МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Государственное образовательное учреждение высшего профессионального образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

А.А. Хамухин

Практикум по информационной безопасности

*Рекомендовано в качестве учебного пособия
Редакционно-издательским советом
Томского политехнического университета*

Издательство
Томского политехнического университета
2011

УДК 004:378.4
ББК 32.81р30
Х19

Хамухин А.А.

Х19 Практикум по информационной безопасности: учебное пособие / под ред. А.А. Захаровой – Томск: Изд-во Томского политехнического университета, 2011. – 196 с.

Пособие содержит краткое описание основных задач информационной безопасности, примеры их решения и задания для организации практических и лабораторных работ. Материалы практикума содержат такие разделы, как настройки безопасности операционной системы и приложений, установка и эксплуатация антивирусного программного обеспечения, криптографическая защита информации, профессиональные программные и аппаратные средства защиты информации. В приложениях к пособию освещен законодательный уровень информационной безопасности. Пособие предназначено для студентов, обучающихся по направлению подготовки бакалавров 230700 «Прикладная информатика».

УДК 004:378.4
ББК 32.81р30

Рецензенты

Доктор технических наук, профессор,
вице-президент по информационным технологиям
ОАО «Востокгазпром», действительный член
Международной академии информатизации
Н.Г. Марков

Кандидат технических наук, доцент,
доцент кафедры медицинской и биологической кибернетики
Сибирского государственного медицинского университета
О.В.Воробейчикова

Предисловие

Томский политехнический университет – старейший технический вуз в азиатской части России, основанный в 1896 году. Он оказал значительное влияние на развитие науки, образования, промышленности и культуры страны. Это достигнуто усилиями ученых, преподавателей, студентов и более чем сотни тысяч выпускников.

Наш университет – это сочетание традиций и инноваций в области высшего технического образования. Этим он отличается от других высших учебных заведений. Ведущая роль Томского политехнического университета и его влияние на культуру общества отмечены включением университета в «Свод особо ценных объектов культурного наследия народов России» Указом Президента Российской Федерации от 2 апреля 1997 года. А с 7 октября 2009 года университету присвоен статус «Национальный исследовательский» в числе первых 12 вузов России.

В своей работе Томский политехнический университет опирается на традиции, сложившиеся за вековую историю университета:

- единство научной и учебной деятельности, дающее специалистам глубокие общенаучные знания;
- фундаментальная инженерная и практическая подготовка, позволяющая выпускникам быстро адаптироваться в современных производственных условиях;
- высокий уровень требований к студентам и преподавателям, гарантирующий соответствующее качество подготовки специалистов;
- новаторство, требующее от студентов, преподавателей, ученых и менеджеров университета постоянно находить лучшие пути решения стоящих перед ними задач.

Томский политехнический университет создает условия и стимулы для свободного выражения мыслей и идей, поддерживает культ знаний и стремления к успеху. Вот почему на нашем гербе девиз: **«Знание. Свобода. Процветание».**

Миссия Томского политехнического университета заключается в том, чтобы нести в мир знания и опыт, позволяющие личности, обществу и Российскому государству видеть и использовать лучшие образцы подготовки высококлассных специалистов и эффективной реализации нововведений в сфере науки и высшего образования. Стратегические направления деятельности университета:

- развитие фундаментальных и прикладных научных исследований;
- формирование и развитие научно-педагогических школ;

• активное взаимодействие с ведущими научными, образовательными и производственными центрами;

• стимулирование студентов, преподавателей и сотрудников к интеграции традиционных академических ценностей и предпринимательских идей;

• формирование гармонично развитой личности и подготовка специалиста, способного быть лидером, работать в команде, действовать и побеждать в условиях конкурентной среды;

• сопровождение образования выпускников через всю жизнь и содействие их успешной деловой карьере.

На этой странице процитирована миссия Томского политехнического университета, сформировавшаяся за более чем за 100 лет его деятельности. Автор книги, выросший и воспитанный в духе этой миссии, надеется, что и студенты, кроме знаний по специальным предметам, унесут с собой в будущую трудовую деятельность заряд энтузиазма и творчества миссии Томского политехнического университета.

Введение

Понятие «информационная безопасность» входит составной частью в информационные технологии, которые в последнее время развиваются наиболее стремительно. Еще не так давно информационная безопасность трактовалась, как «защита компьютерной информации». Причем защищать информацию предполагалось от злоумышленников, которые распространяют вирусы, похищают пароли, совершают хакерские атаки и т. п. Это очень важно, но сейчас уже накоплена статистика, которая показывает, что наибольший информационный урон фирмы получают от собственных сотрудников, нежели от внешних злоумышленников.

Далее пришло понимание, что поломка и простой из-за сбоя или даже просто медленная работа информационной системы могут приводить к убыткам в бизнесе. В событиях 11 сентября 2001 года в США, когда террористами были взорваны две башни-близнеца, наполненные офисами многих фирм, вместе с людьми погибло огромное количество деловой информации, у многих фирм бизнес был парализован. Поэтому физическая сохранность компьютеров и носителей информации тоже вошла в понятие информационной безопасности предприятия.

Знаменитая «Проблема 2000 года» показала, что вовсе не злоумышленники или нерадивые сотрудники, а вполне лояльные программисты могут делать такие ошибки в программировании, которые затем грозят непоправимыми последствиями: от сбоев в работе банковских систем, до падения самолетов.

Такое развитие информационных технологий привело к тому, что в настоящее время понятие информационной безопасности трактуется так: «Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства». Аналогично можно определить информационную безопасность не всего общества в целом, а некоторого конкретного субъекта (фирмы, корпорации, подразделения и т. п.). Тогда защита информации трактуется, как комплекс мероприятий, направленных на обеспечение информационной безопасности этого субъекта.

Защита информации, как и защита физического объекта, может быть пассивной и активной. Так, например, пассивная защита древних городов от нападения кочевников – высокая крепостная стена, земляной вал и ров, заполненный водой. Активная защита в этом примере – это жители города на крепостной стене, поливающие нападающих горячей

смолой из бочек. Поэтому и защита информации должна строиться из двух составляющих: пассивной и активной.

Типичная ошибка начинающих разработчиков – это стремление сначала создать информационную систему, лишь бы она правильно работала, а уж потом ее защищать. Пассивный компонент защиты («крепостную стену») необходимо закладывать с самого начала проектирования информационной системы. Тогда и расходы на активный компонент защиты окажутся гораздо ниже при приемлемом уровне информационной безопасности.

Последний термин появился сравнительно недавно, относится к области менеджмента информационной безопасности и в настоящем пособии не рассматривается. В рамках курса, объемом в две зачетные единицы (72 часа), невозможно рассмотреть все перечисленные аспекты информационной безопасности. Поэтому выделено, на взгляд автора, главное и необходимое для бакалавров направления «Прикладная информатика». Объем примеров и заданий в пособии превышает 2 зачетные единицы, позволяя преподавателю видоизменять практикум во времени или сделать некоторые задания элективными.

В Главе 1 рассматриваются настройки безопасности операционной системы *Windows* 7, которых стало значительно больше по сравнению с предыдущей версией. Также рассмотрены настройки безопасности Интернет-обозревателей и приложений *Microsoft Office* 2010.

В Главе 2 приведены примеры установки бесплатно-распространяемого антивирусного программного обеспечения (ПО). Дана классификация вредоносного ПО, рассмотрен пример эксплуатации сканера доступа и межсетевого экрана.

Глава 3 посвящена задачам криптографической защиты информации. Дана краткая характеристика основных методов криптографии и стеганографии. Приведены примеры шифрования методами замены и перестановки, даны примеры формирования хеш-функций, использования электронной цифровой подписи, алгоритм асимметричного шифрования *RSA*.

В Главе 4 приведены примеры применения профессиональных программных и аппаратных средств защиты информации. Подробно рассмотрено использование пакетов *PGP Desktop* и *Steganos Security Suite*.

Если бы все люди соблюдали законы в сфере информационной безопасности, то все рассмотренные выше меры защиты оказались бы не нужны. Поэтому в Приложениях 1–4 даны основные выписки из дей-

ствующего законодательства РФ в области информационной безопасности. Приведен полный перечень действующих ГОСТ в этой сфере.

Существенную помощь в изучении современной информационной безопасности может оказать самостоятельная работа с имеющимися Интернет-ресурсами. Поскольку в рамках университетского курса невозможно изучить подробно все современные средства информационной безопасности, его следует рассматривать как введение для дальнейшего самостоятельного освоения.

Кроме этого, информационная безопасность – одна из самых быстроразвивающихся отраслей и, чтобы не отстать от прогресса, необходимо постоянно пополнять свои информационные знания в течение всего цикла трудовой деятельности современного специалиста с высшим образованием.

Среди множества Интернет-ресурсов рекомендуем выделить два, которые прямо предназначены для решения сформулированной выше проблемы и имеют ряд выгодных преимуществ перед другими ресурсами. Первый из них – это Интернет-университет информационных технологий (ИНТУИТ*) www.intuit.ru*.

ИНТУИТ учредил в 2003 году Анатолий Шкред, основатель и издатель целого ряда авторитетных периодических изданий, посвященных современным информационным технологиям. Основу обучения составляют курсы лекций с тестовыми заданиями в конце каждой лекции. Каждый курс проходит обязательную сертификацию учебно-методическими объединениями вузов (УМО) и имеет гриф «рекомендовано» или «допущено» для соответствующих специальностей вузов. Все курсы написаны в единой форме изложения, что существенно облегчает их изучение. Авторы курсов – ведущие российские и зарубежные специалисты в области информационных технологий.

Важным достоинством ИНТУИТа является наличие множества альтернативных курсов по одной тематике, что позволяет студенту выбирать того или иного автора курса, а сам ИНТУТ обеспечивает себе постоянное обновление изучаемого материала. На момент написания этого пособия в ИНТУИТе собрано более 450 курсов и их количество продолжает увеличиваться. В настоящем пособии даются ссылки на курсы ИНТУИТа по ходу изложения материала для дальнейшего углубленного самостоятельного изучения. По каждой лекции каждого курса выставляется отдельная оценка, которую можно наблюдать в зачетной книжке (рис. В.1).

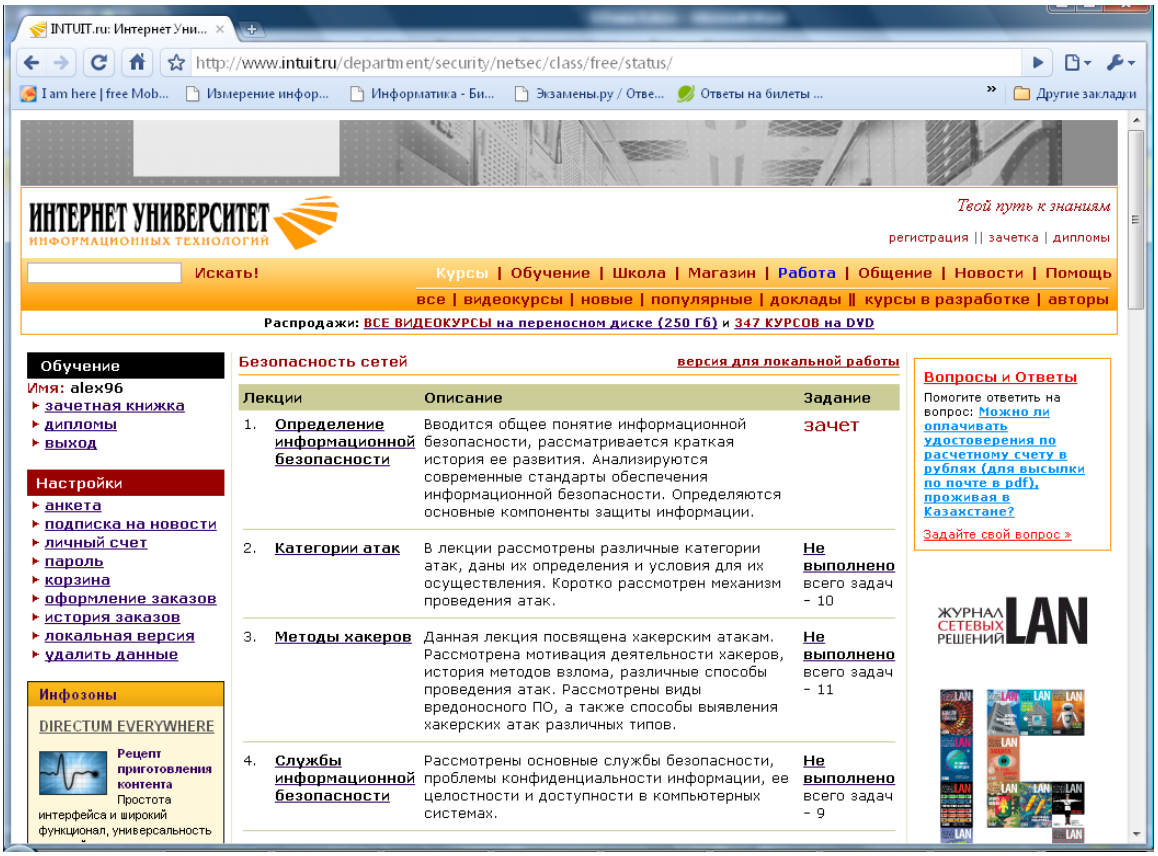


Рис. В.1. Вид зачетной книжки в Интернет-университете информационных технологий

Второй рекомендуемый Интернет-ресурс предназначен для читателей, желающих получать дополнительные знания самостоятельно на английском языке. Это так называемые «Открытые курсы» Массачусетского технологического института (МТИ) США (*http://ocw.mit.edu*). Ресурс содержит более 2000 курсов профессоров МТИ на английском языке и доступен через Интернет всем желающим (рис В.2). Часть курсов представлена и на некоторых других языках.

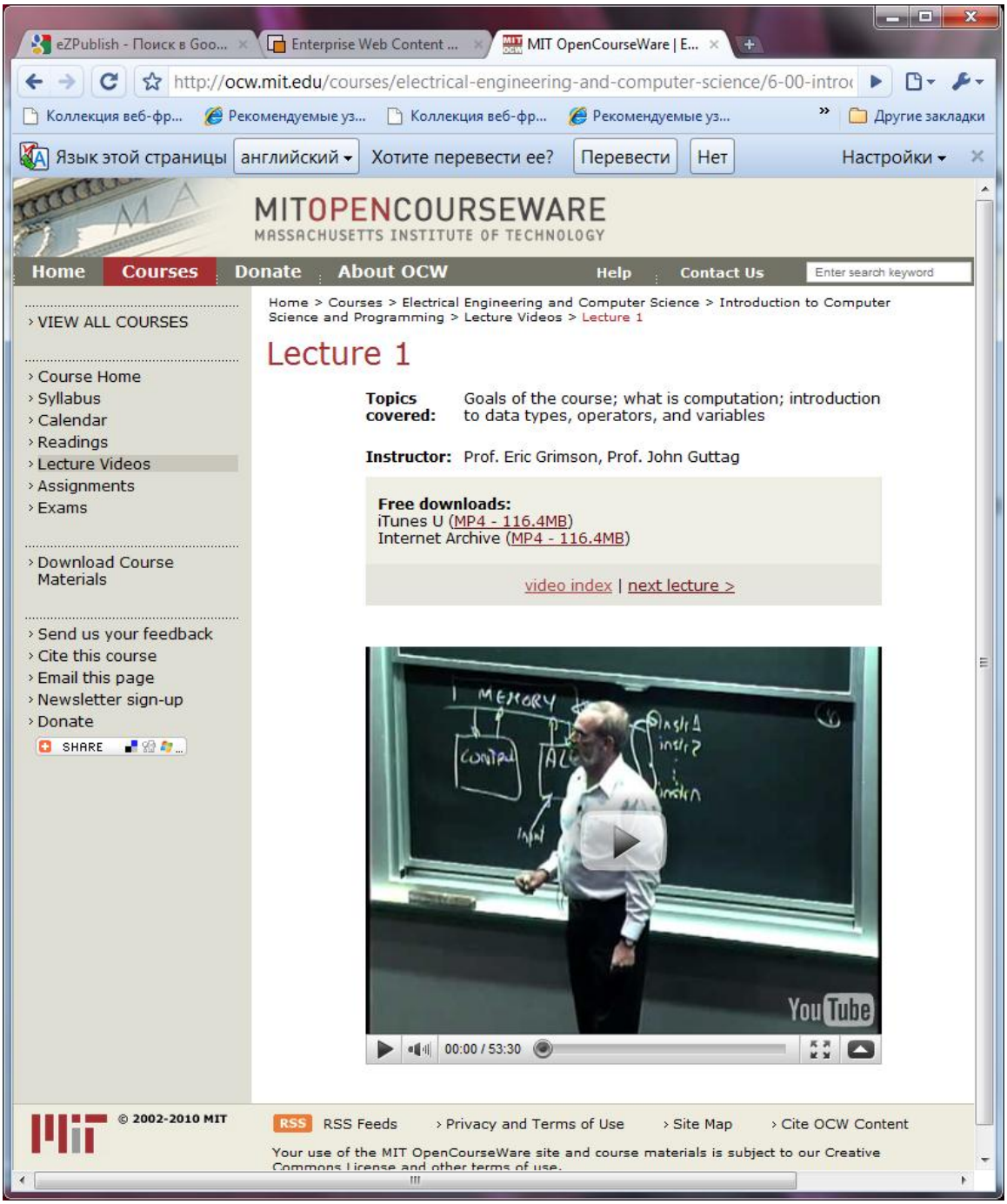


Рис. В.2. Пример видеолекции «Открытых курсов» Массачусетского технологического института США

В последнее время многие текстовые лекции обоих рекомендованных ресурсов пополнились видеолекциями и мультимедийными материалами. Кроме изучения содержания, эти курсы дают прекрасную возможность изучать речевой английский язык от его носителей.

Глава 1. Безопасность на уровне операционной системы и приложений

Наблюдаемая в последние годы тенденция криминализации индустрии вредоносного программного обеспечения привела к тому, что вопросы информационной безопасности стали актуальны не только для корпораций в целом, но и для рядовых пользователей. Если крупные корпоративные клиенты могут приобретать дорогостоящие технические средства информационной безопасности, то остальные в основном пользуются средствами безопасности на уровне операционной системы и приложений.

Производители операционных систем, естественно, учитывают их потребности. В настоящее время смена версии операционной системы и другого программного обеспечения массового использования производится в основном для усиления безопасности. Так было при выпуске *Windows Vista*, продолжилось при выпуске *Windows* 7, *Internet Explorer* 8, *Microsoft Office* 10 и т. д. Соответственно усложнились и доступные пользователю настройки безопасности, которые рассмотрены ниже.

1.1. Настройки безопасности операционной системы *Windows* 7

Поскольку эта операционная система является новейшей на момент написания пособия, рассмотрим настройки безопасности на ее примере. Основные доступные пользователю настройки безопасности можно найти через меню «Пуск»–«Панель управления»–«Администрирование» под заголовком «Локальная политика безопасности» (рис. 1.1–1.3).

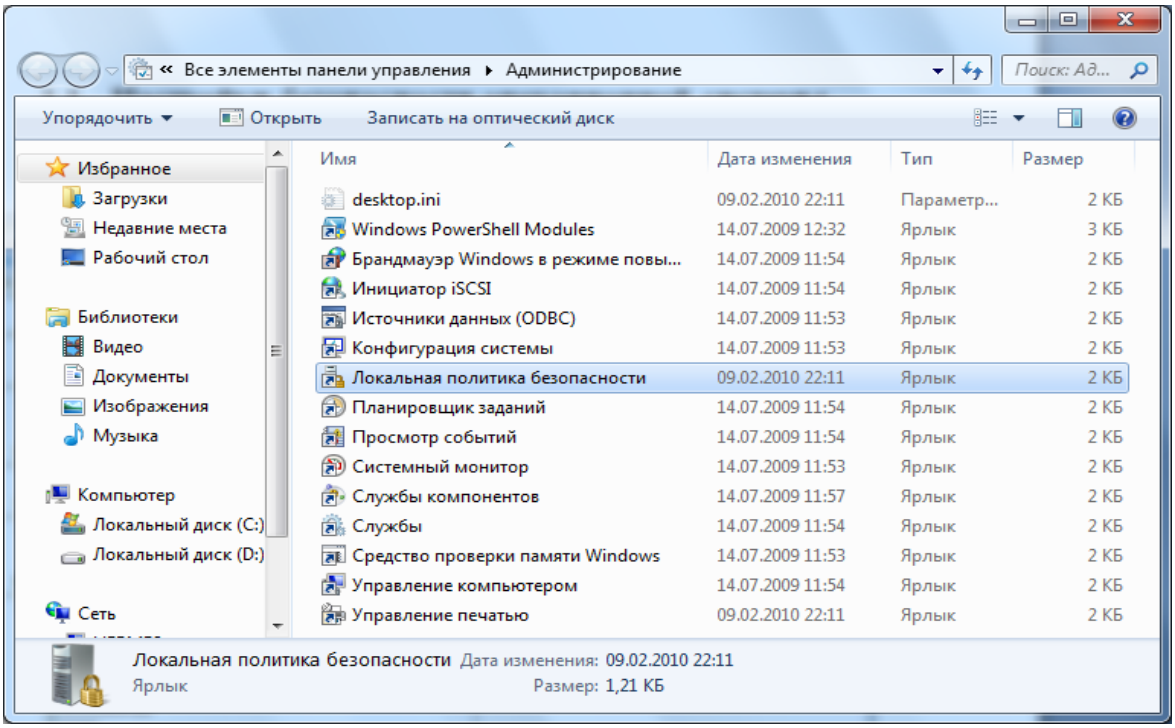


Рис. 1.1. Вход в настройки безопасности операционной системы Windows 7

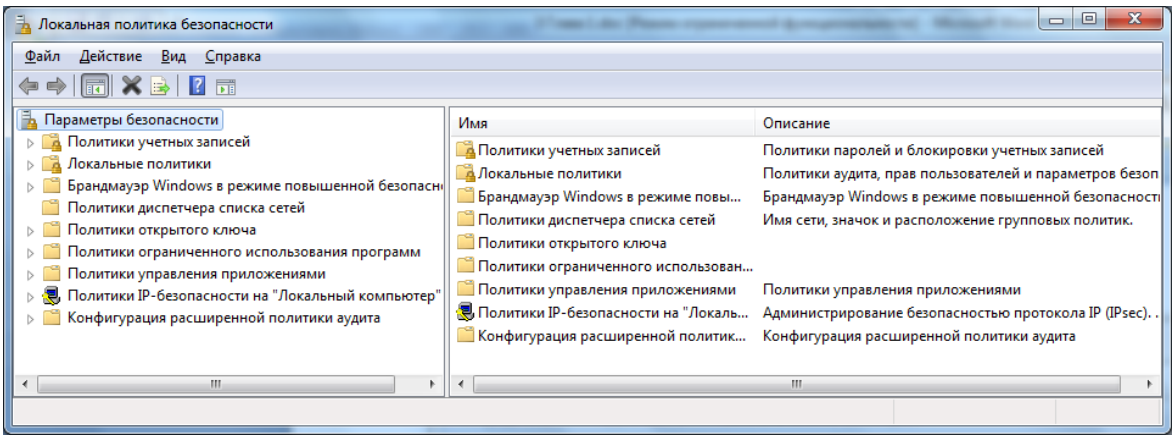


Рис. 1.2. Список политик безопасности операционной системы Windows 7

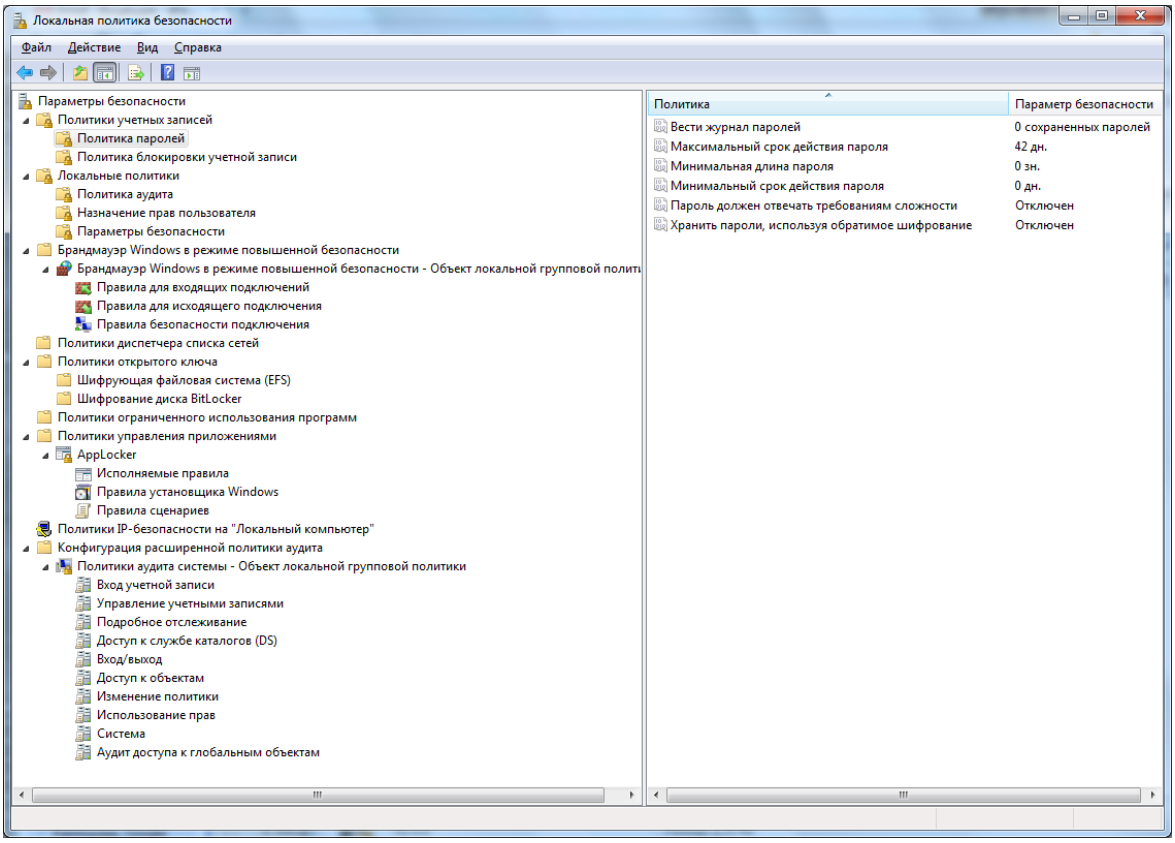


Рис. 1.3. Частично раскрытый список политик безопасности операционной системы Windows 7

Вне папки «Администрирование» панели управления есть еще доступные пользователю средства безопасности. Это «Брандмауэр *Windows*» и «Защитник *Windows*», которые предназначены для выполнения функций антивирусного программного обеспечения (ПО), если не установлено никакое другое антивирусное ПО (рис. 1.4, 1.5).

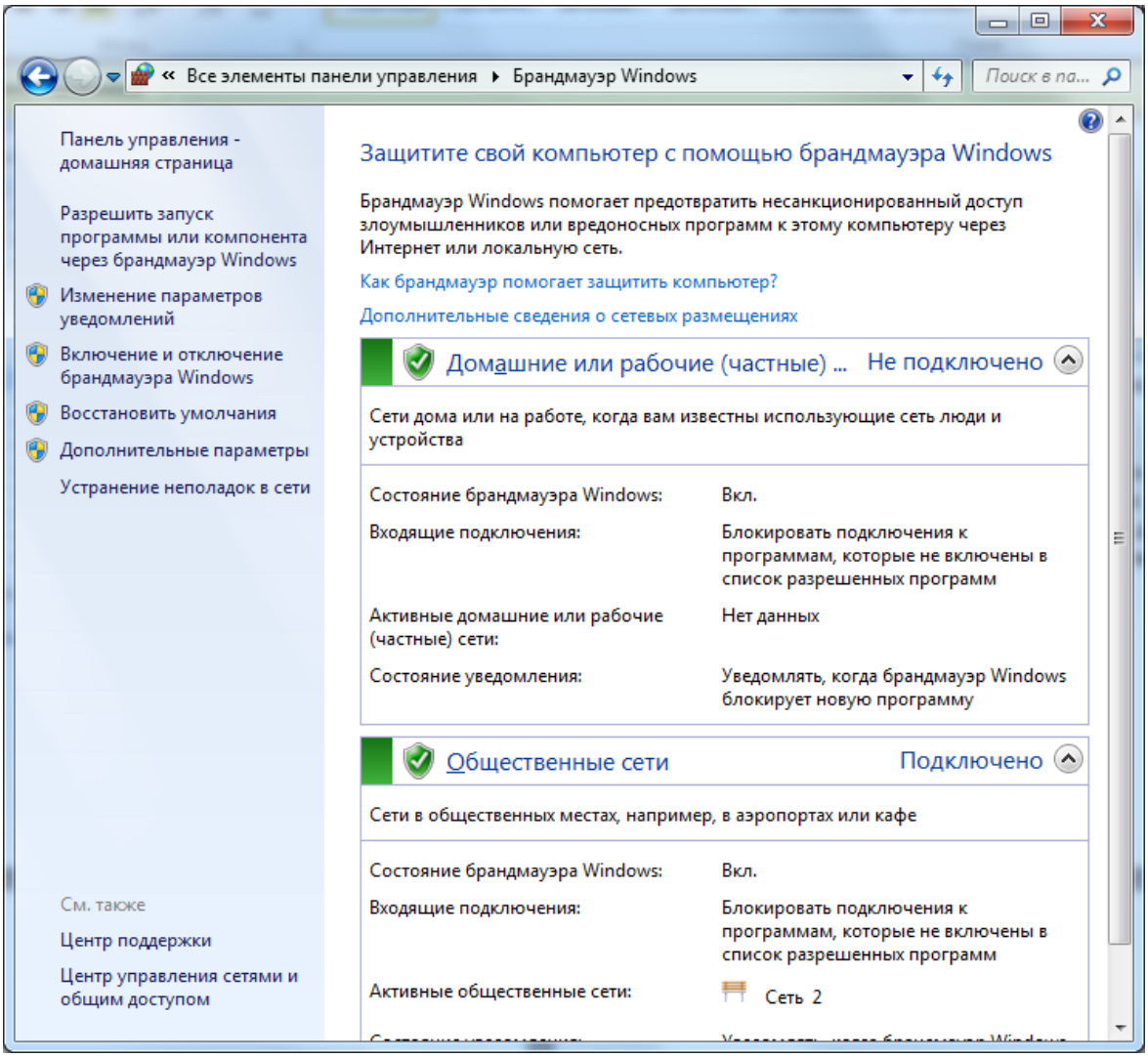


Рис. 1.4. Брандмауэр операционной системы Windows 7

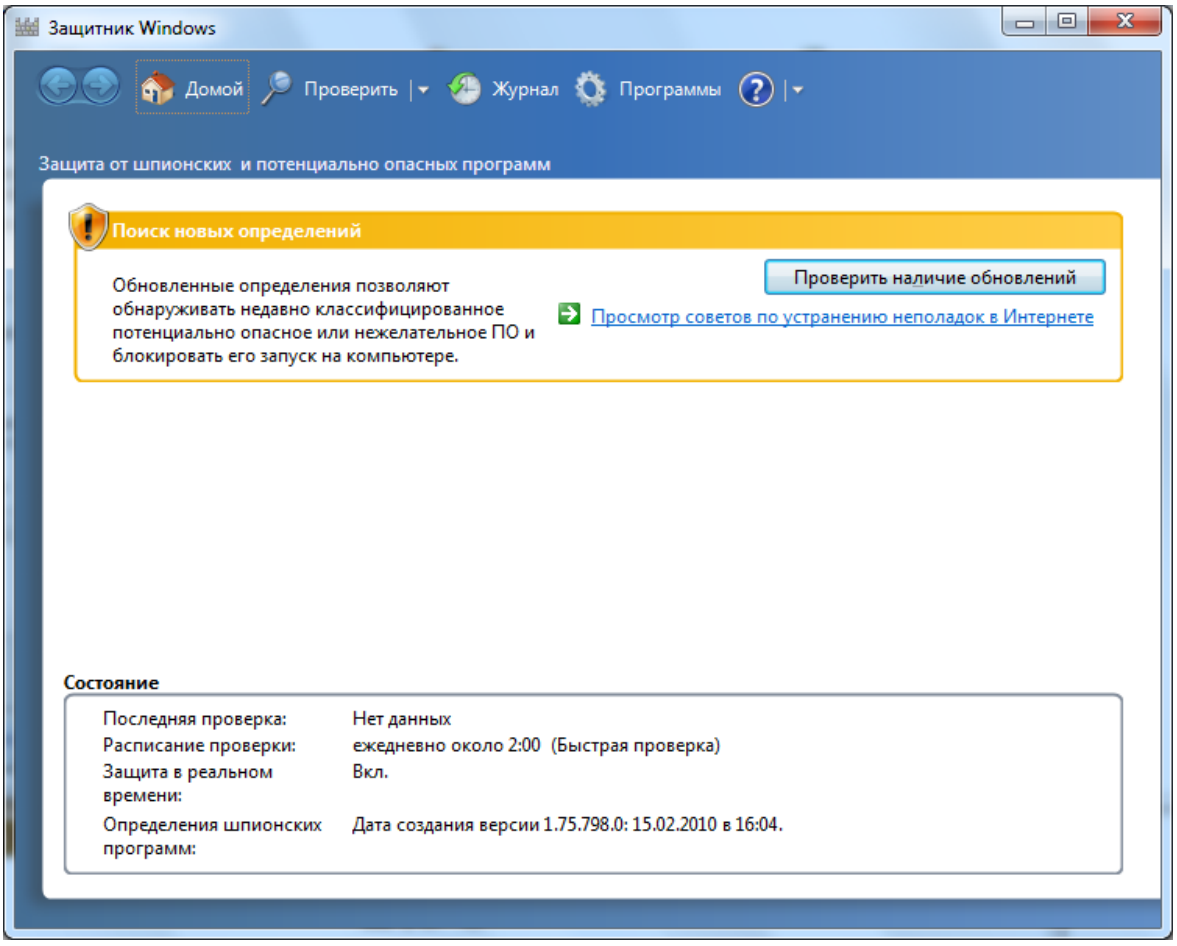


Рис. 1.5. Защитник операционной системы Windows 7

Кроме этих средств, есть еще средства администрирования учетных записей, которые позволяют защитить компьютер от внесения несанкционированных изменений (рис.1.6, 1.7).

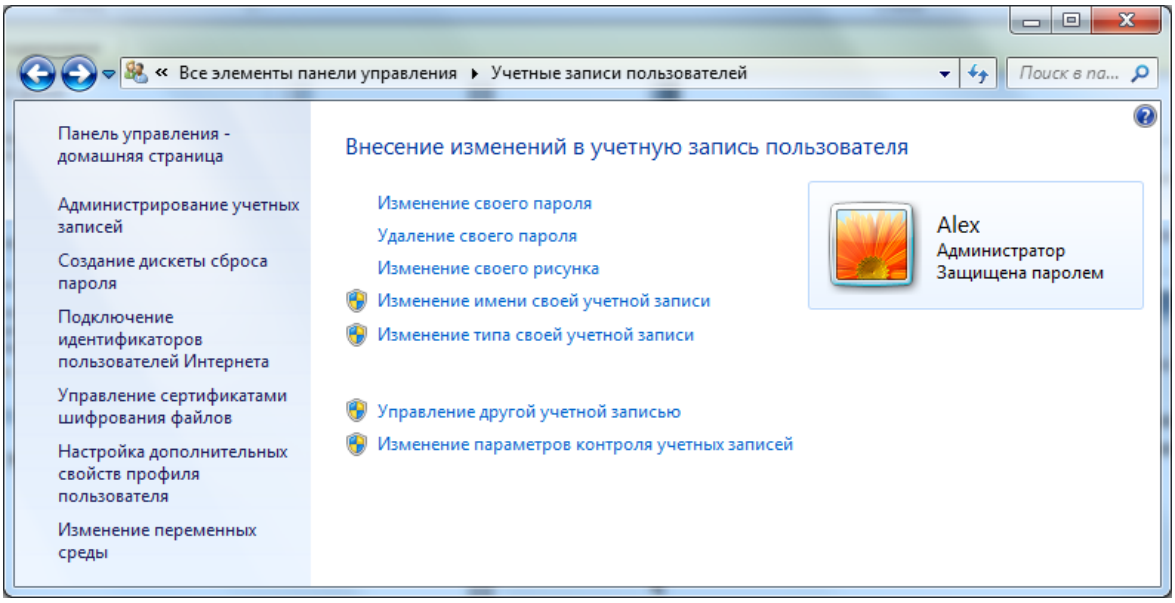


Рис. 1.6. Управление учетными записями операционной системы Windows 7

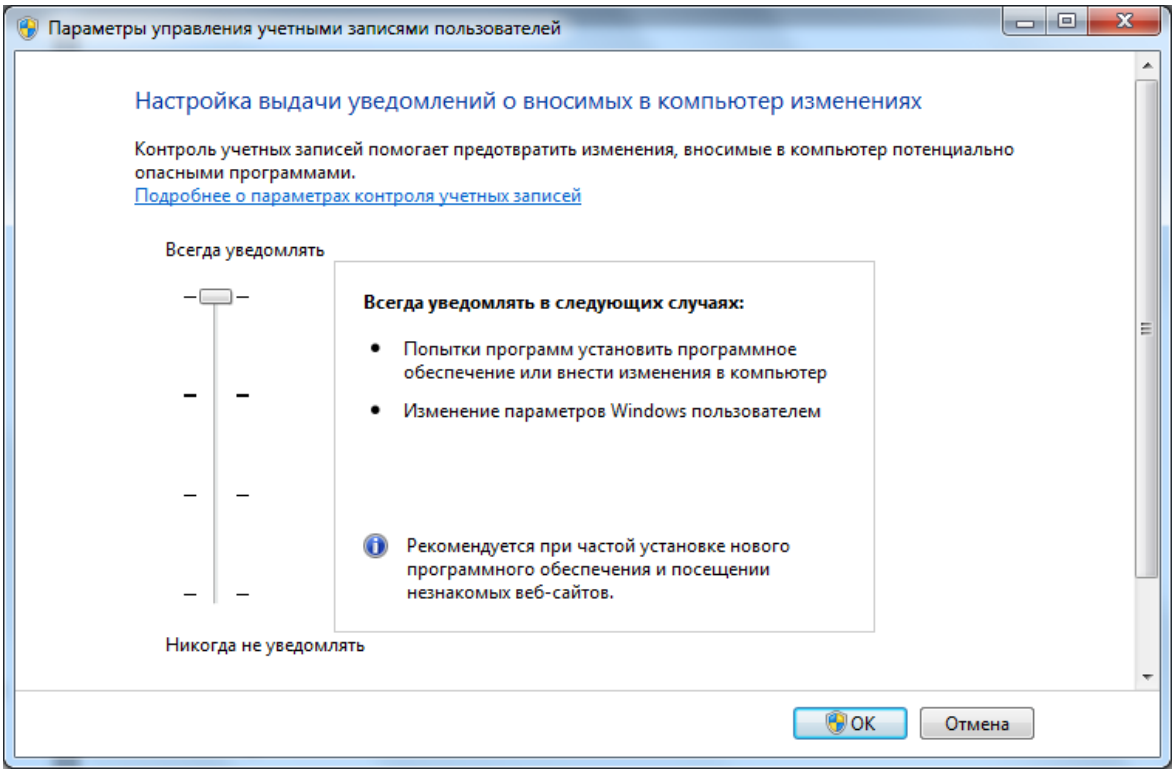


Рис. 1.7. Контроль учетных записей операционной системы Windows 7

Задание № 1

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политика учетных записей»

и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 2

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности»–«Локальные политики» средство «Политика аудита» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 3

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности»–«Локальные политики» средство «Назначение прав пользователей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 4

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности»–«Локальные политики» средство «Параметры безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 5

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Брандмауэр *Windows* в режиме повышенной безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 6

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политики диспетчера списка сетей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 7

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политики открытого ключа» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 8

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политики ограниченного использования программ» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 9

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политики управления приложениями» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 10

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Политики *IP*-безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 11

Открыть через «Панель управления»–«Администрирование»–«Локальная политика безопасности» средство «Конфигурации расширенной политики аудита» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 12

Открыть через «Панель управления»–«Все элементы панели управления» средство «Брандмауэр *Windows*» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

1.2. Настройки безопасности приложений *Microsoft Office*

В состав распространяемого бесплатно пакета *Microsoft Office* 2010 (*beta*) входят приложения: *Microsoft Access (конструктор и система управления базами данных), Microsoft Excel* (электронные таблицы), *Microsoft InfoPath Designer* (конструктор форм для сбора данных), *Microsoft InfoPath Filler* (средство для работы с формами данных), *Microsoft Office FrontPage* (конструктор веб-страниц), *Microsoft OneNote* (средство для сбора, организации и использования заметок) , *Microsoft Outlook* (средство для работы с электронной почтой), *Microsoft PowerPoint* (конструктор презентаций), *Microsoft Publisher* (автоматизация издательских работ), *Microsoft SharePoint Workspace* (средства для работы с контентом сайта *SharePoint*), *Microsoft Word* (приложение для работы с текстовыми документами). Также в его составе есть «Диспетчер рисунков», «Организатор клипов», «Средство создания цифровых сертификатов».

Пакет программ *Microsoft Office* 2010, как и предыдущие версии, содержит мощное встроенное инструментальное средство – объектно-ориентированный язык программирования *Visual Basic for Applications* (*VBA*). С помощью *VBA* можно создавать объекты, задавать и изменять свойства и методы объектов, подключать к ним соответствующий программный код, обращаться к объектам *Windows* и т. п. Программы, написанные на *VBA*, называют макросами. Они не хранятся отдельно, а являются встроенными в любой документ *Microsoft Office*.

Но вместе с большими функциональными возможностями это инструментальное средство несет и дополнительную угрозу информационной безопасности. Злоумышленники имеют возможность записать в макросе вредоносный код и распространять его вместе с документом *Microsoft Office*. Для такого вредоносного кода введен даже специальный термин – макровирус. Поэтому по умолчанию в *Microsoft Office* 2010 макросы отключены. Если пользователь открывает документ с присоединенным к нему макросом, то он получает предупреждение системы безопасности. Пользователь может включить выполнение макросов, если он уверен в их источнике. В противном случае запуск макросов приложением блокируется (рис. 1.8).

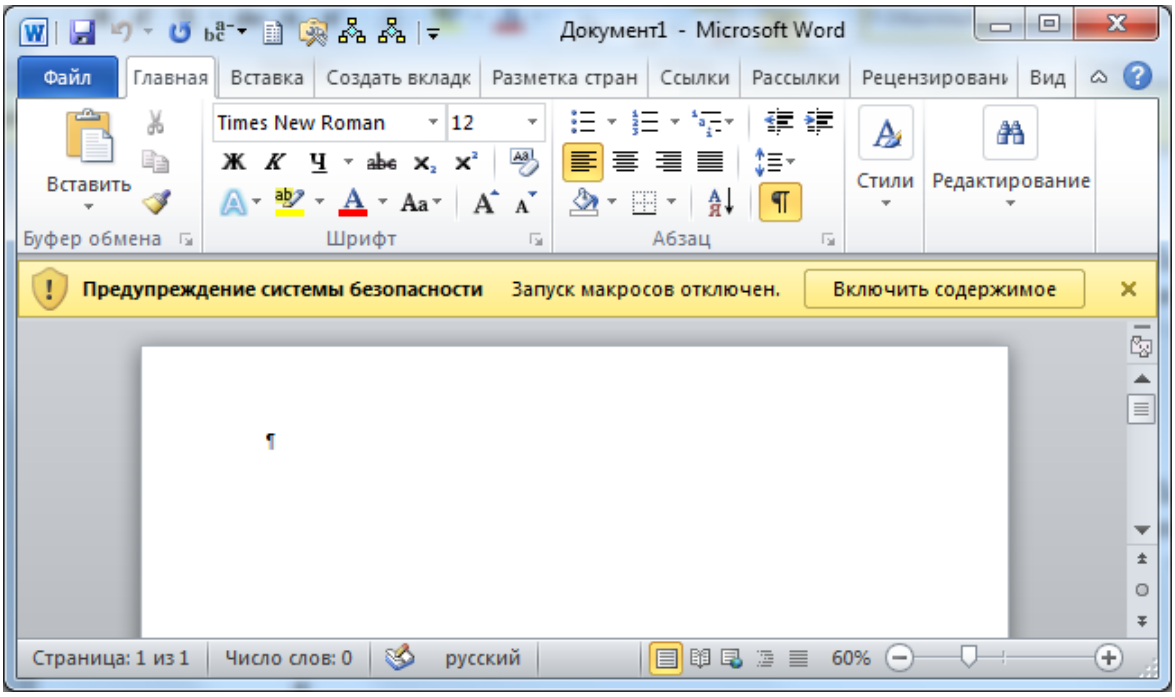


Рис. 1.8. Предупреждение системы безопасности при открытии документов, содержащих макросы

В приложениях *Microsoft Office* 2010 включена возможность создания цифровой подписи и цифрового сертификата макроса.

Получение цифрового сертификата для подписи

Цифровой сертификат можно получить в коммерческом центре сертификации (ЦС), у администратора безопасности локальной сети либо специалиста по информационным технологиям.

Дополнительные сведения о центрах сертификации, обслуживающих продукты Майкрософт, см. в списке участников программы корневых сертификатов *Microsoft* (на английском языке).

Создание сертификата с автоподписью

Windows Vista (*Windows* 7)**.**

1. Нажмите кнопку «Пуск» и выберите последовательно пункты «Все программы»–«*Microsoft Office*»–«Средства *Microsoft Office*»–«Цифровой сертификат для проектов *VBA*» («Средство создания цифровых сертификатов»).

2. Откроется диалоговое окно «Создание цифрового сертификата».

3. В поле «Имя сертификата» введите описательное имя сертификата.

4. Нажмите кнопку «ОК».

5. Когда появится сообщение «*SelfCert*: успех», нажмите кнопку «ОК» (рис 1.9).

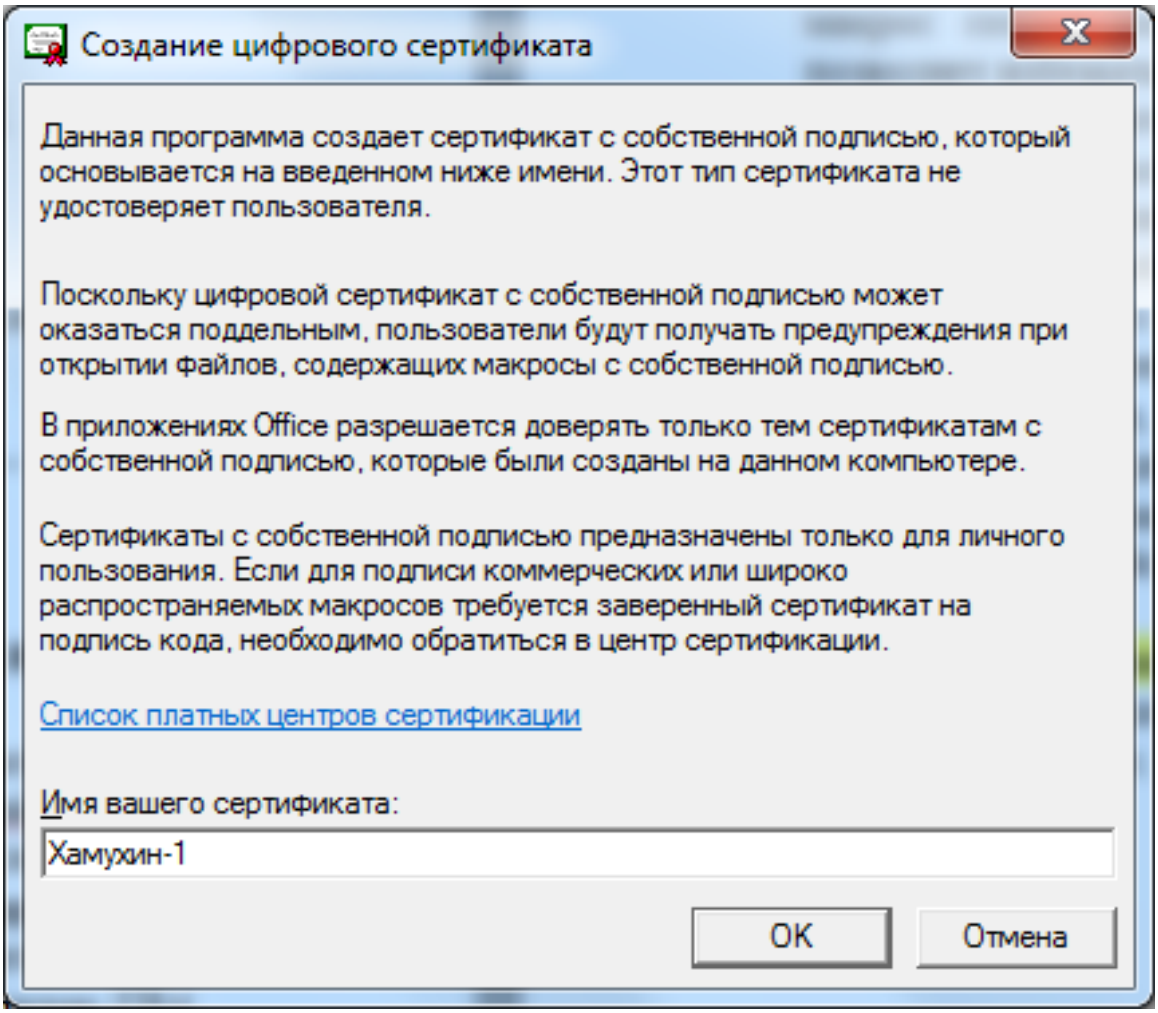


Рис. 1.9. Создание цифрового сертификата с автоподписью

Просмотр сертификата

Чтобы просмотреть хранилище личных сертификатов, выполните следующие действия.

1. Откройте обозреватель *Internet Explorer*.

2. В меню «Сервис» выберите «Свойства обозревателя», а затем – вкладку «Содержание».

3. Нажмите кнопку «Сертификаты» и перейдите на вкладку «Просмотр» (рис 1.10).

