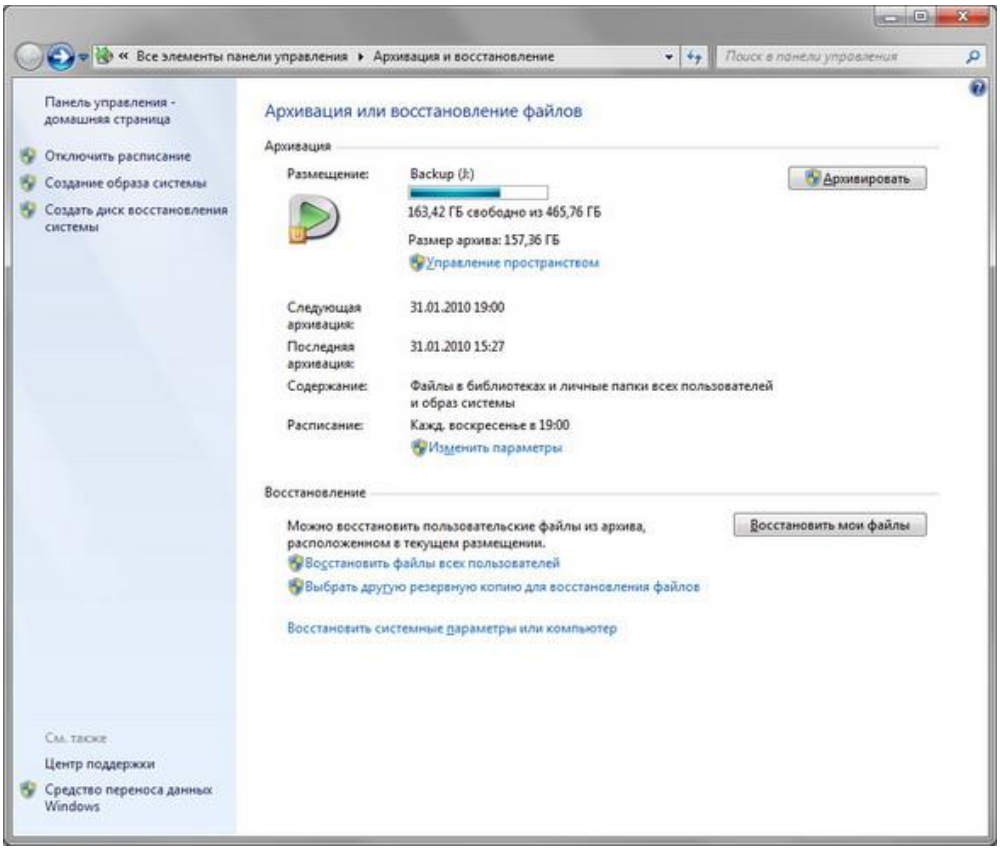
Прежде чем начать действовать, Windows Backup предоставляет отчёт о параметрах резервирования.



Программа предложит вам пересмотреть расписание резервирования. Вам не понадобится диск восстановления системы, если у вас есть оригинальный установочный диск Windows 7.