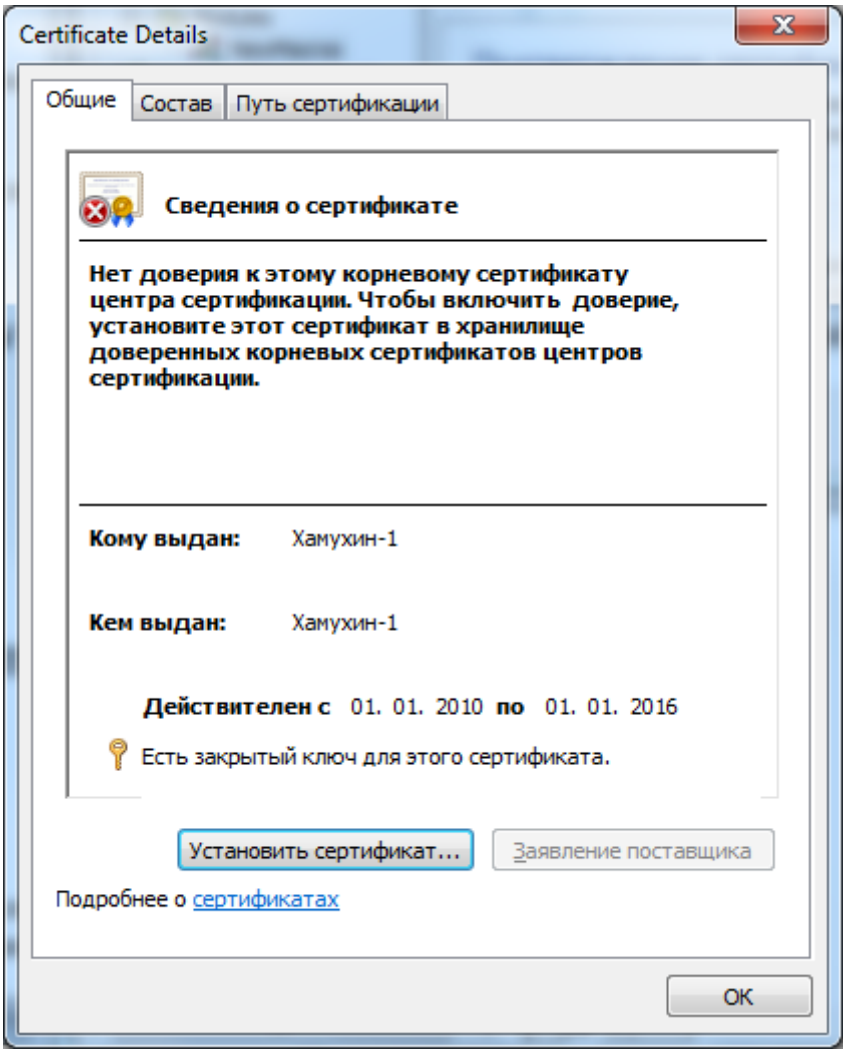


Рис. 1.10. Просмотр цифрового сертификата с автоподписью

Цифровая подпись макроса в *Excel, PowerPoint, Publisher, Visio* и *Word*

1. Откройте лист, содержащий макрос, который необходимо подписать.

2. На вкладке «Разработчик» в группе «Код» нажмите кнопку «*Visual Basic*».

Если вкладка «Разработчик» недоступна, необходимо выполнить следующие действия. Откройте вкладку «Файл». В разделе «Справка» выберите «Параметры». Нажмите «Настройка ленты». В списке «Настройка ленты» выберите пункт «Разработчик», а затем нажмите кнопку «ОК». В *Microsoft Office* 2010 в редактор *VBA* можно зайти че-

рез последовательность «Вид»–«Макросы»–«Запись макроса»–«Остановить запись»–«Макросы»–«Изменить».

3. В редакторе *Visual Basic* в меню «Сервис» («*Tools*») выберите пункт «Цифровая подпись» («*Digital Signature*»).

4. Откроется диалоговое окно «Цифровая подпись» («*Digital Signature*»).

5. Выберите сертификат и нажмите кнопку «ОК» (рис. 1.11).

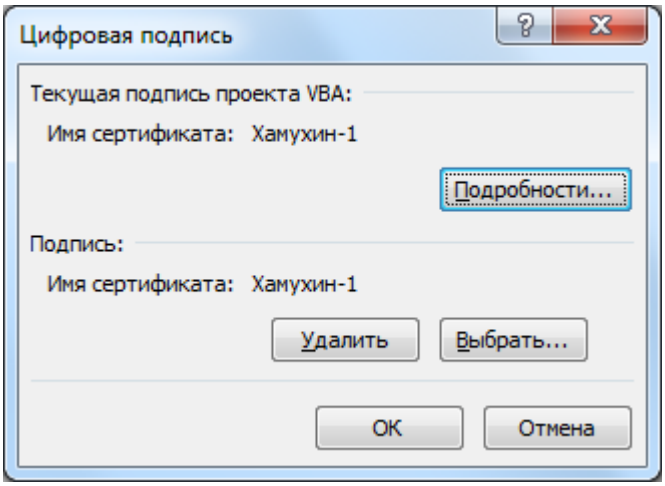


Рис. 1.11. Проверка цифрового сертификата макроса

Если цифровой сертификат не выбран или нужно использовать другой сертификат, нажмите кнопку «Выбрать», выберите сертификат и нажмите кнопку «ОК».

Макросы и *Microsoft Office*

Поскольку самостоятельно созданный цифровой сертификат не был выдан официальным центром сертификации, макросы, подписанные с использованием такого сертификата, называют **макросами с собственной подписью**. В *Microsoft Office* сертификаты с собственной подписью считаются надежными только на том компьютере, на котором они добавлены в персональную папку в хранилище «Сертификаты» – «текущий пользователь» (на английском языке).

Макросы рекомендуется подписывать после завершения всех проверок, когда продукт готов к распространению, так как любое изменение кода в подписанном макросе приводит к удалению цифровой подписи. Однако если на компьютере имеется действительный цифровой сертификат, который ранее использовался для подписи макросов, при сохранении макрос автоматически будет подписан заново.

Если требуется предотвратить случайное изменение пользователями макроса и нарушение цифровой подписи, то перед тем как подписать макрос, следует заблокировать его. Цифровая подпись показывает, что макрос не был изменен с момента добавления этой подписи, но не является подтверждением того факта, что макрос создан владельцем подписи. Таким образом, блокировка макроса не позволяет избежать замены цифровой подписи другой цифровой подписью.

Администратор сети может заново подписать шаблоны и надстройки, чтобы управлять запуском макросов на компьютерах пользователей. При создании надстроек, меняющих код макросов, нужно разработать способ проверки проекта на наличие цифровой подписи и, если проект подписан, выводить для пользователя предупреждение о последствиях внесения изменений.

При добавлении цифровой подписи к макросу необходимо также добавить отметку времени, чтобы пользователи могли проверить подпись даже после истечения срока действия сертификата, с помощью которого она была поставлена. Если подписать макрос без отметки времени, подпись будет действительна только в течение срока действия сертификата.

В приложениях *Microsoft Office* 2010 введена функция «Центр управления безопасностью», доступ к которой осуществляется через меню «Файл»–«Справка»–«Параметры» (рис. 1.12).

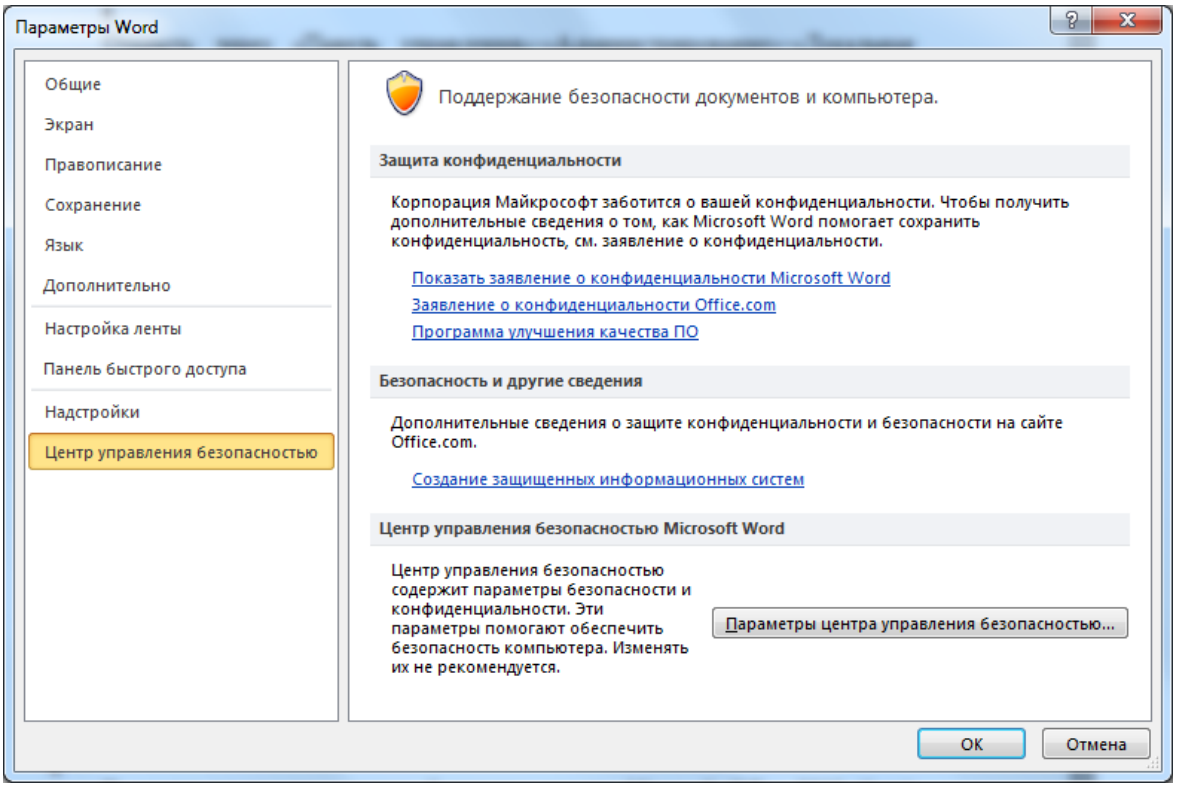


Рис. 1.12. Центр управления безопасностью приложений Microsoft Office 2010

Задание № 1

Создать цифровой сертификат с автоподписью, подписать им любой макрос (если отсутствует – создать), закрыть документ с сохранением, затем вновь открыть и проверить цифровой сертификат макроса. По ходу выполнения задания составить отчет с копиями окон.

Задание № 2

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Надежные издатели» и изучить его (*F*1). В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 3

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство

«Надежные расположения» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 4

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Надежные документы» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 5

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Надстройки» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 6

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Параметры *ActiveX*» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 7

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Параметры макросов» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 8

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Защищенный просмотр» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 9

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Панель сообщений» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 10

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Параметры блокировки файлов» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 11

Открыть через «Файл»–«Параметры»–«Центр управления безопасностью»–«Параметры центра управления безопасностью» средство «Параметры конфиденциальности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

1.3. Настройки безопасности Интернет-обозревателей

Программы, которые позволяют отображать на нашем экране содержимое сайтов сети Интернет, называются браузерами (обозревателями, Интернет-обозревателями). Программы, которые позволяют получать и отправлять электронную почту, называются почтовыми агентами. Исторически сложилось так, что эти программы распространяются совершенно бесплатно. В настоящее время многие компании выпускают браузеры не только для персональных компьютеров, но и для мобильных устройств с небольшим экраном.

По данным компании *Net Applications*, в августе 2009 года рыночная доля наиболее популярных браузеров составляла: *Internet Explorer* – ▼67,97 %, *Firefox* – ▲22,98 %, *Safari* – ▼4,07 %, *Google Chrome* – ▲2,84 %, *Opera* – ▲2,04 %, *Netscape* – ▼0,49 % . Направление треугольника показывает рост (▲) или снижение (▼) доли рынка по сравнению с предыдущим анализом.

Ниже приводятся особенности наиболее популярных обозревателей.

Internet Explorer

Этот браузер, выпускаемый знаменитой компанией *Microsoft* с 1995 г., еще недавно почти монопольно владел рынком благодаря тому, что компания встраивала его в операционную систему *Windows*. В период расцвета он занимал 95 % рынка. Но с 2003 г. его доля неуклонно снижается, особенно на европейском рынке. Этому способствовало 2 события. Компания *Netscape*, проигравшая «войну браузеров» в 90-е годы, уходя с рынка, опубликовала исходный код своего браузера. На его основе потом был создан браузер *Mozilla Firefox*. И второе событие – компания *Opera Software ASA* подала судебный иск против включения браузера *Internet Explorer* в операционную систему *Windows* и выиграла процесс. Теперь на территории стран Европейского союза *Windows* поставляется с возможностью деинсталляции (удаления) из нее браузера *Internet Explorer* (ранее такой возможности не было).

На момент написания книги последней версией браузера является *Internet Explorer* 8. Эта же версия вошла в состав операционной системы *Windows* 7, однако, в отличие от предыдущих версий, ее можно будет полностью удалить из системы. Также были выпущены дополнительные модификации браузера для других операционных систем. Это *Mobile Internet Explorer* (для *Windows CE* и *Windows Mobile*), *Internet Explorer* для *Mac* и *Internet Explorer* для *UNIX*.

Internet Explorer 7 имеет вкладки, блокировщик всплывающих окон, фишинг-фильтр, встроенный *RSS*-агрегатор, поддержку интернациональных доменных имён, средства групповой политики. Имеется и возможность автообновления через *Windows Update*. *Windows*-версия браузера основана на движке *Trident*, который поддерживает стандарты *HTML* 4.01, *CSS Level* 1, *XML* 1.0 и *DOM Level* 1 и частично *CSS Level* 2 и *DOM Level* 2. Также имеет возможность подключения расширений, что реализуется через объектную модель компонентов (*COM*).

Последняя версия называется «*Internet Explorer* 8 для разработчиков» (*IE*8). По сравнению с *IE*7, в *IE*8 повышена производительность, введено восстановление сессии после аварийного завершения, предусмотрен режим приватного просмотра страниц (без сохранения их в истории и кэширования), создан режим цветовой группировки вкладок (вкладки, открытые по ссылкам из других вкладок, выделяются одним цветом), добавлены ускорители, облегчающие работу с выделенными фрагментами текста и многое другое.

Firefox

Разрабатывается и свободно распространяется общественной некоммерческой организацией Европейского союза *Mozilla Foundation.* Бесплатно скачать этот браузер можно с русифицированного сайта производителя *http://www.mozilla-russia.org/*.

В браузере присутствуют вкладочный интерфейс, проверка орфографии, поиск по мере набора, «живые закладки», менеджер закачек, поисковая система. Новые функции можно добавлять при помощи небольших программ-расширений (плагинов). Именно обилие плагинов, отличающее этот браузер от других, является решающим преимуществом для пользователей, занимающихся конструированием собственных сайтов.

Firefox выпускается для *Microsoft Windows, BeOS, Mac OS X, Linux* и множества других *Unix*-подобных операционных систем. Код браузера распространяется под тройной лицензией *GPL/LGPL/MPL*.

Safari

Разработан всемирно известной корпорацией *Apple* (США) и входит в состав операционной системы *Mac OS X*. Также бесплатно распространяется для операционных систем семейства *Microsoft Windows*. Бесплатно скачать этот браузер можно с сайта производителя *http://www.apple.com/safari/* или с русскоязычного сайта *http://soft.softodrom.ru/ap/Apple-Safari-for-Windows-p*4300.

Браузер имеет интерфейс на основе вкладок, удобную систему закладок, блокировку всплывающих окон, *RSS*-ридер, функцию автозаполнения веб-форм и многое другое, включая средства веб-разработки. Поддерживается расширение плагинами. Интерфейс многоязычный.

Позиционируется как самый быстрый браузер в мире. Но с выходом браузера от бурно прогрессирующей компании *Google*, позиционирующей его тоже как самый быстрый, в этой области ожидается конкуренция, несомненно, выгодная для пользователей.

При выборе этого браузера следует учитывать, что изначально он разрабатывался под компьютеры фирмы *Apple* и на них он работает безукоризненно. На ПК с операционной системой *Windows* или другими операционными системами этот браузер работает иногда некорректно.

Google Chrome

Google Chrome – браузер с открытым исходным кодом, разрабатываемый компанией *Google* и использующий для отображения веб-страниц движок *WebKit*, разработанный для браузера *Safari*. Первая публичная бета-версия для *Microsoft Windows* вышла 2 сентября 2008 года, а первая стабильная – 11 декабря 2008 года. В отличие от многих других браузеров, в *Chrome* каждая вкладка является отдельным процессом. В случае если процесс обработки содержимого вкладки зависнет, его можно будет завершить без риска потери данных других вкладок.

В *Chrome* для обработки сценариев *JavaScript* используется движок *V*8. Согласно тесту скорости, время выполнения скриптов в *Chrome* 2.0.172.33 в 2,1 раза больше времени выполнения скриптов в *Safari* 4.0.2 (530.19.1). Однако у браузеров *Firefox, Opera* и *Internet Explorer* этот показатель ещё хуже (*Firefox* 3.5 в 2,2 раза медленнее *Safari* 4.0.2, *Opera* 9.64 (10487) – в 2,6 раза, *IE*8 – в 4,6).

Как и другие браузеры, *Chrome* содержит несколько дополнительных *about: URI.*

Адресная строка браузера, которая называется *Omnibox*, поддерживает автодополнение, которое учитывает такие параметры как:

- популярность сайтов (например, при вводе в адресную строку слова «яндекс» браузер автоматически предложит вариант «*www.yandex.ru*»);
- частоту встречи слова на сайтах (например, при вводе слов «райффайзен банк» одним из вариантов будет неочевидное «*aval.ua*» – заголовок «Райффайзен Банк Аваль»);
- историю посещений сайтов (посещённые ранее сайты индексируются так же, как и сайты предыдущих категорий и, предположительно, обладают большим приоритетом);
- наличие в закладках сайтов с таким же словом в названии сайта или в адресе сайта.

Самое примечательное свойство адресной строки – *Omnibox* перенаправляет в поисковую систему *Google* в том случае, если адрес не соответствует правилам написания *URL*. К примеру, не содержит точек, имени протокола, косых черт, содержит пробелы в начале адреса и т. д.

Кроме самого высокоскоростного браузера, компания *Google* предоставляет бесплатные услуги электронной почты (*http://mail.google.com*), замечательные тем, что размер предоставляемого почтового ящика для каждого пользователя является самым боль-

шим из всех аналогичных сервисов. В момент написания книги это более 7 Гбайт и имеется тенденция к увеличению этого объема. Этот сервис имеет также встроенный чат, видеочат, онлайн календарь-органайзер с напоминаниями предстоящих событий в виде всплывающих окон и СМС, просмотр фото и видео в почте и многое другое.

Opera

Браузеры под этой торговой маркой выпускает компания *Opera Software ASA* (Норвегия). Загрузить бесплатно продукты этой компании можно с сайта *http://www.opera.com/*.

Компания *Opera Softwar*е позиционирует *Opera* как «самый быстрый браузер на Земле» («*the fastest browser on Earth*»). Независимые проверки показали, что *Opera* 9.01 быстрее других браузеров в четырёх тестах из семи на *Microsoft Windows* и *Mac OS X* и в трёх из семи на *Linux*. Самой сильной стороной *Opera* является работа со скриптами *JavaScript*: примерно вдвое быстрее, чем у других браузеров.

Кроме того, *Opera* начинает отображать содержимое страницы до полной её загрузки, что также экономит время пользователя, особенно при медленном соединении и большом количестве внедрённых объектов.

В *Opera* встроен *TDI*-интерфейс, настраивается блокировка всплывающих окон, есть защита от мошенничества, менеджер закачек, *BitTorrent*-клиент, меню поиска, *RSS*-агрегатор. Также в пакет входит почтовый клиент *Opera Mail* и клиент для *IRC*-сетей.

Одна из особенностей браузера – возможность быстрого перехода к наиболее часто посещаемым страницам (*Speed Dial* – «быстрый набор» или «экспресс-панель»). Пользователь может задать адреса веб-страниц в девяти слотах и, после открытия пустой вкладки, на ней будут отображены по умолчанию 9 (3×3) ячеек, в каждой из которых – уменьшенная копия заданной страницы. Эта опция значительно облегчает навигацию между веб-сайтами.

Opera поддерживает так называемые виджеты (*Opera Widgets*) – маленькие веб-приложения, которые можно запустить из среды браузера. Среди прочих существует «*User JavaScript*» – диалект скриптового языка, позволяющего пользователю редактировать скрипты на веб-страницах и добавлять новые. Готовые скрипты можно скачать на сайте *UserJS.org*. Третий способ расширения возможностей браузера – подключение плагинов, меняющих внешний вид браузера или добавляющих к нему новые функции. В то же время, использование плагинов

ограничено. К недостаткам следует отнести то, что можно подключать только плагины, одобренные и распространяемые *Opera Software*. Хотя в некоторых других браузерах есть возможность устанавливать плагины любых разработчиков.

Мировую популярность компания завоевала с помощью браузера для мобильных устройств. *Opera Mobile* появился в 2000 году, став первым мобильным браузером, открывшим полноценный Интернет на экранах мобильных телефонов. С 2004 года он был установлен на 100 миллионах телефонов. *Opera Mobile* отвечает запросам глобального мобильного Интернет-сообщества. Первая бета-версия *Opera Mobile* 9.7 обладает улучшенной производительностью, новым пользовательским интерфейсом и инструментом для разработчиков *Opera Dragonfly*. *Opera Mobile* – законодатель мобильного интернета, поддерживающий новейшие технологии и ставший общепризнанным эталоном отрасли. Сегодня компания *Opera* продолжает расширять возможности мобильного Интернета, выпуская обновленные и усовершенствованные продукты.

Netscape Navigator

Этот когда-то очень популярный браузер выпускался компанией *Netscape Communications* (США) с 1994 по 2007 год. Он был первым в мире браузером с графическим интерфейсом и сначала выпускался под названием *Mozaic*.

Если ранее системой Интернет пользовались только профессионалы, владеющие языком команд, то этот браузер сделал Интернет доступным всем. Браузер имел простой и понятный интерфейс, не требующий от пользователя знания языков программирования. Можно считать, что этот браузер совершил своего рода техническую революцию. Последние его версии выпускались на основе движка браузера *Mozilla Firefox*.

Файлы *Cookie*

К сожалению, вместе с полезной информацией через все эти программы-обозреватели к нам попадает и бесполезная информация, отнимающая у нас время (спам), и вредоносное ПО, которое может блокировать всю работу. Поэтому важно владеть настройками безопасности этих программ и понимать механизм проникновения нежелательного ПО в наш компьютер.

Одной из главных опасностей при работе с любым обозревателем являются файлы *Cookie*, которые *Windows* разрешает сохранять на диске. Вместе с ними на компьютер могут попасть и вирусы. Веб-узлы используют файлы *Cookie* для индивидуального обслуживания пользователей и сбора сведений о посещаемости веб-узла. Многие веб-узлы используют эти файлы для сохранения информации, обеспечивающей взаимосвязь различных разделов узла, например, корзины или пользовательских страниц.

Файлы *Cookie* надежных веб-узлов делают более комфортным просмотр страниц узла благодаря сведениям о личных предпочтениях пользователя или возможности автоматического входа на веб-узел. Однако некоторые файлы *Cookie*, например, файлы, сохраненные рекламными объявлениями, могут поставить под угрозу конфиденциальность пользователя, отслеживая посещаемые веб-узлы.

Следует ли блокировать все файлы *Cookie*? Не всегда. Блокировка всех файлов *Cookie* обеспечивает соблюдение конфиденциальности, однако ограничивает возможности некоторых веб-узлов. Рекомендуется тщательно выбирать веб-узлы, которым будет разрешено сохранять файлы *Cookie*. Можно начать с блокировки всех файлов *Cookie*, а затем по мере необходимости разрешать их надежным веб-узлам.

Чтобы удалить файлы *Cookie*, выполните следующие действия.

- Откройте *Internet Explorer*.
- Нажмите кнопку «Сервис» и выберите пункт «Свойства» веб-обозревателя.
- На вкладке «Общие» в «История просмотра» щелкните «Удалить».
- Установите флажок «Файлы *Cookie*» и нажмите кнопку «Удалить» (если флажок еще не установлен).
- Снимите или установите флажки для других параметров, которые также требуется удалить.

Если необходимо сохранить файлы *Cookie* для некоторых элементов папки «Избранное», установите флажок «Сохранять данные избранных веб-узлов».

Следует отметить, что удаление всех файлов *Cookie* может привести к неправильной работе некоторых веб-страниц. Временные (или сеансовые) файлы *Cookie* удаляются с компьютера после закрытия *Internet Explorer*. Веб-узлы используют их для сохранения временной информации, например, товаров в корзине клиента Интернет-магазина.

Постоянные (или сохраненные) файлы *Cookie* остаются на компьютере после закрытия *Internet Explorer*. Веб-узлы используют их для со-

хранения информации, например, имени пользователя и пароля, чтобы пользователю не приходилось заново входить в систему при каждом посещении веб-узла. Постоянные файлы *Cookie* могут храниться на компьютере в течение нескольких дней, месяцев или даже лет.

Основные файлы *Cookie* сохраняются просматриваемым веб-узлом и могут быть как постоянными, так и временными. Веб-узлы могут использовать эти файлы *Cookie* для сохранения сведений, которые понадобятся при следующем визите пользователя на данный узел.

Сторонние файлы *Cookie* сохраняются рекламными компонентами (в виде всплывающих окон или рекламных объявлений) на просматриваемом веб-узле. Веб-узлы часто используют эти файлы *Cookie* для сбора сведений о посещаемости веб-узлов в маркетинговых целях.

Internet Explorer предоставляет много разных способов управления файлами *Cookie*, сохраненными на компьютере. Можно заблокировать или разрешить все файлы *Cookie* либо выбрать определенные веб-узлы, с которых вы разрешите принимать файлы *Cookie*. При изменениях такого рода те файлы *Cookie*, которые уже сохранены на компьютере, не будут затронуты. По этой причине может потребоваться удалить файлы *Cookie*, уже сохраненные на компьютере, прежде чем выполнять следующие шаги.

Блокирование и разрешение всех файлов *Cookie*

1. Откройте *Internet Explorer*.
2. Нажмите кнопку «Сервис» и затем щелкните «Свойства» веб-обозревателя.
3. Щелкните вкладку «Конфиденциальность» и затем в меню «Настройка» сдвиньте ползунок вверх, чтобы блокировать все *Cookie*, или вниз, чтобы все разрешить, и нажмите кнопку ОК (рис. 1.13).

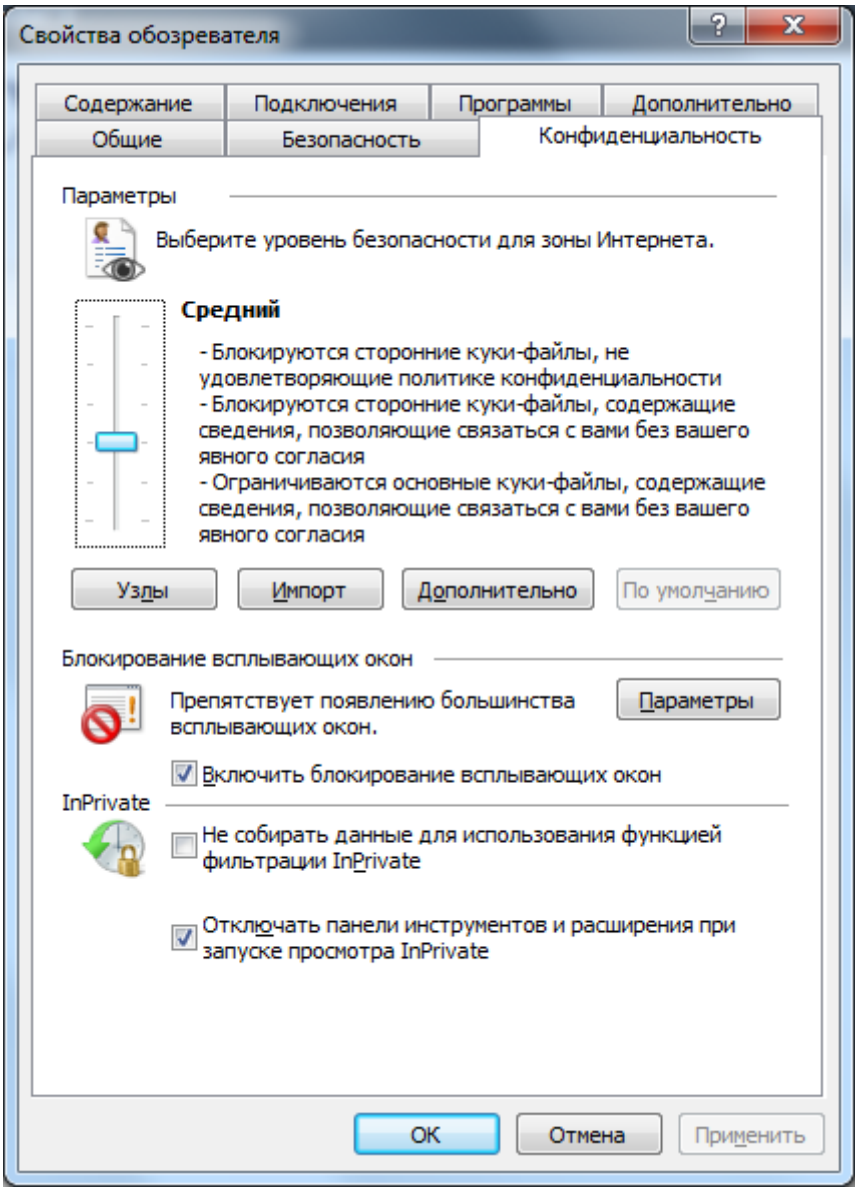


Рис. 1.13. Блокирование файлов Cookie

Еще раз напомним, что блокирование файлов *Cookie* может привести к неправильному отображению некоторых веб-страниц.

Блокирование и разрешение файлов *Cookie* в зависимости от их типа

Вместо того, чтобы выбирать конкретные веб-узлы для их блокировки или разрешения, можно указать общие типы файлов *Cookie*, которые являются приемлемыми. Например, можно разрешить *Cookie* с веб-узлов, имеющих политики конфиденциальности, или блокировать

Cookie с тех узлов, которые сохраняют личные сведения без вашего согласия.

1. Откройте *Internet Explorer*.

2. Нажмите кнопку «Сервис» и выберите пункт «Свойства» веб-обозревателя.

3. Щелкните вкладку «Конфиденциальность», установите ползунок на нужный уровень конфиденциальности и нажмите кнопку ОК.

При перемещении ползунка *Internet Explorer* дает описание тех типов файлов *Cookie*, которые заблокированы или разрешены на данном уровне конфиденциальности.

Блокирование или разрешение файлов *Cookie* с конкретных веб-узлов

1. Откройте *Internet Explorer*.

2. Нажмите кнопку «Сервис» и выберите пункт «Свойства» веб-обозревателя.

3. Щелкните вкладку «Конфиденциальность» и переместите ползунок в положение между верхом и низом так, чтобы не блокировать и не разрешать все файлы *Cookie*.

4. Щелкните «Узлы».

5. В поле «Адрес» веб-узла введите адрес веб-узла и щелкните «Блокировать» или «Разрешить». При вводе будет отображаться список веб-страниц, которые Вы уже посетили. Можно щелкнуть элемент списка, и он будет отображен в поле «Адрес» веб-узла.

6. Повторите шаг 5 для каждого веб-узла, который нужно блокировать или разрешить. Закончив, нажмите кнопку ОК.

7. Верните ползунок в первоначальное положение и нажмите кнопку ОК.

Кроме блокирования файлов *Cookie* почти все обозреватели имеют еще множество настроек безопасности, которые необходимо изучить и использовать на практике (рис.1.14).

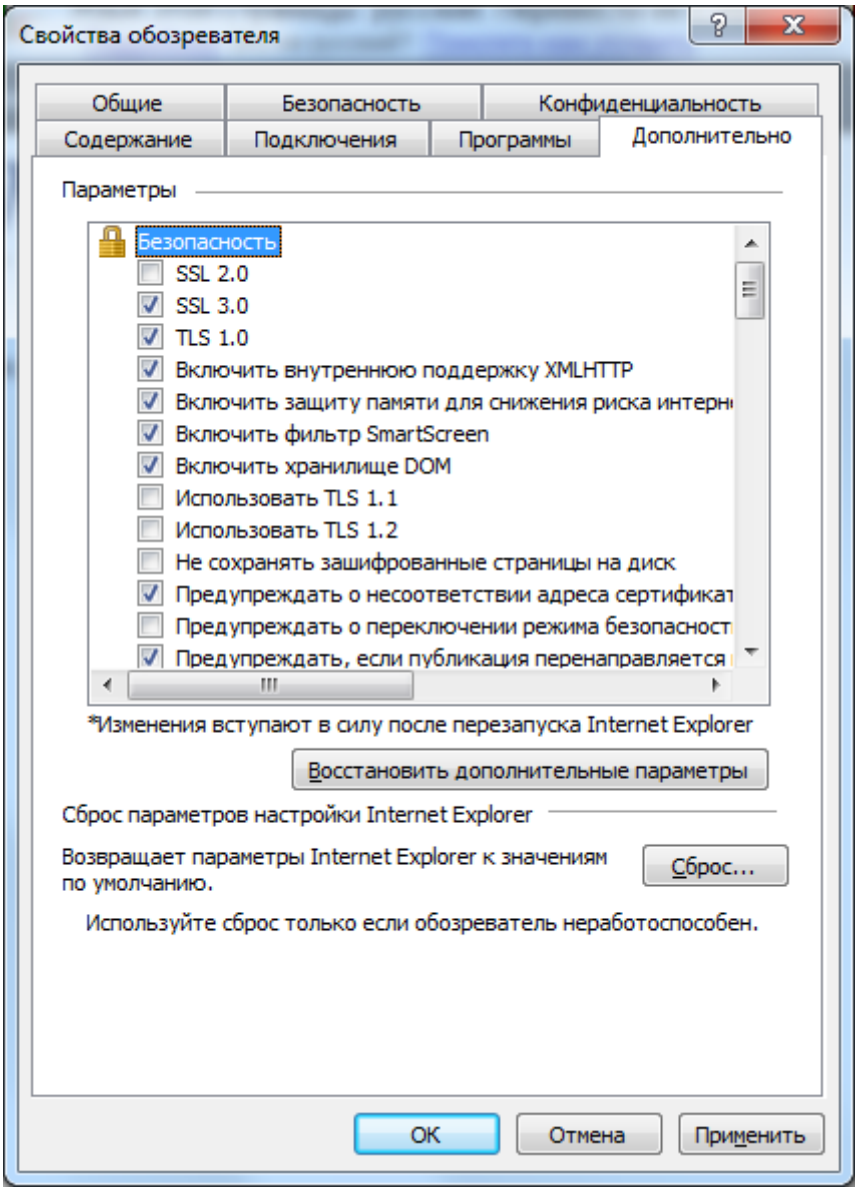


Рис. 1.14. Дополнительные настройки безопасности обозревателя Internet Explorer

Задание № 1

Открыть в *Internet Explorer* на вкладке «Безопасность» режим «Просмотр *InPrivate*» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 2

Открыть в *Internet Explorer* на вкладке «Безопасность» режим «Удалить журнал обозревателя» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 3

Открыть в *Internet Explorer* на вкладке «Безопасность» режим «Политика конфиденциальности веб-страницы» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 4

Открыть в *Internet Explorer* на вкладке «Безопасность» режим «Параметры фильтрации *InPrivate*» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 5

Открыть в *Internet Explorer* на вкладке «Безопасность» режим «Фильтр *SmartScreen*» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 6

Открыть в *Internet Explorer* через «Сервис»–«Свойства обозревателя» вкладку «Общие» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 7

Открыть в *Internet Explorer* через «Сервис»–«Свойства обозревателя» вкладку «Безопасность» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 8

Открыть в *Internet Explorer* через «Сервис»–«Свойства обозревателя» вкладку «Конфиденциальность» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание № 9

Открыть в *Internet Explorer* через «Сервис»–«Свойства обозревателя» вкладку «Содержание» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Задание №10

Открыть в *Internet Explorer* через «Сервис»–«Свойства обозревателя» вкладку «Дополнительно» и изучить ее в части безопасности. В отчете перечислить возможные настройки и назначение этого средства безопасности.

Глава 2. Антивирусное программное обеспечение

Система Интернет, обеспечившая легкое и доступное перемещение файлов по всему миру, привлекает к себе внимание и злоумышленников, создающих вредоносные программы (компьютерные вирусы). Но распространителями этих вирусов могут быть и простые пользователи, которые не имеют знаний и специальных программ для обнаружения вредоносного программного обеспечения или просто пренебрегают мерами безопасности. Чтобы осознанно применять эти меры безопасности, нужно знать это вредоносное ПО и к каким последствиям оно приводит.

2.1. Классификация вредоносного ПО

К вредоносному ПО относятся программы, получившие такие названия, как: сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и пр. Все они наносят либо заведомый вред компьютеру, на котором запускаются на выполнение, либо наносят вред другим компьютерам в сети, либо выполняют другие несанкционированные действия. К таким действиям, не наносящим прямого вреда, можно отнести рассылку спама, назойливую рекламу, передачу конфиденциальной информации пользователя злоумышленнику. Рассмотрим наиболее часто встречающиеся вредоносные программы.

Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (*P2P*) и *IRC*-сети (групповой чат), *LAN* (локальные сети), сети обмена данными между мобильными устройствами (смартфонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или *FTP*-ресурсе в *ICQ*- и *IRC*-сообщениях, файл в каталоге обмена *P2P* и т. д.

Некоторые черви (так называемые «безфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в настройках безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

Классические компьютерные вирусы

К данной категории относятся программы, которые дописывают свой код в тело какой-либо известной программы. Обычно это файлы типа *exe*, *com*, *bat*. Получив управление, классические вирусы могут не сразу наносить вред, а выдерживают некоторое время, которое называют периодом латентности.

Например, известный вирус *CIN* (Чернобыль) срабатывает только в годовщину крупнейшей аварии на Чернобыльской АЭС – 26 апреля. Хотя создана его разновидность, которая срабатывает 26 числа каждого месяца. В первую очередь такие программы распространяют свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера;
- нанесения вреда после истечения периода латентности.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный файл по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;

- пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например, бэкдор-процедуру (скрытное удаленное управление компьютером) или троянскую компоненту (см. далее).

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и передача ее злоумышленнику, внедрение другого вредоносного ПО и др. Они, как правило, не содержат механизма саморазмножения.

Часто троянские программы не нарушают работоспособность заражённого компьютера, а используют его ресурсы в злоумышленных целях. Троян – это не вирус в его классическом понимании, а маленькая программка, которую еще называют «Утилита удаленного администрирования компьютером». Трояны делятся на три типа: ***Back Door***, ***e-mail (Mail sender)***, ***Key Logger.***

Back Door

Сейчас это самый распространенный вид троянов. Состоит из клиента и сервера. Сервер отправляется жертве и в дальнейшем вся работа ведется по принципу клиент-сервер, т. е. злоумышленник посылает команды через клиента, а сервер их выполняет. После подключения к серверу злоумышленник может управлять компьютером точно так же, как и своим: перезагружать, выключать, открывать *CD-ROM*, удалять, записывать, менять файлы.

Также можно пересылать пароли. Функций у этой утилиты может быть много, вплоть до взлома банковских серверов, что уже является серьезным уголовным преступлением.

E-mail trojan

Этот вид троянов работает по принципу отправки информации хозяину на *e-mail.* Одним словом, этот вид вредоносного ПО занимается только сбором информации и жертва даже может не знать что его пароли уже давно кому то известны. Просветление приходит только тогда, когда приходит счет от провайдера за использованный трафик.

Key Logger

Эти трояны еще называют программами-шпионами (*spyware*). Они записывает все клавиши, которые нажимает хозяин зараженного компьютера в отдельный файл и затем они, как и *e-mail* трояны, высылают этот файл злоумышленнику любым доступным способом.

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 способам намеренно наносящие прямой или косвенный ущерб данному или удалённому компьютеру.

Email-Worm – почтовые черви

К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, *URL* на зараженный файл, расположенный на взломанном или хакерском веб-сайте).

В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором – при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков – активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены:

- прямое подключение к *SMTP*-серверу, используя встроенную в код червя почтовую библиотеку;
- использование сервисов *MS Outlook*;

- использование функций *Windows MAPI*.

Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви:

- рассылают себя по всем адресам, обнаруженным в адресной книге *MS Outlook*;
- считывает адреса из адресной базы *WAB*;
- сканируют «подходящие» файлы на диске и выделяет в них строки, являющиеся адресами электронной почты;
- отсылают себя во всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты.

IM-Worm – черви, использующие интернет-пейджеры

Известные компьютерные черви данного типа используют единственный способ распространения – рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих *URL* на файл, расположенный на каком-либо веб-сервере. Данные прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

IRC-Worm – черви в *IRC*-каналах

IRC-каналы созданы до появления браузеров и предназначены для обмена текстовыми сообщениями через общее окно, видное всем клиентам, подключенным к данному каналу.

У этого типа червей, как и у почтовых червей, существуют два способа распространения червя по *IRC*-каналам, повторяющие способы, описанные выше. Первый заключается в отсылке *URL*-ссылки на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение), чтобы код червя был активизирован.

Net-Worm – прочие сетевые черви

Существуют прочие способы заражения удаленных компьютеров, например:

- копирование червя на сетевые ресурсы;
- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- проникновение в сетевые ресурсы публичного использования;
- паразитирование на других вредоносных программах.

Первый способ заключается в том, что червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись (если такие обнаружены). При этом черви данного типа или перебирают доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ.

Для проникновения вторым способом черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос (эксплойт уязвимости), в результате чего код (или часть кода) червя проникает на компьютер-жертву. Если сетевой пакет содержит только часть кода червя, он затем скачивает основной файл и запускает его на исполнение.

Отдельную категорию составляют черви, использующие для своего распространения веб- и *FTP*-сервера. Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и необходимым образом модифицирует служебные файлы сервера (например, статические веб-страницы). Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают зараженную веб-страницу), и таким образом проникает на другие компьютеры в сети.

Существуют сетевые черви, паразитирующие на других червях и/или троянских программах удаленного администрирования (бэкдорах). Данные черви используют тот факт, что многие бэкдоры позволяют по определенной команде скачивать указанный файл и запускать его на локальном диске. То же возможно с некоторыми червями, содержащими бэкдор-процедуры. Для заражения удаленных компьютеров данные черви ищут другие компьютеры в сети и посылают на них команду скачивания и запуска своей копии. Если атакуемый компьютер оказывается уже зараженным «подходящей» троянской программой, червь проникает в него и активизирует свою копию.

P2P-Worm – черви для файлообменных сетей

Механизм работы большинства подобных червей достаточно прост – для внедрения в *P2P*-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса *P2P*-сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

Существуют более сложные *P2P*-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно. При этом червь предлагает для скачивания свою копию.

Следует особо отметить, что в мире постоянно появляются новые вирусы и надо это воспринимать как данность. Например, относительно недавно появился так называемый «вирус подмены страниц».

Вирус подмены страниц (*Phishing*)

Вирус подмены страниц существует в двух вариантах. Первый – относительно безобидный. Если Вы нажали на один из результатов поиска, и оказались не там, где ожидали, – возможно, ваш компьютер заражен вирусом подмены страниц. Как это может выглядеть? При нажатии на ссылку в результатах поиска, Вы оказываетесь на совершенно другом сайте, чем указанном на странице результатов поиска. Проверьте, совпадают ли адрес сайта в адресной строке браузера и в результатах поиска. Этот вирус часто используется недобросовестными рекламодателями.

Второй вариант вируса подмены страниц гораздо более опасен. За рубежом он известен под названием *Phishing* (созвучно со словом «рыбалка»).

В атаках фишинга широко используются методы социальной инженерии. Хакеры рассылают письма тысячам пользователей, представляясь работниками банков, систем *eBay, PayPal* или другими. Адресатам предлагается под разными предлогами зайти на сайты, внешне идентичные оригинальным. Конечно, эти сайты поддельные. После чего пользователь вводит необходимые учётные данные для какой-либо цели, указанной в письме, например, для разблокирования учётной записи или восстановления пароля. Эти учетные данные (пин-коды) попадают к злоумышленнику, который не преминет ими воспользоваться. Очень

многие начинающие пользователи «клюют на крючок» фишинга и теряют деньги со своего банковского счета.

Фарминг (*Pharming*)

Эпидемия фишинга постепенно переходит в эпидемию фарминга, которая требует более серьёзной технической подготовки хакеров.

Фармеры перенаправляют пользователей с легитимных коммерческих сайтов на поддельные. Опять же, они внешне очень похожи, почти клоны. Пользователи вводят учётные данные на сайте-клоне, которые успешно поступают к хакерам.

При фарминге тоже используются различные методы, но наиболее часто хакеры прибегают к помощи троянского ПО – скрытых программ, работающих на компьютере жертвы и позволяющих выполнять разные задачи по выбору хакера. Покажем эту работу на примере.

Злоумышленник рассылает по электронной почте вирусы, например *Banker Trojan*, который переписывает файл на компьютере *hosts*. Известно, что в этом файле находятся записи, сопоставляющие символьные имена (*URL*), например *Google.com,* с *IP*-адресами (например, 64.55.33.22). Изменив такую связку для сайта банка, ничего не подозревающий пользователь будет направлен на другой сайт, внешне идентичный настоящему. То есть при переходе на Вашу страницу Интернет-банка действия хакера перенаправят ничего не подозревающего пользователя на совершенно другую страницу.

В результате хакер получит пин-коды, которые Вы сами же и введете. Затем быстро снимаются деньги с Вашего счета. Причем, хакер снимает деньги не со своего компьютера, а с помощью компьютера-зомби, который он подготовил заранее. Часто используется целая цепочка компьютеров-зомби, чтобы затруднить расследование, если Вы обратитесь в правоохранительные органы. Есть еще один прием хакеров этого вида – снимать со счетов небольшие суммы. Они учитывают психологию наших людей: из-за небольшой суммы в милицию не обращаться.

Вирусы-вымогатели

Программы-вымогатели известны давно, но такое массовое развитие получили сравнительно недавно, благодаря развитию сотовой связи. Точнее, благодаря возможности перевода денег через *SMS*-сообщение сотового телефона. Действия вирусов-вымогателей весьма разнооб-

разны: от полной блокировки компьютера, до вывода небольшого порно-баннера внизу экрана. Общим для них является то, что предлагается отправить *SMS*-сообщение, на которое Вам будет выслан код для снятия блокировки. При этом сообщается, какая должна быть сумма на счете Вашего телефона, которая попадет на счет вымогателя. Нет никакой гарантии, что при отправке *SMS*-сообщения, эти действия не повторятся, поскольку вирус-вымогатель остался в Вашем компьютере.

В настоящее время многие антивирусные центры предлагают услуги по разблокировке вируса-вымогателя. Например, бесплатный сервис *Deblocker* лаборатории Касперского может убрать баннер (рекламный модуль) с рабочего стола, разблокировать *Windows* без отправки *SMS*-сообщения или вернуть зашифрованные вирусом файлы.

Более подробные описания вирусов можно найти, например, на сайте лаборатории Касперского *http://www.securelist.com/ru/descriptions.*

2.2. Антивирусное программное обеспечение

Все эти вредоносные программы, проникающие в основном через систему Интернет, а также через съёмные носители, требуют обязательного применения антивирусного ПО. Следует сразу оговориться, что 100 % защиты ни одно антивирусное ПО не обеспечивает. Это связано с тем, что любой разработчик антивирусного ПО может пополнить свою базу вирусов только после того, как кто-то из пострадавших пришлет файл с неопознанным вирусом. После этого требуется еще некоторое время для работы программистов над созданием обезвреживающего новый вирус ПО и время на обновление антивирусных баз пользователей. В лучшем случае это примерно неделя, за которую новый вирус может успеть распространиться по всей системе Интернет. Но, тем не менее, применять антивирусное ПО необходимо, потому что кроме новых вирусов система Интернет наполнена большим количеством старых вирусов, от которых защита гарантирована.

Антивирусное ПО подразделяется на бесплатно распространяемое и коммерческое, которое может распространяться условно-бесплатно на ограниченный срок действия.

В последнее время появился новый вид антивирусных услуг: онлайн проверка Вашего компьютера на вирусы через Интернет. Но здесь нужно быть очень осторожным и прибегать к услугам только известных антивирусных брендов. Это, например, лаборатория Касперского (рис. 2.1), фирма *Symantec* (рис. 2.2), фирма *MCAfee* (рис. 2.3). Если Вы не хо-

тите, чтобы сканировался весь компьютер, а хотите только проверить один подозрительный на вирус файл, то можно воспользоваться сервисом от *VirusTotal* и отправить туда этот файл (рис. 2.4).

Последний вариант проверки самый мощный, поскольку она производится с помощью множества самых современных антивирусных средств от компаний, участвующих в этом проекте (рис. 2.5).

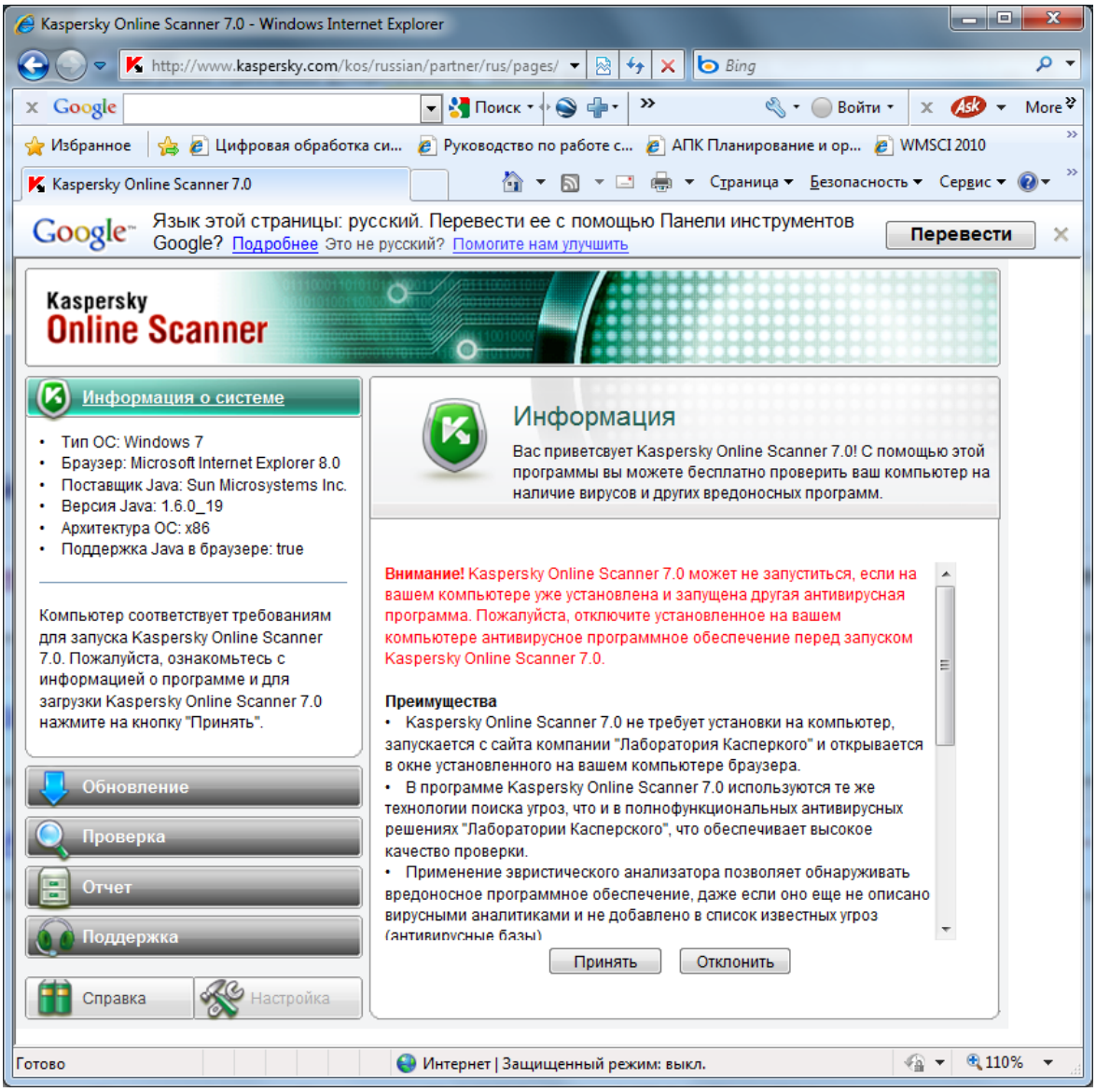


Рис. 2.1.Онлайн проверка на вирусы лаборатории Касперского

Рис. 2.2.Онлайн проверка на вирусы фирмы Symantec

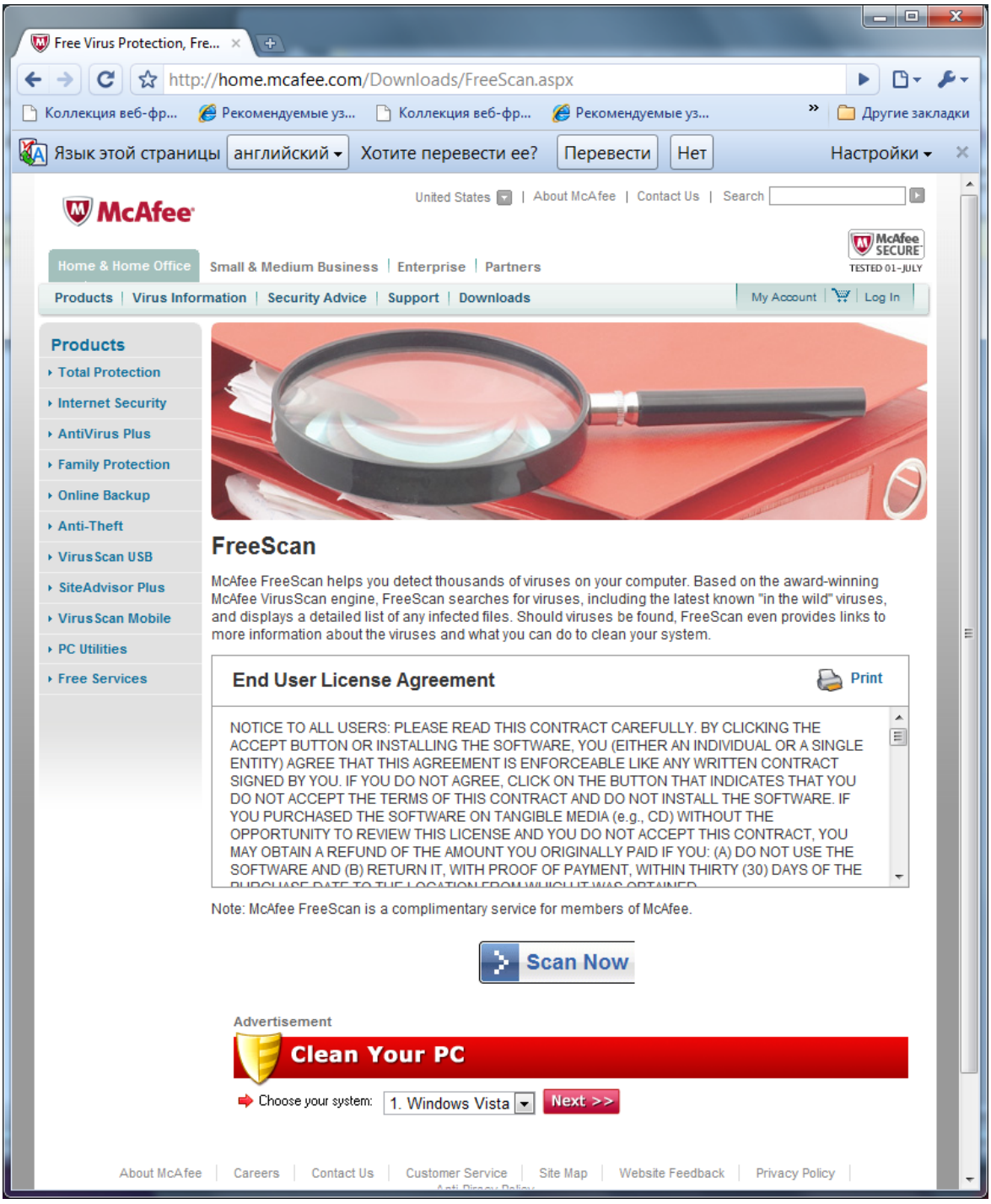


Рис. 2.3.Онлайн проверка на вирусы фирмы McAfee

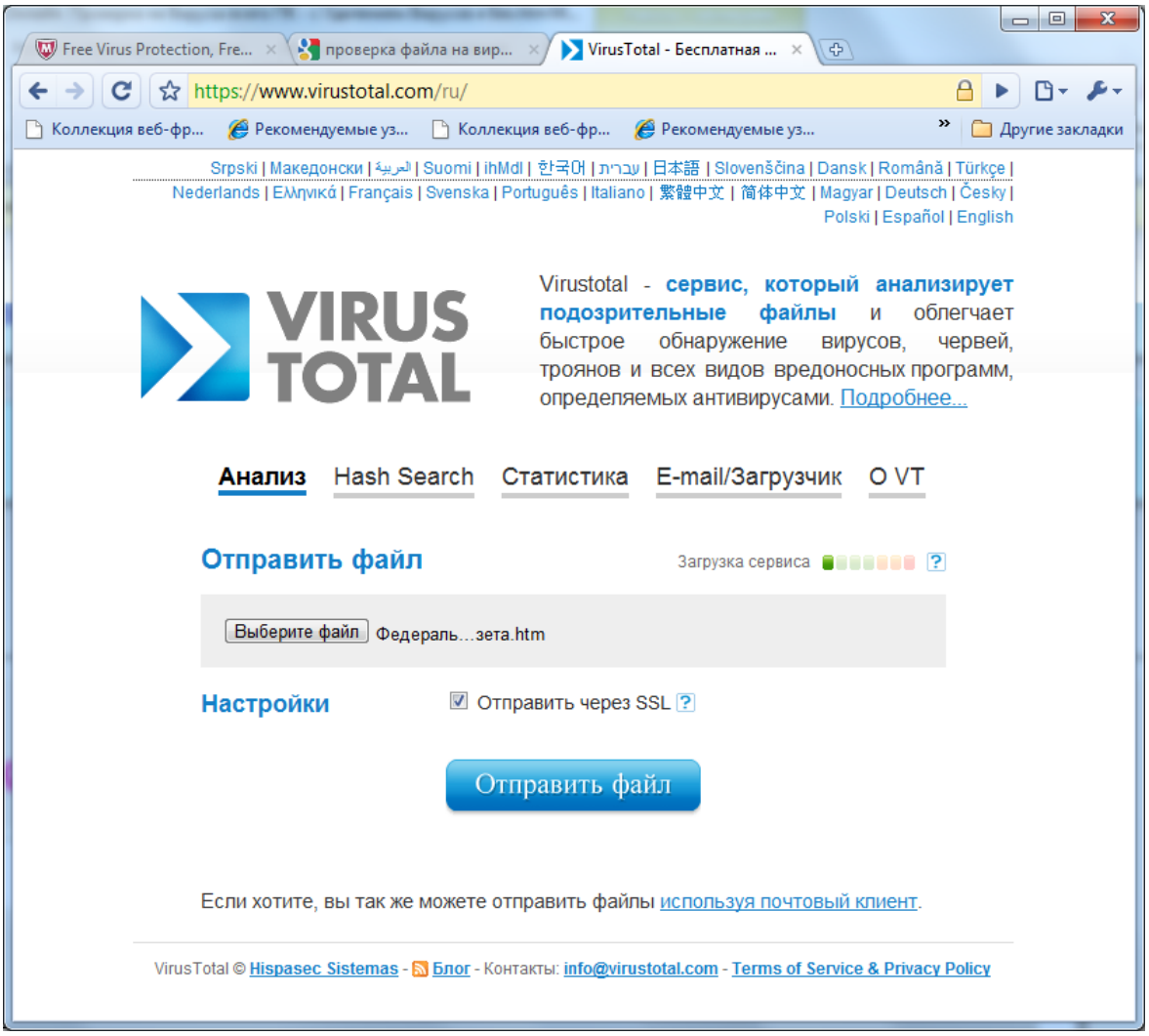


Рис. 2.4.Отправка файла для проверки на вирусы

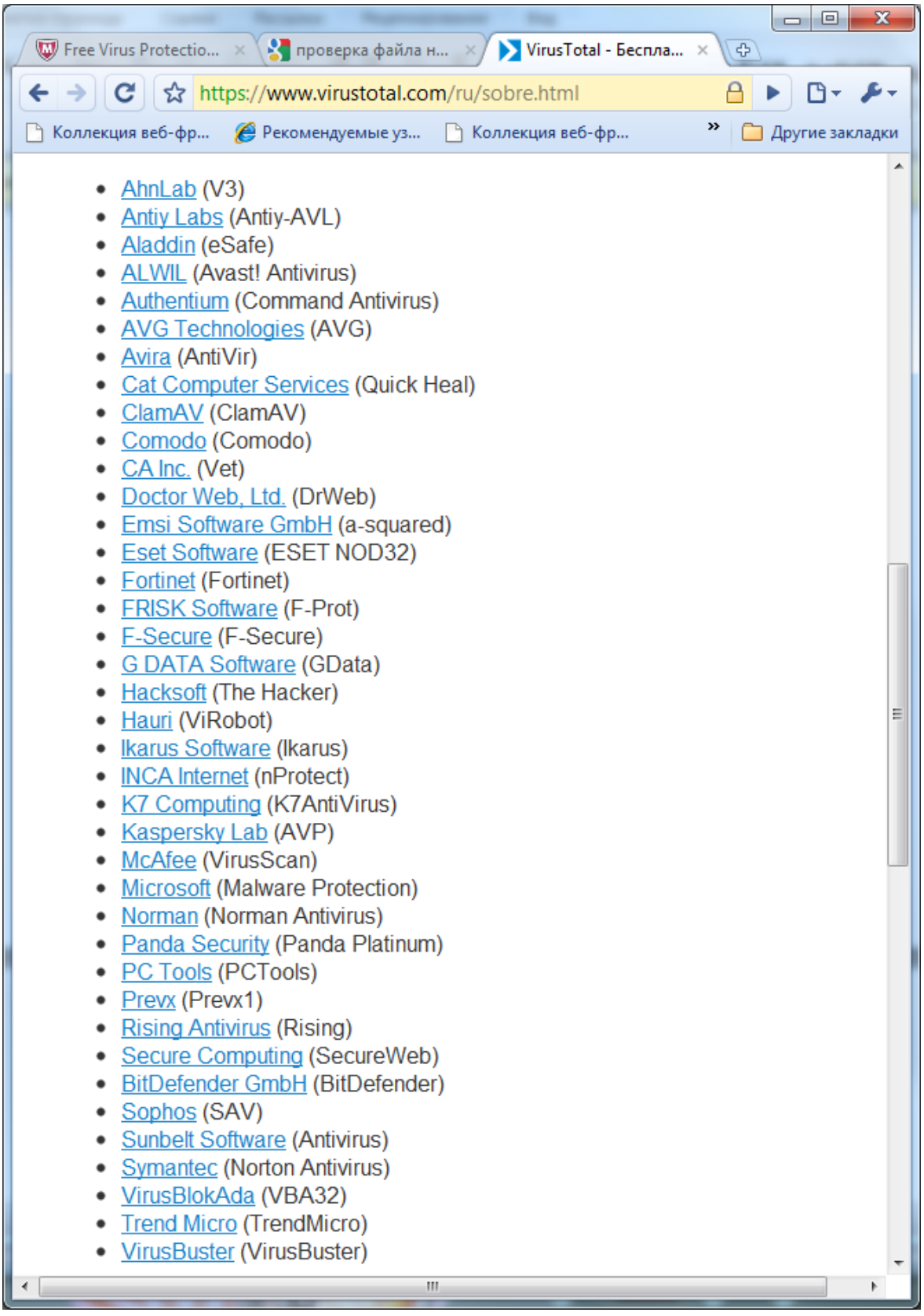


Рис. 2.5. Список антивирусных компаний, участвующих в проекте VirusTotal

В настоящее время многие антивирусные программы имеют и встроенные межсетевые экраны, которые рассматривались нами в предыдущей главе.

Задание № 1

Научиться устанавливать антивирусные программы, имеющиеся в распоряжении.

В качестве примера используем бесплатно распространяемое ПО *Avast*! (рис. 2.6 – 2.18).

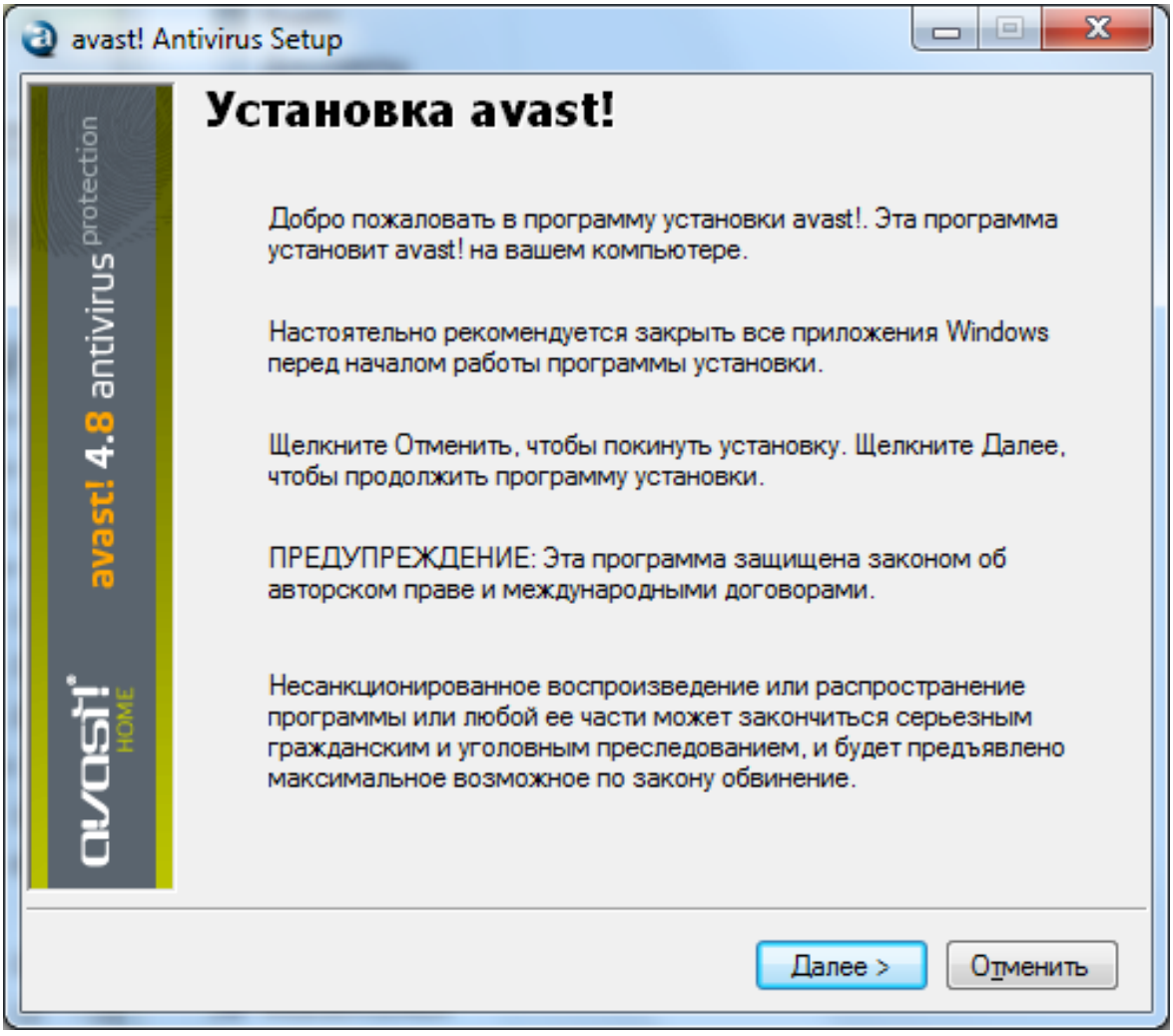


Рис. 2.6. Стартовое окно антивирусной программы Avast!

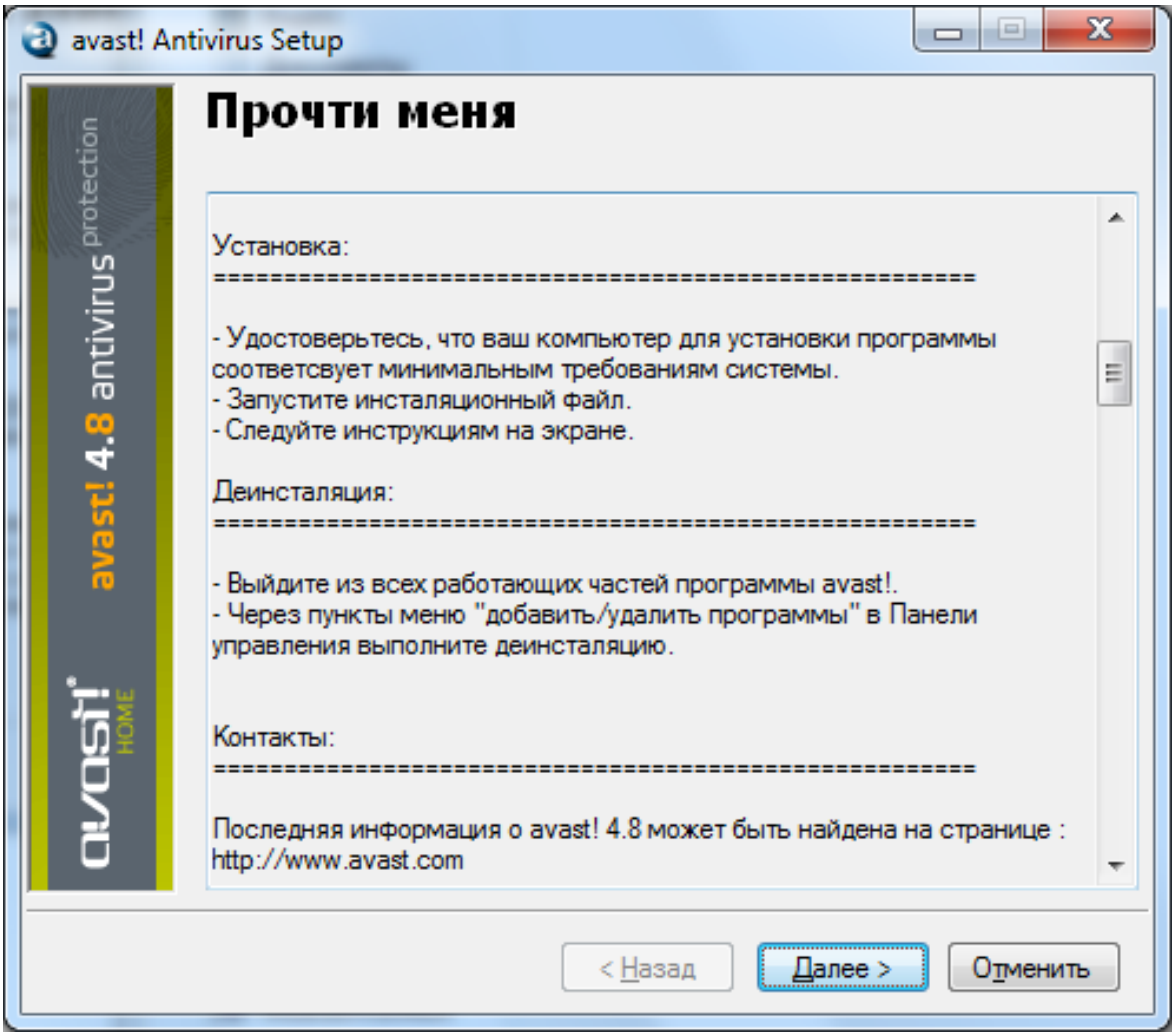


Рис. 2.7. Инструкция начала установки антивирусной программы Avast!

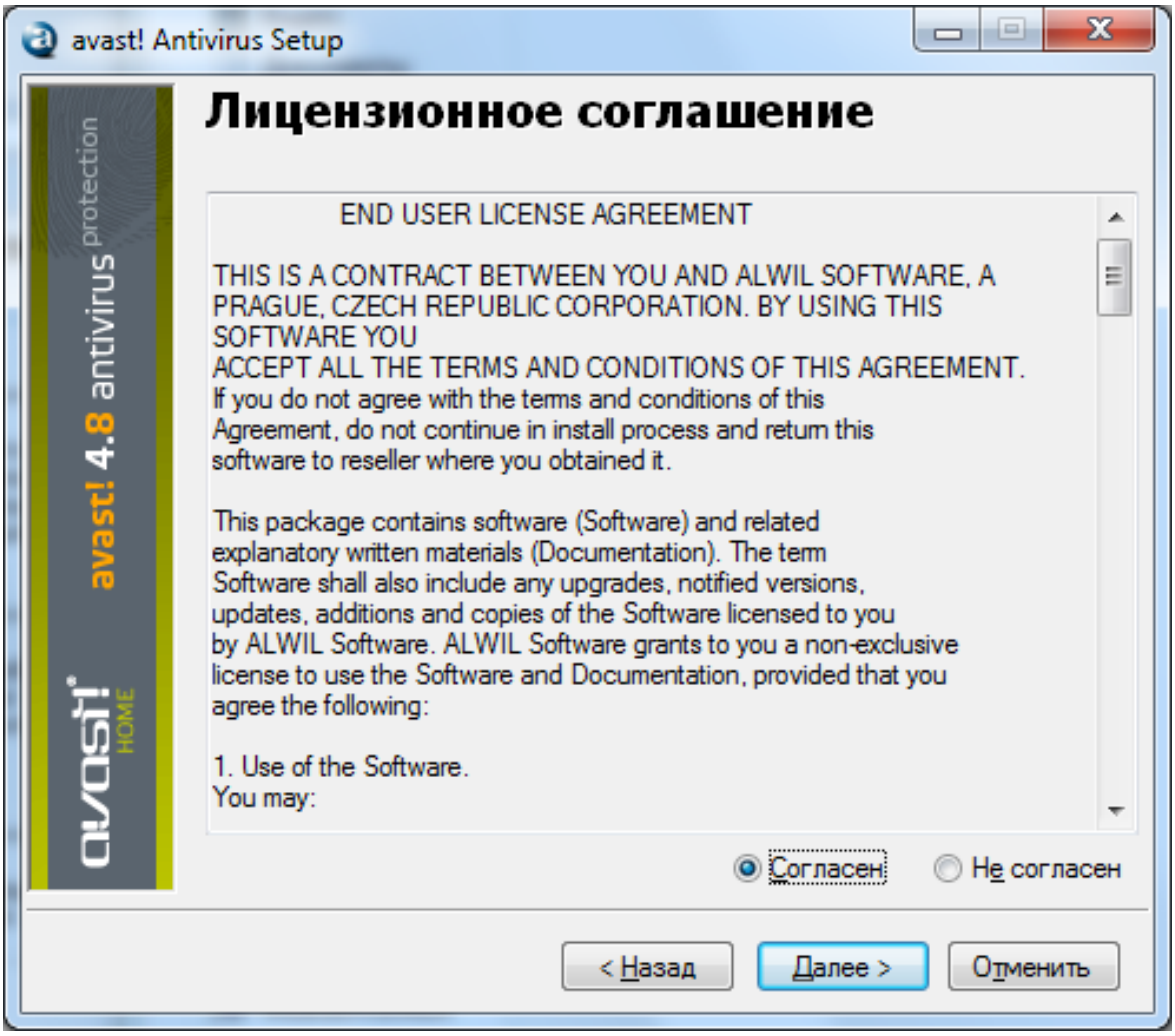


Рис. 2.8. Лицензионное соглашение антивирусной программы Avast!

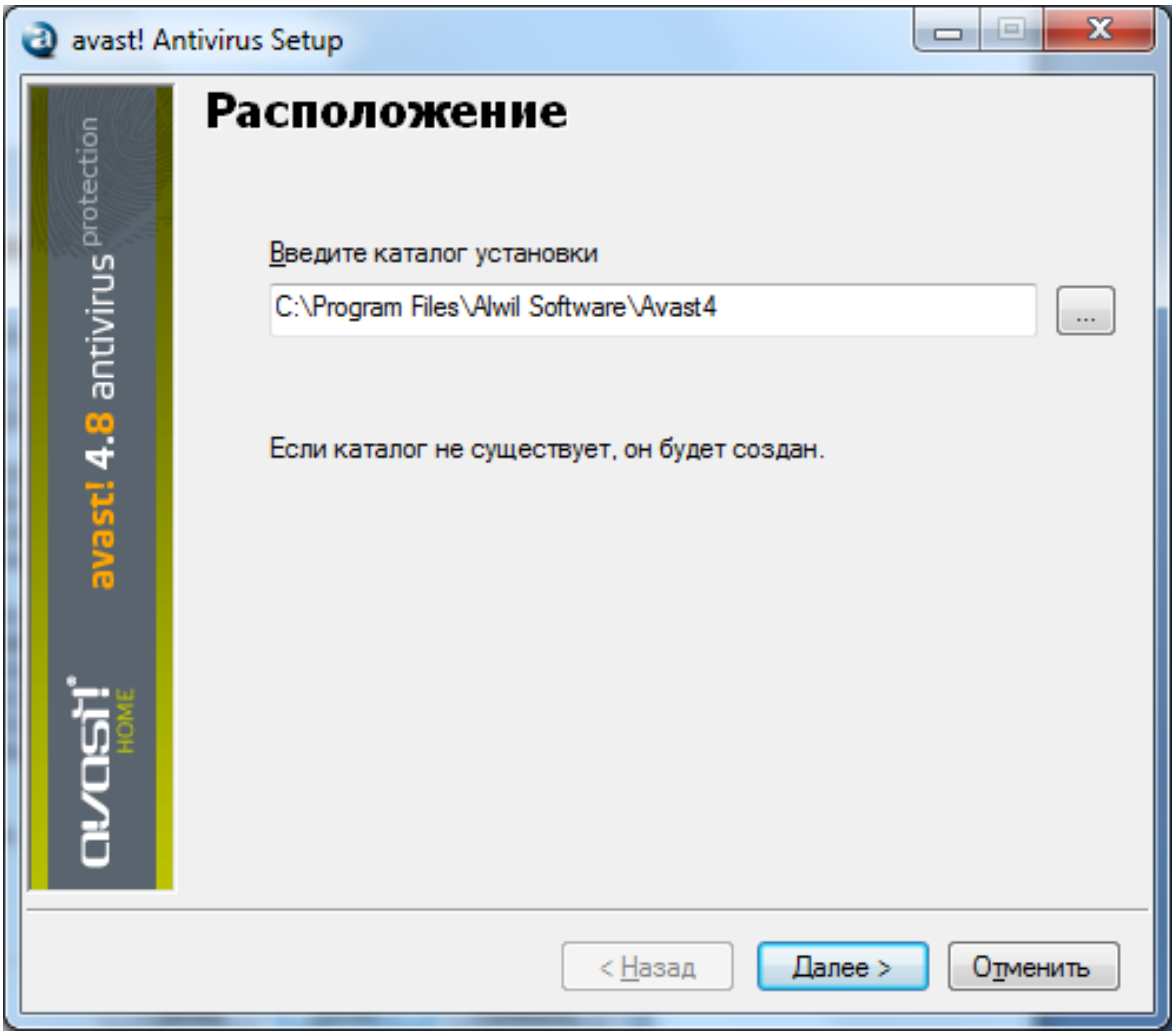


Рис. 2.9. Расположение на диске антивирусной программы Avast!

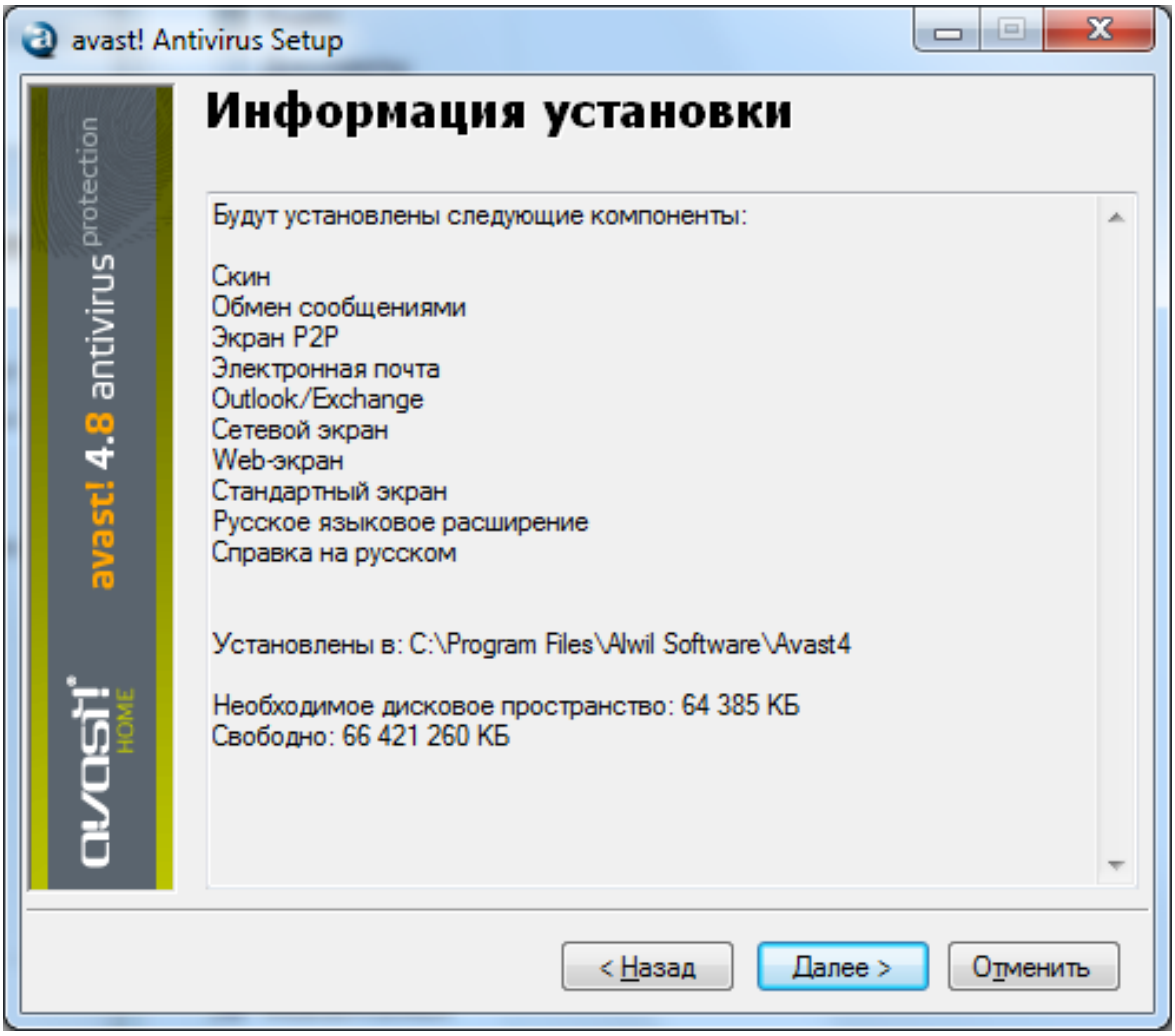


Рис. 2.10. Устанавливаемые компоненты антивирусной программы Avast!

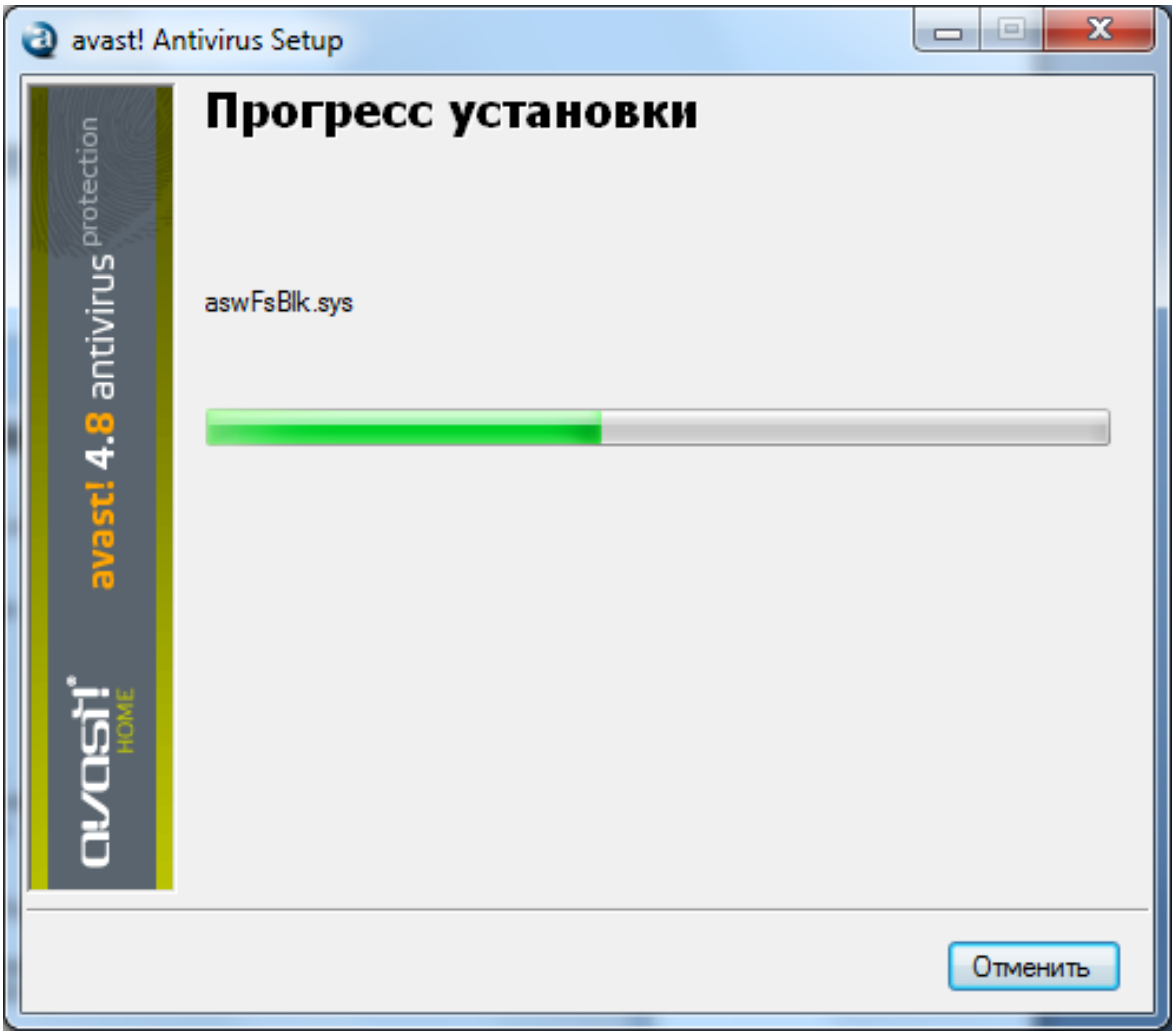


Рис. 2.11. Процесс установки антивирусной программы Avast!

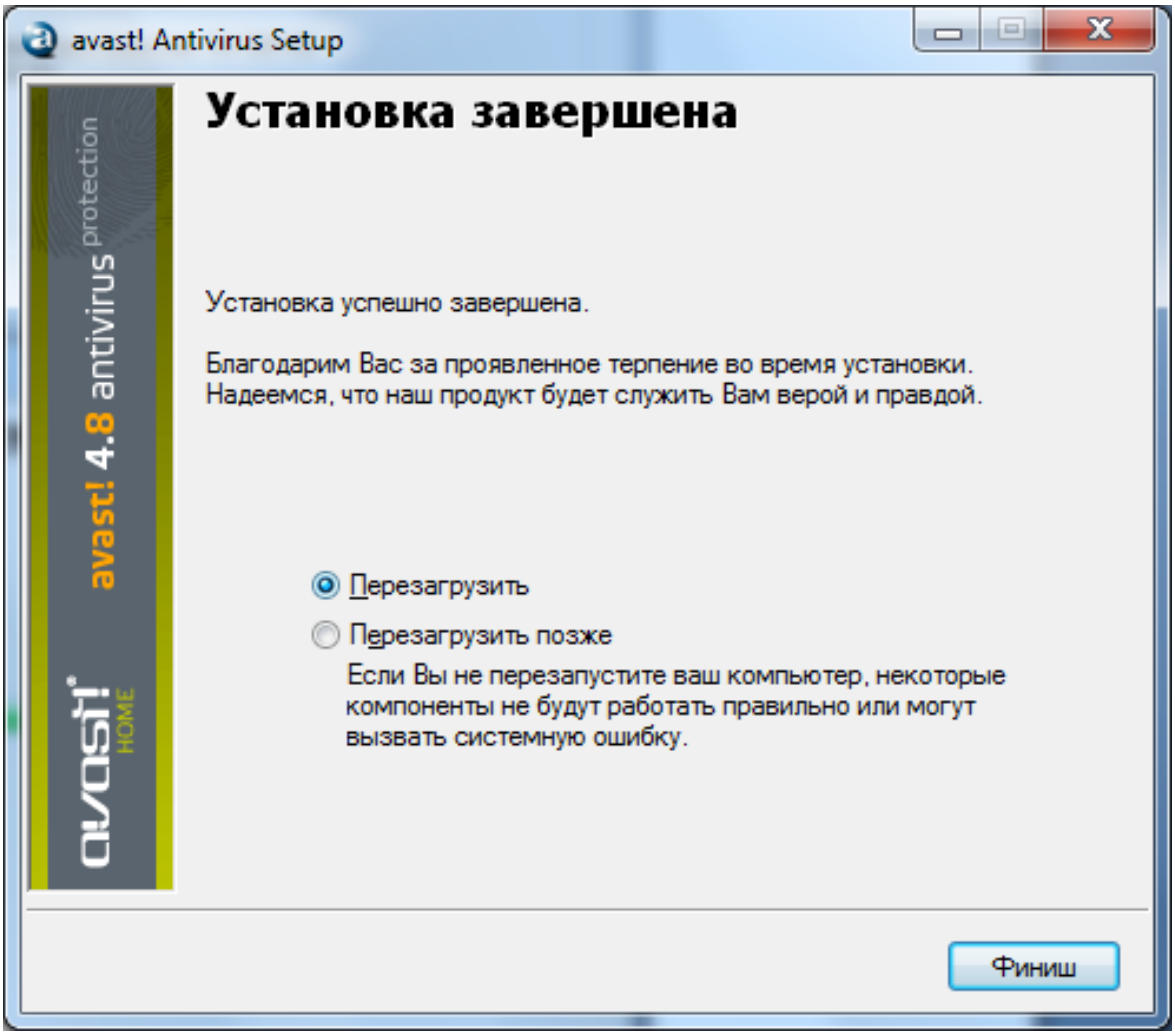


Рис. 2.13. Завершение установки антивирусной программы Avast!

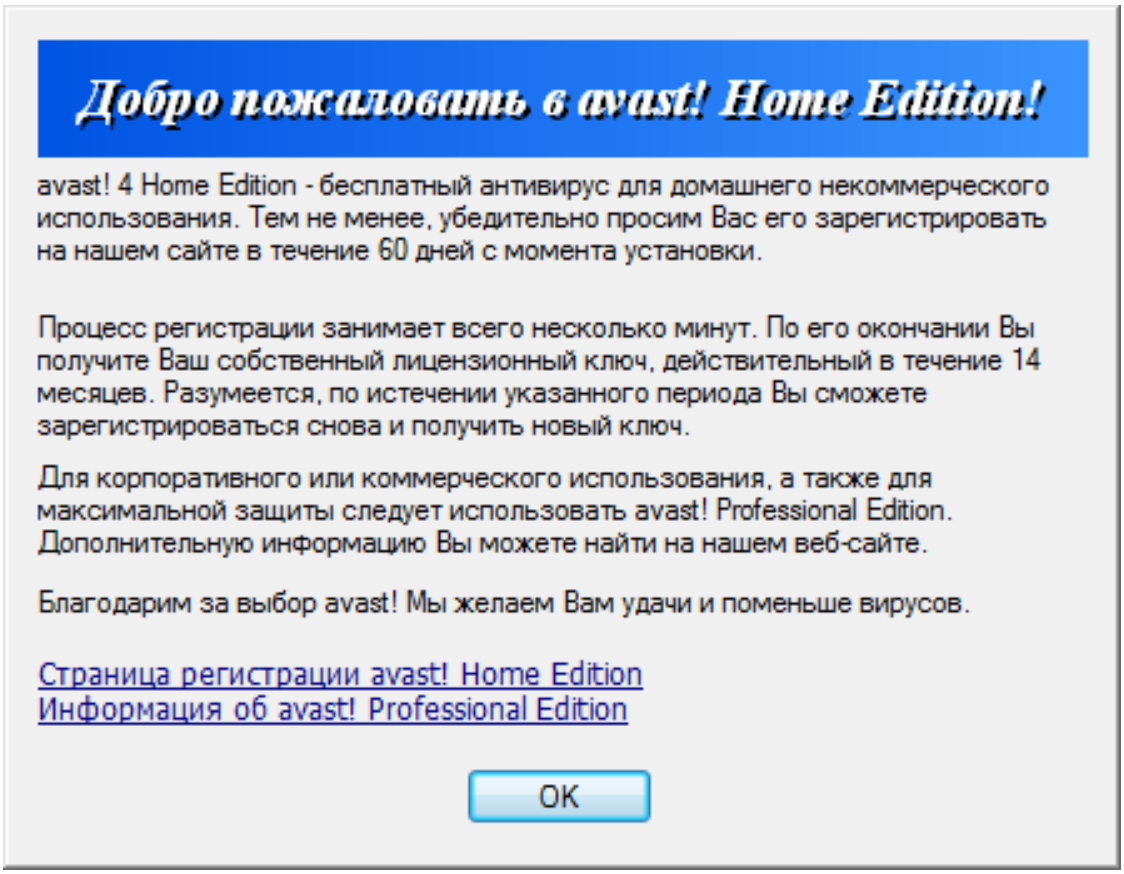


Рис. 2.14. Предложение зарегистрировать установленную программу Avast!

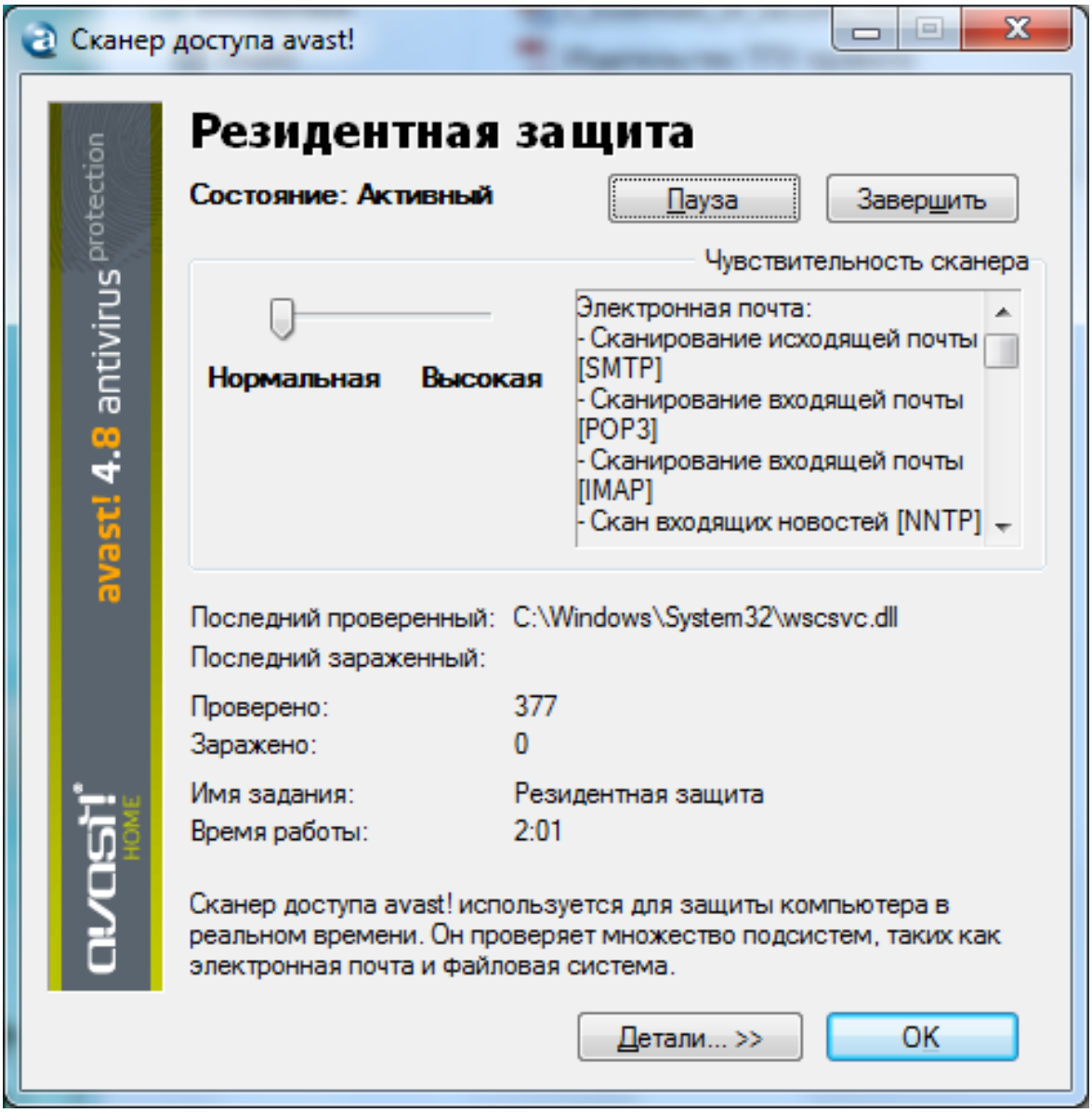


Рис. 2.15. Проверка резидентной защиты программы Avast!

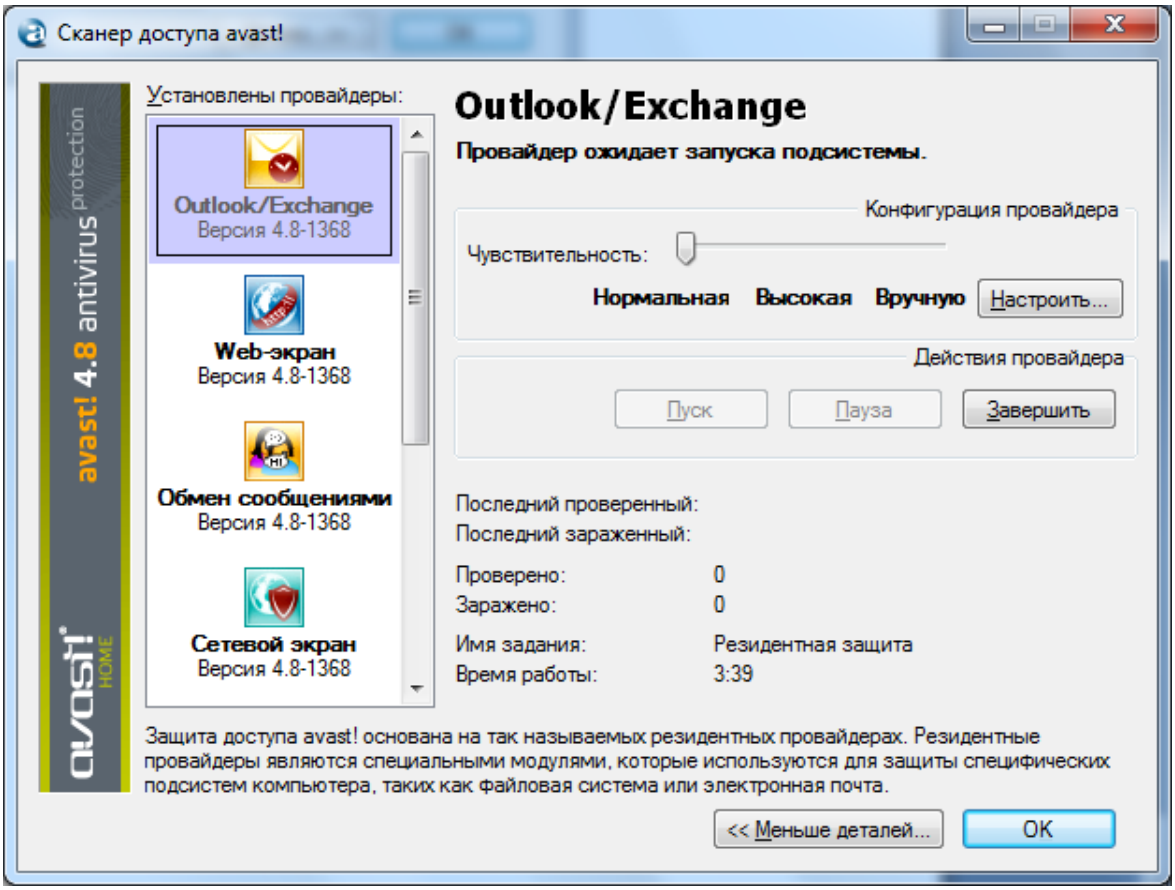


Рис. 2.16. Проверка защиты электронной почты программы Avast!