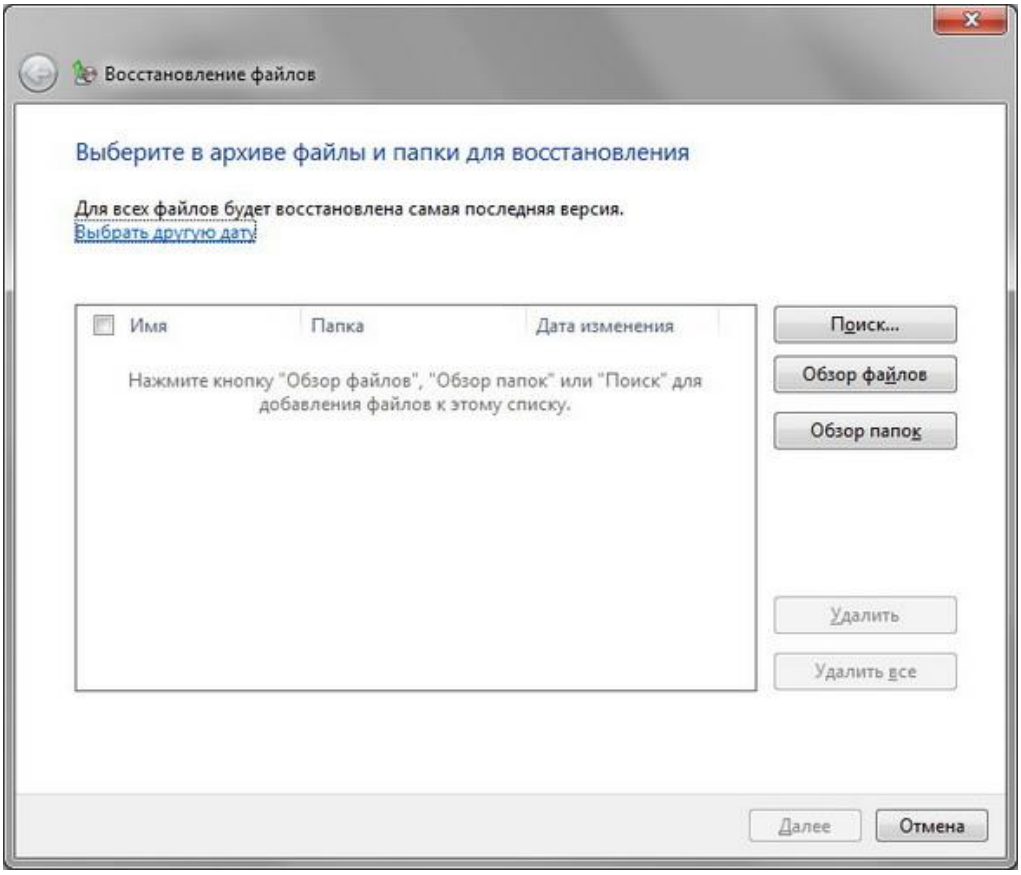


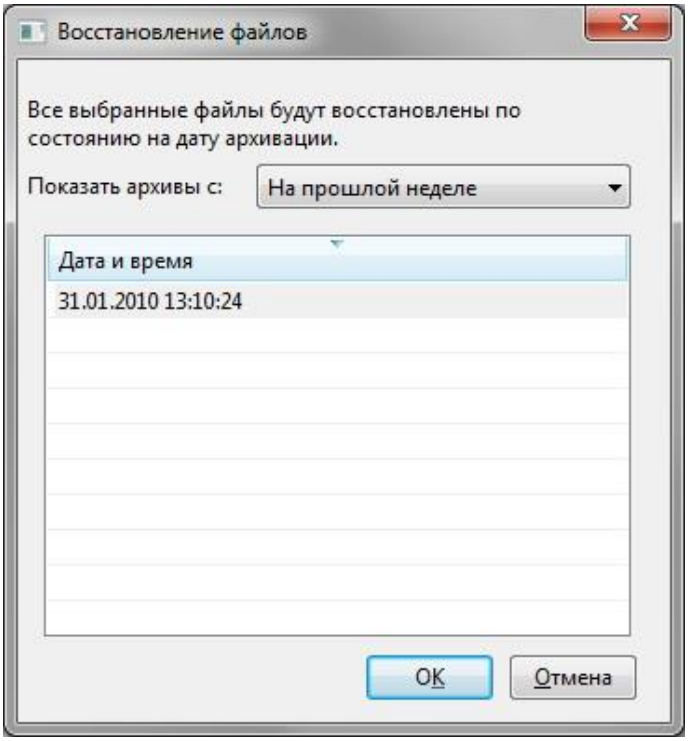
В окне наблюдения за ходом процесса вы можете видеть всю необходимую информацию в стиле Windows Vista/7. Главное окно «Архивация и восстановление/Backup and Restore» позволяет выбрать имеющийся набор резервирования для восстановления.