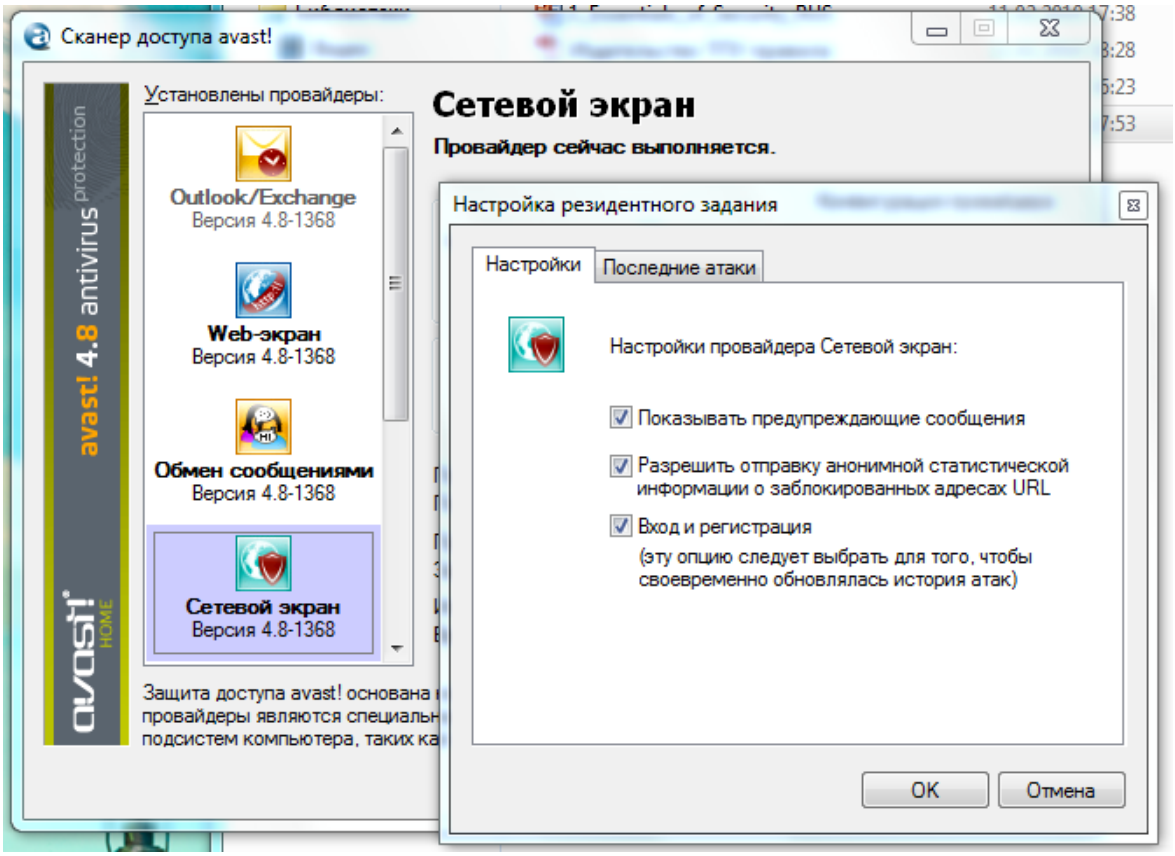


Рис. 2.17. Проверка работы сетевого экрана программы Avast!

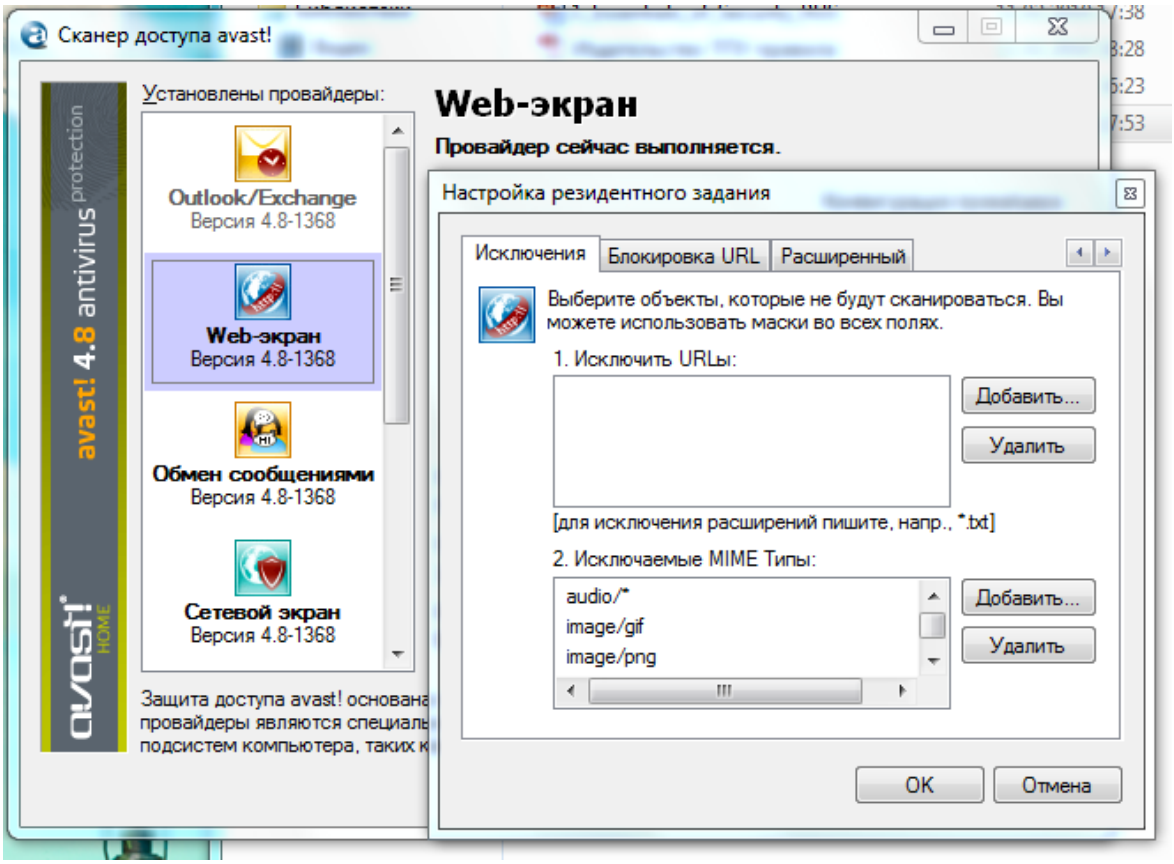


Рис. 2.18. Проверка работы Web-экрана программы Avast!

Задание № 2

Научиться эксплуатировать антивирусные программы, имеющиеся в распоряжении.

В качестве примера используем антивирусное ПО: *Symantec AntiVirus.*

Ход работы:

1. Запускаем антивирусную программу: Пуск – Программы – *Symantec Client Security – Symantec AntiVirus* (рис. 2.19).

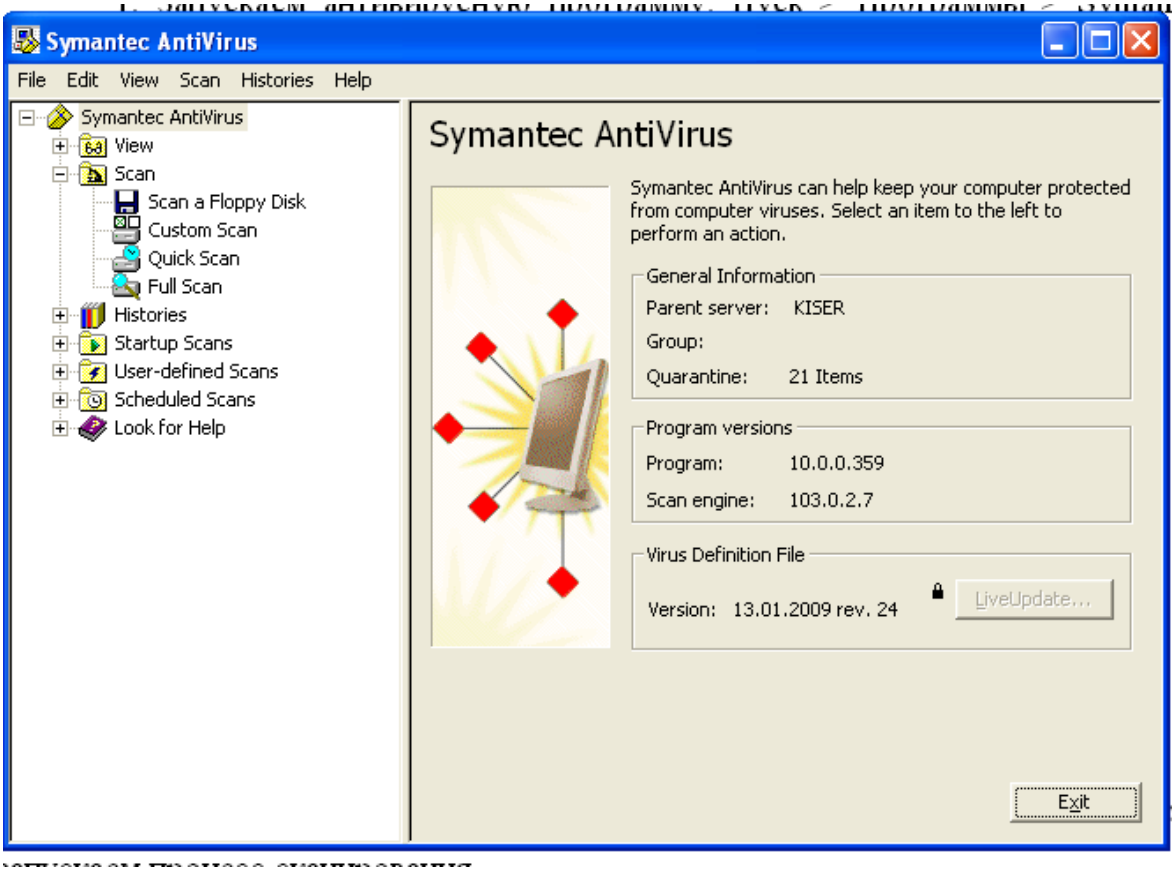


Рис. 2.19. Стартовое окно Symantec AntiVirus

2. Выбираем на панели инструментов *Scan – Custom Scan – CD*-дисковод (*E*:) и запускаем процесс сканирования (рис. 2.20).

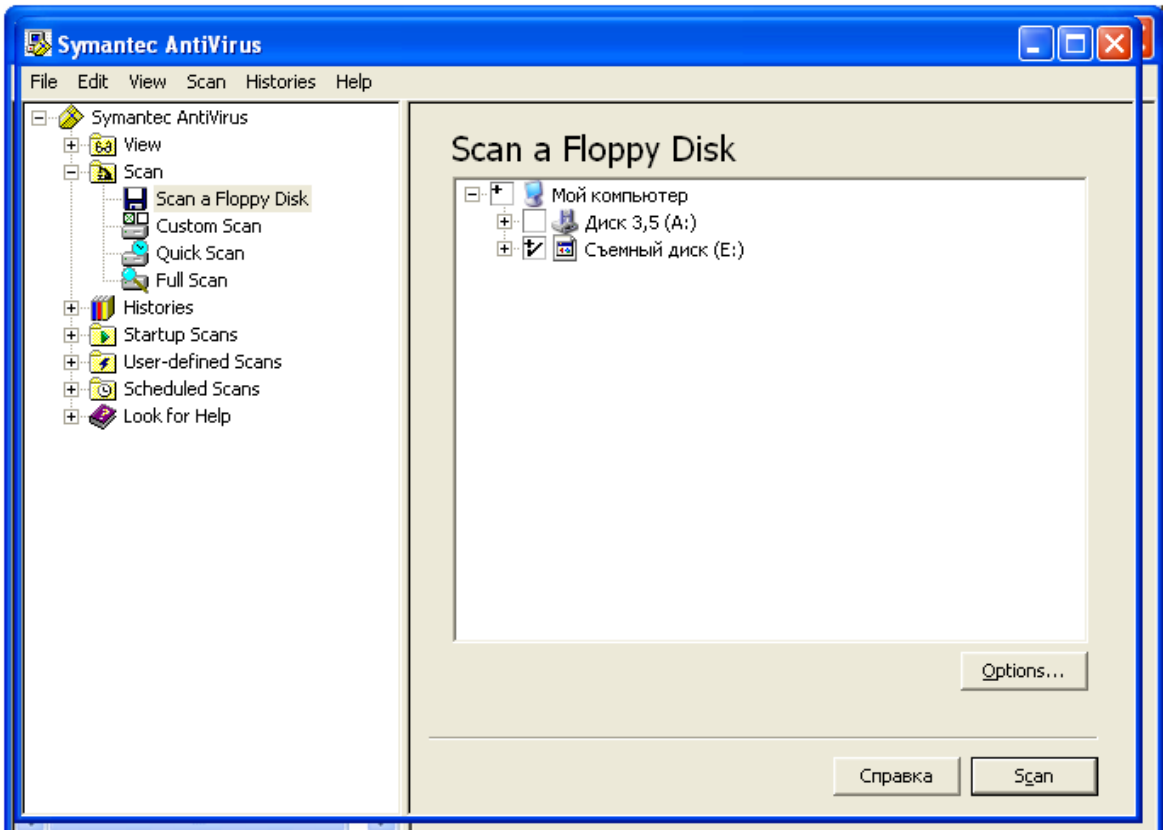


Рис. 2.20. Выбор сканирования съемного диска

3. Фиксируем в отчете результаты поиска: обнаружено 3 вредоносных программы, содержащих один и тот же вирус. Определяем его назначение (рис. 2.21).

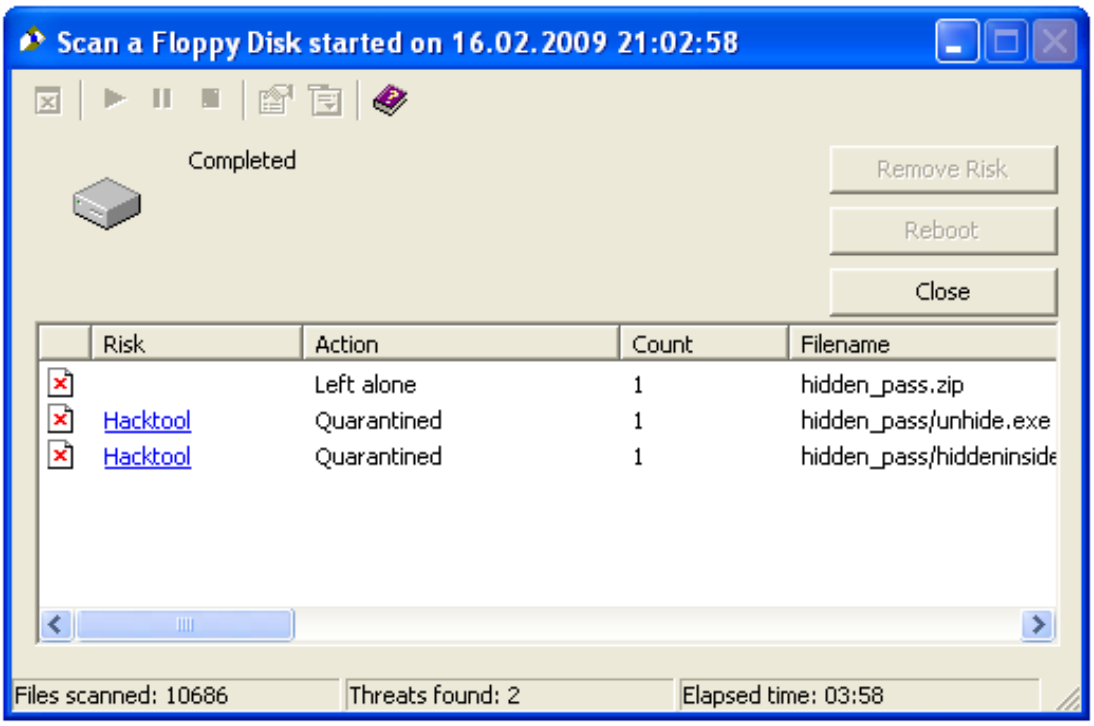


Рис. 2.21. Найденные файлы, зараженные вирусами

Hacktool – программа, используемая злоумышленниками при организации атак на локальный или удаленный компьютер. Например, несанкционированное пользователем внесение нелегального пользователя в список разрешенных посетителей системы; очистка системных журналов с целью сокрытия следов присутствия в системе; снифферы с выраженным вредоносным функционалом и т. д. (*http://www.securelist.com/ru/descriptions/88695/HackTool.Win32.Whoisadm*).

4. Просмотрим историю работы антивируса и классифицируем найденные ранее вирусы (рис. 2.22).

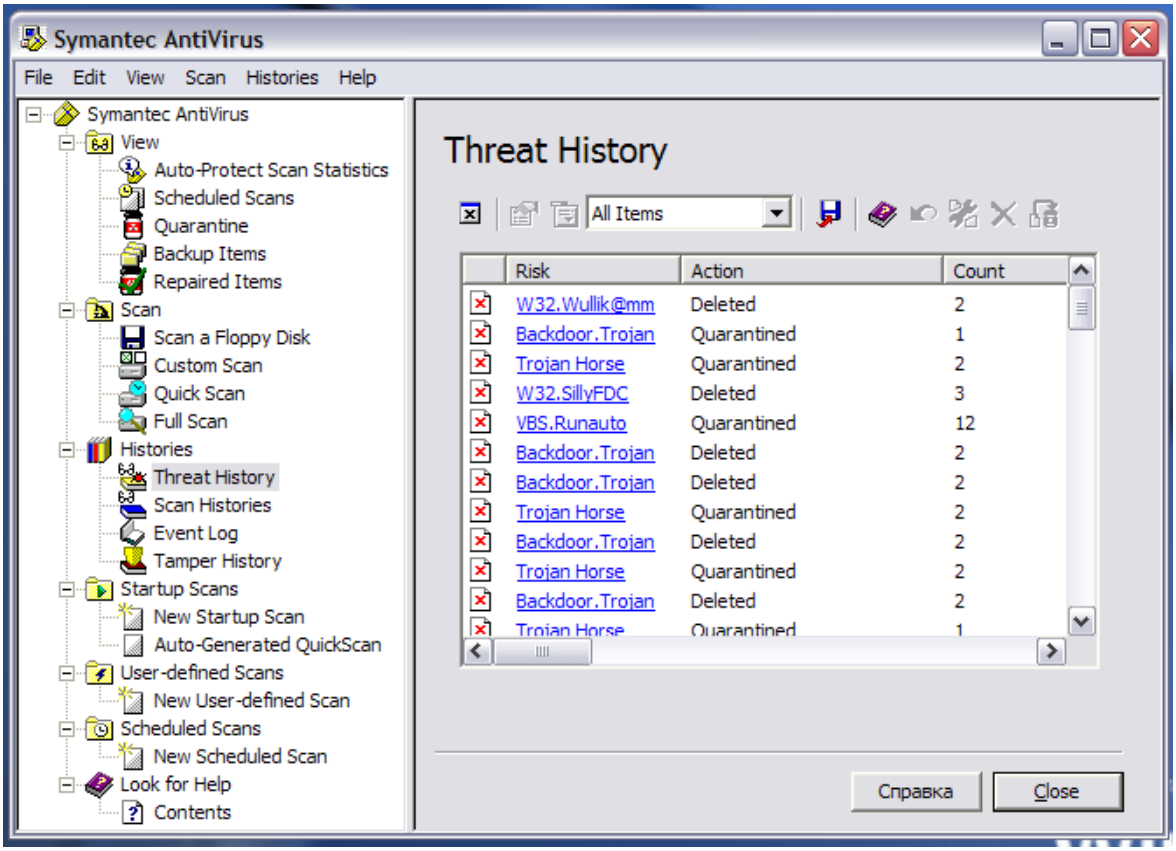


Рис. 2.22. Найденные ранее вирусы

В листе истории присутствуют следующие вирусы:

1) **W32.Wulik@mm** – червь для массовой спам-рассылки, который пытается рассылать себя по всем контактам в адресной книге *Windows*, а также может распространяться через сетевые ресурсы.

2) **Backdoor.Trojan** – вредоносный троянский бэкдор, который работает в фоновом режиме и обеспечивает удаленный доступ к зараженной системе. С его помощью злоумышленники могут выполнять все действия на Вашем ПК.

3) **Trojan Horse** – троянский конь, программа-инсталлятор любого другого вируса, сама по себе вред ПК не наносит.

4) **W32.SillyFDC** – червь, специально предназначенный для распространения через файл *AutoRun* съемного носителя. Вредоносные действия этого червя:

- скачивание файлов с заданного *URL*;
- копирование себя в сетевые ресурсы;
- понижение настройки безопасности;

- изменение файлов хостов;
- отключение обновления *Windows* и восстановления системы;
- обход брандмауэра *Windows*;
- отключение диспетчера задач, редактора реестра и другого программного обеспечения системы.

(*http://www.symantec.com/security_response/writeup.jsp?docid*=2006-071111-0646-99).

5) **VBS.Runauto** – безобидный червь. Распространяется копированием себя на все съемные диски, кроме дискет. Заменяет заголовок окна *Microsoft Internet Explorer* на англоязычный бранный текст. Больше никак не проявляется.

6) **Infostealer.Gampass** – троянская программа, предназначенная для похищения паролей, ключей для установки и входа в онлайн-игры.

7) **Win32.Spybot.Worm** – червь, выполняющий функции шпионской программы. Отличительным признаком его внедрения является повышенный сетевой трафик.

8) **DialupPwd** – червь, предназначенный для похищения паролей доступа к Интернету через модем, или *VPN*.

9) **Trojan.Win32.Agent2.dtb** – троянская программа, которая без ведома пользователя производит дозвон на платные телефонные номера.

Выводы: 1) Нами были обнаружены вирусы на флеш-накопителе (E:), и произведена их очистка. 2) Все вирусы, найденные на ПК и съемных носителях, были опознаны и описаны. Цель работы – научиться эксплуатировать антивирусное ПО на конкретном примере – достигнута.

Глава 3. Криптографическая защита информации

Криптографические методы защиты информации (шифрование) являются наиболее эффективным средством защиты данных в автоматизированных системах (АС). А при передаче информации по протяженным линиям связи или по радиоканалу, они являются единственным реальным средством предотвращения несанкционированного доступа.

Шифрование человечество использовало давно. Да наших времен сохранилась информация о таких шифрах, как «код Цезаря», «квадрат Полибия», «решетка Кардано» и т. п. Известно, что во время Второй мировой войны все немецкие части передавали по рациям зашифрованные сообщения, используя для шифрования специальную машинку «Энигма».

Известно также, что английские и польские ученые сконструировали частично электронную, частично механическую машину *Turing Bombe*, которая «взламывала» код, генерируемый шифровальной системой «Энигма». На расшифровку каждой радиограммы требовалось в среднем 11 минут. Наиболее известные из этих ученых – это Алан Тьюринг, автор теоремы о «машине Тьюринга», трагически погибший в 1954 г. и Дональд Мичи – профессор Эдинбургского университета, академик, погибший в автокатастрофе в 2007 г.

Любой криптографический метод характеризуется такими основными характеристиками, как стойкость (криптостойкость) и трудоемкость. Криптостойкость метода – это минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, стойкость определяет допустимый объем информации, зашифровываемой с использованием одного ключа. Трудоемкость метода определяется количеством элементарных операций, необходимых для шифрования одного символа исходного сообщения.

Алгоритмы шифрования и дешифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами. Главным принципом криптографии является условие, что передатчик (респондент) и приемник (резидент) заранее знают алгоритм шифрования и ключ, без которых сообщение представляет собой всего лишь набор символов, не имеющих смысла.

Если для шифрования и дешифрования используется один и тот же ключ, то такие алгоритмы называются симметричными. Главный недостаток симметричных криптосистем заключается в том, что резидент, генерирующий ключ, должен его скрытно передать респонденту, что

само по себе имеет риск обнаружения злоумышленником. К достоинствам симметричных криптосистем относится простота реализации.

В асимметричных криптографических алгоритмах для шифрования и дешифрования используются разные ключи. Резидент генерирует два ключа: закрытый (секретный), который никому не передает и хранит только у себя, и открытый (публичный), который передает респонденту, не опасаясь обнаружения злоумышленником. Респондент шифрует сообщения открытым ключом, а расшифровать их можно только закрытым ключом, хранящимся у резидента. Возможны и другие варианты использования пары ключей. Например, закрытый ключ используется для формирования электронной цифровой подписи, а открытый ключ – для проверки подлинности этой подписи.

Асимметричные криптосистемы основаны на использовании хэш-функций, которые обладают одним характерным свойством – высокой сложностью обратного преобразования. Чем выше эта сложность, тем выше и криптостойкость асимметричного метода. Наиболее известный асимметричный алгоритм шифрования – *RSA*, названный по первым буквам фамилий его создателей: *Rivest, Shamir, Aldeman*.

3.1. Симметричное шифрование

Симметричные криптографические алгоритмы – это способ криптографической защиты информации, в котором для шифрования и дешифрования применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете обеими сторонами (резидентом и респондентом).

Симметричные криптографические алгоритмы подразделяются на блочные и поточные. Блочные алгоритмы обрабатывают информацию блоками определённой длины (64, 128, 192, 256 бит), применяя к блоку данных ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект – нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

К достоинствам блочных алгоритмов относят схожесть процедур шифрования и дешифрования, которые отличаются только порядком действий. Это упрощает создание аппаратуры для реализации этих алгоритмов. Наиболее распространенные блочные алгоритмы шифрования – это метод перестановки и метод замены с различными вариациями.

В поточных алгоритмах шифрование производится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования (наложения на исходный текст гамма-последовательности битов с логической операцией *XOR* – «Исключительное ИЛИ»).

Поточный шифр может быть легко создан на основе блочного шифра, запущенного в специальном режиме (например, по ГОСТ 28147-89 в режиме гаммирования). Поточные алгоритмы шифрования также удобны для аппаратурной реализации и широко использовались задолго до появления компьютеров.

Широкому применению поточных (потоковых) алгоритмов шифрования положила начало работа Клода Шеннона, опубликованная в 1949 году. В ней Шеннон доказал абсолютную стойкость шифра Вернама (также известного, как одноразовый блокнот). В шифре Вернама ключ имеет длину, равную длине самого передаваемого сообщения. Ключ используется в качестве гаммы и, если каждый бит ключа выбирается случайно, то вскрыть шифр невозможно (т. к. все возможные открытые тексты будут равновероятны).

К настоящему времени создано немало алгоритмов поточного шифрования. Наиболее известные из них: *A*3, *A*5, *A*8, *RC*4, *PIKE*, *SEAL*, *eSTREAM* и др.

Известно и комбинированное применение алгоритмов блочного и поточного шифрования. Например, в известном алгоритме *DES* процедуры *CFB* и *OFB* используют алгоритмы блочного шифрования в режиме поточного шифрования.

Преимуществом поточных алгоритмов по сравнению с блочными является высокая скорость шифрования, соизмеримая со скоростью поступления входной информации. Недостатком поточных алгоритмов шифрования является существенно большее количество методов их взлома (криптоанализа) по сравнению с блочными алгоритмами.

3.1.1. Шифрование методом перестановки

Общие сведения

Шифрование методом перестановки относится к симметричным криптографическим алгоритмам. Простейшее шифрование перестановкой состоит в перестановке символов сообщения по заданным порядковым номерам (ключу). Например, слово «ура» по ключу 3–1–2 зашифруется в «аур». Если длина сообщения превышает длину ключа, то ключ применяют повторно.

На практике применяют более сложные алгоритмы перестановки по двум и более ключам. Например, требуется зашифровать открытый исходный текст: «ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ». По ключу ***k*1=5–3–1–2–4–6** записываем этот текст в таблицу по строкам (табл. 3.1). Начинаем со строки 5. Когда ячейки этой строки заполнятся, продолжаем записывать исходный текст в строку 3, затем – в строку 1 и так далее в соответствии с ключом ***k*1**.

Таблица 3.1. Шифрование методом перестановки по ключам *k*1 и *k*2

	1	2	3	4
1	**И**	**Е**	**_**	**П**
2	**Е**	**Р**	**Е**	**С**
3	**О**	**В**	**А**	**Н**
4	**Т**	**А**	**Н**	**О**
5	**Ш**	**И**	**Ф**	**Р**
6	**В**	**К**	**О**	**Й**

По ключу ***k*2=4–2–3–1** считываем текст по столбцам из таблицы. Начинаем со столбца 4, затем читаем столбец 2 и так далее в соответствии с ключом ***k*2**. Получим зашифрованный текст: «ПСНОРЙ-ЕРВАИК_ЕАНФОИЕОТШВ».

Дешифрование производится в обратном порядке. Сначала по ключу ***k*2** записываем зашифрованный текст в таблицу по столбцам. Затем по ключу ***k*1** считываем записанный текст из таблицы по строкам.

Требования к ключам:

- номера в ключе должны быть целыми положительными числами больше 0;
- номера в ключе не должны повторяться;
- максимальное значение номера в ключе должно не превышать количества номеров в ключе.

Если сообщение, подлежащее шифрованию, не умещается в таблице, заданной ключами ***k*1** и ***k*2** (шифротаблице), то его необходимо разделить на блоки, размер каждого из которых соответствует размеру шифротаблицы. Поэтому этот метод называют еще блочным шифрованием.

Существуют и более сложные алгоритмы шифрования методом перестановки, например, основанные на алгоритме кубика Рубика, реализованные в известном пакете программ для шифрования «Рубикон».

Задание № 1

Зашифровать вручную свои данные: «фамилия имя отчество» по ключам ***k*1** и ***k*2**, заданным в табл. 3.2. Свой вариант ключей выбрать по номеру в журнале преподавателя. Подобрать размер шифротаблицы под длину своих данных.

Таблица 3.2. Варианты заданий

№ варианта	Ключ ***k*1**	Ключ ***k*2**
01	1–2–3–4–5-6	4–3–2–1
02	1–2–3–4–6–5	4–3–1–2
03	1–2–3–6–5–4	4–2–3–1
04	1–2–6–4–5–3	4–1–2–3
05	1–6–3–4–5–2	1–3–2–4
06	6–2–3–4–5–1	1–2–4–3
07	6–2–5–4–3–1	2–3–2–4
08	5–2–4–3–1–6	2–4–3–1
08	5–2–3–4–5–1	2–3–4–1
10	5–2–4–3–5–1	2–4–1–3
11	4–2–1–3–5–6	3–4–2–1
12	4–1–3–2–5–6	3–2–4–1
13	5–2–6–4–1–3	3–1–4–2
14	3–2–1–6–5–4	3–1–2–4
15	3–1–4–2–6–5	1–4–2–3
16	6–5–4–3–2–1	4–3–2–1
17	1–5–4–3–2–6	4–3–1–2
18	2–5–4–3–6–1	4–2–3–1
19	3–5–4–6–2–1	4–1–2–3
20	4–5–6–3–2–1	1–3–2–4
21	5–6–4–3–2–1	1–2–4–3
22	6–1–4–3–2–5	2–3–2–4
23	6–5–1–3–2–4	2–4–3–1
24	6–5–4–1–2–3	2–3–4–1
25	2–1–4–3–6–5	2–4–1–3
26	3–1–4–5–2–6	3–4–2–1
27	4–1–6–3–2–5	3–2–4–1
28	5–1–4–3–6–5	3–1–4–2
29	6–1–4–3–2–5	3–1–2–4
30	6–5–1–3–2–4	1–4–2–3

По результатам выполнения задания составить отчет, в котором привести свою шифротаблицу и последовательность преобразования исходного текста в зашифрованный и обратно.

Задание № 2

Составить программу для шифрования методом перестановки. При составлении программы использовать образец (рис. 3.1–3.4), в который необходимо внести изменения, соответствующие Вашему индивидуальному заданию.

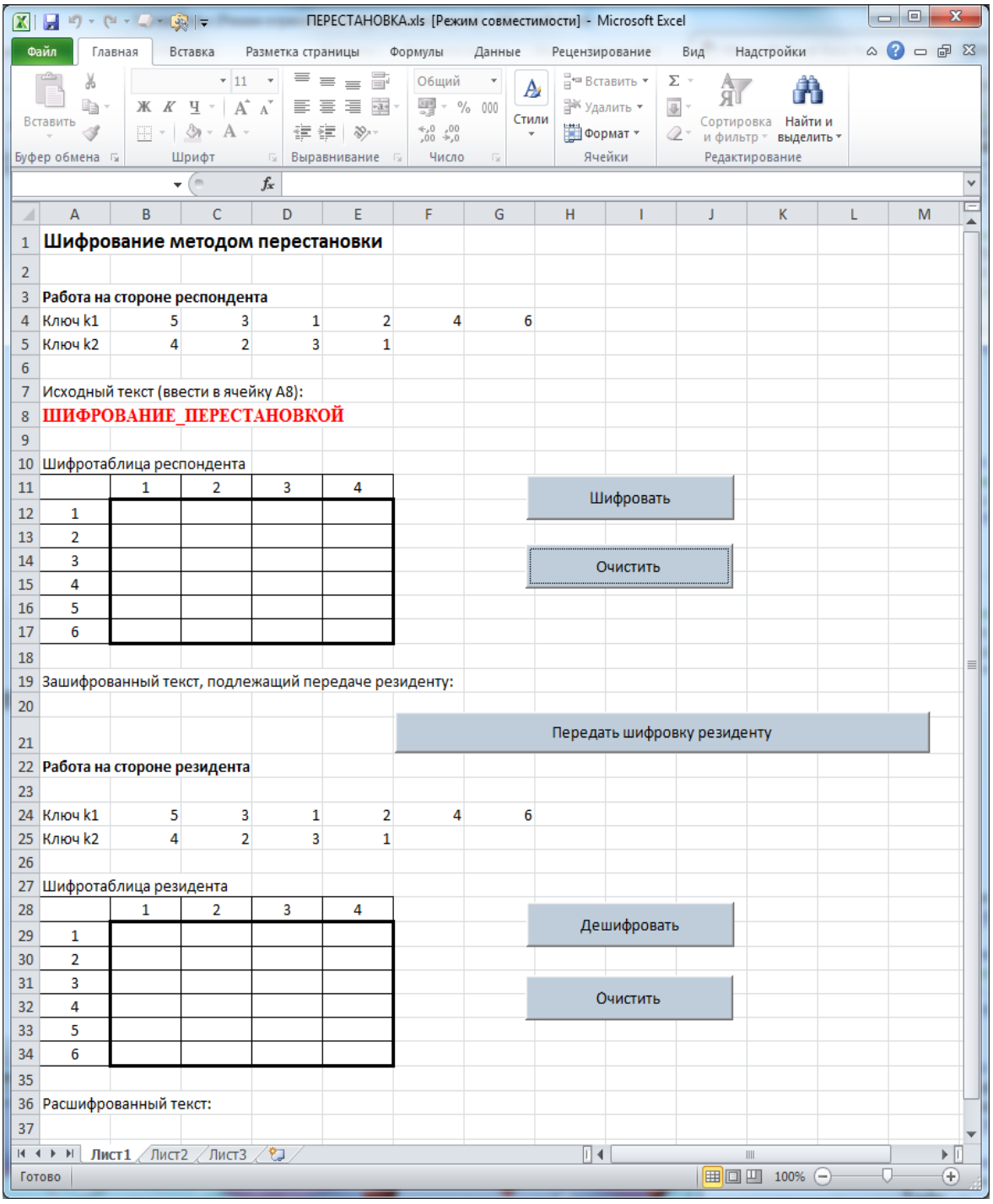


Рис. 3.1. Образец интерфейса для программы шифрования методом перестановки

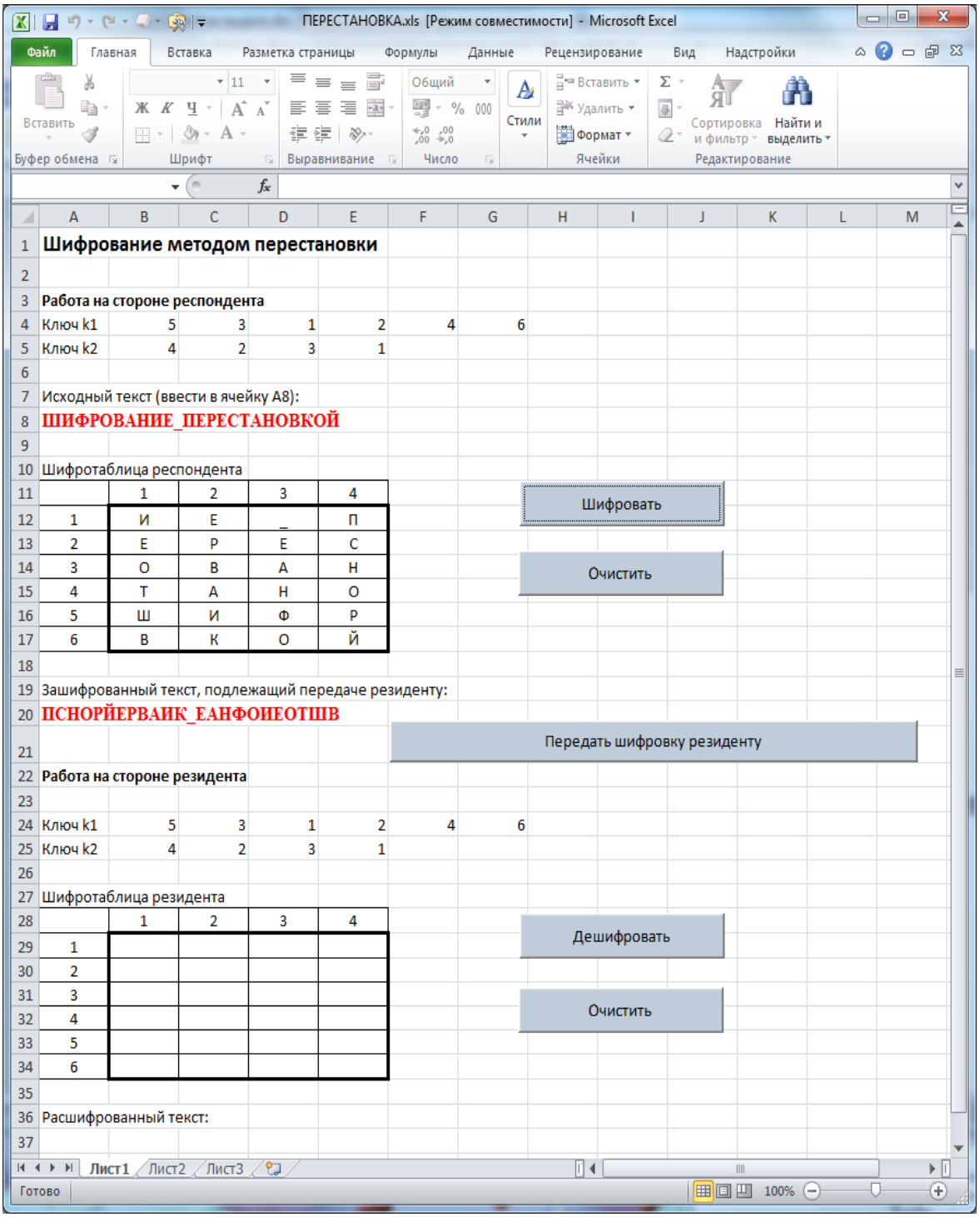


Рис. 3.2. Вид окна программы шифрования методом перестановки после нажатия кнопки «Шифровать»

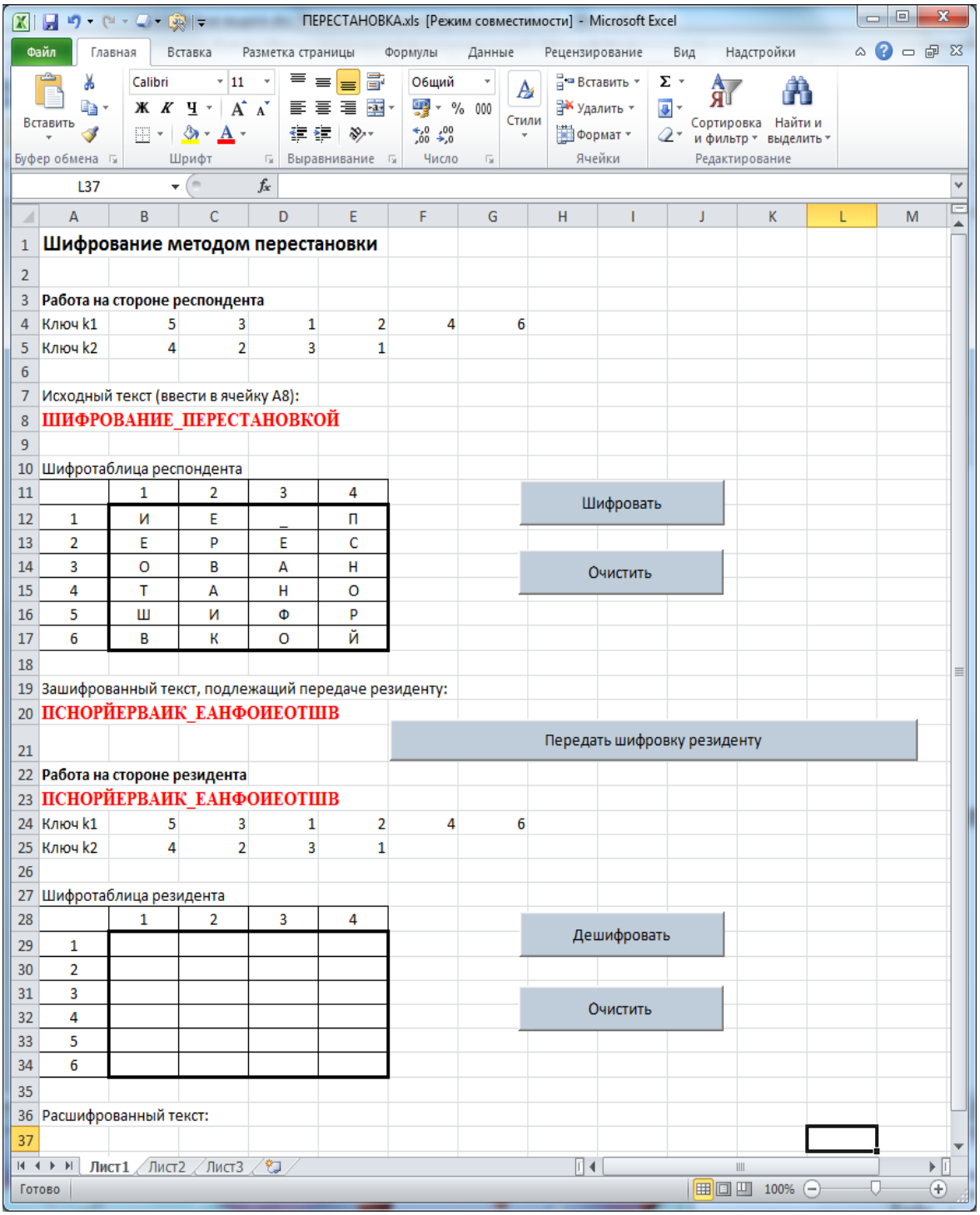


Рис. 3.3. Вид окна программы шифрования методом перестановки после нажатия кнопки «Передать шифровку резиденту»

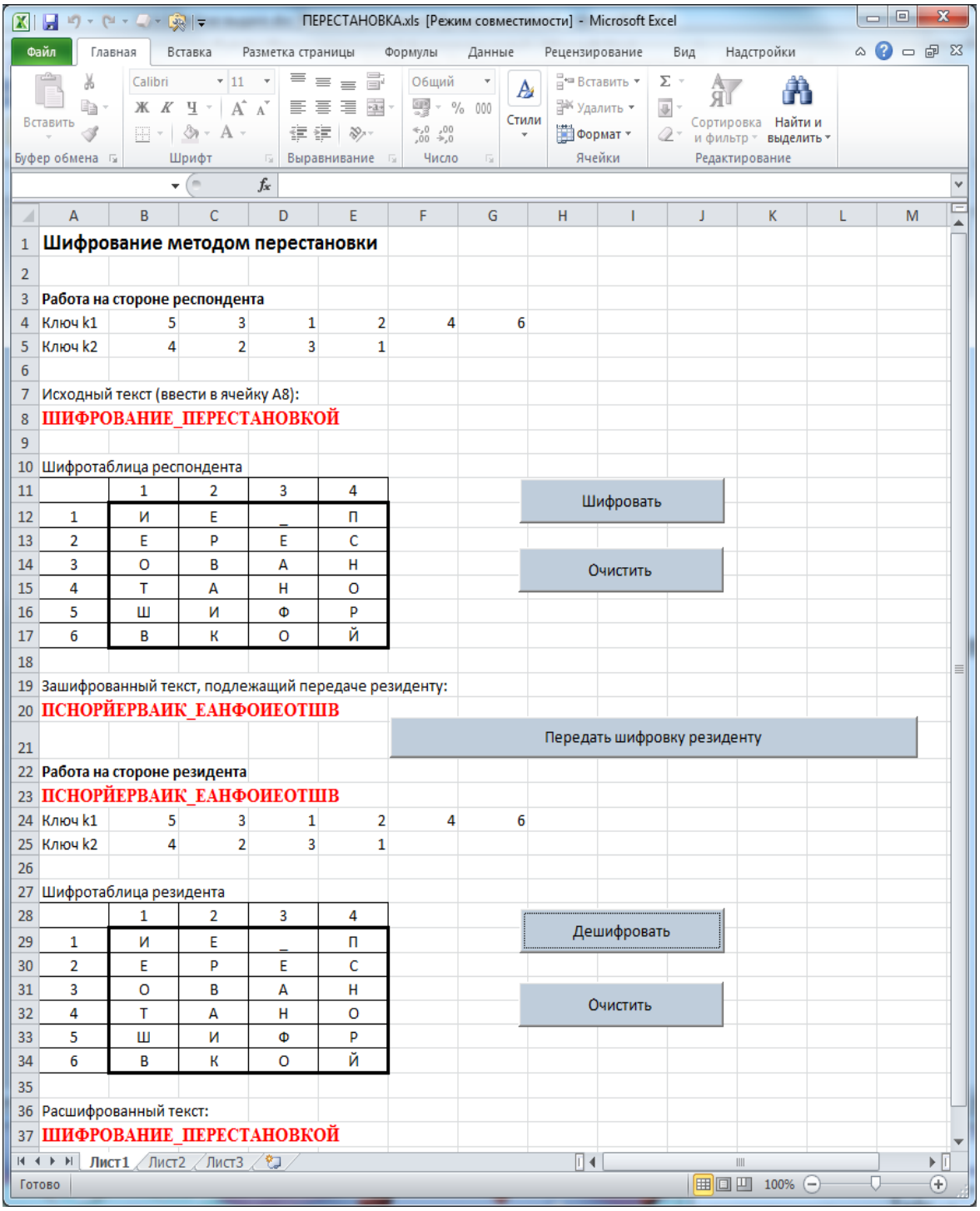


Рис. 3.4. Вид окна программы шифрования методом перестановки после нажатия кнопки «Дешифровать»

Текст программы для шифротаблицы заданного размера на языке *VBA* представлен на рис. 3.5 и 3.6.

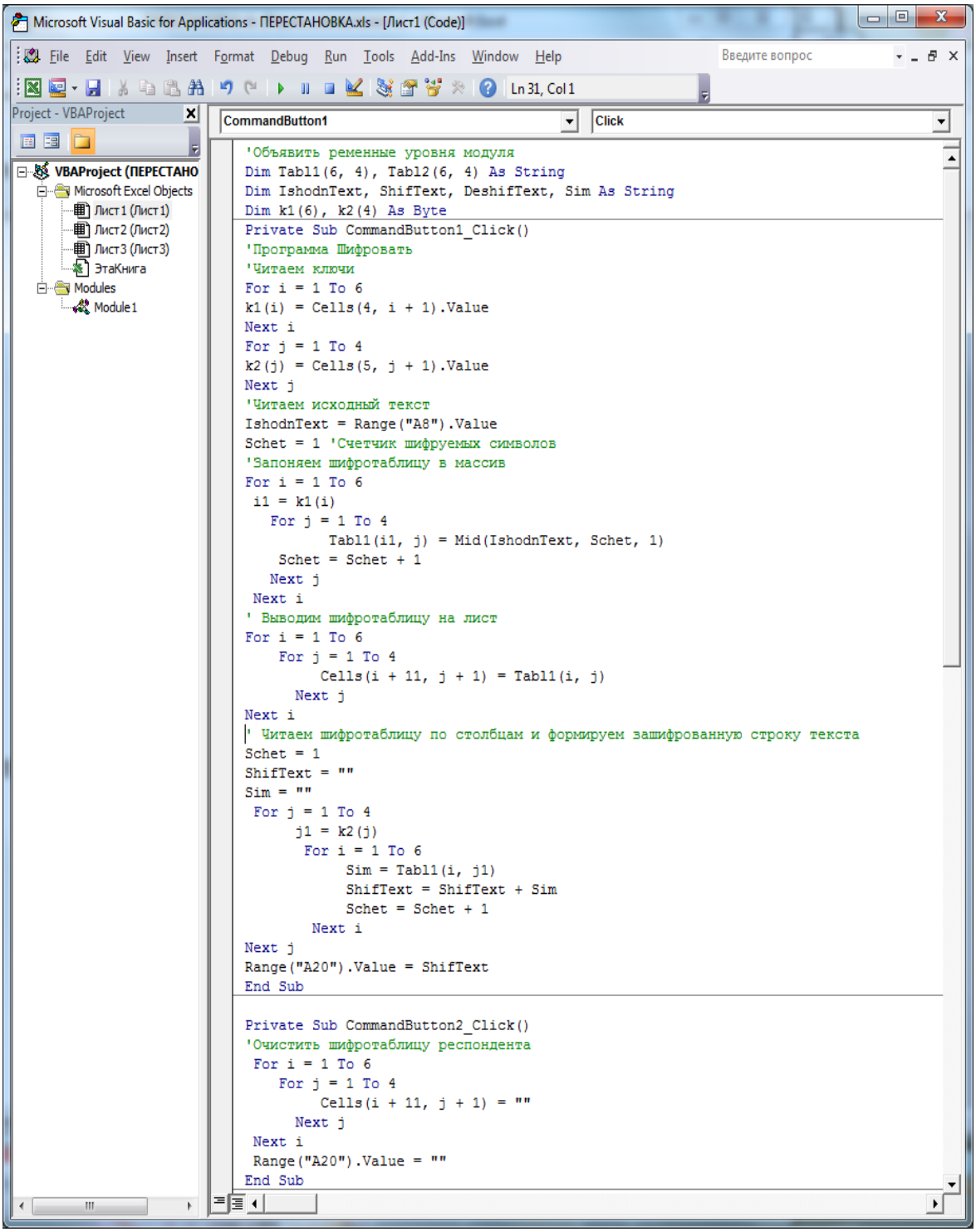


Рис. 3.5. Вид окна программы шифрования методом перестановки на стороне респондента

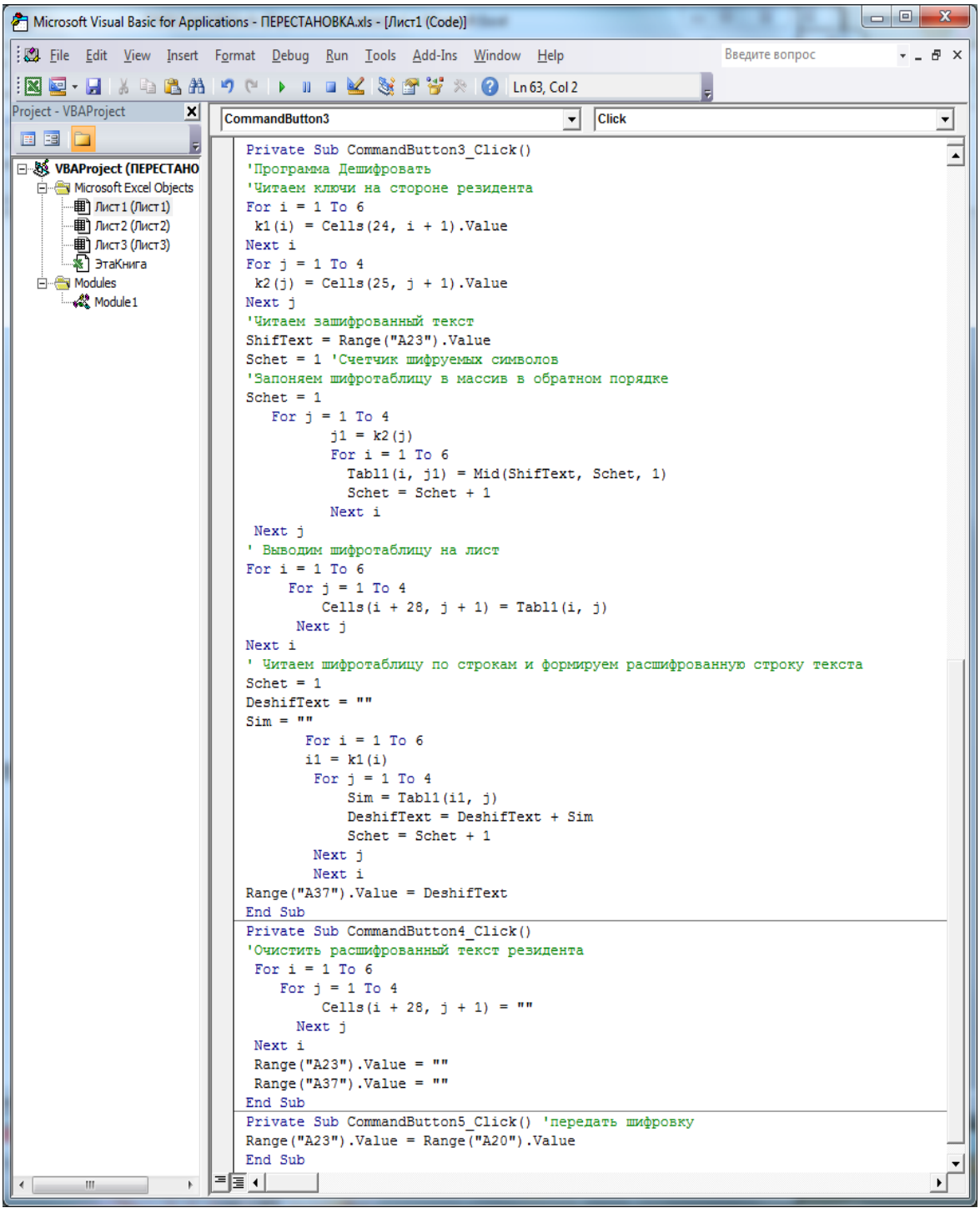


Рис. 3.6. Вид окна программы шифрования методом перестановки на стороне резидента

Задание № 3

Составить программу для шифрования методом перестановки с произвольной длиной сообщения.

Для выполнения этого задания в программу Задания 2 необходимо внести изменения:

- сообщение разделяется на блоки, каждый из которых умещается в шифротаблицу;
- размер самой шифротаблицы должен остаться таким же, как и в предыдущем задании;
- определить количество блоков, необходимых размещения сообщения произвольной длины, с помощью функции *Len*(*IshodnText*)/(*n*1**n*2), где *IshodnText* – строка, содержащая сообщение произвольной длины, *n*1 и *n*2 – размеры ключей ***k*1** и ***k*2**;
- организовать по определенному количеству блоков внешний цикл, внутри которого использовать тот же алгоритм шифрования одного блока;
- по результатам выполнения заданий составить отчет.

Задание № 4. Дополнительно для самостоятельной работы

Составить программу для шифрования методом перестановки с повышенной криптостойкость одним из следующих способов.

1. Для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования. При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы – они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы.

2. Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

3.1.2. Шифрование методом замены

Общие сведения

Шифрование методом замены (подстановки) состоит в замене символов одного алфавита на символы другого алфавита, называемого **шифроалфавитом**. Последний получают перестановкой букв алфавита в произвольном порядке. Шифроалфавит и является **ключом** для шифрования и дешифрования. Замена может быть заменой «символы на символы» либо «символы на цифры». По стойкости и трудоемкости методы замены подразделяются на: одноалфавитную подстановку, многоалфавитную одноконтурную подстановку, многоалфавитную одноконтурную монофоническую подстановку, многоалфавитную многоконтурную подстановку.

Одноалфавитная подстановка

Одноалфавитная подстановка – это прямая замена символов шифруемого сообщения другими символами того же самого или другого алфавита **(**или соответствующими им цифрами**)**. Трудоемкость этого метода невелика, но также низка и стойкость: 20–30.

Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому зная стандартные частоты появления символов в том языке, на котором написано сообщение и, подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко.

Поскольку ключ (шифроалфавит) необходимо хранить в секрете, исторически сложилось использовать не произвольную перестановку, которую трудно запомнить, а парольную фразу из какой-нибудь известной отправителю и получателю книги.

Парольная фраза построчно заполняется в матрицу-ключ размером, например, 6×6. При этом повторяющиеся в парольной фразе символы в матрицу-ключ не заносятся. Если после этого в таблице остались пустые клетки, их заполняют недостающими буквами по, например, алфавитному порядку.

Возьмём в качестве примера парольную фразу: «Зима! Крестьянин, торжествуя, на дровнях обновляет путь» и занесем её в таблицу без повторов букв (табл. 3.3).

Таблица 3.3. Таблица с парольной фразой

	1	2	3	4	5	6
1	**З**	**и**	**м**	**а**	**!**	**К**
2	**р**	**е**	**с**	**т**	**ь**	**я**
3	**н**	**,**	**о**	**ж**	**в**	**у**
4	**д**	**х**	**б**	**л**	**п**	
5						
6						

Часть букв алфавита осталась не представленной в табл. 3.3, поэтому заполняем ими оставшиеся пустые поля и получим итоговую матрицу-ключ для шифрования (табл. 3.4).

Таблица 3.4. Матрица-ключ для шифрования методом замены с одноалфавитной подстановкой по парольной фразе способом «символы на цифры»

	1	2	3	4	5	6
1	З	и	м	а	!	К
2	р	е	с	т	ь	я
3	н	,	о	ж	в	у
4	д	х	б	л	п	**г**
5	**й**	**ф**	**ц**	**ч**	**ш**	**щ**
6	**ы**	**ъ**	**э**	**ю**		**.**

Далее каждый символ текста, подлежащего шифрованию, заменяется парой чисел: номером строки и номером столбца, на пересечении которых этот символ находится в матрице-ключе. Например, слово «**ура**» будет иметь зашифрованный вид: **36 21 14.** Это способ замены «символы на цифры».

При замене «символы на символы» в матрицу-ключ необходимо дописать символы исходного алфавита по порядку. По этим символам находятся заменяющие их символы. В этом случае матрицу-ключ использовать не обязательно, можно просто расположить символы шифроалфавита и алфавита в столбец (строку). Чтобы различать маленькие

и большие буквы, их легко добавить в шифроалфавит (в этом примере они не различаются).

Для дешифрования необходимо составить дешифроалфавит в обратном порядке**.** В табл. 3.5 представлена матрица-ключ, содержащая шифроалфавит с той же парольной фразой (знаки препинания для упрощения опущены) и дешифроалфавит для замены способом «символы на символы», которая будет использована в Задании 2.

Таблица 3.5. Матрица-ключ для шифрования методом замены с одноалфавитной подстановкой по парольной фразе способом «символы на символы»

Шифроалфавит	Алфавит	Поряд. №	Исходный текст	Зашифрованный текст	Дешифроалфавит
з	а	1	а	з	г
и	б	2			т
м	в	3			о
а	г	4			х
к	д	5			р
р	е	6			ж
е	ж	7			н
с	з	8			а
т	и	9			б
ь	й	10			ц
я	к	11			д
н	л	12			у
о	м	13			в
ж	н	14			л
в	о	15			м
у	п	16			ф
д	р	17	р	д	е
х	с	18			з
б	т	19			и
л	у	20	у	л	п
п	ф	21			ч
г	х	22			с
й	ц	23			ш
ф	ч	24			щ
ц	ш	25			ъ

Окончание табл. 3.5

ч	щ	26			ы
ш	ъ	27			э
щ	ы	28			ь
ы	ь	29			й
ъ	э	30			ю
э	ю	31			я
ю	я	32			к

Таким образом, при шифровании методом замены «символы на символы» слово «ура» будет иметь зашифрованный вид «лдз», а слово «сон» – «хвж».

Многоалфавитная одноконтурная обыкновенная подстановка

Для замены символов можно использовать несколько алфавитов, причем смена алфавитов проводится последовательно и циклически. Первый символ шифруемого сообщения заменяется на соответствующий символ первого алфавита, второй – на символ из второго алфавита и т. д., пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

Рассмотрим шифрование с помощью ***таблицы Вижинера*** – квадратной матрицы с n^2 элементами, где n – число символов используемого алфавита. В первой строке матрицы содержится исходный алфавит, каждая следующая строка получается из предыдущей циклическим сдвигом влево на один символ (табл. 3.6).

Для шифрования необходимо задать ключ – слово с неповторяющимися символами. Таблицу замены получают следующим образом: строку «Символы шифруемого текста» формируют из первой строки матрицы Вижинера, а строки из раздела «Заменяющие символы» образуются из строк матрицы Вижинера, первые символы которых совпадают с символами ключевого слова.

При шифровании и дешифровании нет необходимости держать в памяти всю матрицу Вижинера, поскольку используя свойства циклического сдвига, можно легко вычислить любую строку матрицы по ее номеру и первой строке.

Таблица 3.6. Таблица Вижинера для русского алфавита

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

При шифровании символы из первой строки заменяются символами остальных строк по правилу

$a(1,i) => a(k, i)$, (3.1)

где k – номер используемой для шифрования строки.

Используя свойства циклического сдвига влево, элементы k-ой строки можно выразить через элементы первой строки

$$a(k, i) = \begin{cases} a(1, i+k-1), \text{ если } i <= n-k+1 \\ a(1, i-n+k-1), \text{ если } i > n-k+1. \end{cases} \quad (3.2)$$

При дешифровании производится обратная замена

$$a(k, i) => a(1, i). \quad (3.3)$$

Поэтому необходимо решить следующую задачу: пусть очередной дешифруемый символ в тексте – $a(1,j)$ и для дешифрования используется k-ая строка матрицы Вижинера. Необходимо найти в k-ой строке номер элемента, равного $a(1,j)$. Очевидно,

$$a(1, j) = \begin{cases} a(k, j-k+1), \text{ если } j >= k \\ a(k, n-k+j+1), \text{ если } j < k. \end{cases} \quad (3.4)$$

Таким образом, при дешифровании по k-ой строке матрицы Вижинера символа из зашифрованного текста, значение которого равно $a(1, j)$, проводится обратная подстановка

$$a(1, j) => \begin{cases} a(1, j-k+1), \text{ если } j >= k \\ a(1, n-k+j+1), \text{ если } j < k. \end{cases} \quad (3.5)$$

Стойкость метода равна стойкости метода подстановки, умноженной на количество используемых при шифровании алфавитов, т. е. на длину ключевого слова и равна $20*L$, где L – длина ключевого слова.

С целью повышения стойкости шифрования предлагаются следующие усовершенствования таблицы Вижинера:

1. Во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке.

2. В качестве ключа используются случайные последовательности чисел, которые задают номера используемых строк матрицы Вижинера для шифрования.

Многоалфавитная одноконтурная монофоническая подстановка

В монофонической подстановке количество и состав алфавитов выбирается таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается большее число заменяющих символов, чем для редко встречающихся (табл. 3.7).

Таблица 3.7. Пример таблицы монофонической замены

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 Ь Ы Ъ Э Ю Я _
Ф Н (Щ И Г Е R А Д Ы ~ @ S Л Я Ж ^ С Ш М Б Q П Т Х Ю Ъ Р } \ _ #
* Н У Щ D + Е R = Д Ц Й Ч [В Ь) О & { М Б Q П Т Х Ю Ъ Р } \ _ <
Л Н (Щ И] Е R % Д Ы ~ @ G / Я Э З " Ш М Б Q П Т Х Ю Ъ Р } \ _ W
Ф Н У Щ D К Е R А Д Ц Й Ч S + Ь Ж ^ С { М Б Q П Т Х Ю Ъ Р } \ _ V

Шифрование проводится так же, как и при простой подстановке, с той лишь разницей, что после шифрования каждого символа соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию. Таким образом, столбцы алфавитов как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака исходного текста.

Многоалфавитная многоконтурная подстановка

Многоконтурная подстановка заключается в том, что для шифрования используются несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Общая модель шифрования подстановкой может быть представлена в следующем виде:

$$t_ш = t_о + w \; mod \; (k–1), \qquad (3.6)$$

где $t_ш$ – символ зашифрованного текста; $t_о$ – символ исходного текста; w – целое число в диапазоне (0 – (k–1)); k – число символов используемого алфавита.

Если w фиксировано, то формула описывает одноалфавитную подстановку, если w выбирается из последовательности w_1, w_2, ..., w_n, то получается многоалфавитная подстановка с периодом n.

Если в многоалфавитной подстановке $n > m$ (где m – число знаков шифруемого текста) и любая последовательность w_i, $i = 1, 2, ...,$ n используется только один раз, то такой шифр является теоретически не раскрываемым. Этот шифр получил название шифра Вернама.

Стойкость простой многоалфавитной подстановки оценивается величиной 20*n, где n – число различных алфавитов, используемых для замены. Усложнение многоалфавитной подстановки существенно повышает ее стойкость. Монофоническая подстановка может быть весьма

стойкой (и даже теоретически не раскрываемой), однако строго монофоническую подстановку реализовать на практике трудно, а любые отклонения от монофоничности снижают реальную стойкость шифра.

Задание № 1

Зашифровать вручную свои данные «фамилия имя отчество» по парольной фразе из любого известного классического произведения двумя способами: «символы на символы» и «символы на цифры». В отчете представить матрицы-ключи в соответствии с таблицами 3.3 и 3.4.

Задание № 2

Составить программу для шифрования методом замены. При составлении программы использовать образец (рис. 3.7–3.9), в который необходимо внести изменения, соответствующие Вашему индивидуальному заданию. Учесть различие строчных и прописных букв русского алфавита.

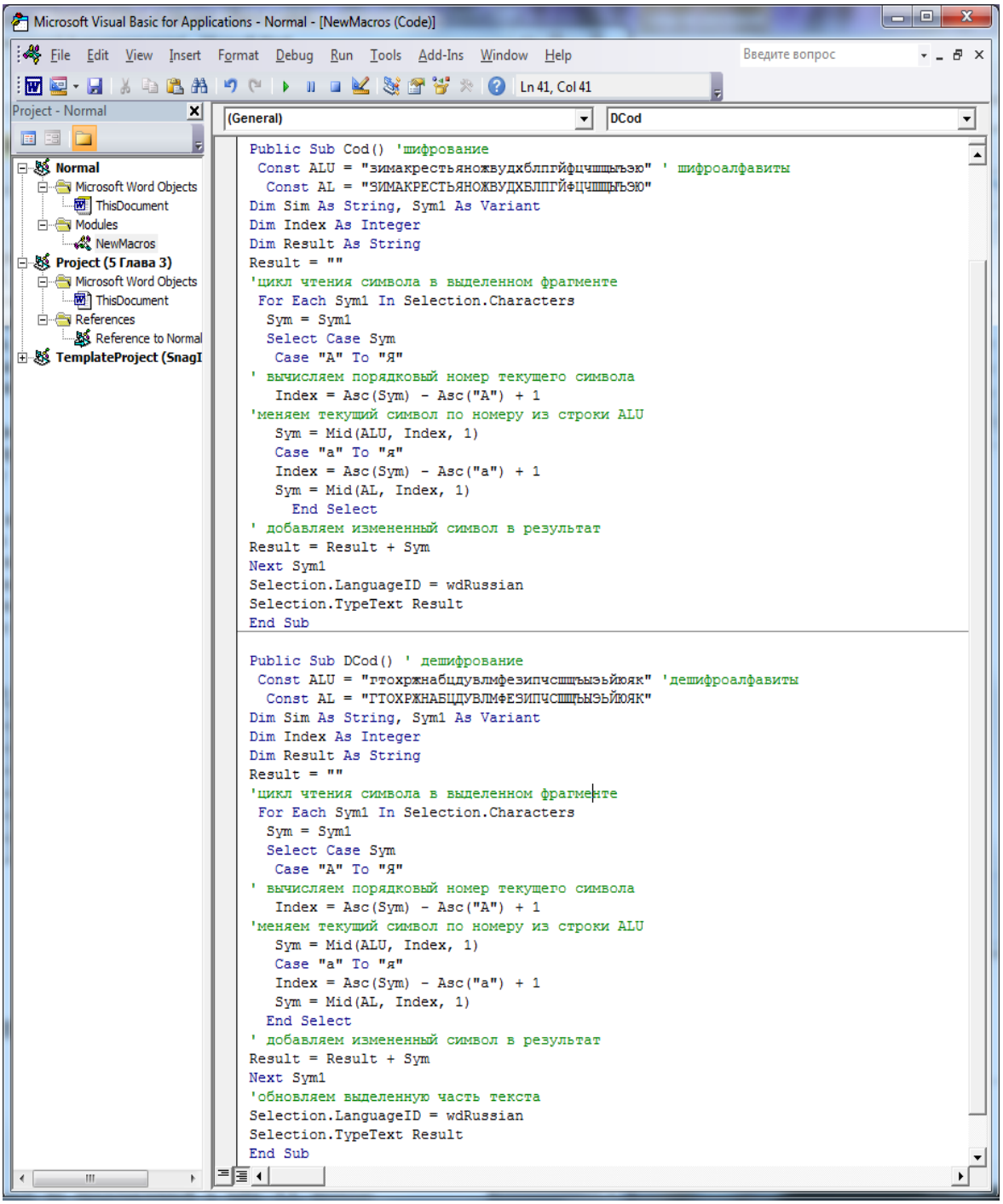
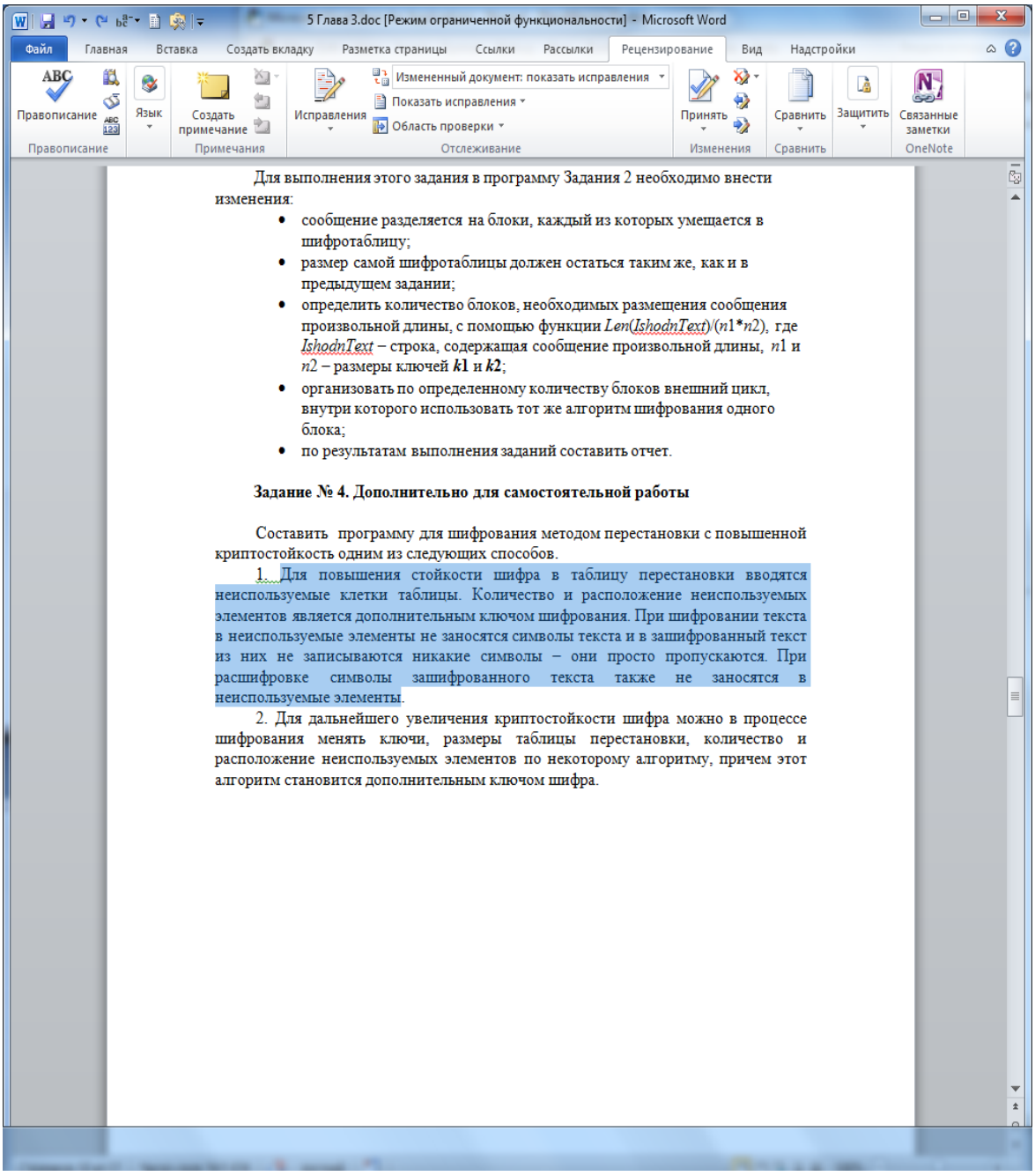


Рис. 3.7. Вид окна программы шифрования и дешифрования методом замены «символы на символы»



Для выполнения этого задания в программу Задания 2 необходимо внести изменения:

- сообщение разделяется на блоки, каждый из которых умещается в шифротаблицу;
- размер самой шифротаблицы должен остаться таким же, как и в предыдущем задании;
- определить количество блоков, необходимых размещения сообщения произвольной длины, с помощью функции *Len*(*IshodnText*)/(*n*1**n*2), где *IshodnText* – строка, содержащая сообщение произвольной длины, *n*1 и *n*2 – размеры ключей ***k*1** и ***k*2**;
- организовать по определенному количеству блоков внешний цикл, внутри которого использовать тот же алгоритм шифрования одного блока;
- по результатам выполнения заданий составить отчет.

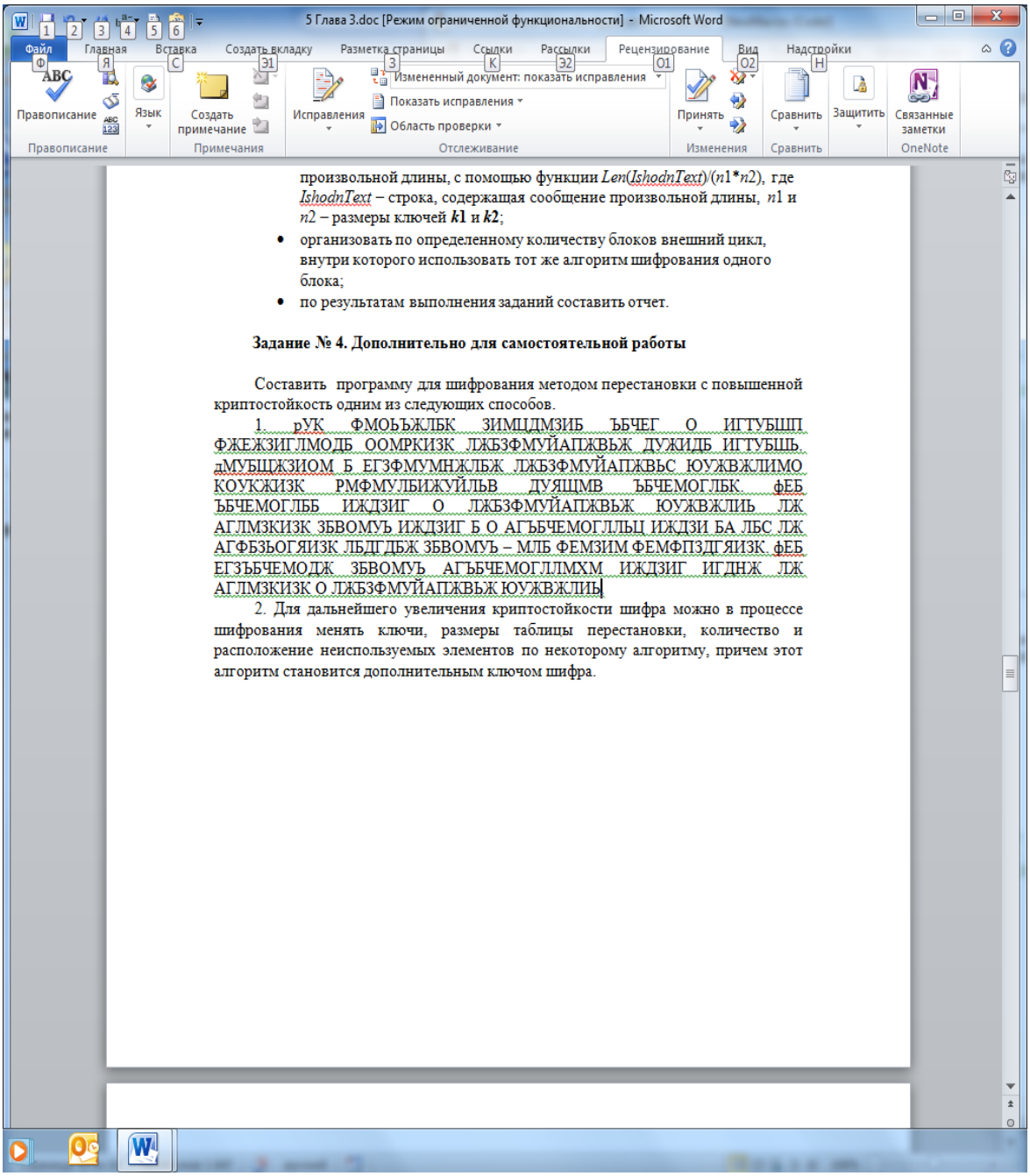
Задание № 4. Дополнительно для самостоятельной работы

Составить программу для шифрования методом перестановки с повышенной криптостойкость одним из следующих способов.

1. Для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования. При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы – они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы.

2. Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

Рис. 3.8. Вид окна исходного текста перед шифрованием методом замены «символы на символы»



произвольной длины, с помощью функции *Len*(*IshodnText*)/(*n*1**n*2), где *IshodnText* – строка, содержащая сообщение произвольной длины, *n*1 и *n*2 – размеры ключей ***k*1** и ***k*2**;

- организовать по определенному количеству блоков внешний цикл, внутри которого использовать тот же алгоритм шифрования одного блока;
- по результатам выполнения заданий составить отчет.

Задание № 4. Дополнительно для самостоятельной работы

Составить программу для шифрования методом перестановки с повышенной криптостойкость одним из следующих способов.

1. рУК ФМОЬЪЖЛБК ЗИМЦДМЗИБ ЬБЧЕГ О ИГТУБШП ФЖЕЖЗИГЛМОДБ ООМРКИЗК ЛЖБЗФМУЙАПЖВЬЖ ДУЖИДБ ИГТУБШЬ дМУБЩЖЗИОМ Б ЕГЗФМУМНЖЛБЖ ЛЖБЗФМУЙАПЖВЬС ЮУЖВЖЛИМО КОУКЖИЗК РМФМУЛБИЖУЙЛЬВ ДУЯЩМВ ЬБЧЕМОГЛБК ФЕБ ЬБЧЕМОГЛББ ИЖДЗИГ О ЛЖБЗФМУЙАПЖВЬЖ ЮУЖВЖЛИЬ ЛЖ АГЛМЗКИЗК ЗБВОМУЬ ИЖДЗИГ Б О АГЬБЧЕМОГЛЛЬЦ ИЖДЗИ БА ЛБС ЛЖ АГФБЗЬОГЯИЗК ЛБДГДБЖ ЗБВОМУЬ – МЛБ ФЕМЗИМ ФЕМФПЗДГЯИЗК ФЕБ ЕГЗЬБЧЕМОДЖ ЗБВОМУЬ АГЬБЧЕМОГЛЛМХМ ИЖДЗИГ ИГДНЖ ЛЖ АГЛМЗКИЗК О ЛЖБЗФМУЙАПЖВЬЖ ЮУЖВЖЛИЬ

2. Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

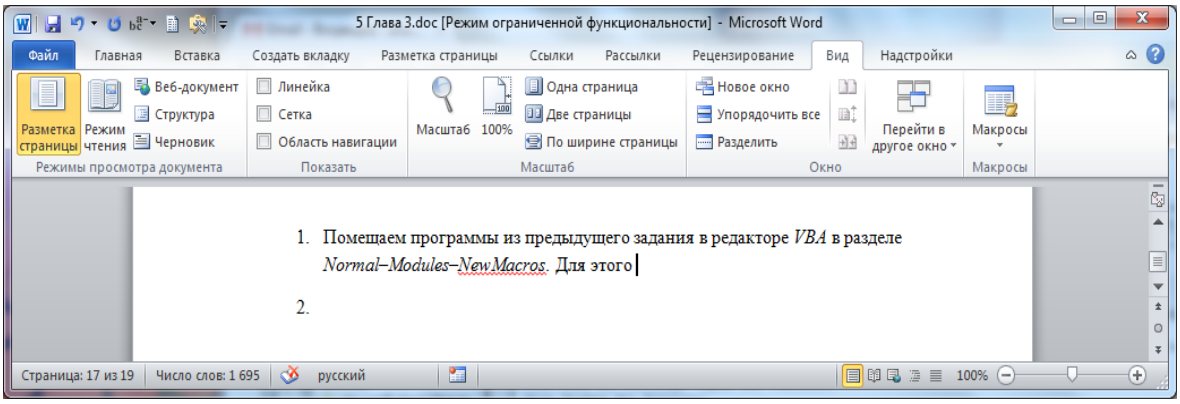
Рис. 3.9. Вид окна исходного текста после шифрования методом замены «символы на символы»

Зашифрованную часть текста необходимо вновь выделить и выполнить программу дешифрования. Текст должен принять первоначальный вид (рис. 3.8).

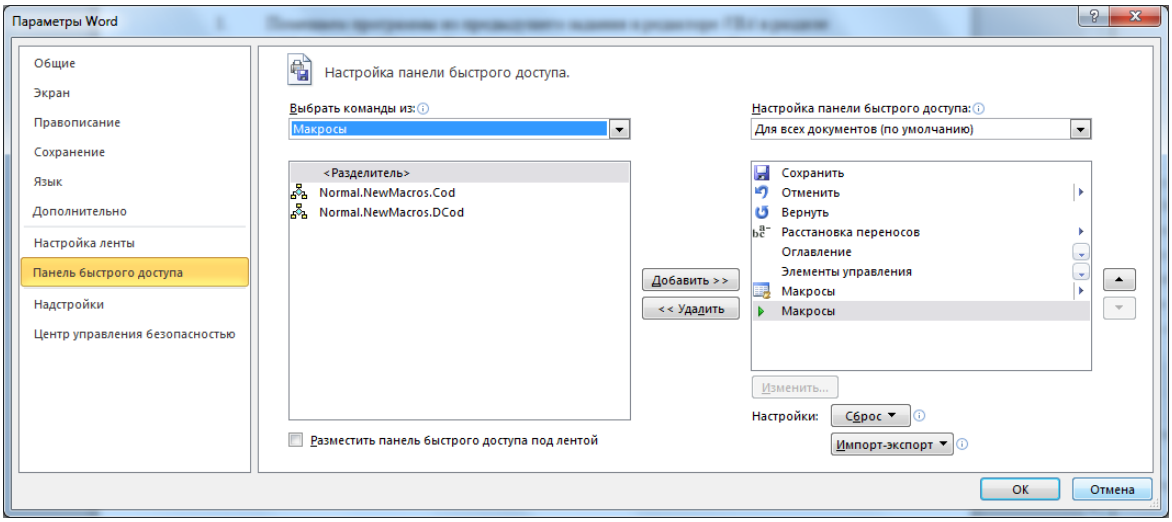
Задание № 3

Создать кнопки запуска программ шифрования и дешифрования на панели инструментов *Word*. Пример отчета приведен ниже.

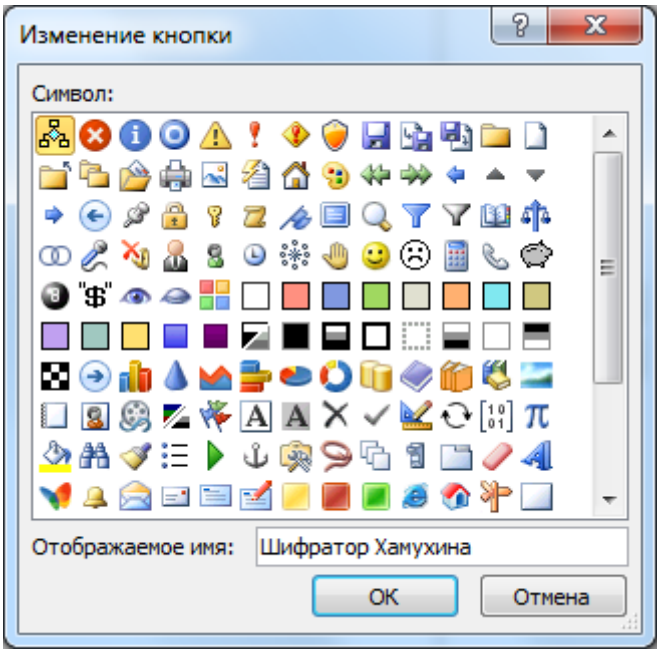
1. Помещаем программы из предыдущего задания в редакторе *VBA* в разделе *Normal–Modules–NewMacros*. Для этого открываем на ленте вкладку «Вид» и щелкаем «Макросы». Вставим скопированные предварительно программы в указанный раздел.



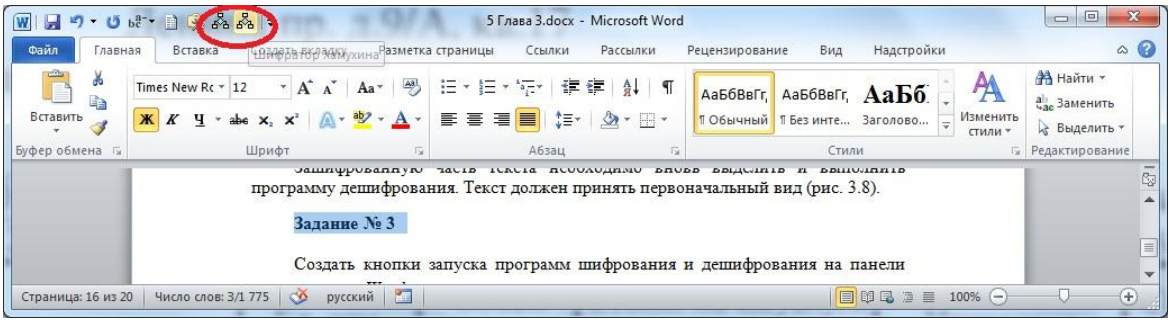
2. Открываем окно настройки панели быстрого доступа через меню «Файл»–«Параметры»–«Панель быстрого доступа». Выбираем команды из меню «Макросы». При этом должно открыться окно с именами макросов, которые мы вставили в предыдущем пункте:



3. Выделяя поочередно оба наименования макросов, нажимаем «Добавить» и внизу окна нажимаем «Изменить». В появившемся окне вводим новое имя кнопки (со своей фамилией). Копию экрана со своей кнопкой вставим в отчет.



4. Проверяем работу наших кнопок с панели быстрого доступа.



Вывод: выделенный текст при последовательном нажатии наших кнопок сначала зашифровался, затем дешифровался, следовательно, работа выполнена правильно.

Задание № 4. Дополнительно для самостоятельной работы

Составить программу для шифрования методом замены с повышенной криптостойкость. Применить многоалфавитную одноконтурную подстановку.

3.1.3. Поточное шифрование

При поточном шифровании секретный ключ называют гаммой, которая представляет собой последовательность битов, вырабатываемых по некоторому алгоритму генератором гаммы. Эта последовательность с помощью логической операции *XOR* («Исключительное ИЛИ») накладывается на биты исходного текста и получается шифротекст. Такой процесс называют гаммированием. Для повышения криптостойкости его можно повторять несколько раз. Само количество повторов и алгоритм работы генераторов гаммы должны быть секретными. Получатель шифротекста должен иметь в точности такой же набор генераторов гаммирования. Операция «Исключительное ИЛИ» имеет такое замечательное свойство, как восстановление исходного значения бита после повторного применения. Поэтому, в точности повторяя гаммирование шифротекста, получатель дешифрует исходный текст.

Если длина ключа (гаммы) равна длине сообщения, и он используется один раз, то такое сообщение взломать невозможно (теорема Шеннона). Такие алгоритмы называют шифром Вернама или одноразовым блокнотом. В шифре Вернама ключ имеет длину, равную длине самого передаваемого сообщения и, если каждый бит ключа выбирается случайно, то вскрыть шифр невозможно (т. к. все возможные открытые тексты будут равновероятны).

Однако на практике длинные ключи использовать неудобно, и они используются только в исключительно важных случаях. Гораздо чаще применяют ключи с фиксированной длиной (128, 256 бит) и гаммирующая последовательность получается псевдослучайной. Это создает возможности злоумышленникам для взлома, но существенно упрощает затраты на шифрование.

Другим недостатком поточного шифрования является проблема синхронизации. Если при передаче произойдет потеря хоть одного бита, то все остальные будут дешифрованы неправильно. По способу решения этой проблемы криптосистемы подразделяют на **синхронные** и системы **с самосинхронизацией.**

В синхронных криптосистемах синхронизация производится путем вставки в сообщение специальных маркеров. Поэтому потеря бита приводит к неверному дешифрованию только до тех пор, пока не будет принят очередной маркер. Эти потери тем меньше, чем чаще расположены маркеры. Но этот способ удлиняет само сообщение.

В криптосистемах с самосинхронизацией применяются асинхронные поточные шифры, в которых поток ключей (гамма) является функ-

цией генератора потока и фиксированного числа знаков шифротекста, которые называют заголовком. Дешифрующий генератор ключей, приняв этот заголовок автоматически синхронизуется с шифрующим генератором.

Известны также алгоритмы поточного шифрования на регистрах сдвига с линейной обратной связью, с нелинейной комбинацией генераторов, с генераторами на нелинейных фильтрах и др.

Задание № 1

Зашифровать вручную свои данные «фамилия имя отчество» методом поточного шифрования по заданному ключу. В отчете представить таблицу в соответствии с примером, приведенным в табл. 3.8.

Таблица 3.8. Пример таблицы поточного шифрования

Исходный текст	Кодировка	Биты	Ключ (гамма)	Гаммирование отправителем	Кодировка	Шифротекст	Гаммирование получателем
1	2	3	4	5	6	7	8
х	22	10110	11111	01001	9	и	10110
а	1	00001	11111	11110	30	э	00001
м	13	01101	11111	10010	18	с	01101
у	20	10100	11111	01011	11	к	10100
х	22	10110	11111	01001	9	и	10110
и	9	01001	11111	10110	22	х	01001
н	14	01110	11111	10001	17	р	01110
а	1	00001	11111	11110	30	э	00001
л	12	01100	11111	10011	19	т	01100
е	6	00110	11111	11001	25	ш	00110
к	11	01011	11111	10100	20	у	01011
с	18	10010	11111	01101	13	м	10010
а	1	00001	11111	11110	30	э	00001
н	14	01110	11111	10001	17	р	01110
д	5	00101	11111	11010	26	щ	00101
р	17	10001	11111	01110	14	н	10001

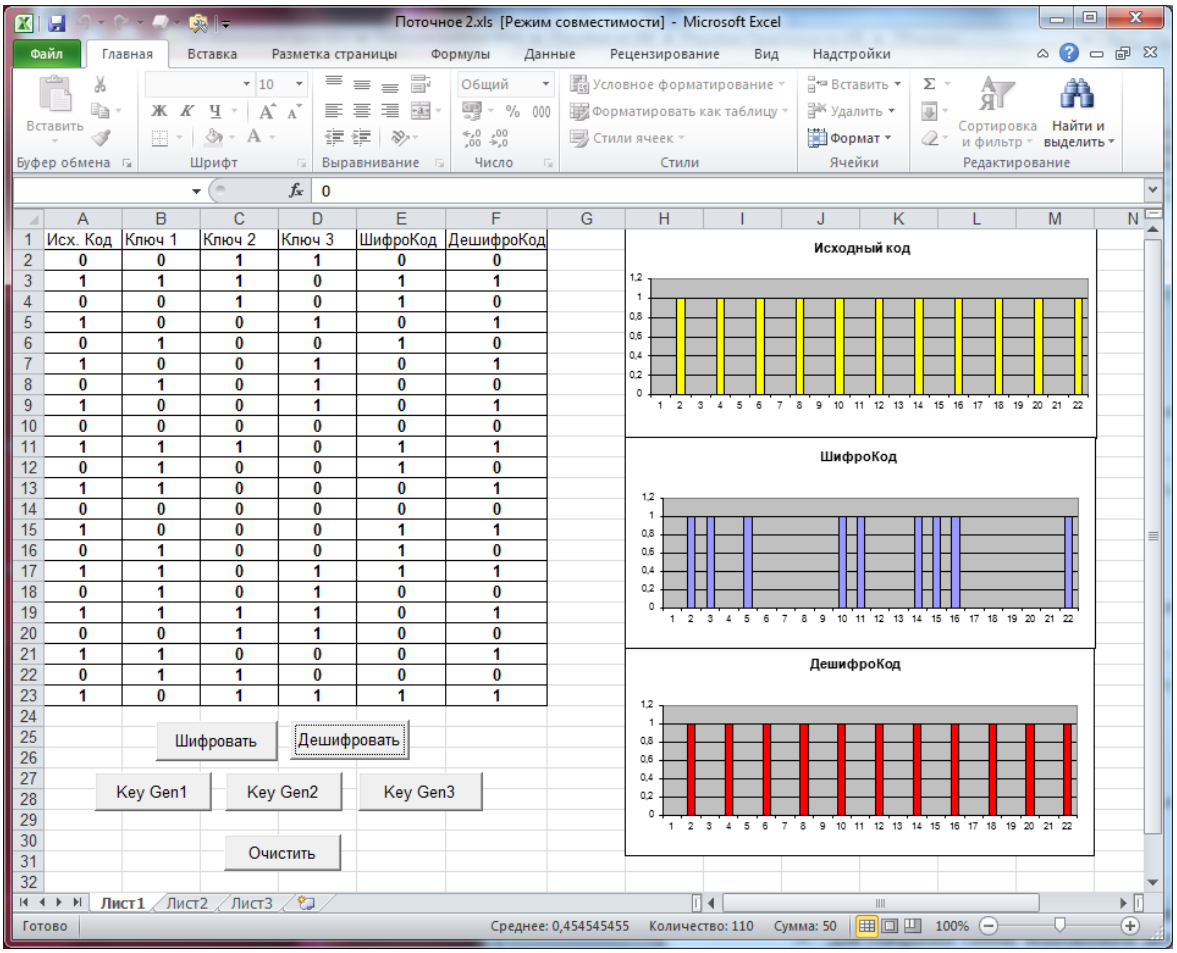
Кодировку алфавита взять из табл. 3.5. При побитном гаммировании использовать логическую операцию «Исключительное ИЛИ», которая дает значение «Истина» (1) только в том случае, когда значения аргументов противоположны. Если значения аргументов совпадают, эта операция дает значение «Ложь» (0). Для упрощения задачи для всех символов взять один и тот же ключ.

Сделать вывод.

Таким образом, исходный текст «**хамухин александр**» был отправителем заменен на шифротекст «**иэскихр этшумэрщн**» методом поточного шифрования и получателем успешно дешифрован, что видно из совпадения значений 8-го и 3-го столбцов.

Задание № 2

Составить программу для метода поточного шифрования Вернама (одноразовый блокнот). При составлении программы использовать образец (рис. 3.10–3.12), в который необходимо внести изменения, соответствующие Вашему индивидуальному заданию, которое выдается преподавателем по номеру в журнале *N*. Для генерации гаммы использовать датчик случайных чисел (функция *RND*) с аргументом *N* (пусковое число для генерации последовательности псевдослучайных чисел). Длина сообщения (ключа) равна *N*+5.