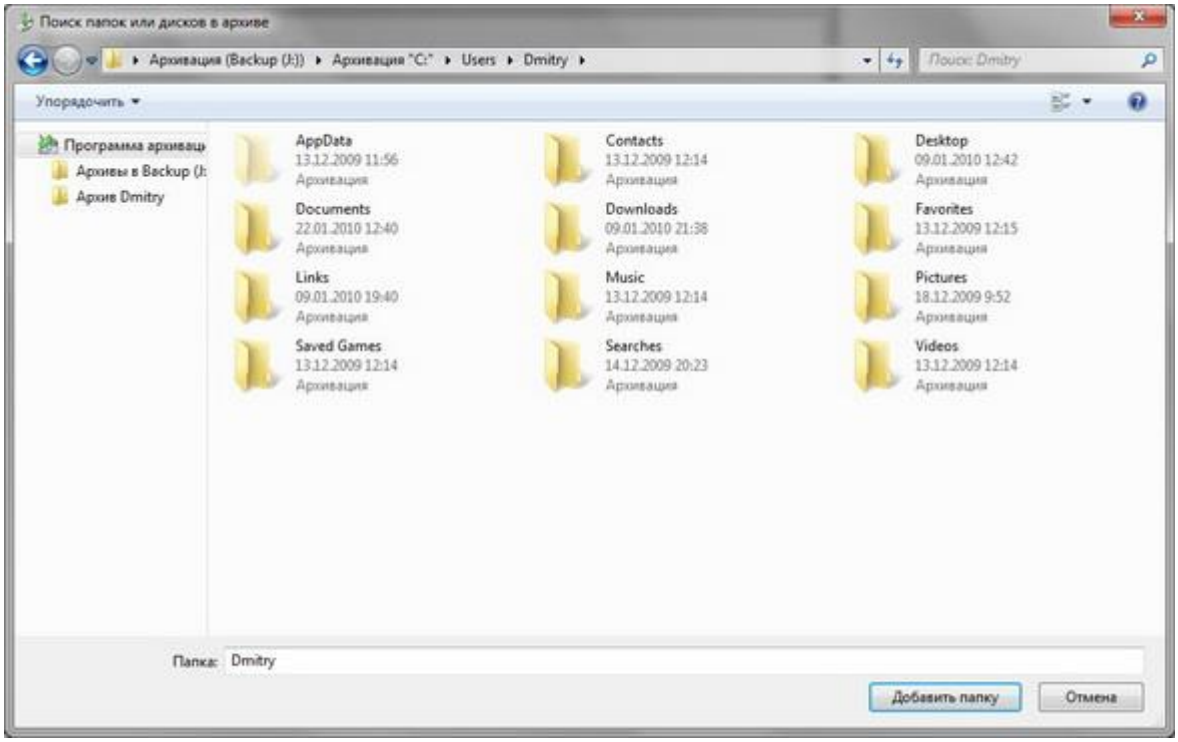
Восстановление

Разумеется, мы попробовали восстановить наши резервные копии, чтобы посмотреть, как они работают.

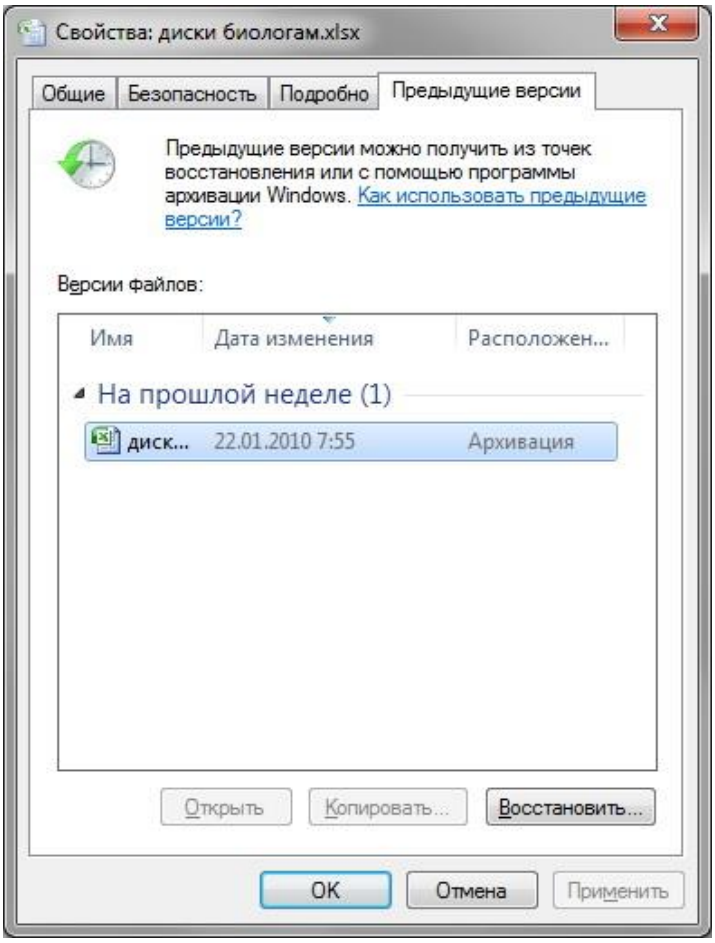




Сначала нужно выбрать резервный набор, который вы хотите восстановить.



Затем можно внутри этого набора выбирать отдельные файлы. Возможно, эта функция пригодится вам чаще всего, если, скажем, вы изменили или переписали документ.



Windows автоматически создаёт и поддерживает версии файлов. Их можно посмотреть в свойствах файла. На нашем скриншоте показана возможность восстановления документа Excel.