	A	B	C	D	E	F
1	Исх. Код	Ключ 1	Ключ 2	Ключ 3	ШифроКод	ДешифроКод
2	0	0	1	1	0	0
3	1	1	1	0	1	1
4	0	0	1	0	1	0
5	1	0	0	1	0	1
6	0	1	0	0	1	0
7	1	0	0	1	0	1
8	0	1	0	1	0	0
9	1	0	0	1	0	1
10	0	0	0	0	0	0
11	1	1	1	0	1	1
12	0	1	0	0	1	0
13	1	1	0	0	0	1
14	0	0	0	0	0	0
15	1	0	0	0	1	1
16	0	1	0	0	1	0
17	1	1	0	1	1	1
18	0	1	0	1	0	0
19	1	1	1	1	0	1
20	0	0	1	1	0	0
21	1	1	0	0	0	1
22	0	1	1	0	0	0
23	1	0	1	1	1	1

Рис. 3.10. Вид окна интерфейса программы для алгоритма поточного шифрования Вернама

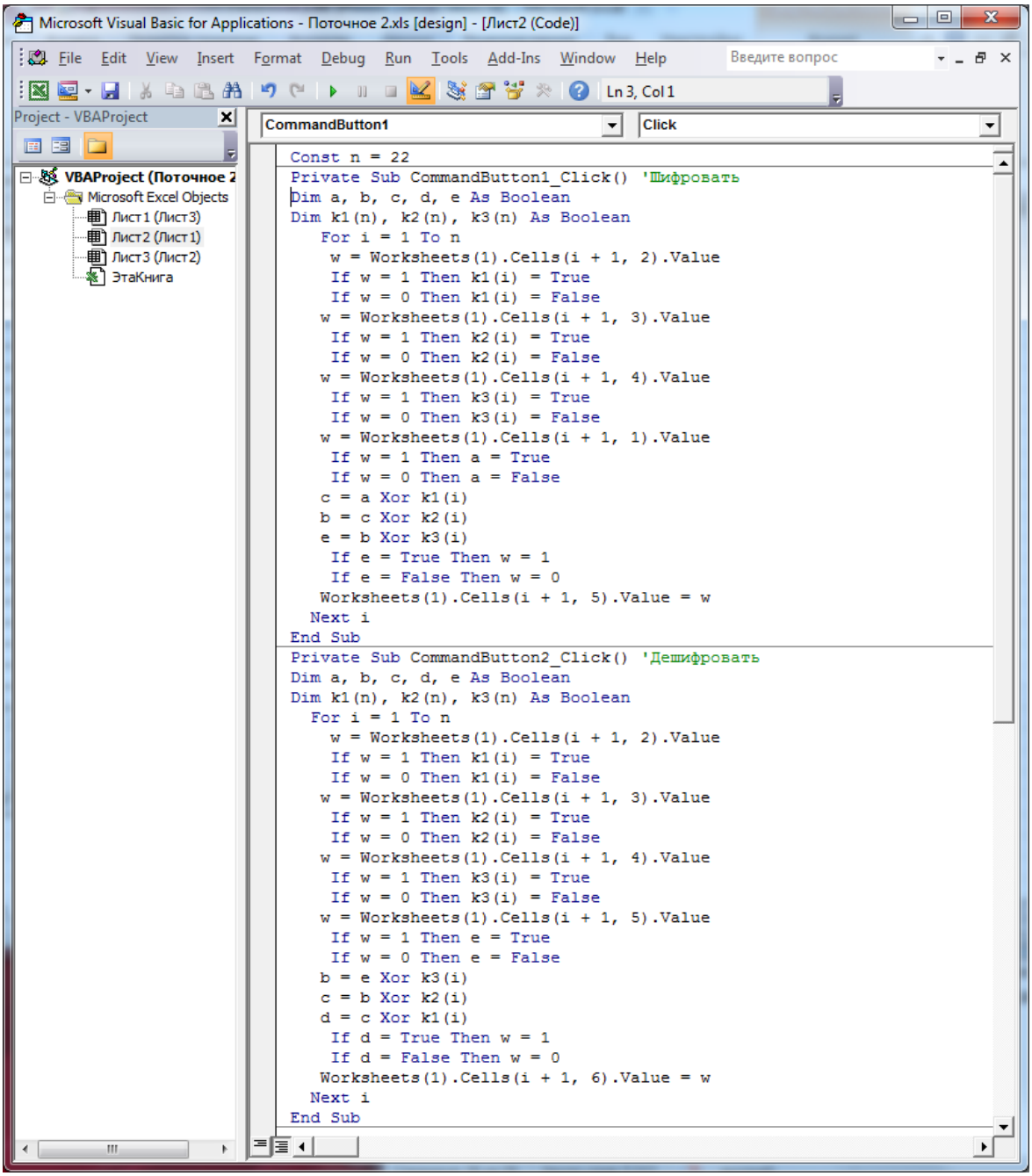


Рис. 3.11. Вид окна текста программы для алгоритма поточного шифрования Вернама (часть 1)

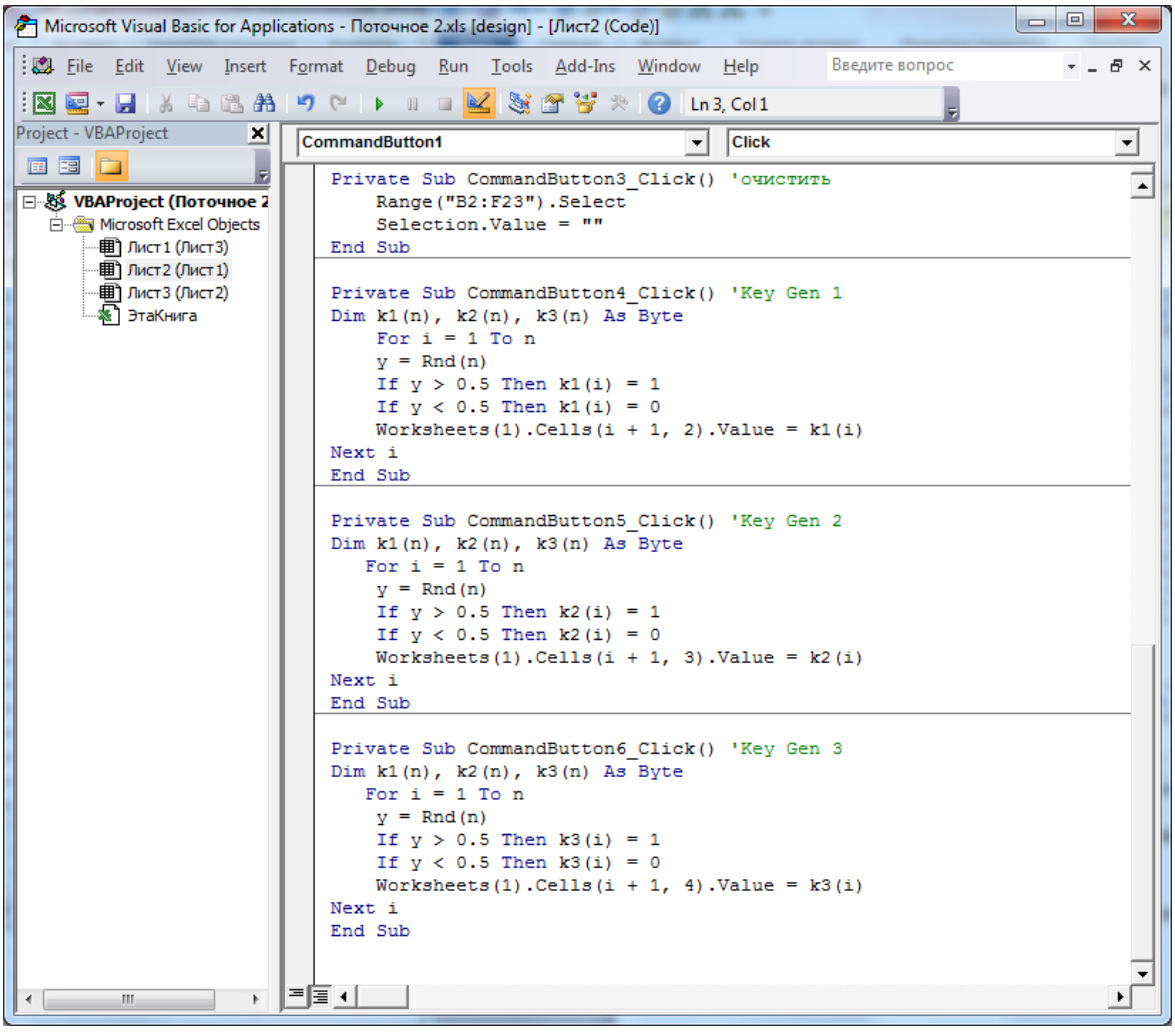


Рис. 3.12. Вид окна текста программы для алгоритма поточного шифрования Вернама (часть 2)

Задание № 3

Составить программу для метода поточного шифрования с ключом фиксированной длины. При составлении программы использовать образец (рис. 3.13–3.15), в который необходимо внести изменения, соответствующие Вашему индивидуальному заданию, которое выдается преподавателем по номеру в журнале *N*. Для генерации гаммы использовать датчик случайных чисел (функция *RND*) с аргументом *N* (пусковое число для генерации последовательности псевдослучайных чисел). Количество битов сообщения должно превышать длину ключа на *N*+5.

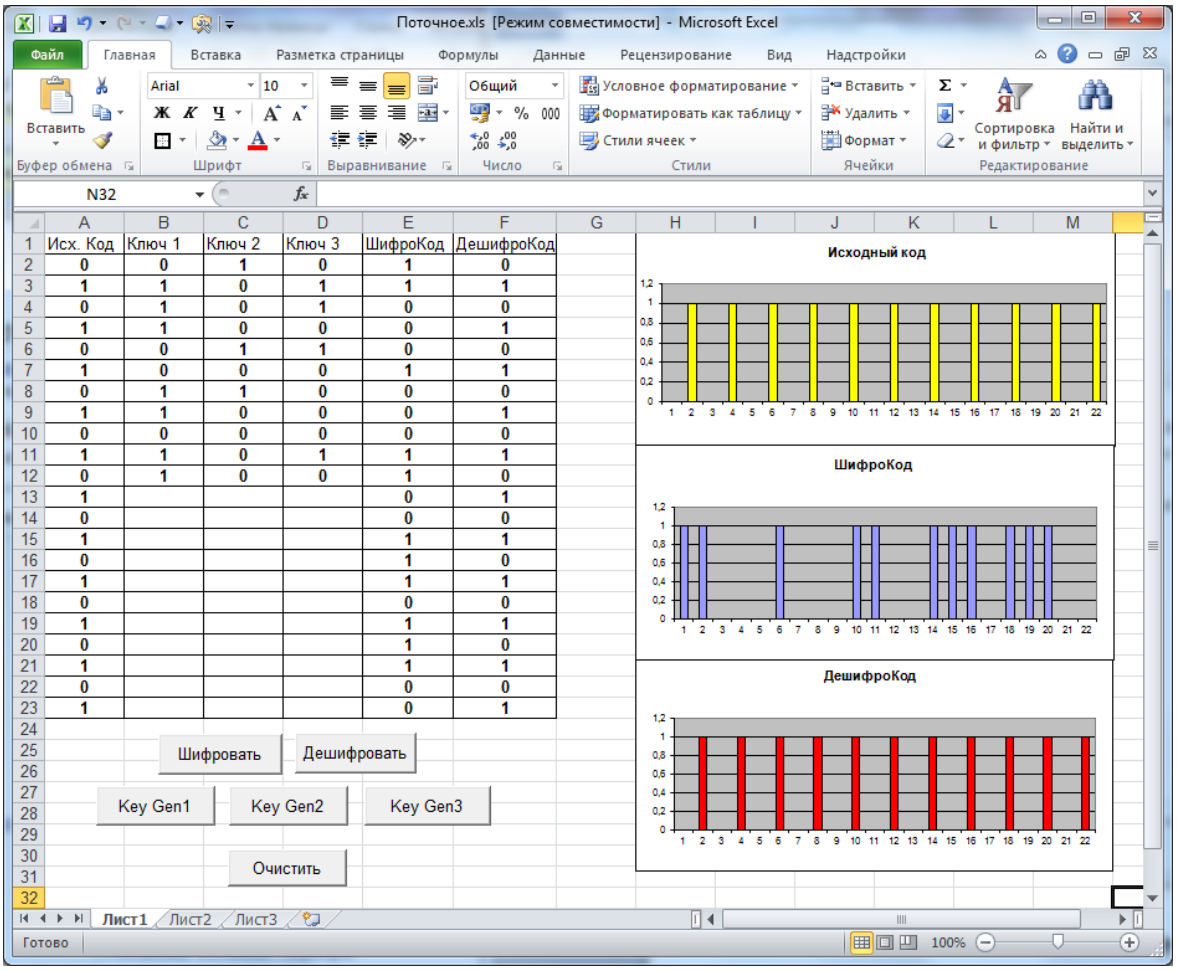


Рис. 3.13. Вид окна интерфейса программы поточного шифрования (количество ключей – 3, длина каждого ключа – 11 бит, длина сообщения – 22 бит)

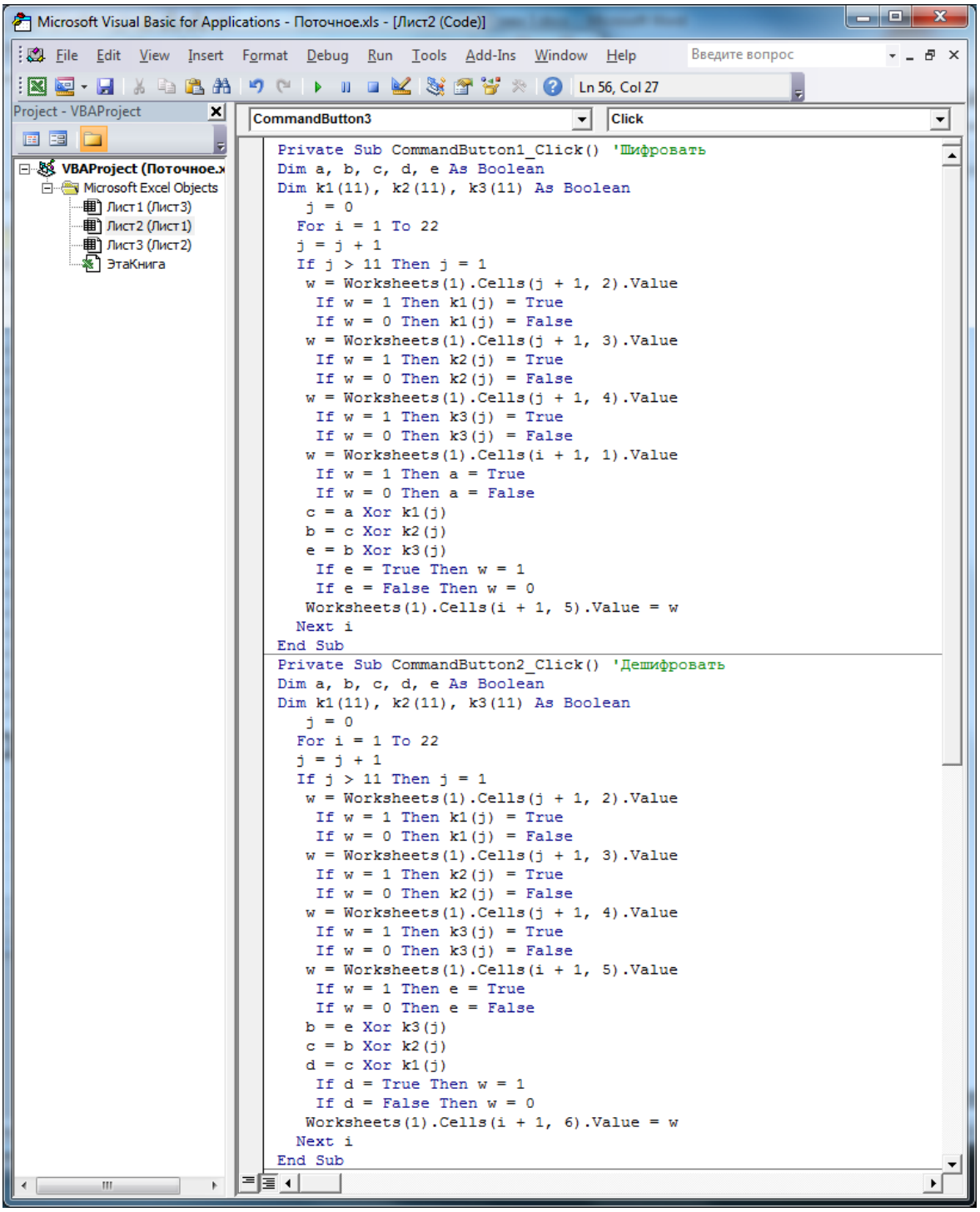


Рис. 3.14. Вид окна текста программы поточного шифрования и дешифрования (количество ключей – 3, длина каждого ключа – 11 бит, длина сообщения – 22 бит)

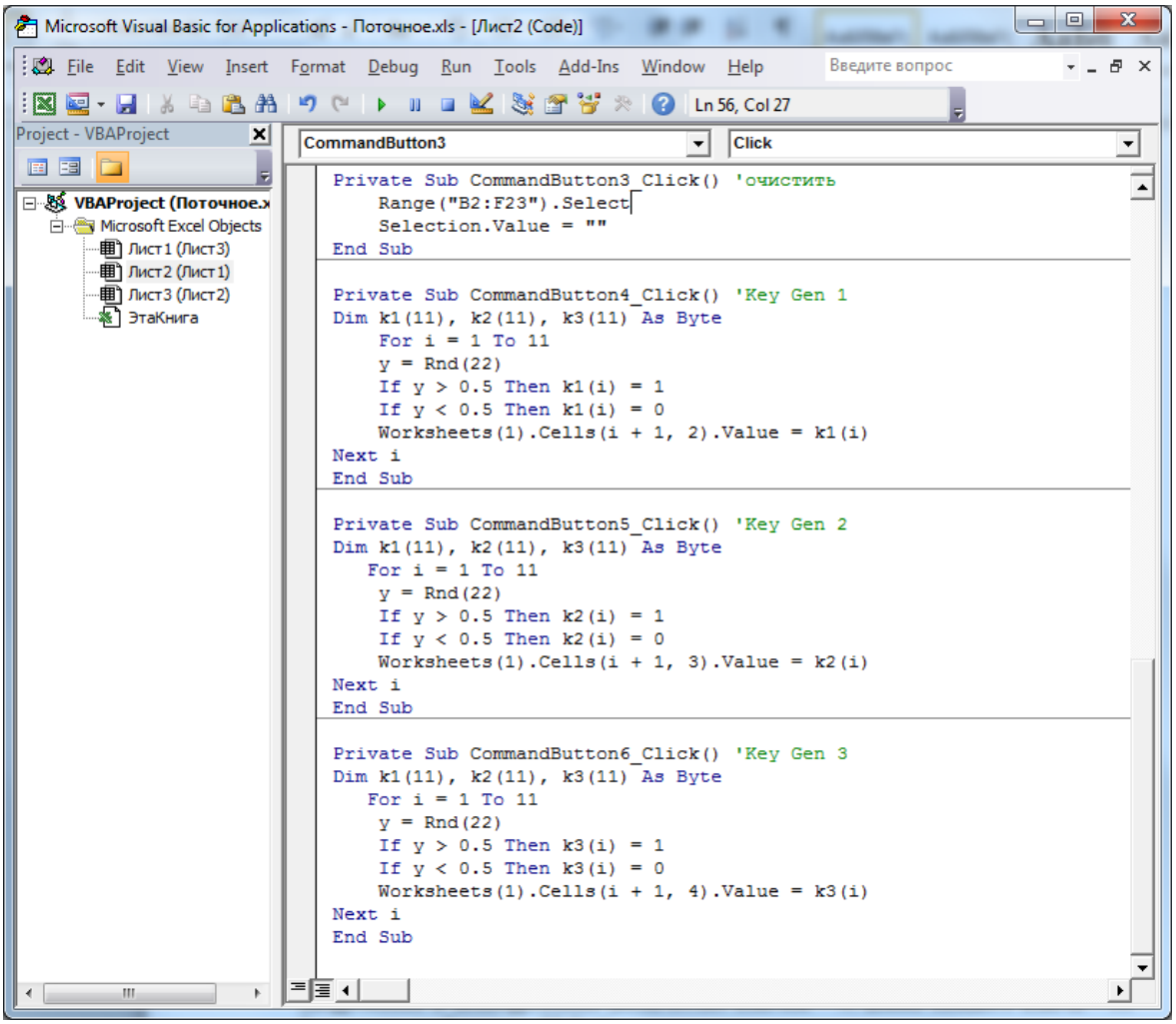


Рис. 3.15. Вид окна текста программы генератора ключей для поточного шифрования и дешифрования (количество ключей – 3, длина каждого ключа – 11 бит)

Задание № 4. Дополнительно для самостоятельной работы

Составить программу для алгоритма поточного шифрования с повышенной защищенностью от помех. Применить способ синхронизации маркерами.

3.2. Асимметричное шифрование

Большим достижением криптографии последней четверти XX века стало изобретение метода шифрования, основанного на использовании пары ключей, один из которых предназначен только для шифрования, а другой – только для дешифрования. Резидент генерирует два ключа: закрытый (секретный), который никому не передает и хранит только у себя, и открытый (публичный), который передает респонденту, не опасаясь обнаружения злоумышленником. Респондент шифрует сообщения открытым ключом, а расшифровать их можно только закрытым ключом, хранящимся у резидента. Возможны и другие варианты использования пары ключей. Например, закрытый ключ используется для формирования электронной цифровой подписи, а открытый ключ – для проверки подлинности этой подписи.

Математической основой этого метода стала разработка так называемых хеш-функций, которые обладают особым характерным свойством – высокой сложностью обратного преобразования. Чем выше эта сложность, тем выше и криптостойкость асимметричного алгоритма.

3.2.1. Хеш-функции

Хеширование (иногда пишется хэширование, англ. *hashing*) – преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или дайджестом сообщения.

Хеширование применяется для сравнения данных: если у двух массивов данных хеш-коды разные, массивы гарантированно различаются; если одинаковые – массивы, скорее всего, одинаковы. В общем случае однозначного соответствия между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше чем вариантов входного массива, но вероятность таких совпадений или коллизий у хороших хеш-функций очень мала.

Существует множество алгоритмов хеширования с различными характеристиками (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшим примером хеш-функции может служить контрольная сумма. Примером такого алгоритма является деление сообщения на 32- или 16- битные слова и их суммирование, что приме-

няется, например, в протоколе *TCP*/*IP*. По скорости вычисления такие алгоритмы в сотни раз быстрее, чем алгоритмы для вычисления криптографических хеш-функций, и значительно проще в аппаратной реализации.

Платой за столь высокую скорость является отсутствие криптостойкости – лёгкая возможность подогнать сообщение под заранее известную сумму. Поэтому такие быстрые и простые алгоритмы используются только для защиты от непреднамеренного искажения информации.

Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии. Чтобы хеш-функция H считалась криптографически стойкой, она должна удовлетворять трем основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

- необратимость: для заданного значения хеш-функции m должно быть вычислительно неосуществимо найти блок данных X, для которого $H(X) = m$;
- стойкость к коллизиям первого рода: для заданного сообщения M должно быть вычислительно неосуществимо подобрать другое сообщение N, для которого $H(N) = H(M)$;
- стойкость к коллизиям второго рода: должно быть вычислительно неосуществимо подобрать пару сообщений, имеющих одинаковый хеш.

Следует отметить, что не доказано существование необратимых хеш-функций, для которых вычисление какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Обычно нахождение обратного значения является лишь вычислительно сложной задачей.

Для криптографических хеш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно изменялось (лавинный эффект). В частности, значение хеша не должно давать утечки информации даже об отдельных битах аргумента. Это требование является залогом криптостойкости алгоритмов хеширования, хеширующих пользовательский пароль для получения ключа.

Наиболее известные хеш-функции*: Adler*-32, *CRC, HashCart, HAVAL, Keccak, LM-хеш, MD*2 – *MD*6, *N-Hash, PJW*-32, *RIPEMD*-128 – *RIPEMD*-320, *SHA*-1, *SHA-2, Skein, Snefru, Tiger, TTH, Whirlpool,* ГОСТ Р 34.11-94**.**

Рассмотрим в качестве примера алгоритм вычисления хеш-функции *Adler*-32, которая достаточно широко распространена. Этот алго-

ритм разработан Марком Адлером и является модификацией хеш-функции *Fletcher*, работающей на основе вычисления контрольной суммы.

Adler-32 вычисляется по формуле:

$$Adler\text{-}32(D) = B \times 2^{16} + A, \quad (3.7)$$

где D – байт-коды символов исходного текста; A, B – вспомогательные коэффициенты, которые вычисляются итерационно по байт-кодам символов исходного текста:

$$A_0 = 1;$$
$$B_0 = 0;$$
$$A_i = (A_{i-1} + D_i) \bmod 65521; \quad (3.8)$$
$$B_i = (B_{i-1} + A_i) \bmod 65521.$$

Число 65521 – это самое большое простое число меньшее, чем 2^{16}(65536). Результат обычно преобразуют в 16-ричную систему счисления (*hex*). Пример вычисления хеш-функции *Adler*-32 приведен в табл. 3.9.

Таблица 3.9. Пример вычисления хеш-функции *Adler*-32

Исходный текст, *D*	Код *ASCII*	Коэфф. *A*	Коэфф. *B*	*Adler*-32
		1	0	
H	72	73	73	
a	97	170	243	
m	109	279	522	
u	117	396	918	
h	104	500	1418	
i	105	605	2023	
n	110	715	2738	
				179438283_{10} $AB202CB_{16}$

В данном примере операция *mod* не понадобилась, так как все коэффициенты меньше 65521. Если изменить исходный текст *D* хотя бы на 1 (например, вместо 97 ввести 98), то значение хеш-функции *Adler*-32 меняется на 179831500. Это существенное изменение подтверждает лавинный эффект, необходимый для криптографических хеш-функций.

Задание № 1

Вычислить вручную значение хеш-функции *Adler*-32 для своей фамилии, записанной на латинице. Коды *ASCII* взять из табл. 3.10.

Таблица 3.10. Коды ASCII

Символ	Код *ASCII*	Символ	Код *ASCII*	Символ	Код *ASCII*	Символ	Код *ASCII*
a	97	*i*	105	*q*	113	*y*	121
b	98	*j*	106	*r*	114	*z*	122
c	99	*k*	107	*s*	115	!	33
d	100	*l*	108	*t*	116	+	43
e	101	*m*	109	*u*	117	,	44
f	102	*n*	110	*v*	118	-	45
g	103	*o*	111	*w*	119	.	46
h	104	*p*	112	*x*	120	?	63

Отчет представить в форме табл. 3.9, продемонстрировать лавинный эффект хеш-функции *Adler*-32 для своей фамилии, записанной на латинице.

Задание № 2

Вычислить в *Excel* значение хеш-функции *Adler*-32 для своих исходных данных «Фамилия Имя Отчество». Коды ASCII можно получить с помощью следующего фрагмента программы:

```
Dim Sym As String
For i = 1 To 8
 Sim = InputBox ("vvedi simvol", 1)
 MsgBox "ascii= " & Asc(Sym)
Next i
```

Для перевода результата из десятичной в шестнадцатеричную систему использовать встроенную функцию *Excel* =ДЕС.В.ШЕСТН(*F*13), где *F*13 – адрес ячейки с числом в десятичной системе счисления. Продемонстрировать лавинный эффект, отчет представить в форме копии листа *Excel*.

Задание № 3

Составить программу на *VBA* для вычисления значения хеш-функции *Adler*-32 заданного текстового файла. Продемонстрировать лавин-

ный эффект, отчет представить в форме копий экрана текстового файла и окна программы. Для чтения файла с диска использовать следующий пример.

```
Dim n, Str, Sym As String
Open "c:\2050.txt" For Input As #1
  While Not EOF(1)
    Input #1, n ‘ читаем очередную строку текста из файла
    Str = Str + n ‘ добавляем прочитанную строку ко всему тексту
  Wend
‘ сюда вставить вычисление значения хеш-функции Adler-32
‘ байты выделять из текста с помощью функции Sym = Mid(Str, i, 1)
‘ ASCII коды байтов получать с помощью функции Asc(Sym)
Close #1
```

Задание № 4. Дополнительно для самостоятельной работы

Составить программу для вычисления хеш-функции с повышенной криптостойкостью. Хеш-функцию выбрать самостоятельно.

3.2.2. Алгоритм *RSA*

RSA – наиболее известный алгоритм асимметричного шифрования, названный по первым буквам фамилий его создателей: *Rivest*, *Shamir*, *Aldeman*. Для применения этого алгоритма потребуется несколько определений.

Простое число – число, которое делится только на 1 и на само себя.

Взаимно простые числа – числа, которые не имеют ни одного общего делителя, кроме 1.

Операция (i ***mod*** j) – дает остаток от целочисленного деления i на j. Например, (20 ***mod*** 3) = 2, (20 ***mod*** 10) = 0, (3 ***mod*** 20) = 3.

Генерация пары ключей по алгоритму *RSA*

1. Выбираем два взаимно простых числа (чем больше эти числа, тем выше криптостойкость алгоритма): $\boldsymbol{p}$ и $\boldsymbol{q}$.

2. Определим число $\boldsymbol{n} = \boldsymbol{p}\times\boldsymbol{q}$; заметим, что ($\boldsymbol{n}$ – 1) – максимальное число, которое можно будет использовать при шифровании.

3. Выберем простое число $\boldsymbol{d}$, которое будет взаимно простым с результатом умножения: ($\boldsymbol{p}$ – 1)×($\boldsymbol{q}$ – 1).

4. Подберем такое число ***e***, для которого истиной будет следующее соотношение: ((***e*** × ***d***) *mod* ((***p*** – 1)×(***q*** – 1))) = 1.

5. Назовем открытым ключом пару чисел (***e***, ***n***), а закрытым ключом – пару чисел (***d***, ***n***).

Шифрование данных по алгоритму *RSA*

1. Заменяем в исходном тексте символы на числа $M(i)$ в диапазоне от 0 до (***n*** – 1).

2. Преобразуем числа по следующей формуле (хеш-функция):

$$C(i) = \left(M(i)^e\right) \bmod(n) \qquad (3.6)$$

3. Заменяем числа $C(i)$ на буквы алфавита, получаем шифротекст $T(i)$.

Как видно из алгоритма, для шифрования был использован только открытый ключ – пара чисел (***e***, ***n***).

Дешифрование данных по алгоритму *RSA*

1. Заменяем символы шифротекста $T(i)$ на числа $C(i)$.

2. Преобразуем числа по следующей формуле (хеш-функция):

$$M(i) = \left(C(i)^d\right) \bmod(n) \qquad (3.7)$$

3. Заменяем числа $M(i)$ на буквы алфавита, получаем исходный текст.

Как видно из алгоритма, для дешифрования был использован только закрытый ключ – пара чисел (***d***, ***n***).

Задание № 1

Зашифровать вручную три первых буквы алфавита методом шифрования по алгоритму *RSA*. В отчете представить таблицу в соответствии с примером, приведенным на рис. 3.16. Номер варианта индивидуального задания выдается преподавателем (рис. 3.16).

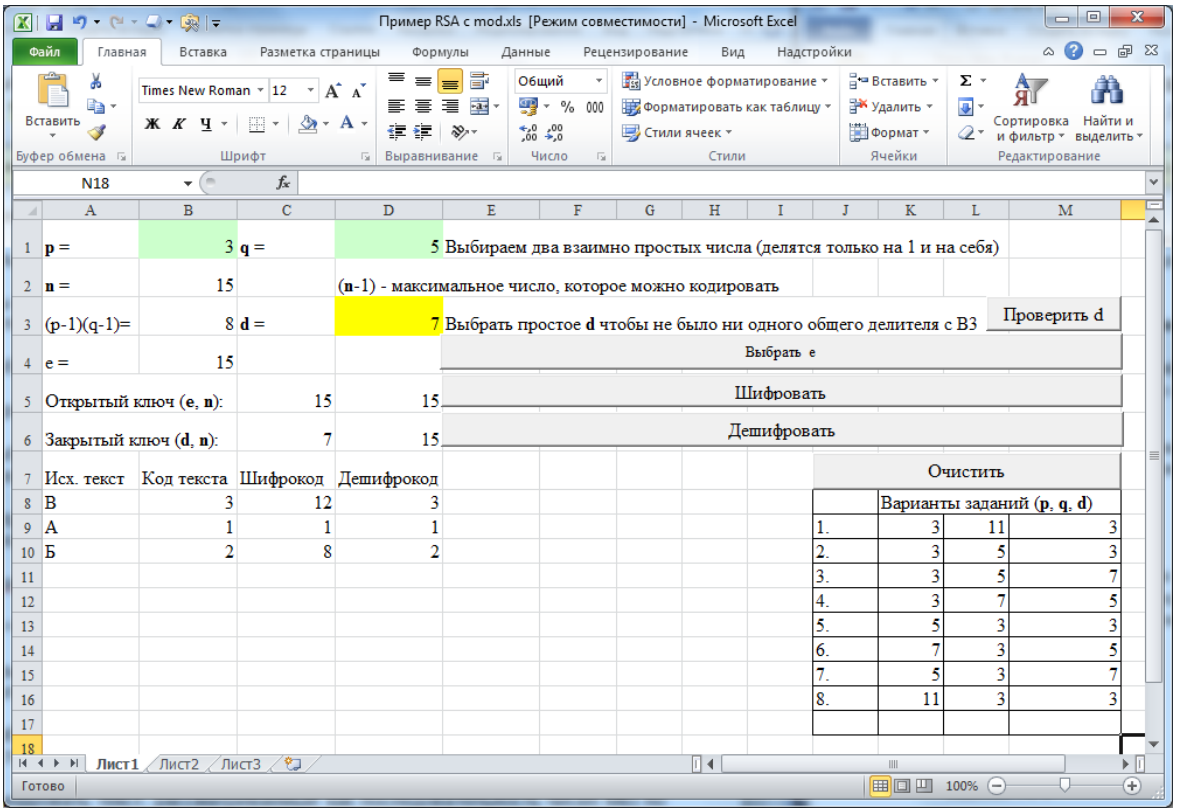


Рис. 3.16. Варианты заданий и результаты применения алгоритма RSA

Задание № 2

Составить программу для асимметричного шифрования по алгоритму *RSA*. При составлении программы использовать образец (рис. 3.16–3.18), в который необходимо внести изменения, соответствующие Вашему индивидуальному заданию.

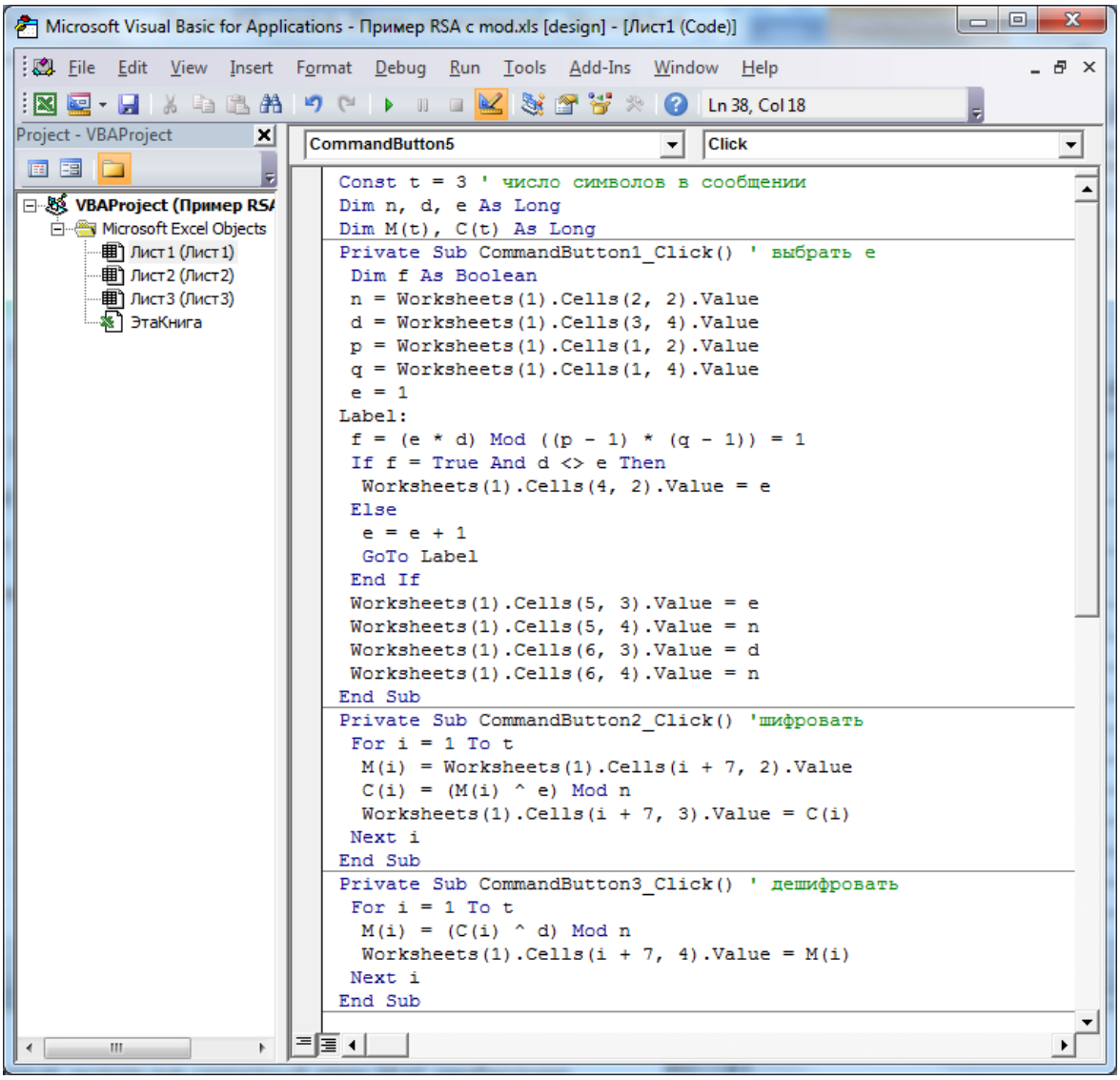


Рис. 3.17. Окно текста программы алгоритма RSA (часть 1)

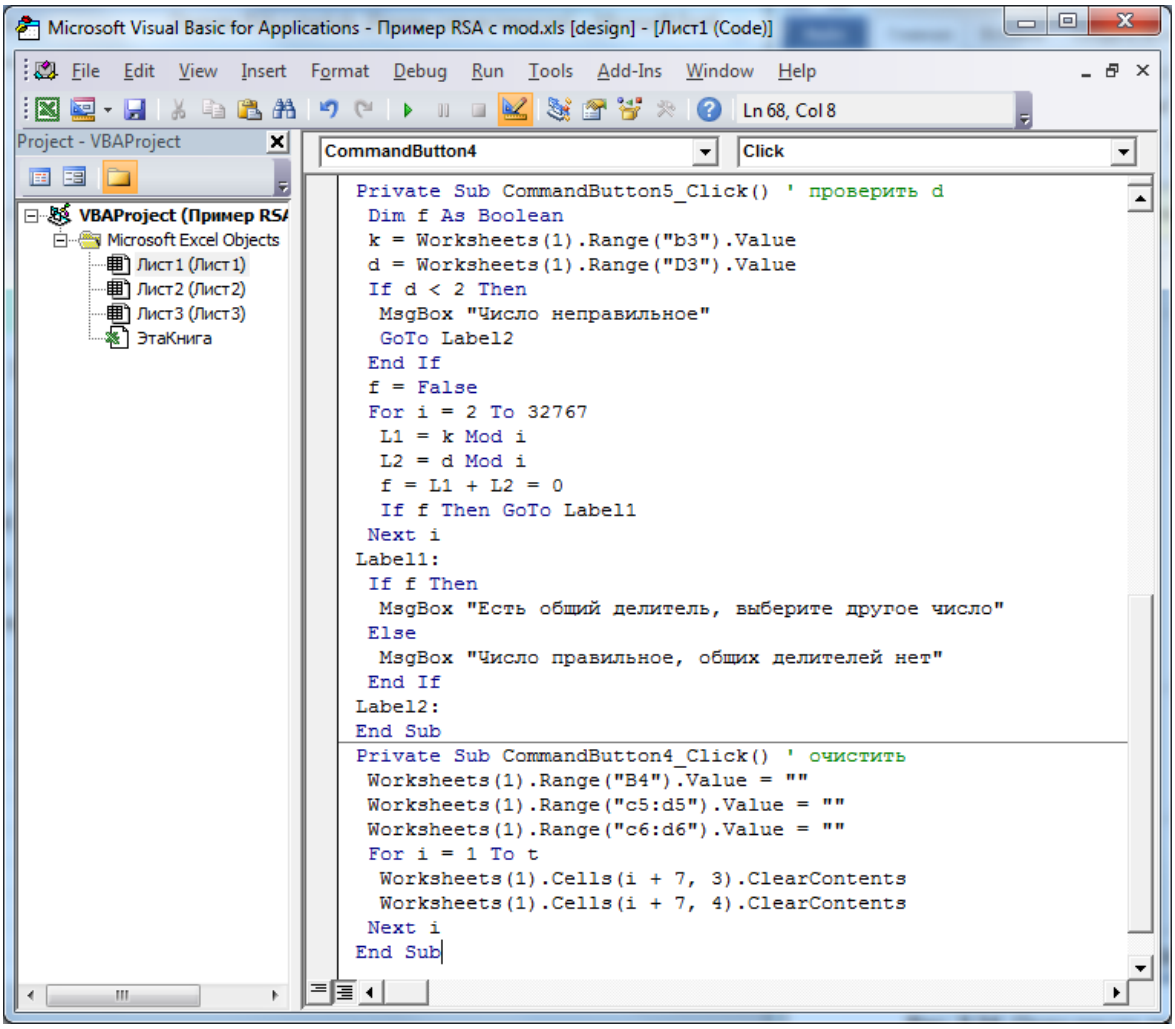


Рис. 3.18. Окно текста программы алгоритма RSA (часть 2)

Задание № 3

В программе, составленной по заданию 2 заменить операцию *mod*, которая может выполняться только над целыми числами, и ограничена максимумом примерно 2 млрд. Для этого требуется написать функцию, которая выполняла бы аналогичную операцию над числами типа *Double*. После замены продемонстрировать работу алгоритма *RSA* над своей фамилией и именем. Пример приведен на рис. 3.19–3.21.

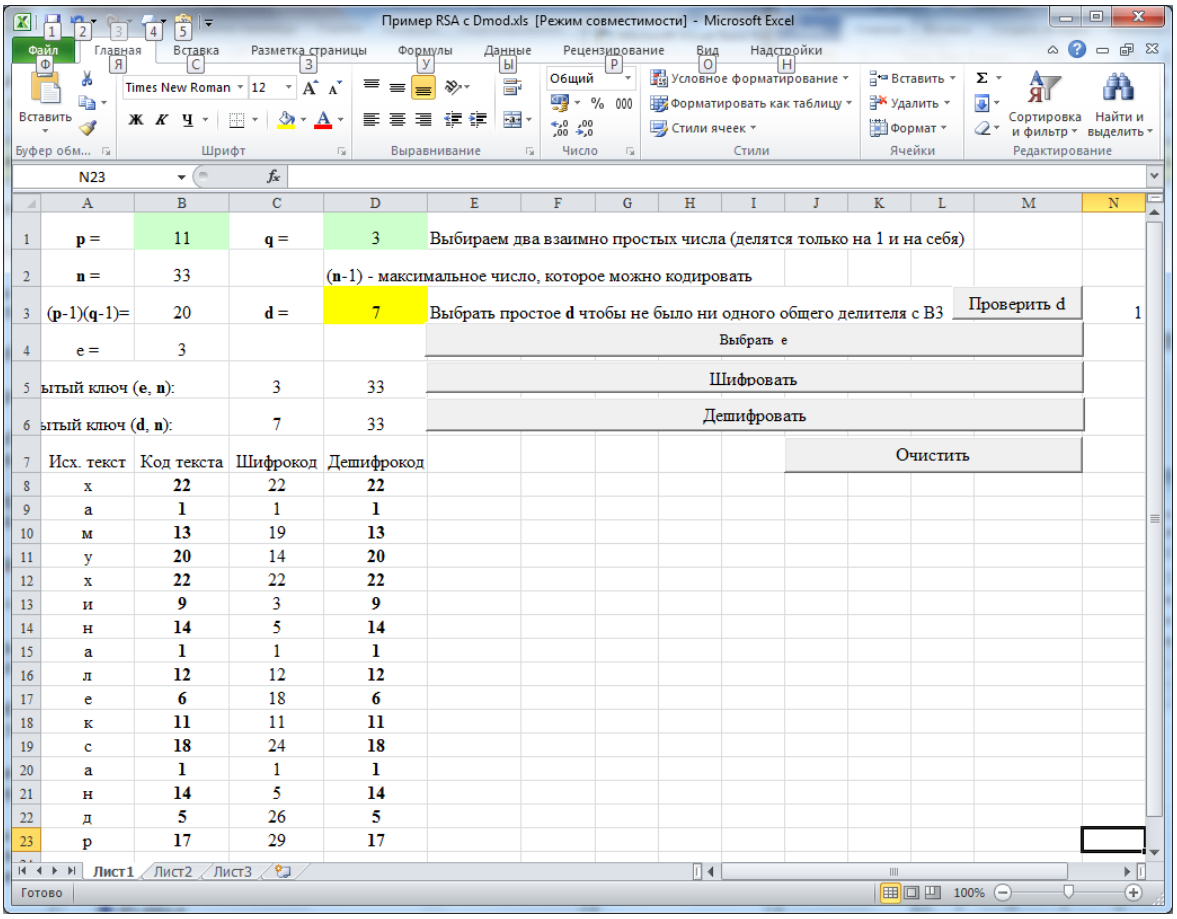


Рис. 3.19. Интерфейс программы алгоритма RSA с замененной операцией mod

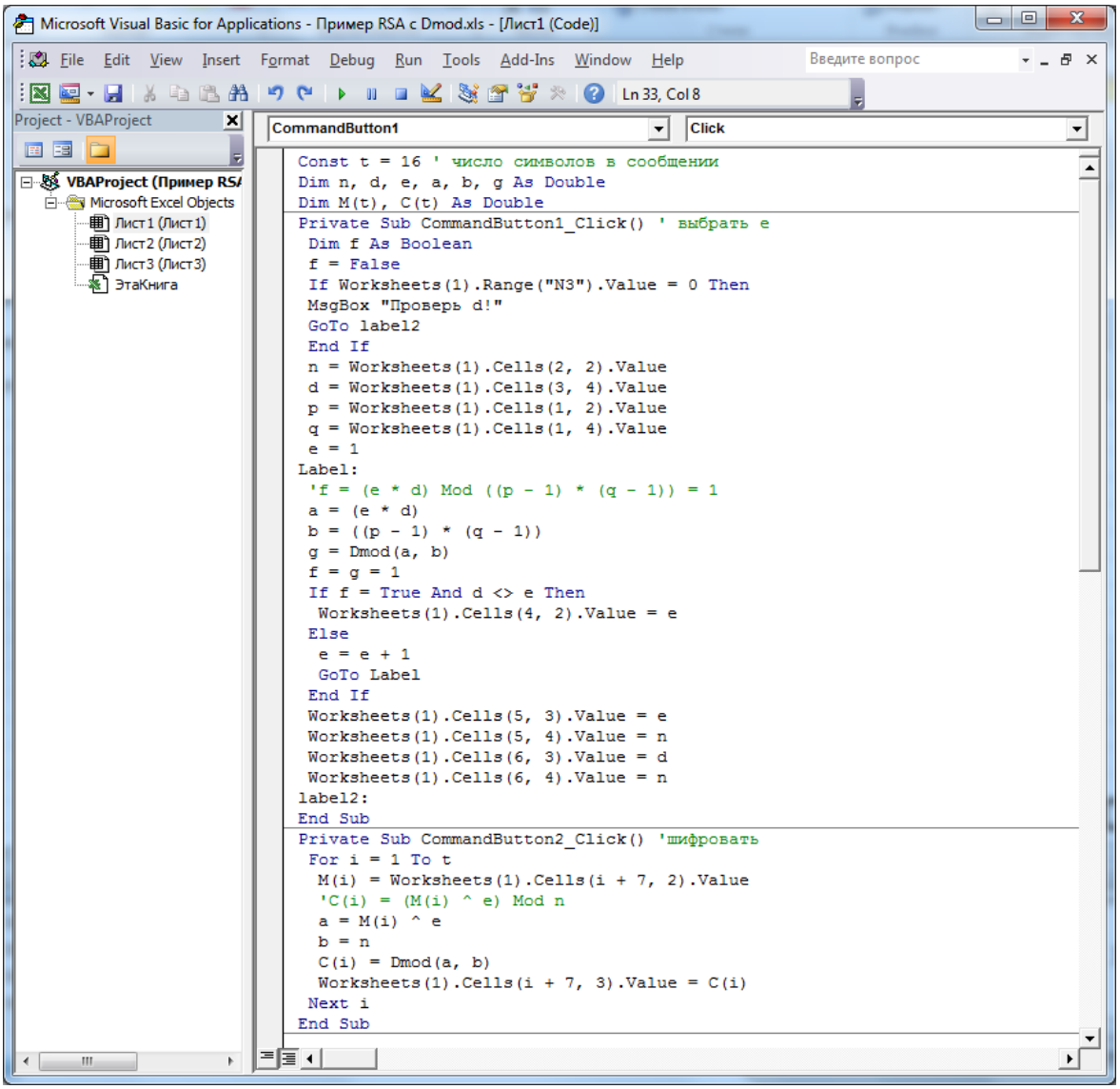


Рис. 3.20. Пример замены операции mod функцией Dmod в программе алгоритма RSA (часть 1)

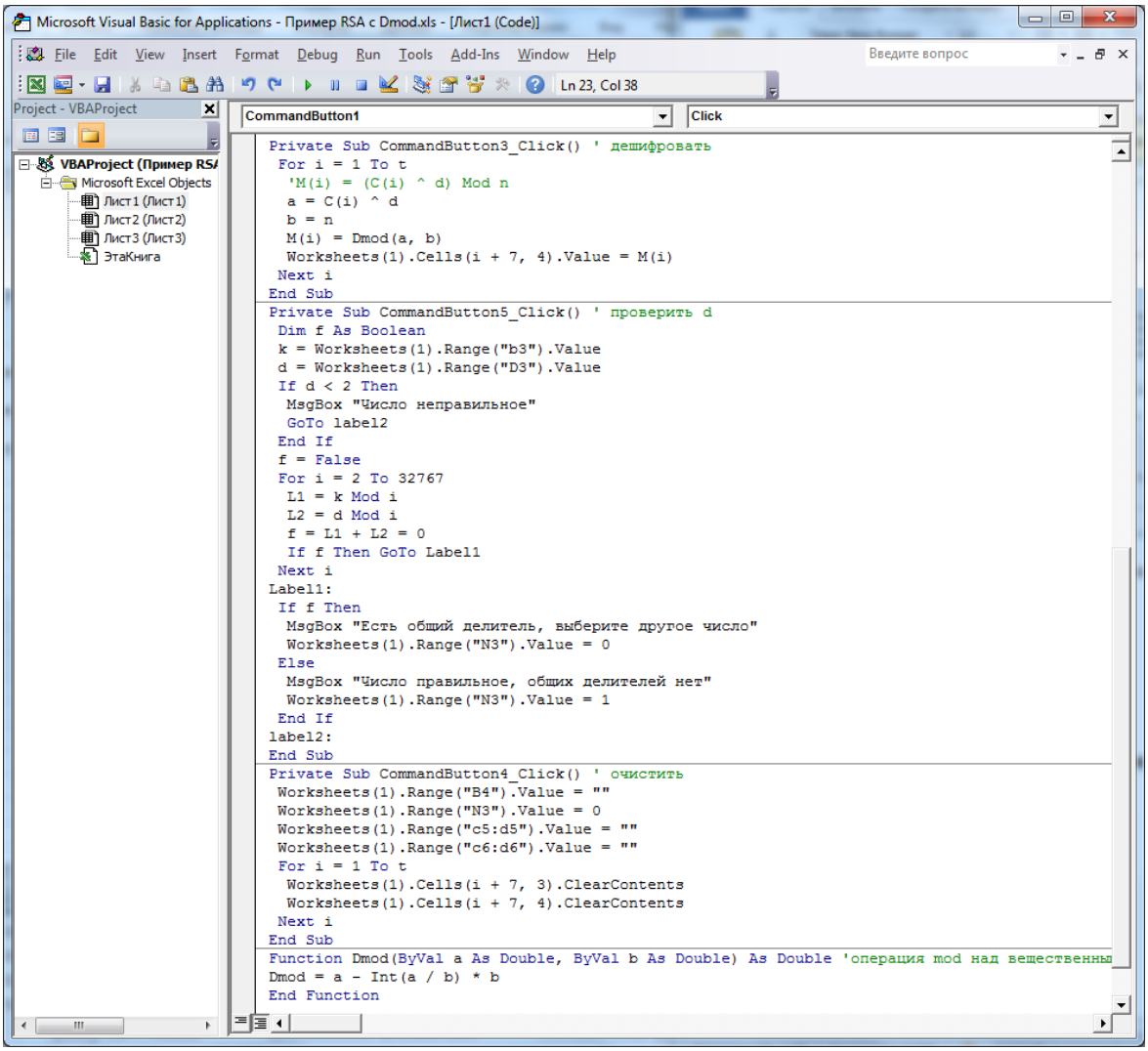


Рис. 3.21. Пример замены операции mod функцией Dmod в программе алгоритма RSA (часть 2)

Задание № 4. Дополнительно для самостоятельной работы

Составить программу для алгоритма *RSA* с увеличенным количеством символов алфавита для шифрования.

3.3. Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) – это средство, позволяющее на основе криптографических методов надежно установить авторство и подлинность электронного документа. Электронная цифровая подпись позволяет заменить при безбумажном документообороте традиционную печать и подпись. Проставление подписи под документом не меняет самого документа, а только дает возможность проверить подлинность и авторство полученной информации.

Первоначально были попытки создания механизма ЭЦП на основе алгоритмов симметричного шифрования, но затем, используя преимущества двух ключей, механизм функционирования ЭЦП полностью перешел на алгоритмы асимметричного шифрования.

Секретный (закрытый) ключ подписи используется для выработки электронной цифровой подписи. Только сохранение пользователем в тайне своего секретного ключа гарантирует невозможность (точнее – большую вычислительную сложность) подделки злоумышленником документа и цифровой подписи от имени заверяющего.

Открытый ключ подписи формируется как значение некоторой функции от секретного ключа, но знание открытого ключа не дает возможности определить секретный ключ. Открытый ключ может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего в виде отказа его от подписанного им документа.

В настоящее время разработаны средства поддержки механизма ЭЦП, например система комплексной защиты информации (СКЗИ) «Верба-*OW*». В СКЗИ «Верба-*OW*» реализована система электронной цифровой подписи на базе асимметричного криптографического алгоритма согласно ГОСТ Р 34.10-94 (ГОСТ Р3 4.11-94 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ»). Электронная цифровая подпись вырабатывается на основе электронного документа, требующего заверения, и секретного ключа. В соответствие со стандартом документ «сжимается» с помощью функции хэширования. Однонаправленная хэш-функция получает на входе исходное сообщение произвольной длины и преобразует его в хэш-значение фиксированной длины (256 бит согласно ГОСТ Р34.11-94). Значение хэш-функции сложным образом зависит от содержания документа, но не позволяет восстановить сам документ. Хэш-функция чувствительна к всевозможным изменениям в тексте. Кроме того, для данной функции нельзя вычислить,

какие два исходных сообщения могут генерировать одно и то же хэш-значение, поскольку хэш-значения двух 256-битовых документов могут совпасть в одном из 2*256*1077 случаев. Далее к полученному хэш-значению применяется некоторое математическое преобразование, в результате которого и получается собственно цифровая подпись электронного документа.

При проверке подписи проверяющий должен располагать открытым ключом пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности открытого ключа (а именно в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя). Процедура проверки подписи состоит из вычисления хэш-значения документа и проверки некоторых соотношений, связывающих хэш-значение документа, подпись под этим документом и открытый ключ подписавшего пользователя. Документ считается подлинным, а подпись – правильной, если эти соотношения выполняются. В противном случае ЭЦП документа считается недействительной.

Для разрешения споров между отправителем и получателем информации, связанных с возможностью искажения пересылаемого документа или открытого ключа проверки подписи, достоверная копия этого ключа может выдаваться третьей стороне (Центру компетентности) и применяться им при возникновении конфликта между отправителем и получателем. Наличие у абонента секретного ключа не позволяет ему самому сменить свой номер в сети или выработать подпись под номером другого абонента.

Для контроля целостности и подлинности справочников открытых ключей Центром компетентности должна использоваться процедура выработки имитовставки, определяемая ГОСТ 28147-89. При проверке подписи проверяющий должен располагать открытым ключом пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности открытого ключа (а именно в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя).

В настоящее время применение электронной цифровой подписи утверждено в России на законодательном уровне (Приложение 1. Федеральный закон Российской Федерации «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ» от 10 января 2002 г. № 1-ФЗ). В качестве примера функционирующего Центра компетентности можно привести независимый Удостоверяющий центр *http://www.ekey.ru,* а также Национальный Удостоверяющий центр РФ (рис.3.22).

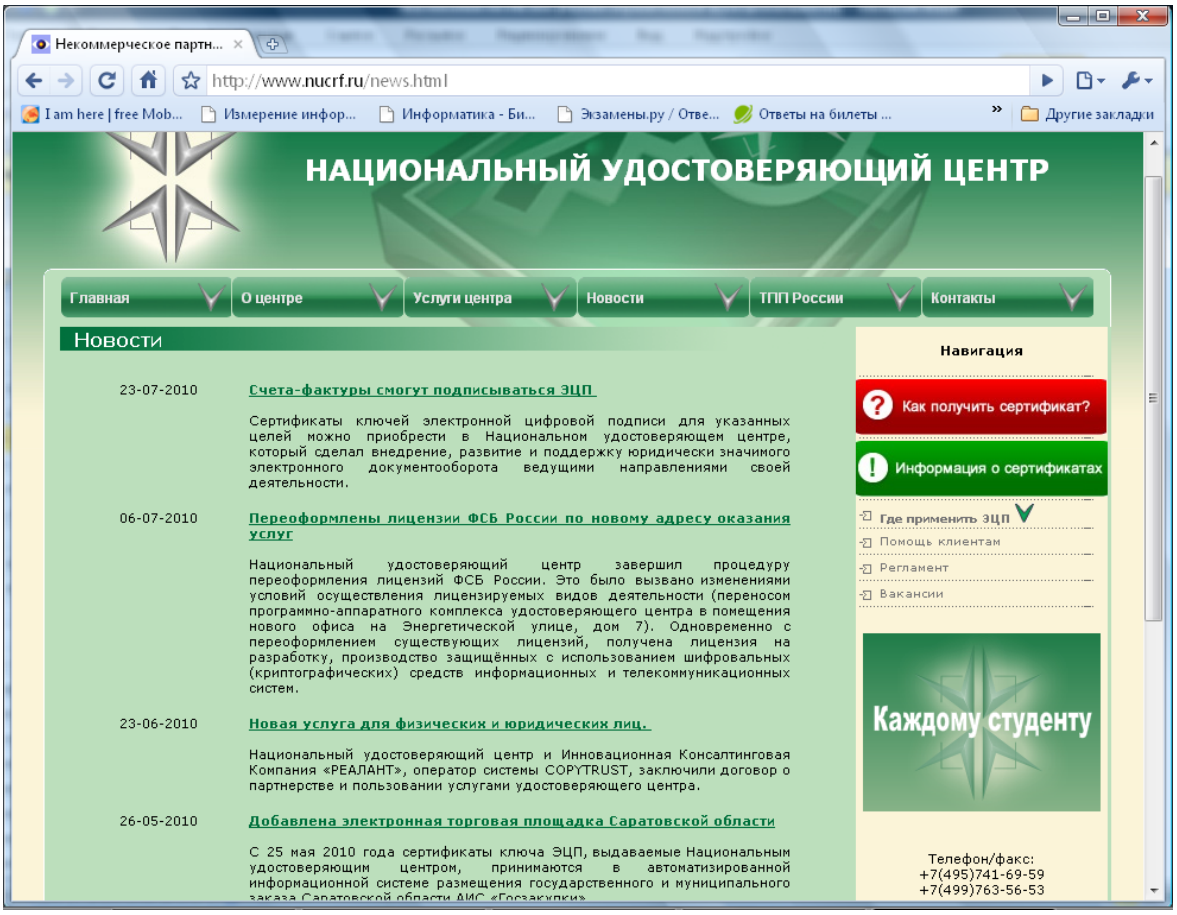


Рис. 3.22. Национальный Удостоверяющий центр РФ

Задание № 1

Используя программу пп. 3.1.2 (Задание 2) составить программу для формирования ЭЦП выделенного фрагмента текста в документе *Word* по алгоритму симметричного ключа. Продемонстрировать использование ЭЦП. Для этого в выделенный фрагмент внести небольшое изменение и повторить процедуру. По результатам работы составить отчет с копиями экранов. В качестве образца использовать пример на рис. 3.23.

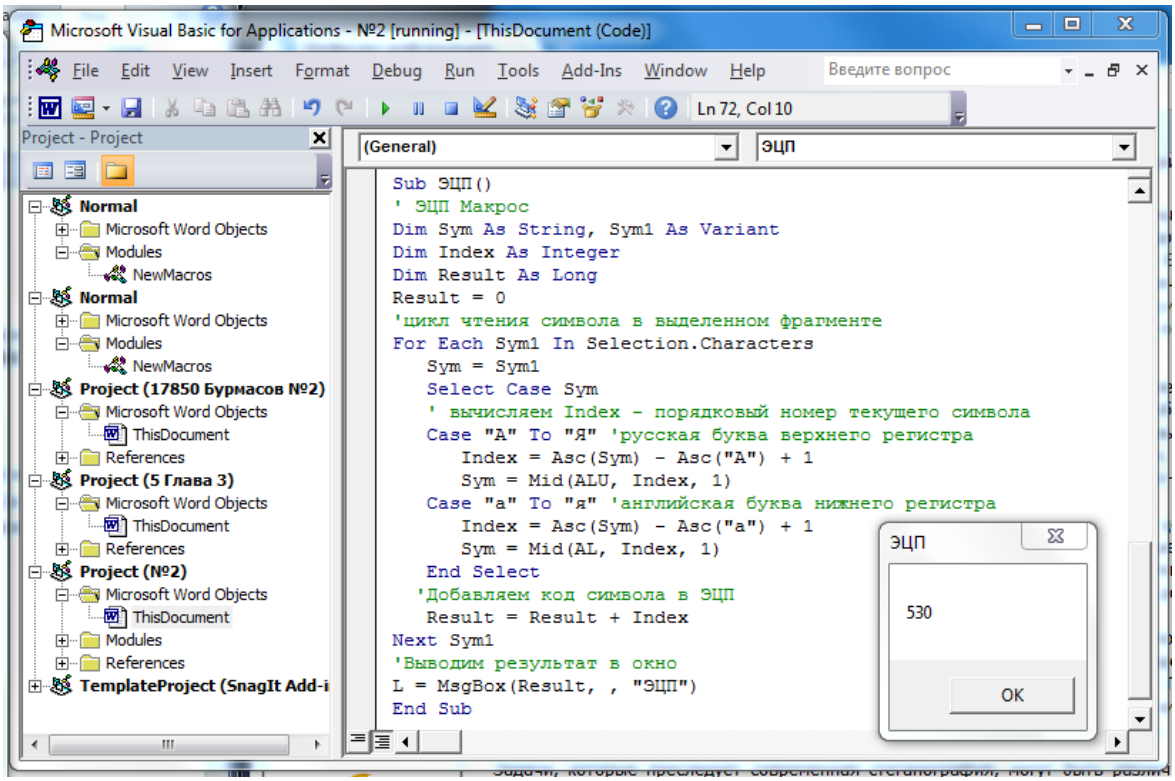


Рис. 3.23. Пример программы формирования ЭЦП выделенного текста по алгоритму контрольной суммы

Задание № 2

Создать кнопки запуска программ «Формировать ЭЦП» и «Проверить ЭЦП» на панели инструментов *Word* аналогично пп. 3.1.2 (Задание 3). По результатам работы составить отчет с копиями экранов.

Задание № 3

Используя программу пп. 3.2.2 (Задание 2) составить программу для формирования ЭЦП по алгоритму *Adler-32*. По результатам работы составить отчет с копиями экранов.

Задание № 4. Дополнительно для самостоятельной работы

Составить программу «Формировать ЭЦП» и «Проверить ЭЦП» с повышенной криптостойкостью на основе более сложного алгоритма хеширования.

3.4. Стеганография

Стеганогра́фия (от греческих – скрытый и пишу, буквально «тайнопись») – это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Наиболее известные исторические примеры применения стеганографии восходят к рабовладельческому строю до нашей эры. Например, рабу наголо брили голову и писали на ней сообщение. Через некоторое время волосы отрастали, но сообщение сохранялось. После этого раб отсылался к получателю информации, где его опять брили и читали само сообщение. Более поздний исторический пример применения стеганографии – это письма В.И.Ленина из тюрьмы, написанные молоком. Они были не видны в обычных условиях, но при нагревании текст проявлялся.

Простейший пример современного применения стеганографии – это вставка секретного текста, цвет которого совпадает с цветом фона, например, – белым цветом в документы *Word*.

Профессиональные современные средства стеганографии гораздо более надежны, чем упомянутый выше прием. В настоящее время употребляют термин «стегосистемы», которые состоят из контейнера, стегоканала, сообщения и стегоключа. Контейнер – это любая информационная система, в рамках которой организуется канал передачи скрытых данных (стегоканал). Стегоключ – это секретный ключ, необходимый для открытия скрытой информации.

Способы встраивания сообщения в контейнер подразделяются на:

- деструктивные;
- не деструктивные;
- конструктивные.

Деструктивные способы встраивания сообщения в контейнер основаны на незначительном изменении файлов, выполняющих роль контейнера. Например, для передачи информации через 16-разрядный *wav*-файл секретных сообщений можно использовать младший бит, изменив его. Младший бит называет «шумовым», поскольку он существенно не влияет на качество звука, получаемого из *wav*-файла. Поэтому такая замена остается почти незаметной для слушателя. Таким образом, *wav*-файл емкостью 16 Мб может «перенести» 1 Мб секретных данных. А на

CD-диске среди музыкальных файлов можно упаковать уже около 40 Мб секретных данных.

Не деструктивные способы встраивания сообщения в контейнер не разрушают целостности данных этого контейнера, а используют только имеющиеся там пустоты или дописывают сообщение в конец файла. По этому принципу в файлы встраиваются и вирусы.

Конструктивные способы встраивания сообщения в контейнер предполагают создание специальных контейнеров, имеющих достаточно много места для размещения тайного сообщения. Это могут быть как файлы известных типов, так и просто безликие файлы, которые не открываются никакими приложениями. Внутри у них хранится информация, которую можно вскрыть, только имея стегоключ.

Задание № 1

Записать в текстовый файл секретные данные «фамилия имя отчество» и сохранить его с расширением, соответствующим графическому файлу, например, *–.gif*. Убедиться, что при открытии этого файла по умолчанию, секретные данные на экране не появляются и файл выглядит, как пустой графический файл.

Задание № 2

Записать в текстовый файл секретные данные «фамилия имя отчество» и сохранить его с расширением, неизвестным операционной системе *Windows*, например, – *qwe*. Убедиться, что файл не открывается. Прочитать информацию из файла с помощью фрагмента программы из Задания 3 из раздела 3.2.1.

Задание № 3

Создать пустой текстовый файл и сохранить его с расширением, неизвестным операционной системе *Windows*. Записать в это файл секретную информацию с помощью следующего фрагмента программы:

```
Open "c:\2050.qwe" For Output As #2
    Print #2, "Хамухин" ' запись в файл построчно
    Print #2, "Александр"
    Print #2, "Анатольевич"
Close #2
```

Прочитать информацию из файла с помощью фрагмента программы, составленного в предыдущем задании. По результатам работы составить отчет с копиями экранов.

Задание № 4. Дополнительно для самостоятельной работы

Текстовый файл даже с небольшим количеством символов занимает на диске от 1 до 4 Кбайт. На языке низкого уровня (ассемблер, си) написать программу двоичного чтения открытой части текстового файла, после символа «конец файла» дописать секретный текст и сохранить на диске. Составить программу двоичного чтения секретной части записанного текстового файла.

Глава 4. Профессиональные программные и аппаратные средства защиты информации

В настоящее время разработано и распространяется достаточно большое количество программных, аппаратных и программно-аппаратных средств обеспечения информационной безопасности. Среди программных средств наиболее известна криптографическая программа *PGP* Фила Циммермана, которая первоначально распространялась бесплатно. Сейчас – это коммерческий продукт с возможностью бесплатного использования либо в режиме ограниченной функциональности, либо в течение 30 дней в полнофункциональном режиме.

В РФ наибольшую известность имеют аппаратные средства защиты серии «Криптон», которые признаны официально на государственном уровне и используются правительственными организациями, банками, крупными корпорациями (*http://www.ancud.ru/catalog/crypton.html*).

Вторыми по распространенности являются аппаратно-программные средства фирмы «*Aladdin*» (*http://www.aladdin.ru/*). Их продуктовая линейка включает в себя средства аутентификации (*eToken*), средства шифрования дисков (*SecretDisk*), средства контентной фильтрации (*eSafe*), средства защиты программ (*HASP*), а также всевозможные картридеры и смарт-карты.

Находят достаточно широкое применение и продукты группы компаний «Информзащита», например, такие как: «*Secret Net*» – система защиты информации на серверах и рабочих станциях от несанкционированного доступа, «*Security Studio*» – система комплексной аппаратно-программной защиты информации и ряд других.

4.1. Криптографический пакет *PGP Desktop*

PGP (*Pretty Good Privacy*) – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности. В *PGP* применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только Вы, а свой открытый ключ Вы распространяете среди своих респондентов.

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т. к. эта программа построена на новом принципе работы – публичной криптографии или обмене откры-

тыми (публичными) ключами. Пользователи этого пакета могут открыто посылать друг другу свои публичные ключи с помощью сети Интернет и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям. Расшифровать их можно только вторым (секретным) ключом, который никому не посылается, а хранится только у человека-генератора пары ключей.

Создатель *PGP* Филипп Циммерман открыто опубликовал код программы, который неоднократно был исследован специалистами криптоаналитиками высочайшего класса и ни один из них не нашел в программе каких-либо слабых мест. Первоначально программа *PGP* распространялась абсолютно бесплатно, затем автор продал свое право фирме *PGP Corporation* за 1 млн. долларов, которая создала на основе этой программы коммерческий пакет *PGP Desktop*. Но даже при коммерческом распространении осталось возможность бесплатного использования этого пакета в режиме ограниченной функциональности, который вполне достаточен для изучения в вузе и выполнения лабораторных работ.

В полном объеме пакет *PGP Desktop* позволяет шифровать сообщения электронной почты, любые файлы, в том числе и графические, папки и все содержимое дисков. Также пакет предоставляет все необходимые сервисы для электронной цифровой подписи и гарантированного уничтожения файлов. В режиме ограниченной функциональности пакет позволяет шифровать только текстовые файлы.

При использовании асимметричного шифрования важно правильное использование пары ключей. Для этого определим роли отправителей и получателей. Человек, который генерирует пару ключей (закрытый и открытый) называется резидентом. Резидент хранит закрытый ключ только у себя (для дешифрования поступающих сообщений), а открытый ключ свободно передает респондентам. Респондент – это лицо, которое шифрует сообщения для резидента полученным от него открытым ключом.

Порядок использования программы *PGP Desktop*

1. Устанавливаем программу на свой компьютер.

Руководствуемся краткой инструкцией по инсталляции программы, приведенной ниже.

2. Создаем закрытый и открытый ключи.

Перед тем, как начать использовать программу *PGP*, Вам необходимо генерировать пару ключей. Она состоит из закрытого ключа, к которому имеете доступ только Вы, и открытого ключа, который Вы копируете и свободно передаете другим людям (Вашим респондентам).

3. Распространяем свой открытый ключ среди своих респондентов.

Ваш открытый ключ – это небольшой файл с расширением *asc*, который появляется после выполнения команды *Export*. Затем его можно передать респонденту любым способом: вставить в сообщение, копировать в файл, прикрепить к почтовому сообщению, разместить на сервере, копировать на съёмный носитель.

4. Получаем открытые ключи от своих резидентов.

Сначала принимаем файл с расширением *asc* и выполняем для него команду *Import*. Здесь необходимо удостовериться в верности открытого ключа. Как только Вы получите открытые ключи своих резидентов, то их можно внести в «кольцо» открытых ключей. После этого Вам необходимо убедиться в том, что у Вас действительно открытый ключ Вашего резидента. Вы можете это сделать, связавшись с этим резидентом и попросив его зачитать вам по телефону «отпечатки пальцев» (уникальный идентификационный номер) его открытого ключа. Также сообщите ему номер Вашего открытого ключа. Как только Вы убедитесь в том, что ключ действительно принадлежит ему, Вы можете его подписать и таким образом подтвердить свое доверие к этому ключу.

5. Шифруем и/или удостоверяем свою корреспонденцию Вашей цифровой подписью.

После генерации пары ключей и обмена открытыми ключами Вы можете начать шифрование и/или удостоверение Ваших сообщений и файлов своей цифровой подписью. Если Вы используете почтовую программу, которая поддерживается программой *PGP*, то Вы можете шифровать и дешифровать всю Вашу корреспонденцию, находясь прямо в этой программе. Если же Ваша почтовая программа не поддерживается программой *PGP*, то Вы можете шифровать Вашу корреспонденцию другими способами (через буфер обмена или шифрованием файлов целиком).

6. Дешифруем поступающие к Вам сообщения и/или проверяем подлинность ЭЦП отправителя.

Когда кто-либо высылает Вам зашифрованное сообщение, Вы можете дешифровать его или проверить подлинность отправителя этого сообщения и целостность самого сообщения. Если Ваша почтовая программа не поддерживается *PGP*, то Вы можете сделать это через буфер обмена.

7. Уничтожение файлов.

Средства операционных систем при удалении файлов физически их не стирают, а только удаляют запись об этом файле в каталоге. Поэтому злоумышленник может восстановить удаленные операционной системой файлы с выброшенного или украденного носителя. Пакет *PGP Desktop* позволяет Вам полностью удалить любой файл с носителя. Для этого Вы можете исполнить команду *wipe* (стереть). Таким образом, удаленный файл уже невозможно будет восстановить, он будет стерт с носителя информации физически.

4.1.2. Индивидуальные задания для программы *PGP Desktop*

Задание № 1

Выполнить роль резидента *X*. Для этого установить программу *PGP Desktop*, генерировать пару ключей под своей фамилией, передать (экспортировать) открытый ключ респонденту, получить от него зашифрованное сообщение, расшифровать. Сверить с респондентом исходный текст для контроля правильности выполнения задания. По результатам работы составить отчет с копиями экранов. В качестве примера использовать рис. 4.1–4.12.

Задание № 2

Выполнить роль респондента *Y*. Для этого установить программу *PGP Desktop*, получить открытый ключ от резидента и импортировать его, зашифровать этим ключом сообщение, передать его резиденту. Сверить с резидентом исходный текст для контроля правильности выполнения задания. По результатам работы составить отчет с копиями экранов. В качестве примера использовать рис. 4.1–4.12.

Задание № 3

Выполнить роль злоумышленника-резидента *Z*-*X*. Для этого перехватить (взять) файл респондента *X*1, который работает с резидентом *Y*1, и попытаться его расшифровать своим закрытым ключом. По результатам работы составить отчет с копиями экранов. В качестве примера использовать рис. 4.1–4.12.

Задание № 4.

Выполнить роль злоумышленника-респондента *Z-Y*. Для этого зашифровать файл своим открытым ключом и отправить (передать) его чужому резиденту *X*1. По результатам работы составить отчет с копиями экранов. В качестве примера использовать рис. 4.1–4.12.

4.1.3. Примеры установки и использования программы *PGP Desktop*

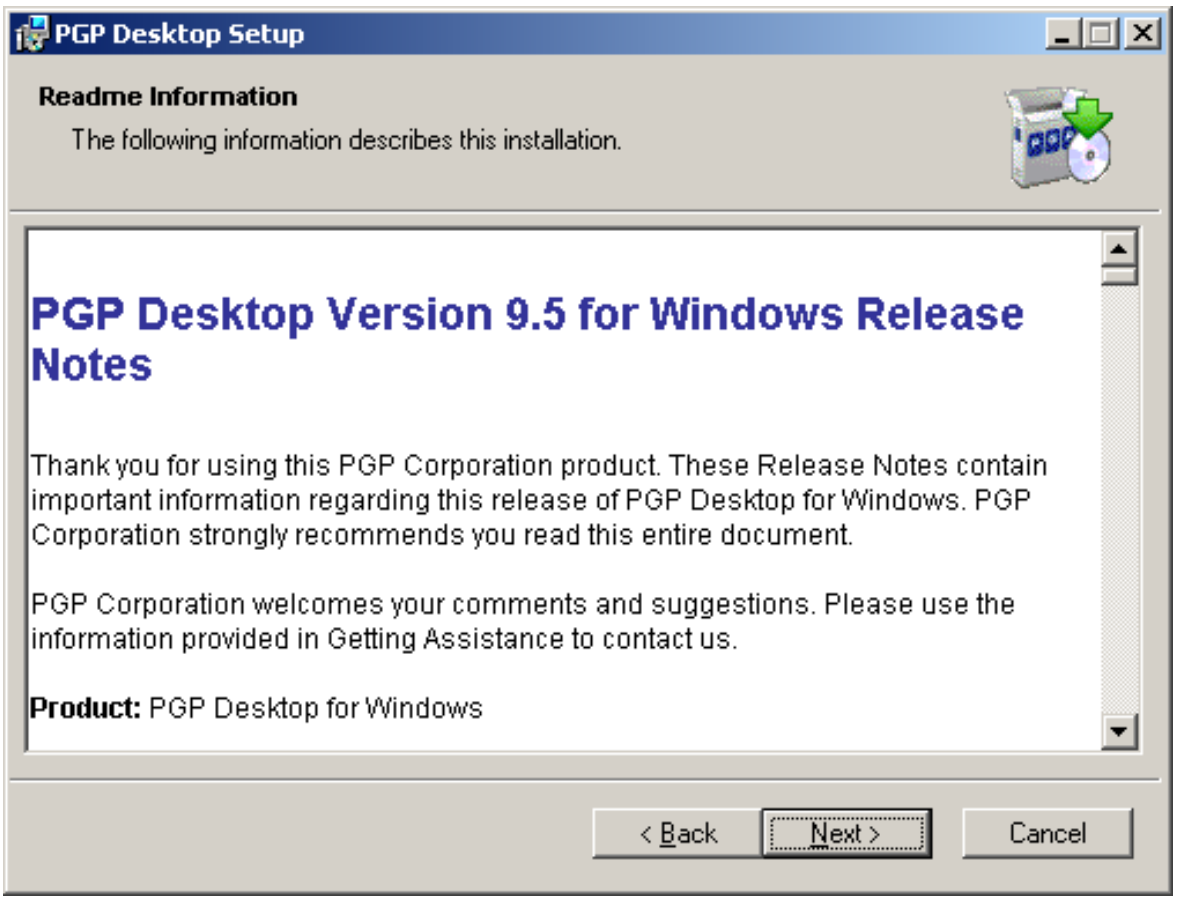


Рис. 4.1. Начало установки программы PGP Desktop

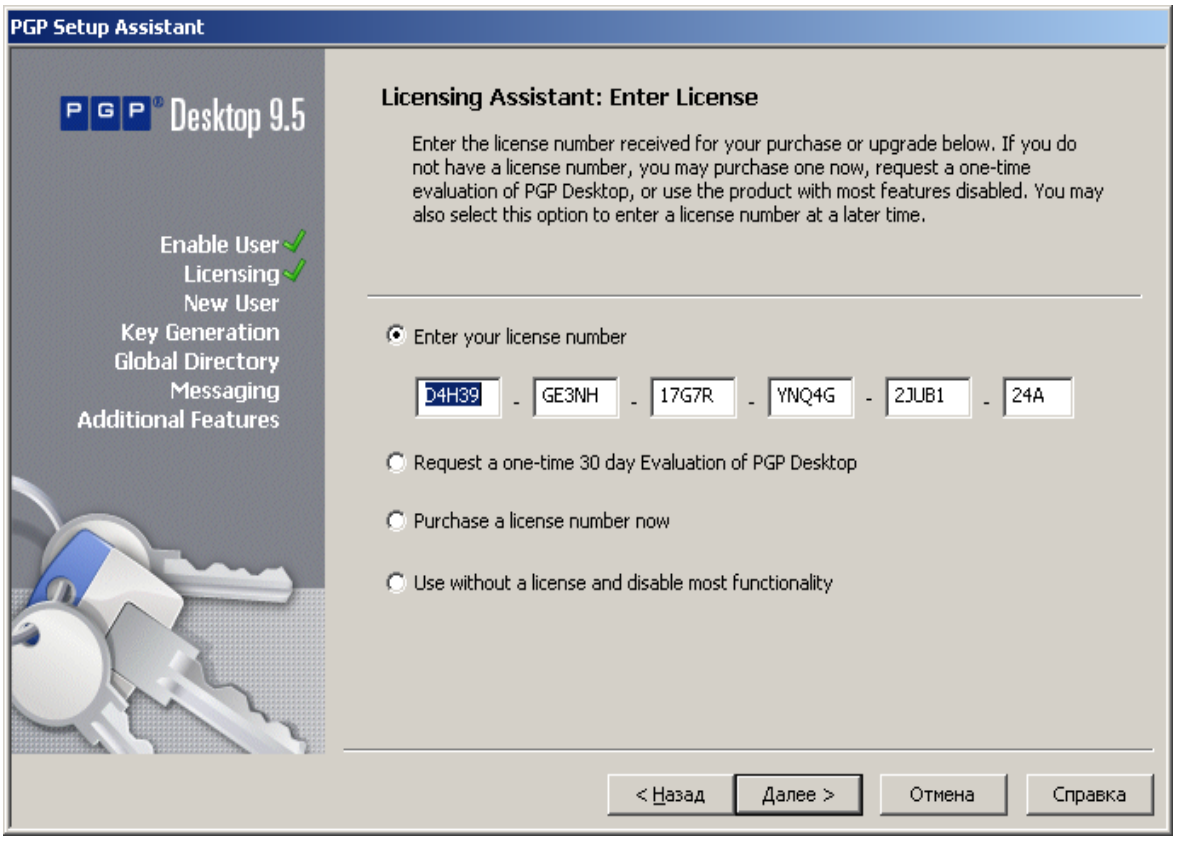


Рис. 4.2. Выбор типа лицензии программы PGP Desktop

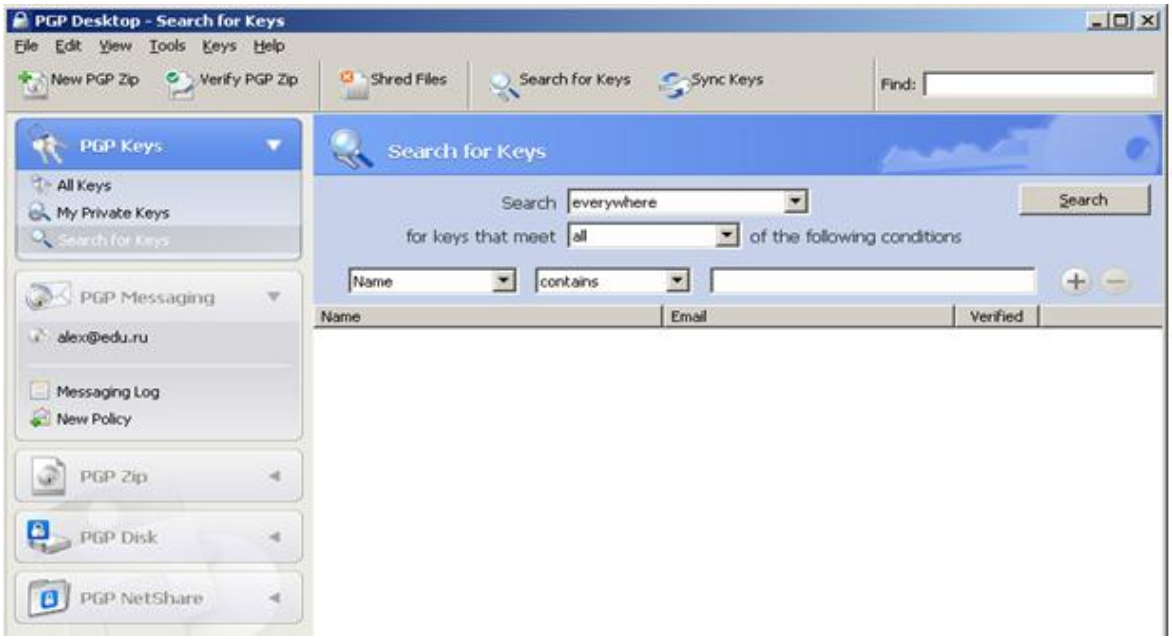


Рис. 4.3. Стартовое окно программы PGP Desktop. Зайдите в меню File и выполните команду New PGP Key

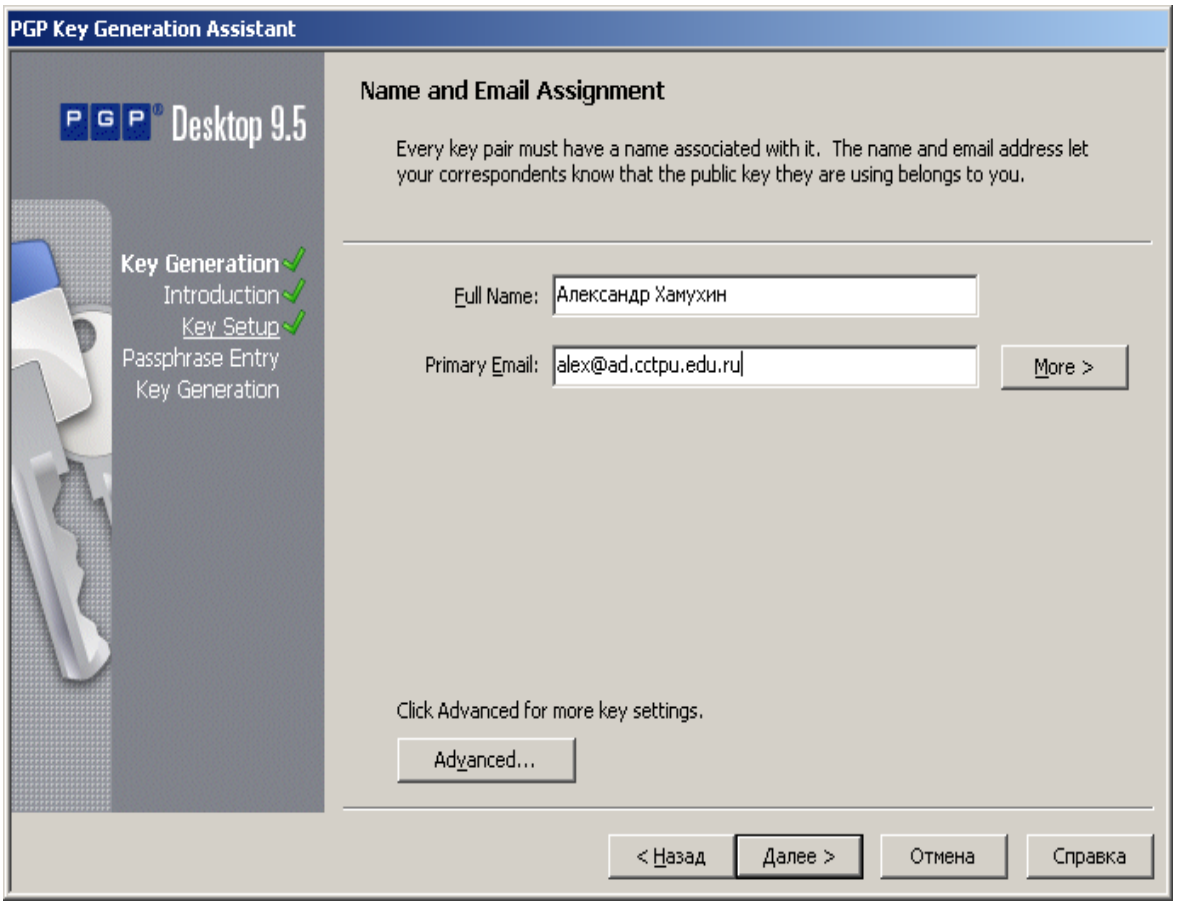


Рис. 4.4. Присвоение ключу имени и e-mail адреса. Присвойте своему ключу свою фамилию, e-mail адрес может быть любым

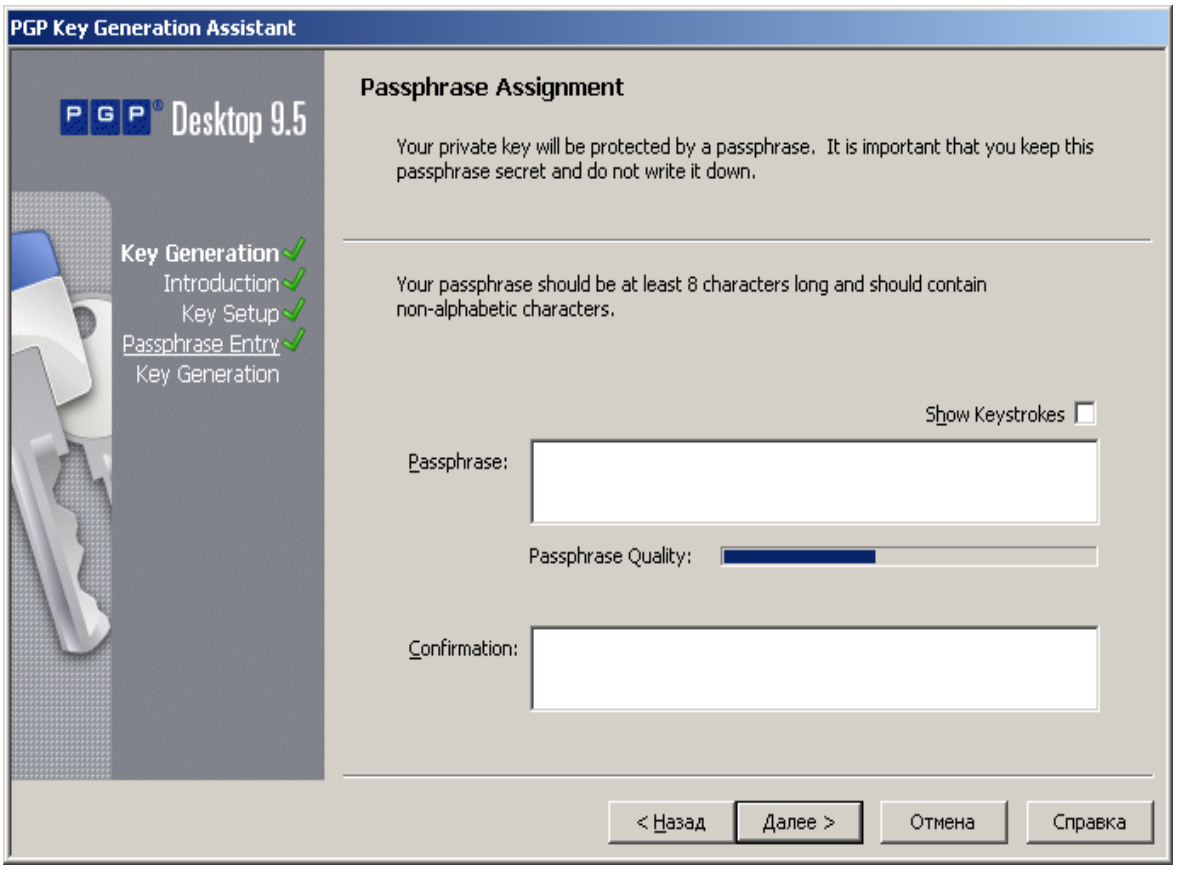


Рис. 4.5. Защита секретного ключа парольной фразой

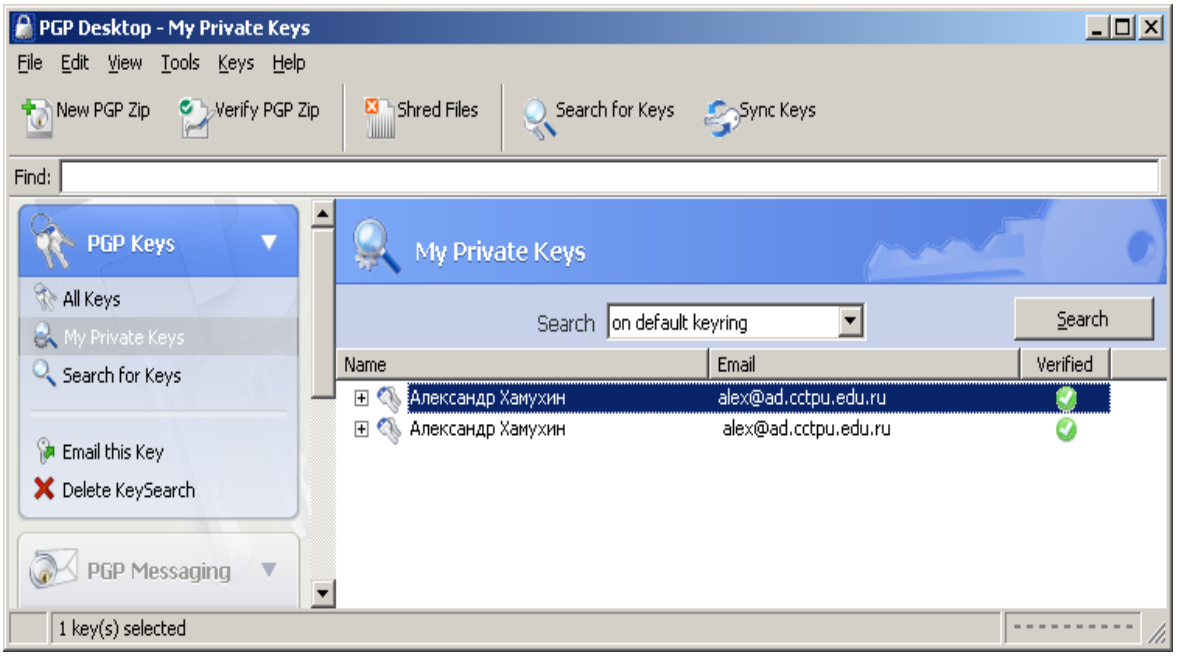


Рис. 4.6. Окно с закрытыми ключами. Чтобы генерировать открытый ключ резидент должен пкм щелкнуть на закрытом ключе и выбрать команду Export

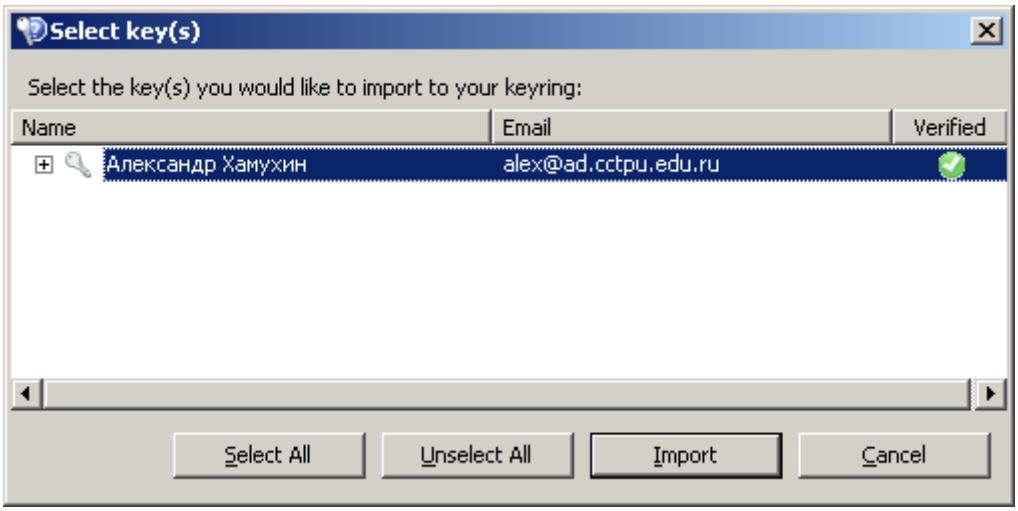


Рис. 4.7. Окно с открытым ключом, полученным респондентом. Для интеграции в пакет щелкнуть кнопку «Import»

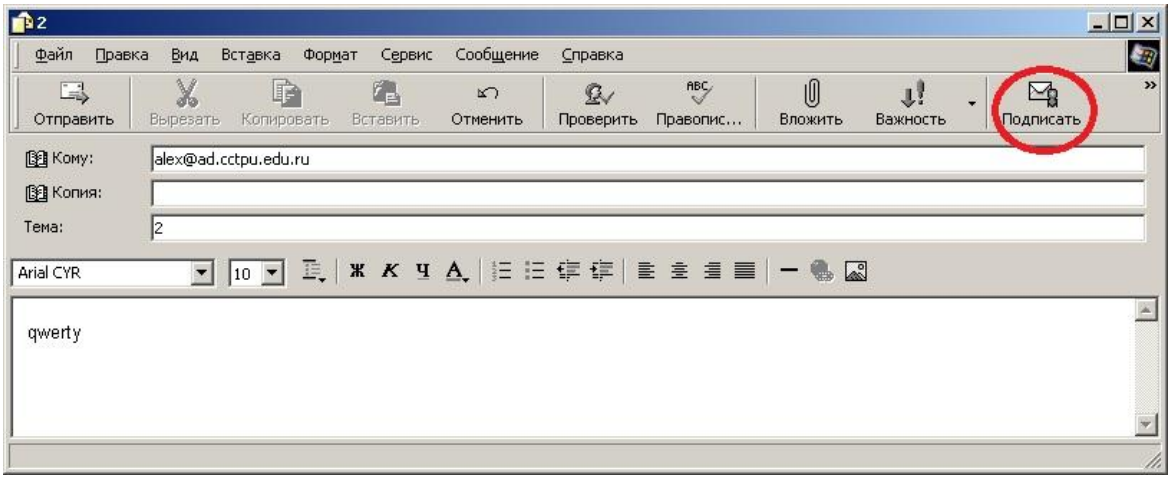


Рис. 4.8. Окно почтового клиента после правильной установки программы PGP Desktop

При отсутствии почтового клиента сообщение нужно набрать в текстовом файле, сохранить его, щелкнуть правой кнопкой мыши (пкм) на его имени и выполнить команду *encrypt* (на стороне респондента). Переслать зашифрованный файл резиденту, который должен щелкнуть правой кнопкой мыши на его имени и выполнить команду *decrypt.*

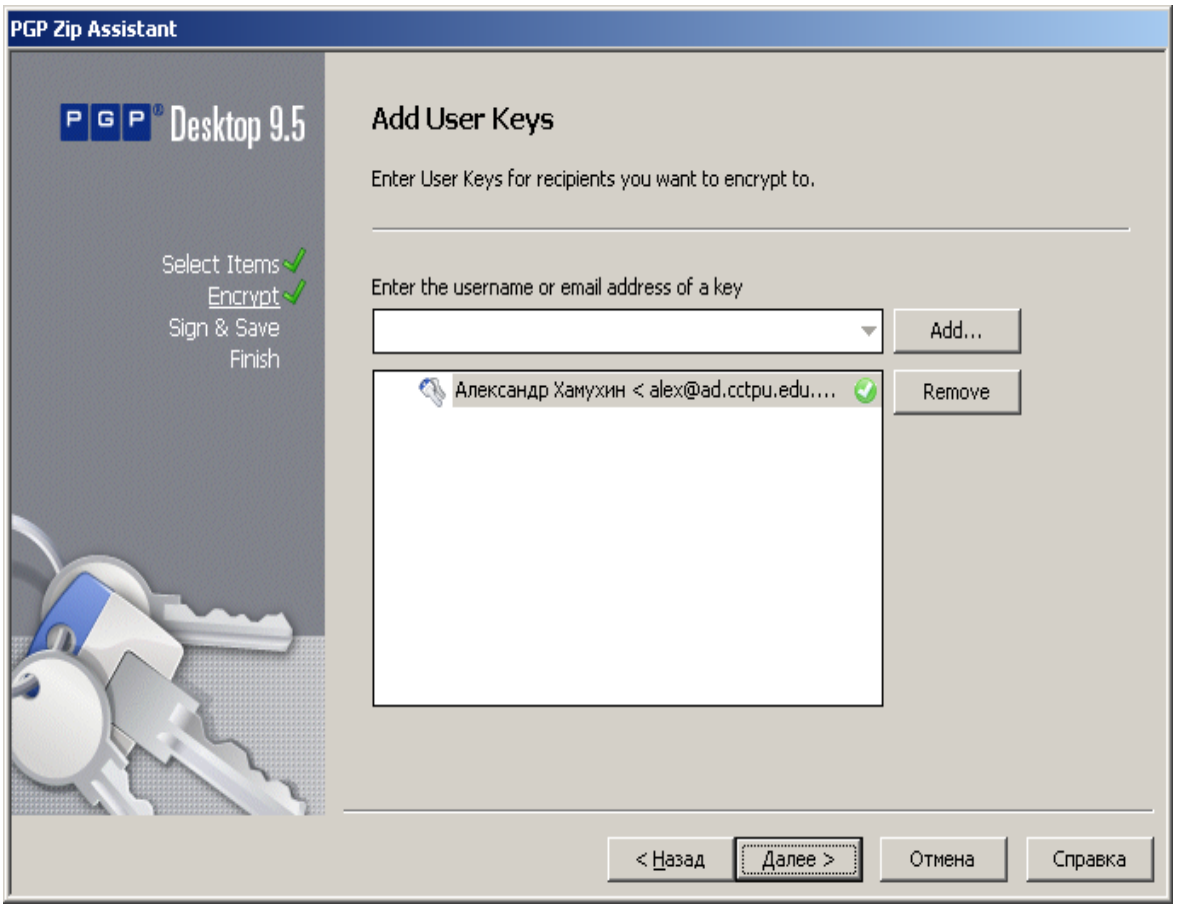


Рис. 4.9. Окно выбора респондентом открытого ключа для шифрования

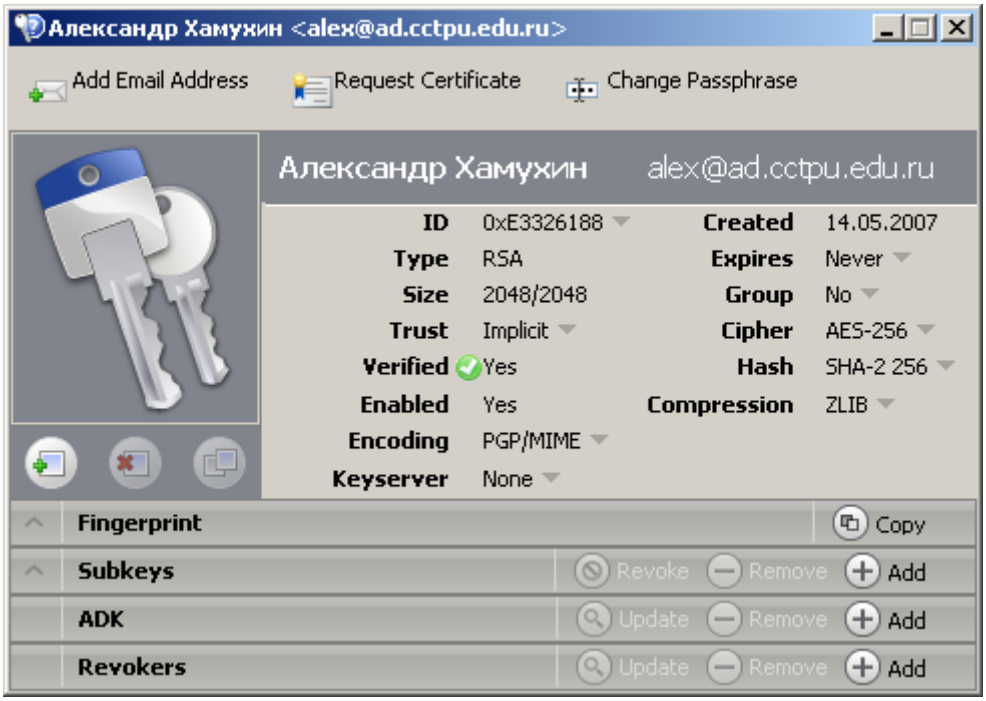


Рис. 4.10. Окно свойств пары ключей (для сверки ID)

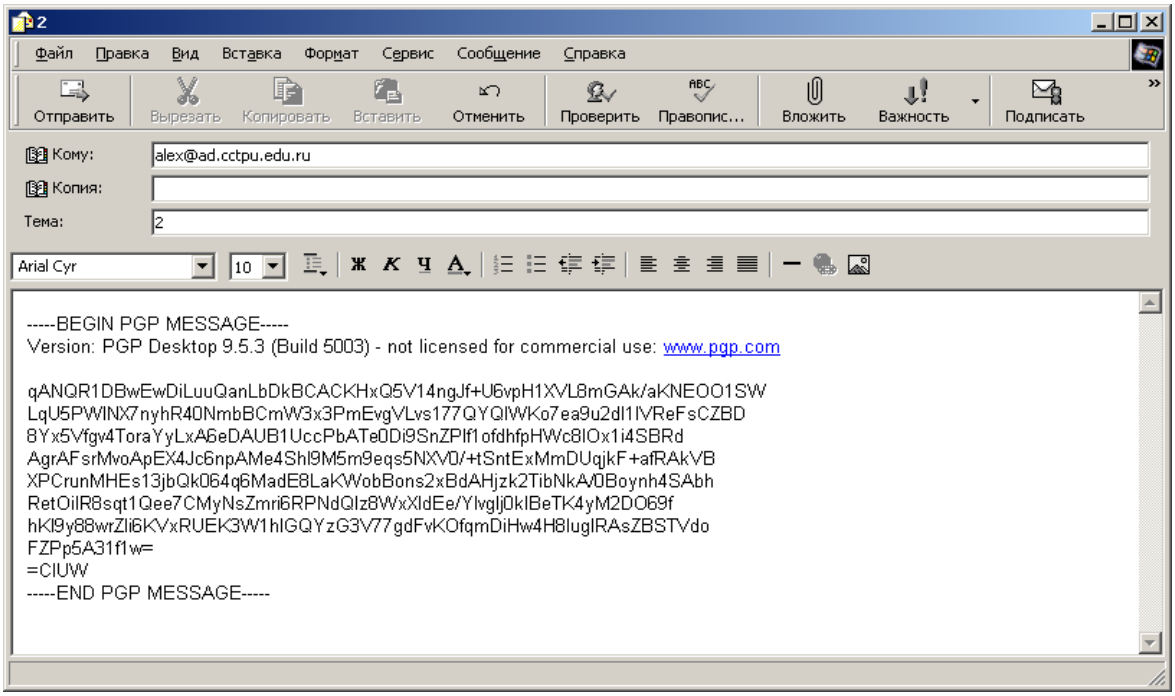


Рис. 4.11. Окно зашифрованного сообщения, полученного резидентом

Рис. 4.12. Окно на стороне резидента

Окно на стороне резидента (рис. 4.12) приведено при попытке дешифровать сообщение, показывающее, каким открытым ключом оно было зашифровано и требующее ввода парольной фразы. После правильного ввода сообщение будет дешифровано. Если сообщение было передано в файле, то должен появиться одноименный файл с дешифрованным текстом.