Если вы хотите восстановить систему целиком, придётся загрузиться с установочного диска Windows 7 или создать диск восстановления системы, который можно использовать для загрузки в случае отсутствия установочного диска.

Несмотря на то, что операционная система имеет встроенный функционал для создания резервных копий, он не вызывает достаточного доверия. Если точки восстановления очень часто выручают пользователей-экспериментаторов, то с восстановлением архивированных данных часто возникают проблемы. Использование стороннего программного обеспечения значительно повышает надежность копирования, избавляет от ручного труда, автоматизируя процесс, и предоставляет достаточно точную настройку для максимального удобства.

Резервные копии желательно хранить на других разделах, в идеале — на сторонних физически отключаемых носителях. В облачные сервисы резервные копии загружайте только зашифрованными надежным паролем для безопасного хранения личных данных. Регулярно создавайте новые копии системы во избежание утери ценных данных и настроек.

Способ 3: Использование сторонних программ

Теперь посмотрим на утилиты, которые, по мнению многих экспертов, сегодня являются наиболее востребованными у пользователей. Сразу отметим, что рассмотреть все программы резервного копирования просто невозможно, поэтому остановимся на некоторых из них, учитывая уровень популярности и сложности их использования. Приблизительно список таких утилит может выглядеть следующим образом:

- Acronis True Image.
- Norton Ghost.
- Back2zip.
- Comodo BackUp.
- Backup4all.
- ABC Backup Pro.
- Active Backup Expert Pro.
- ApBackUP.
- File Backup Watcher Free.
- The Copier.
- Auto Backup и многие другие.

Системы контроля и управления доступом (СКУД) разграничивают права прохода в помещения (зоны, территории) определенных категорий лиц и ограничивают доступ лиц, не обладающих такими правами. Сегодня СКУД – это не только набор пропускных конструкций, контроллеров, считывателей и т. д., а сложный комплекс организационных и технических мероприятий, процесс управления доступом в котором автоматизирован и практически не требует участия персонала. Система контроля доступа помогает не только обеспечивать сохранность материальных ценностей, безопасность персонала и посетителей, но и организовать учет рабочего времени сотрудников, а также упорядочивать порядок передвижения людей по объекту. В общем виде СКУД может иметь в своем составе следующие элементы:

- исполнительные механизмы (замки, турникеты, шлюзы);
- электронные идентификаторы (пластиковые карточки, «электронные таблетки» и другие устройства);
- считыватели (пластиковых карточек и прочих электронных идентификаторов);
- устройства ввода персонального кода (PIN-кода);
- биометрические устройства идентификации личности;

- устройства управления исполнительными механизмами (контроллеры, концентраторы);
- оборудование сопряжения локальной сети СКУД с компьютером;
- программное обеспечение администратора системы.

Основой любой системы являются блоки концентраторов с подключенными считывателями идентификационных ключей, охранными датчиками и электромеханическими запорными устройствами (замки, шлагбаумы, турникеты).

Контроллер – это основная часть системы управления доступом. Именно контроллер принимает решение, пропустить или нет человека в данную дверь. Контроллеры исполнительных устройств СКУД – сложные электронные приборы, которые могут быть реализованы в виде отдельных блоков либо встроены в корпус соответствующего исполнительного устройства. Контроллер хранит в своей памяти коды идентификаторов со списком прав доступа каждого.

Кроме обмена информацией с концентраторами СКУД по линиям связи осуществляют: анализ информации, поступающей с устройств чтения электронных идентификаторов, устройств ввода PIN-кода и биометрических идентификаторов, выдачу на основании этого анализа управляющих сигналов на отпирание (запирание) исполнительных устройств; контроль состояния исполнительных устройств (открыто или закрыто); хранение в оперативной энергонезависимой памяти журнала перемещений; регистрацию попыток несанкционированного доступа. Важно, чтобы контроллер мог работать даже в случае аварии электросети, имел резервный источник питания.

Задание

1 Создайте резервную копию системы использую как встроенные утилиты системы, так и предложенные программы для резервирования данных;

2 Выполните восстановление системы с флеш-карты.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №15:

1. Что такое отказоустойчивость?
2. Назовите способы создания резервной копии в Windows 7
3. Что такое точка восстановление и как с ней работать?
4. Что такое Бэкап системы? Основной принцип работы и варианты функционирования

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Партыка Т.Л., Попов И. И. Информационная безопасность : учебное пособие. / Т.Л. Партыка, И.И. Попов. – М. : Форум, 2012. – 432 с.
2. Бабаш А.В. Информационная безопасность : учебное пособие / А.В. Бабаш – М. : Кнорус, 2013. – 136 с.
3. http://www.intuit.ru