4.2. Стеганографический пакет *Steganos Security Suite*

Одним из самых популярных профессиональных пакетов стеганографии является пакет *Steganos Security Suite* 7 (рис. 4.13).

Рис. 4.13. Интерфейс пакета стеганографии Steganos Security Suite 7

С помощью *Steganos Security Suite* 7 можно создавать скрытые диски, записывать секретную информацию на внешние носители (например, *CD-RW*), упаковывать зашифрованную информацию в мультимедийные файлы типа *GIF*, *JPG*, *BMP*, *WAV*, кодировать данные, связанные с посещением интернета и так далее.

Утилита *Steganos Safe* позволяет на базе имеющегося свободного дискового пространства организовать виртуальный диск, защищенный паролем. Он хранится в файле с расширением **.sle*. Когда опция *Safe* открыта и секретный диск активизирован, он отображается в проводнике *Windows* и с ним можно работать как с отдельным накопителем.

При закрытии опции информация кодируется, и диск становится невидимым (рис. 4.14).

Рис. 4.14. Создание секретного диска в пакете стеганографии Steganos Security Suite

Утилита *Steganos Portable Safe* позволяет создавать виртуальные секретные части на внешних накопителях, таких, ка например, *CD-R*(*W*). На диске формируется некая виртуальная часть, размеры которой варьируются от 20 Мб до 4.7 Гб (*DVD*). Создается специальный каталог с названием *Portable Safe package files*, куда записывается файл **.sle*, а также установочные файлы для программы *Steganos Security Suite*.

В промежуточном этапе настройки **.sle* файл выглядит как отдельный диск, куда можно копировать информацию. По завершению операции вся информация кодируется. После этого можно воспользоваться любой программой записи *CD-R*(*W*), перенеся на него данные из папки *Portable Safe package files.* Как понятно, данный модуль позволяет кодировать большие объемы информации, включая кинофильмы. Все, что необходимо для дальнейшего раскодирования – пароль (рис. 4.15).

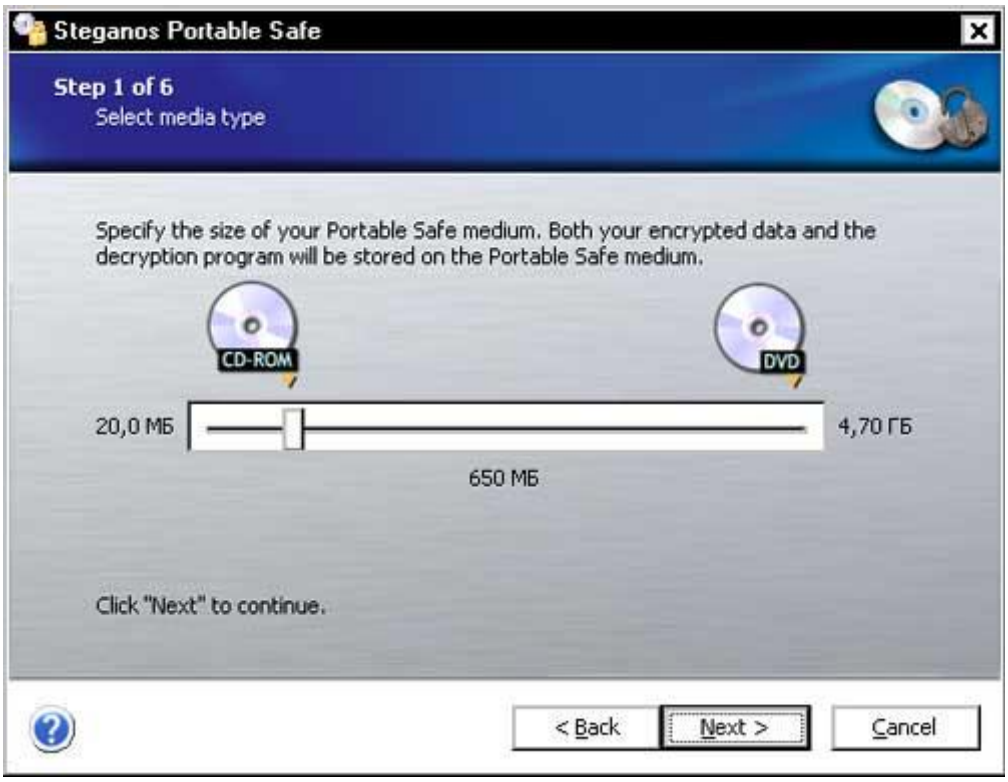


Рис. 4.15. Создание секретной части на внешнем накопителе в пакете стеганографии Steganos Security Suite

Особенно удобно в пакете *Steganos Security Suite* реализована функция шифрования сообщений электронной почты, для дешифрования которых получателю не нужно устанавливать сам пакет *Steganos Security Suite*. Любое сообщение, включая варианты «текст + вложенные файлы», кодируется в один самораскрывающийся файл с расширением **.cab* или **.exe*. При кодировании нужно ввести пароль и сообщить его получателю. Зашифрованный файл пересылается в аттачменте напрямую из почтовой программы, либо его можно сохранить на диске и послать любым другим удобным способом. При декодировании получателю совсем не обязательно иметь установленный *Steganos Security Suite*, достаточно знать пароль.

Утилита *Steganos File Manager* позволяет прятать зашифрованную информацию в файлах. В утилите реализовано два способа. Первый заключается в создании файла с расширением **.sef*, в который можно загружать сколь угодно данных, включая каталоги и т. п. Файл сохраняется на диске. Второй метод связан с «контейнерами». Данные помещаются в тело какого-либо файла (лучше всего мультимедийного *WAV*, *BMP*, *JPG* и т. п.) и деструктивно примешиваются к его данным. Например, в *wav* или *bmp*-файлах будет изменен младший бит. При воспроиз-

ведении либо отображении подобных файлов скрытая информация не видна и контейнер ведет себя как обычный файл.

Причем при деструктивном способе добавлении секретной информации размер файла не изменится. Отличительной особенностью данной утилиты является возможность автоматического поиска «контейнера», то есть программа сама укажет, можно ли вместить Вашу информацию в указанный мультимедийный файл и предложит Вам свои варианты.

Утилита *Steganos Password Manager* позволяет хранить множество паролей и сама защищена собственным паролем. Кроме этого, утилита позволяет генерировать сложные пароли с редкими сочетаниями символов на основе 128-битных ключей по стандарту *AES* (рис. 4.16).

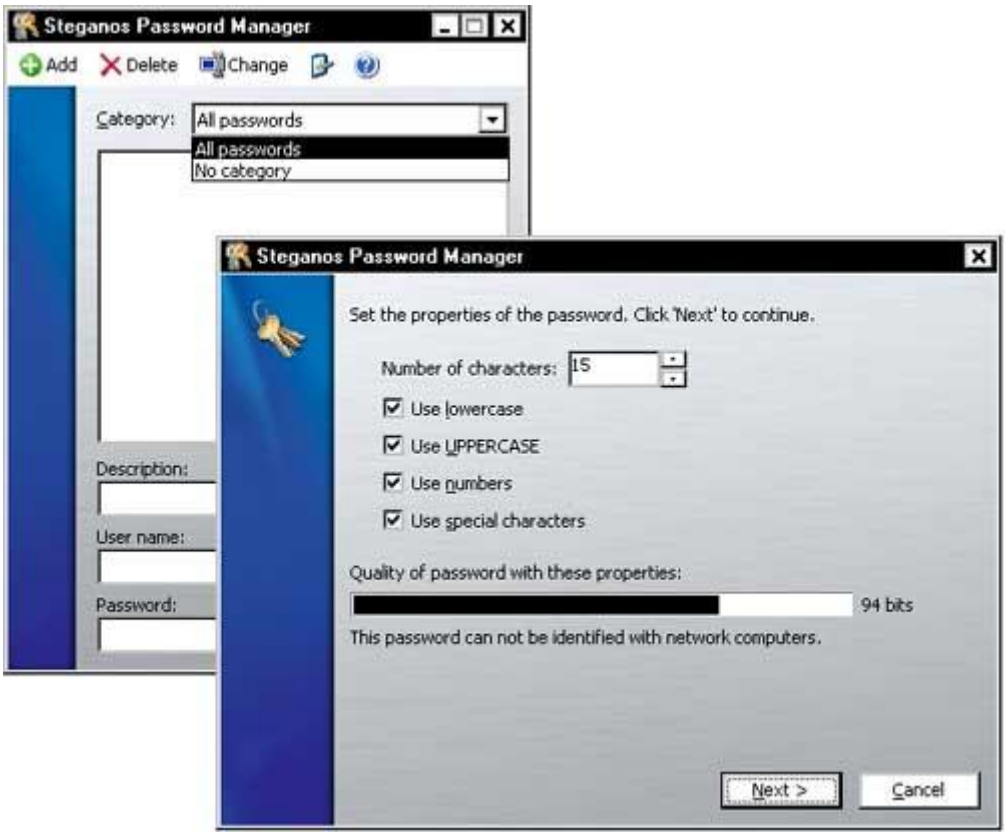


Рис. 4.16. Интерфейс утилиты работы с паролями пакета Steganos Security Suite

Утилита *Internet Trace Destructor* позволяет выборочно или полностью удалять информацию, связанную с посещением сетевых ресурсов, которая может быть использована злоумышленниками. Посещение сайтов Интернет обычно сопряжено с сохранением на диске множества временных и постоянных файлов, которыми могут воспользоваться сто-

ронние люди, в том числе удаленно. Это касается кэша, *cookies*, обмена онлайн-информацией, работы офисных приложений, браузера, настроек *AOL* и т. п. Данных накапливается достаточно много и далеко не все из них являются необходимыми и безопасными. *Internet Trace Destructor* имеет достаточно много настроек, но они подобраны по принципу «не навреди» (рис. 4.17).

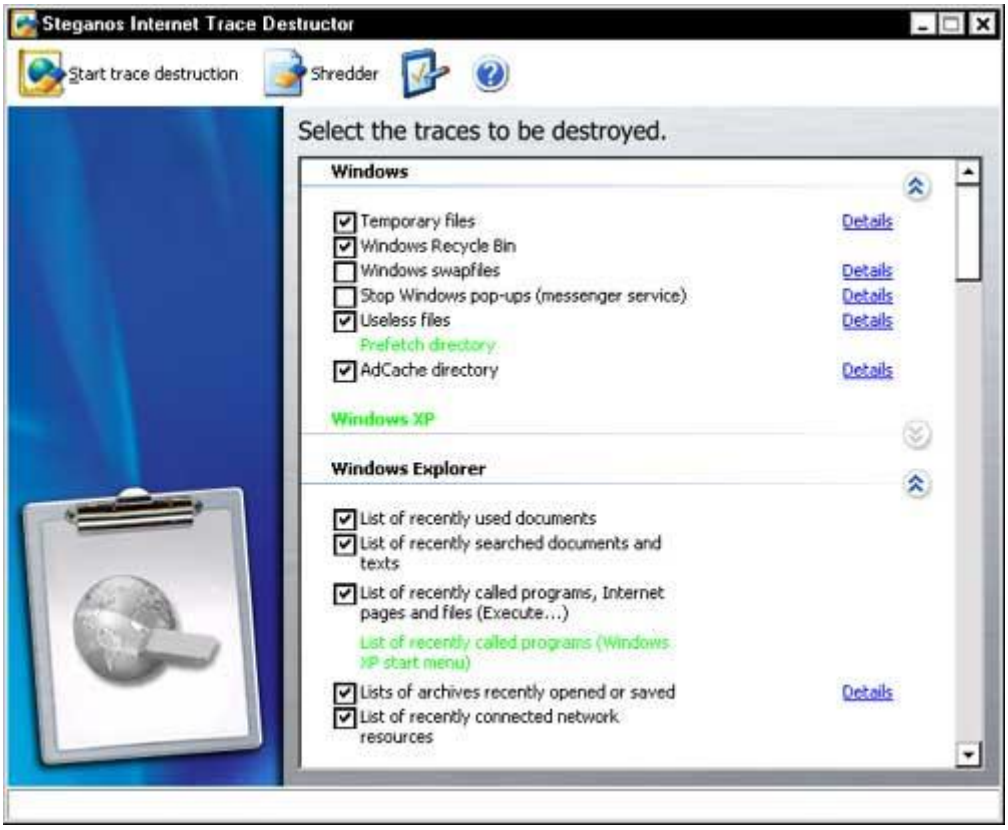


Рис. 4.17. Интерфейс утилиты Internet Trace Destructor пакета Steganos Security Suite

Утилита *Steganos Shredder* предназначена для надежного (физического) удаления файлов с диска. Существует множество программ, которые позволяют восстановить файл даже после его удаления из корзины *Windows*. Чтобы злоумышленники не могли ими воспользоваться, требуется физическая очистка диска. *Steganos Shredder* состоит из двух основных модулей – *File Shredder* (конкретное удаление файла без права на восстановление) и *Free Space Shredder* (полноценная очистка свободного дискового пространства). На рис. 4.18 представлен интерфейс этих модулей.

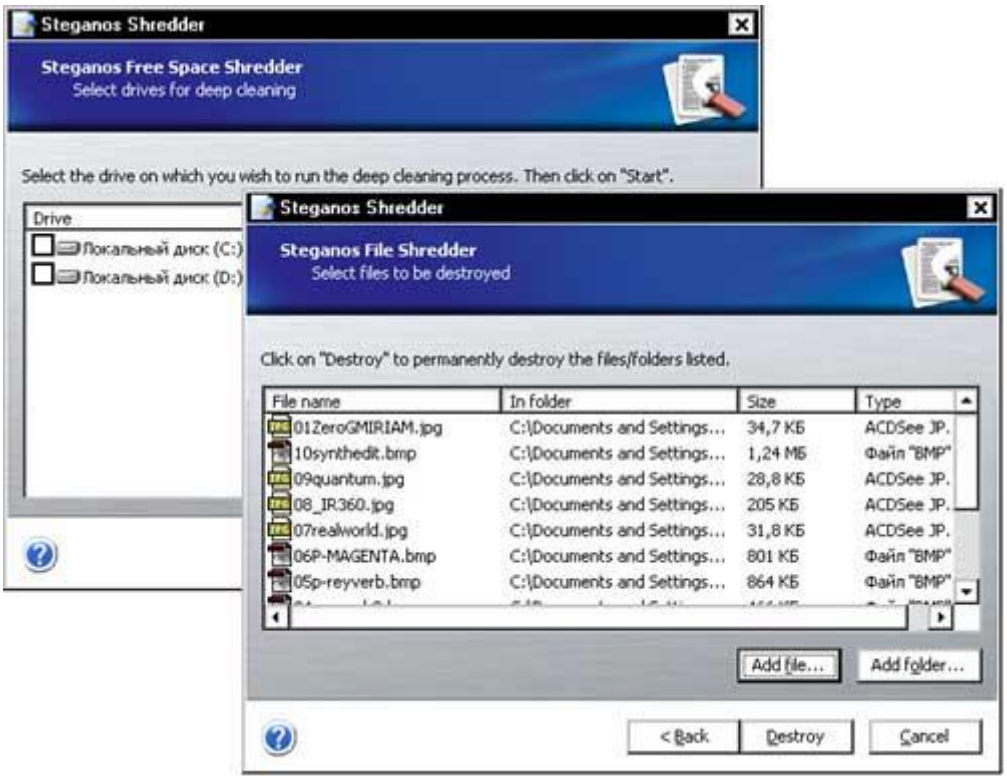


Рис. 4.18. Интерфейс утилиты Steganos Sredder пакета Steganos Security Suite

Таким образом, рассмотрены все функции *Steganos Security Suite* 7 – одного из самых современных и удачных решений в области компьютерной стеганографии. Помимо обеспечения секретной переписки, скрытия файлов, физического удаления файлов с дисков, данная система может скрывать зашифрованные данные в файлах типа *wav, bmp, html* и др. Следует отметить, что этот пакет находится в развитие. На момент написания этих строк уже вышла версия *Steganos Security Suite* 2008. Все описанные выше функции в ней сохранены. Улучшен интерфейс и добавлены утилиты *AntiTheft* (АнтиКража) и *Private Favorites* (работа с наиболее важными объектами).

Индивидуальные задания

Освоить работу с пакетом *Steganos Security Suite* на примере скрытия своей секретной информации «фамилия имя отчество» в файлы разных типов. По результатам работы представить отчет.

Глоссарий

Администратор безопасности
Security administrator
Администратор безопасности – должностное лицо, устанавливающее политику безопасности и идентифицирующее объекты и участников, к которым применяется эта политика.

Алгоритм поточного шифра
Stream cipher algorithm
Алгоритм поточного шифра – криптографическая система, в которой открытый и зашифрованный тексты обрабатываются как непрерывный поток.

Антивирусные программы
Antivirus
Антивирусные программы – в информатике – программы, которые предотвращают заражение компьютерным вирусом и/или ликвидируют последствия заражения.

Архитектура безопасности
Security architecture
Архитектура безопасности – официальное дополнение *ISO* к модели *OSI*, определяющее меры безопасности в информационной сети.
Архитектура безопасности предполагает:

- предотвращение чтения сообщений любыми лицами;
- защиту трафика от его анализа посторонними;
- обнаружение изменений потоков сообщений;
- определение искажений блоков данных.

В зависимости от используемых методов различают:

- сети со слабой защитой, в которых усилия нарушителя пропорциональны затратам отправителя;
- сети с сильной защитой, требующие резкого увеличения затрат нарушителя.

Асимметричная криптографическая система
(Асимметричная криптосистема; двухключевая криптосистема; криптосистема с открытым ключом)
Asymmetric cryptographic system

Асимметричная криптографическая система – криптосистема, содержащая преобразования (алгоритмы), наборы параметров которых различны и таковы, что по одному из них вычислительно невозможно определить другие параметры.

Атака
Attack
Атака – попытка злоумышленника вызвать отклонения от нормального протекания информационного процесса. Успех атаки зависит от уязвимости и эффективности системы защиты.

Аудит
Auditing
Аудит – в сетевых технологиях – стандартный процесс защиты сети, отслеживающий операции пользователей. Аудит:

- создает списки пользователей, обращавшихся к сетевым ресурсам;
- фиксирует модификации паролей и параметров регистрации;
- выявляет несанкционированные действия.

Аутентификация
Authentication
Аутентификация – процедура проверки подлинности данных и субъектов информационного взаимодействия исключительно на основе внутренней структура самих данных.

Аутентичность информации
Authenticity information
Аутентичность информации – избежание недостатка полноты или точности информации при ее санкционированных изменениях.

Безопасность
Safety; Security
Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.
Различают:

- социальную безопасность: правовую, интеллектуальную, духовно-культурную;
- экономическую безопасность: финансовую, хозяйственную, технологическую;

• территориальную безопасность: экологическую, сырьевую, жизненную;

• информационную безопасность.

Безопасность данных
Data security
Безопасность данных – защита данных от несанкционированной случайной или намеренной модификации, разрушения или раскрытия.

Безопасность информации
Information security
Информационная безопасность – по законодательству РФ – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
Информационная безопасность имеет три основные составляющие:

• конфиденциальность – защита чувствительной информации от несанкционированного доступа;

• целостность – защита точности и полноты информации и программного обеспечения;

• доступность – обеспечение доступности информации и основных услуг для пользователя в нужное для него время.

Безопасность сети
Network security
Безопасность сети – меры, предохраняющие информационную сеть:

• от несанкционированного доступа;

• от случайного или преднамеренного вмешательства в нормальные действия сети;

• от попыток разрушения ее компонентов.

Безопасность информационной сети включает защиту оборудования, программного обеспечения, данных и персонала.

Блочный шифр
Block cipher
Блочный шифр – разновидность симметричного шифра. Особенностью блочного шифра является обработка блока из нескольких байт за одну итерацию (как правило, 8 или 16). Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа.

Брандмауэр (Межсетевой экран)
Firewall
Брандмауэр – в информатике – программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения. Брандмауэр защищает соединяемую с Интернет корпоративную сеть от проникновения извне и исключает возможность доступа к конфиденциальной информации.

Брешь в безопасности
Security flaw
Брешь в безопасности – ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты.

Вирус-компаньон
Companion virus
Вирус-компаньон – вирус, исполняемый файл которого имеет то же имя, что и приложение, но другое расширение. Часто вместо расширения *EXE* вирус-компаньон располагается в файле с расширением *COM*, что обеспечивает его загрузку и запуск при активизации программы по имени.

Вирус-невидимка
Stealth virus
Вирус-невидимка – файловый вирус, остающийся «невидимым» для антивирусных программ. При проверке системы вирус-невидимка пытается перехватить запросы и выдать сфальсифицированный ответ, сигнализирующий, что все в порядке.

Вычислительная неосуществимость
(Вычислительная невозможность)
Computational infeasibility
Вычислительная неосуществимость – невозможность выполнить определенное преобразование данных с использованием имеющихся на сегодняшний день или предполагаемых к появлению в обозримом будущем вычислительных средств за разумное время.

Вычислительно необратимая функция
(Односторонняя функция)

One-way function
Вычислительно необратимая функция – функция, для которой:

- легко вычисляется значение функции по заданному аргументу;
- сложно вычисляется значение аргумента по заданному значению функции.

Для хорошо спроектированной вычислительно необратимой функции вычисление аргумента по заданному значению функции невозможно способом более эффективным способом, чем перебор по множеству возможных значений аргументов.

Гамма (Гаммирование)
Секретный ключ при поточном шифровании. Последовательность битов, вырабатываемых генератором псевдослучайных чисел, накладываемых на биты исходного текста с помощью логической операции «Исключительное ИЛИ».

Дезинформация
Misinformation
Дезинформация – целенаправленная передача информации от объекта-источника объекту-получателю в ситуации, когда реализация информации оказывается целесообразной (только) для объекта-источника.

Домен безопасности
Domain Security
Домен безопасности – совокупность объектов и участников информационного процесса, подчиняющихся единой политике безопасности и единой администрации безопасности.

Достоверность информации
Accuracy of information
Достоверность информации – в криптографии – общая точность и полнота информации. Достоверность информации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Доступность информации
Accessibility
Доступность информации – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Загрузочный вирус

Boot-sector virus
Загрузочный вирус – компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера.

Закрытый канал
Closed channel
Закрытый канал – логический канал, протокол которого расположен над транспортным уровнем и гарантирует секретность передачи между взаимодействующими абонентами. Закрытые каналы используются в коммуникационных сетях для обеспечения конфиденциальности.

Закрытый ключ электронно-цифровой подписи
The private key digital signature
Закрытый ключ электронно-цифровой подписи – по законодательству РФ – уникальная последовательность символов:

- известная владельцу сертификата ключа подписи;
- предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Защита информации
(Защита данных)
Data protection
Защита информации – совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Защищенность информационной системы
Security
Защищенность информационной системы – способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению. Различают два аспекта защищенности:

- техническую защиту (свойство недоступности);
- социальную защищенность (свойство конфиденциальности).

Злоумышленник
Intruder; hacker

Злоумышленник – субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. В криптографии считается, что в распоряжении злоумышленника имеются все необходимые для выполнения его задачи технические средства, созданные на данный момент.

Идентификационная политика безопасности
Identity-based security policy
Идентификационная политика безопасности – политика безопасности, основанная на идентифицирующих свойствах и/или атрибутах:

- пользователей или объектов, действующих от имени пользователей;
- ресурсов/объектов, к которым осуществляется доступ.

Имитозащита
Imitation protection
Имитозащита – защита систем передачи и хранения информации от навязывания ложных данных.

Имитовставка
Imitation Box
Имитовставка – последовательность данных фиксированной длины, полученная по определенному правилу из открытых данных и секретного ключа и добавленная к данным для обеспечения имитозащиты.

Инструкционная политика безопасности
Rule-based security policy
Инструкционная политика безопасности – политика безопасности, основанная на общих правилах, обязательных для всех пользователей. Обычно эти правила основываются на сравнении чувствительности ресурсов, к которым требуется доступ, и наличии соответствующих атрибутов у пользователей или объектов, выступающих от имени пользователей.

Код аутентификации
Authentication code
Код аутентификации – имитовставка; код фиксированной длины, вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу связи данных.

Код обнаружения манипуляций
Manipulation detection code
Код обнаружения манипуляций – код фиксированной длины, вырабатываемый из данных с использованием вычислительно необратимой функции с целью обнаружения факта изменения хранимых или передаваемых по каналу связи данных.

Компьютерные преступления
Computer crime
Компьютерные преступления – в уголовном праве РФ – преступления, посягающие на нормальное, безопасное функционирование компьютерных информационных систем:

- неправомерный доступ к компьютерной информации (Статья 272 УК РФ);
- создание, использование и распространение вредоносных программ для ЭВМ (Статья 273 УК РФ);
- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (Статья 274 УК РФ).

Компьютерный взлом
Hacking
Компьютерный взлом – несанкционированное проникновение в компьютерную сеть с целью получения собственной выгоды.

Компьютерный вирус
Computer virus
Компьютерный вирус – фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом. Дублируя себя, вирус записывается в другие программы. Вирус выполняется только при запуске зараженной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ.

Контроль безопасности
(Аудит безопасности)
Security Audit
Контроль безопасности – независимое изучение системных записей и действий:

- для проверки адекватности системных средств управления;

• для обеспечения их соответствия установленной политике и рабочим процедурам;

• для обнаружения брешей в безопасности и выдачи рекомендаций по изменению управления, политики и процедур.

Контроль доступа
Access auditing
Контроль доступа – процесс защиты данных и программ от их использования объектами, не имеющими на это права.
В сетях для контроля доступа используются:

• фильтрующие маршрутизаторы, реализующие алгоритмы анализа пакетов в части адресов отправления и назначения;

• фильтры пакетов, запрещающие установление соединений, пересекающих границы защищаемой сети;

• шлюзы прикладных программ, проверяющие права доступа к программам.

Контроль доступа для записи
Access auditing to records
Контроль доступа для записи – контроль доступа с целью изменения информации или данных в определенной информационной системе.

Контроль доступа для чтения
Access auditing to reading
Контроль доступа для чтения – контроль доступа с целью инициирования перемещения информации или данных из определенной информационной системы.

Контроль доступа к информации
Access auditing to information
Контроль доступа к информации – разрешение доступа к информации только полномочным пользователям.

Конфиденциальная информация
Confidential information
Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам.

Корпоративная политика безопасности
Corporate Security Policy
Корпоративная политика безопасности – совокупность законов, правил и мероприятий, регулирующих управление, защиту и распределение информационных ресурсов в пользовательской среде.

Криптографическая защита
Cryptographic protection
Криптографическая защита – защита информационных процессов от целенаправленных попыток отклонить их от нормальных условий протекания. Криптографическая защита базируется на криптографических преобразованиях данных.

Криптографическая система
(Криптосистема)
Cryptographic system (Cryptosystem)
Криптографическая система – набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса.

Криптографическая стойкость
(Криптостойкость)
Cryptographic strength
Криптографическая стойкость – устойчивость криптографического алгоритма к его криптоанализу.

Криптографический алгоритм
Cryptographic algorithm
Криптографический алгоритм – алгоритм преобразования данных:

- либо являющийся полностью или частично секретным;
- либо использующий при работе набор секретных параметров.

Дополнительно к криптографическим алгоритмам относят алгоритмы, не использующие секретные параметры, но применяющиеся в единой технологической цепочке с криптографическими алгоритмами.

Криптографический анализ (Криптоанализ)
Cryptanalysis

Криптоанализ – наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого.

Криптографический блок (Блок)
Cryptographic block (Block)
Криптографический блок – порция данных фиксированного для заданного криптоалгоритма размера, преобразуемая им за один цикл его работы.

Криптографический ключ (Ключ)
Cryptographic key (Key)
Криптографический ключ – конкретное секретное значение набора параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма. Криптографический ключ управляет процедурами шифрования и дешифрования.

Криптографическое преобразование
Cryptographic transformation
Криптографическое преобразование – преобразование данных по криптографическому алгоритму.

Криптографический протокол
Cryptographic protocol
Криптографический протокол – набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Криптология
Cryptology
Криптология – наука, исследующая криптографические преобразования. В криптологии различают два направления: криптографию (сокрытие информации) и криптоанализ несанкционированное вскрытие сокрытой информации).

Лазейка
Loophole

Лазейка – скрытый программный или аппаратный механизм, позволяющий обойти системные механизмы защиты. Обычно этот механизм активизируется некоторым неочевидным способом.

Логическая бомба
(Ловушка)
Logic bomb
Логическая бомба – программа, выполняемая периодически или в определенный момент времени с целью исказить, уничтожить или модифицировать данные.

Макровирус
Macro virus
Макровирус – файловый вирус, существующий в виде макроса (программы на встроенном языке) для определенного приложения. При открытии зараженного файла вирус выполняет свой код и заражает все файлы, к которым обращается приложение.

Маскарад
Masquerading
Маскарад – в информатике – нападение на систему, в котором участвует несанкционированный объект, выдающий себя за санкционированный объект с целью получения доступа к системным ресурсам.

Нарушение безопасности информации
Breach of Information Security
Нарушение безопасности информации – событие, при котором компрометируется один или несколько аспектов безопасности информации (доступность, конфиденциальность, целостность и достоверность).

Односторонняя хэш-функция
One-way hash function
Односторонняя хэш-функция – хэш-функция, являющаяся вычислительно необратимой функцией.

Оранжевая книга
Orange Book
Оранжевая книга – «Критерии определения безопасности компьютерных систем» (*Trusted Computer System Evaluation Criteria*) – стандарт Министерства обороны США, устанавливающий основные усло-

вия для оценки эффективности средств компьютерной безопасности, в котором:

- приводятся критерии оценки надежности компьютерных систем;
- определяются семь уровней безопасности, образующих в свою очередь четыре группы безопасности.

Открытый ключ
Public key
Открытый ключ – несекретный набор параметров асимметричной криптографической системы, необходимый и достаточный для выполнения отдельных криптографических преобразований.

Открытый ключ электронно-цифровой подписи
Electronic digital signature Public key
Открытый ключ электронно-цифровой подписи – по законодательству РФ – уникальная последовательность символов:

- соответствующая закрытому ключу электронной цифровой подписи;
- доступная любому пользователю информационной системы;
- предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Пассивная угроза безопасности
Passive threat
Пассивная угроза безопасности – угроза несанкционированного раскрытия информации без изменения состояния автоматизированной системы.

Перемешивание
Confusion
Перемешивание – свойство шифрующего преобразования усложнять взаимосвязи между элементами данных. Перемешивание затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифротекстом.

Перестановка
Permutation
Перестановка – криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных.

Подтверждение подлинности ЭЦП
Confirmation of authenticity of an electronic digital signature
Подтверждение подлинности ЭЦП – положительный результат проверки правильности ЭЦП.

Полиморфный вирус
Polymorphic virus
Полиморфный вирус – файловый вирус, изменяющий свой код при заражении очередного файла.

Политика информационной безопасности
Security policy
Политика информационной безопасности – совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников, системы информационной безопасности.

Пото́чный шифр
Stream cipher
Пото́чный шифр – это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. Поточный шифр реализует другой подход к симметричному шифрованию, нежели блочные шифры.

Принцип Кирхгофа
The principle of Kirchhoff
Принцип Кирхгофа – принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор параметров алгоритма (ключ), а остальные детали могут быть открыты без снижения стойкости алгоритма ниже допустимой величины.

Программа преимущественного права на защиту личной информации
Platform for privacy preferences initiative (*P3P*)
Программа преимущественного права на защиту личной информации – набор стандартов и технологических спецификаций для коммерческих веб-сайтов и браузеров. Программа обеспечивает пользователям возможность автоматического контроля информации, которую они оставляют на сайте.

Развертывание ключа
Key sheduling
Развертывание ключа – алгоритм, позволяющий получить по относительно короткому ключу шифрования последовательность раундовых ключей.

Рандомизация
Randomisation
Рандомизация – в криптографии – преобразование исходных данных перед или во время шифрования с помощью генератора псевдослучайных чисел. Рандомизация применяется для того, чтобы скрыть в исходном тексте идентичные блоки данных.

Рассеивание
Diffusion
Рассеивание – распространение влияния одного знака открытого текста или одного элемента ключа на множество знаков шифротекста.

Секретность
Privacy
Секретность – свойство криптосистемы обеспечивать секретность защищаемых данных.

Секретность данных
Data Privacy
Секретность данных – свойство данных быть известными и доступными только тому кругу субъектов, для которого они предназначены.

Секретный ключ
Secret key
Секретный ключ – набор секретных параметров одного из алгоритмов асимметричной криптосистемы.

Сервер защиты данных
Server Data Protection
Сервер защиты данных – сервер, оснащенный набором средств обеспечения безопасности данных.

Симметричная криптографическая система

(Симметричная криптосистема)
Symmetric cryptosystem
Симметричная криптографическая система – криптографическая система, реализующая алгоритмы шифрования (симметричные шифры), выполняемые на одном наборе параметров – на одном ключе.

Симметричный шифр
Symmetric cipher
Симметричный шифр – шифр, использующий для шифрования и дешифрования:

- либо один и тот же ключ;
- либо формально различные ключи, допускающие простое преобразование одного ключа в другой ключ.

Система защиты данных
Data protection system
Система защиты данных – комплекс программных, технических, криптографических и организационных средств, обеспечивающих защиту данных от несанкционированного использования, а также преднамеренного или случайного их разрушения и искажения.

Система обеспечения безопасности
Security system
Система обеспечения безопасности – совокупность стандартных защитных мер: криптографическое кодирование, паролирование, присваивание идентификатора, электронная цифровая подпись и т. д.

Слой безопасных соединений
Secure Sockets Layer (*SSL*)
Слой безопасных соединений – протокол, обеспечивающий защиту данных, передаваемых по сети Интернет. Протокол *SSL* обеспечивает безопасность и целостность канала передачи с помощью шифрования и опознавательных кодов сообщения.

Спам
Spam
Сообщения, массово рассылаемые людям, не дававшим согласие на их получение. В первую очередь, термин «спам» относится к электронным письмам.

Средства защиты информации
Means of Protection information
Средства защиты информации в РФ:

- технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну;
- средства реализации средств защиты информации;
- редства контроля эффективности защиты информации.

Средства электронно-цифровой подписи
Means of electronic signature
Средства электронно-цифровой подписи – по законодательству РФ – аппаратные и/или программные средства, обеспечивающие:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи;
- подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;
- создание закрытых и открытых ключей электронных цифровых подписей.

Троянский конь
Trojan horse
Троянский конь – в информатике – компьютерная программа, реализующая полезную функцию и содержащая дополнительные скрытые функции, которые тайно используют законные полномочия инициирующего процесса в ущерб безопасности.

Угроза безопасности
Threat
Угроза безопасности – в широком смысле – потенциальное нарушение безопасности. Угроза безопасности – в системах обработки данных – потенциальное действие или событие, которое может привести к нарушению одного или более аспектов безопасности информационной системы.

Управление безопасностью
Security Management

Управление безопасностью – в компьютерных сетях – средства, обеспечивающие безопасность данных и защищающие ресурсы сети. Средства управления безопасностью осуществляют:

- шифрование и управление ключами расшифровки;
- регистрацию паролей;
- идентификацию пользователей;
- обслуживание и анализ файлов безопасности;
- защиту от компьютерных вирусов.

Управление данными
Data management
Управление данными – процесс, связанный с накоплением, организацией, запоминанием, обновлением, хранением данных и поиском информации.

Уязвимость
Vulnerability
Уязвимость – слабое место в информационной системе, которое может привести к нарушению безопасности. Различают:

- техническую уязвимость, возникающую в результате неисправности технологического компонента информационной системы;
- программную уязвимость, возникающую в результате недоработки разработчиков системы или ошибок обслуживающего персонала в настройках безопасности программы.

Файловый вирус
File virus
Файловый вирус – компьютерный вирус, прикрепляющий себя к файлу или программе и активизирующийся при каждом использовании файла. Различают вирусы-компаньоны, макровирусы, полиморфные вирусы, вирусы-невидимки и т. п.

Фи́шинг
Phishing, от *password* – пароль и *fishing* – рыбная ловля, выуживание – вид Интернет-мошенничества, цель которого – получить идентификационные данные пользователей. Организаторы фишинг-атак используют массовые рассылки электронных писем от имени популярных брендов. В эти письма они вставляют ссылки на фальшивые сайты, являющиеся точной копией настоящих. Оказавшись на таком сайте, пользователь может сообщить преступникам ценную информацию, позволяющую

управлять своим счётом из Интернета (имя пользователя и пароль для доступа), или номер и пин-код своей кредитной карты.

Хакер
Hacker
От англ. *Hack* – кромсать.
Хакер – лицо, совершающее различного рода незаконные действия в сфере информатики:

- несанкционированное проникновение в чужие компьютерные сети и получение из них информации;
- незаконные снятие защиты с программных продуктов и их копирование;
- создание и распространения компьютерных вирусов и т. п.

Действия хакера образуют различные составы уголовных преступлений и гражданских правонарушений во многих странах мира.

Хэш
(Хэш-блок; Хэш-значение, Хеш)
Hash; *Hash-block*; *Hash-value*
Хэш – блок данных фиксированного размера, полученный в результате хэширования массива данных.

Хэш-функция
Hash-function
Хэш-функция – функция, осуществляющая хэширование массива данных посредством отображения значений из очень большого множества-значений в существенно меньшее множество значений фиксированной длины. Причем обратное отображение должно быть как можно более вычислительно сложной задачей.

Хэширование
Hashing
Хэширование – в криптографии – преобразования массива данных произвольного размера в блок данных фиксированного размера, существенно меньше исходного. Хеширование применяется для формирования электронных цифровых подписей документов.

Целостность данных
Data integrity

Целостность данных – свойство, при выполнении которого данные сохраняют заранее определенный вид, содержание и качество.

Центр сертификации
Certificate authority
Центр сертификации (удостоверяющий центр) – третья сторона, удостоверяющая аутентичность открытых ключей пользователей или других центров сертификации.
В обязанности центров сертификации входит:

- проверка данных и выдача сертификатов;
- связывание открытых ключей с уникальными именами посредством подписанных сертификатов;
- управление порядковыми номерами сертификатов;
- отзыв сертификатов.

Червь
Worm
Червь – независимая программа, которая размножается путем копирования самой себя из одного сетевого компьютера в другой. Обычно червь не портит данные или программы и не вызывает непредсказуемого поведения, однако может вызвать неоправданную загрузку каналов связи и памяти.

Цифровой сертификат
Digital certificate

Цифровой сертификат – выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов. Сертификат открытого ключа удостоверяет принадлежность открытого ключа некоторому субъекту, например, пользователю. Сертификат открытого ключа содержит имя субъекта, открытый ключ, имя удостоверяющего центра, политику использования соответствующего удостоверяемому открытому ключу закрытого ключа и другие параметры, заверенные подписью удостоверяющего центра. Структура сертификата атрибутов аналогична структуре сертификата открытого ключа. Отличие заключается в том, что сертификат атрибутов удостоверяет не открытый ключ субъекта, а какие-либо его атрибуты – принадлежность к какой-либо группе, роль, полномочия и т. п.

Чувствительная информация
(Критическая информация)
Sensitive information
Чувствительная информация – информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.

Шифр
Cipher; Cypher
Шифр – совокупность алгоритмов криптографических преобразований, отображающих множество возможных понятных данных на множество возможных непонятных данных и обратных им преобразований.

Электронное устройство защиты
Dongle
Электронное устройство защиты – электронное устройство в составе компьютера, предназначенное для защиты программ и данных от несанкционированного доступа. Электронное устройство защиты выполняет функции замка, ответчика и т. п.

Электронная цифровая подпись (ЭЦП)
Electronic digital signature
Электронная цифровая подпись – последовательность символов, полученная в результате криптографического преобразования электронных данных. ЭЦП добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки. ЭЦП используется в качестве аналога собственноручной подписи в электронных документах.

Список литературы

Основная

1. Галатенко В.А. Основы информационной безопасности. 4-е издание. – М.: ИНТУИТ, 2008. – 208 с.

2. Мещеряков Р.В. Информационная безопасность: учебное пособие . – Томск: Изд-во ТПУ, 2004. – 168 с.

3. Введение в криптографию / под общей ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.

4. Ложников П.С. Михайлов Е.М. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем *Microsoft*. – М.: ИНТУИТ, 2008. – 247 с.

5. Каталог государственных стандартов, 2010. *URL*: *http://www.gostbaza.ru/* (дата обращения: 13.07.2010).

Дополнительная

6. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2006. – 544 с

7. Спицын В.Г., Столярова Н.А. Защита информации и информационная безопасность: учебное пособие /. – Томск: Изд-во ТПУ, 2003. – 166 с.

8. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография / Серия «Учебники для вузов. Специальная литература». – СПб.: Лань, 2000. – 224 с.

9. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебное пособие для вузов / под ред. А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. и доп.– М.: Горячая линия–Телеком, 2009. – 616 с.

10. Федеральный закон о государственной тайне от 06.10.97 N 131-ФЗ. *URL*: *http://www.fsb.ru/under/secret.html*#02 (дата обращения: 31.03.2010).

11. Никифоров С.В. Введение в сетевые технологии. Элементы применения и администрирования сетей: учебное пособие. – М.: Финансы и статистика, 2003. – 224 с.

12. Галатенко В.А. Стандарты информационной безопасности. – М.: ИНТУИТ, 2003. *URL*: *http://www.intuit.ru/department/security/secst/* (дата обращения: 13.07.2010)

13. Лапонина О.Р. Криптографические основы безопасности. – М.: ИНТУИТ, 2003. *URL*:

http://www.intuit.ru/department/security/networksec/ (дата обращения: 13.07.2010).

14. Джонс К.Д., Шема М., Джонсон Б.С. Инструментальные средства обеспечения безопасности. – М.: ИНТУИТ, 2007. *URL*: *http://www.intuit.ru/department/security/issec/* (дата обращения: 13.07.2010).

15. Хаулет Т. Инструменты безопасности с открытым ключом. – М.: ИНТУИТ, 2006. *URL*:

http://www.intuit.ru/department/security/secopen/ (дата обращения: 13.07.2010).

16. Анисимов А.А. Менеджмент в сфере информационной безопасности. – М.: ИНТУИТ, 2009. *URL*:

http://www.intuit.ru/department/itmngt/manofis/ (дата обращения: 13.07.2010).

17. Лапонина О.Р. Протоколы безопасного сетевого взаимодействия. – М.: ИНТУИТ, 2005. *URL*:

http://www.intuit.ru/department/security/networksec2/ (дата обращения: 13.07.2010).

18. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. – Томск: Изд-во В-Спектр, 2007.– 278 с.

19. Мещеряков Р.В., Шелупанов А.А. Специальные вопросы информационной безопасности: Монография. – Томск: Изд-во Института оптики атмосферы СОРАН.2003. – 224 с.

20. Система ТЕХНОРМАТИВ – российские стандарты и нормативная документация, 2010. *URL*: *http://technormativ.ru/*

Приложения

Приложение 1. Федеральный закон Российской Федерации «Об электронной цифровой подписи»

Принят Государственной Думой 13 декабря 2001 года
Одобрен Советом Федерации 26 декабря 2001 года

Глава I. Общие положения

Статья 1. Цель и сфера применения настоящего Федерального закона

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Статья 2. Правовое регулирование отношений в области использования электронной цифровой подписи

Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информатизации и защите информации», Федеральным законом «О связи», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также осуществляется соглашением сторон.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1. электронный документ – документ, в котором информация представлена в электронно-цифровой форме;

2. электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

3. владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

4. средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

5. сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

6. 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;

7. 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;

8. сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

9. подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

10. пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

11. информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

12. корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Глава II. Условия использования электронной цифровой подписи

Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

1. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

• подтверждена подлинность электронной цифровой подписи в электронном документе;

• электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

2. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Статья 5. Использование средств электронной цифровой подписи

1. Создание ключей электронных цифровых подписей осуществляется для использования в:

• информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;

• корпоративной информационной системе в порядке, установленном в этой системе.

2. При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации.

3. Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.

4. Сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

Статья 6. Сертификат ключа подписи

1. Сертификат ключа подписи должен содержать следующие сведения:

• уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

• фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;

• открытый ключ электронной цифровой подписи;

• наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;

• наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

• сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

2. В случае необходимости в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме - иные сведения, подтверждаемые соответствующими документами.

3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

4. Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот серти-

фикат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре

1. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

2. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

3. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Глава III. Удостоверяющие центры

Статья 8. Статус удостоверяющего центра

1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

2. Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности.

Статья 9. Деятельность удостоверяющего центра

1. Удостоверяющий центр:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

2. Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в статье 6 настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственно-

ручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

3. При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй – остается в удостоверяющем центре.

4. Услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

Статья 10. Отношения между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти

1. Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

2. Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров.

3. Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих электронных цифровых подписей для целей, не свя-

занных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

4. Уполномоченный федеральный орган исполнительной власти:

• осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

• осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

Статья 11. Обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

• вносить сертификат ключа подписи в реестр сертификатов ключей подписей;

• обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;

• приостанавливать действие сертификата ключа подписи по обращению его владельца;

• уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

• иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Статья 12. Обязательства владельца сертификата ключа подписи

1. Владелец сертификата ключа подписи обязан:

• не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

• хранить в тайне закрытый ключ электронной цифровой подписи;

• немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

2. При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

Статья 13. Приостановление действия сертификата ключа подписи

1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

Статья 14. Аннулирование сертификата ключа подписи

1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

- по истечении срока его действия;
- при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;
- в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;
- по заявлению в письменной форме владельца сертификата ключа подписи;
- в иных установленных нормативными правовыми актами или соглашением сторон случаях.

2. В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

Статья 15. Прекращение деятельности удостоверяющего центра

1. Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством.

2. В случае прекращения деятельности удостоверяющего центра, указанного в пункте 1 настоящей статьи, сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей. Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение в соответствии со статьей 7 настоящего Федерального закона уполномоченному федеральному органу исполнительной власти.

3. Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников этой системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

Глава IV. Особенности использования электронной цифровой подписи

Статья 16. Использование электронной цифровой подписи в сфере государственного управления

1. Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

2. Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном настоящим Федеральным законом для удостоверяющих центров.

3. Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

Статья 17. Использование электронной цифровой подписи в корпоративной информационной системе

1. Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным настоящим Федеральным законом для информационных систем общего пользования.

2. Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

3. Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Статья 18. Признание иностранного сертификата ключа подписи

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

Статья 19. Случаи замещения печатей

1. Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

2. В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Глава V. Заключительные и переходные положения

Статья 20. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом

1. Нормативные правовые акты Российской Федерации подлежат приведению в соответствие с настоящим Федеральным законом в течение трех месяцев со дня вступления в силу настоящего Федерального закона.

2. Учредительные документы удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом в течение шести месяцев со дня вступления в силу настоящего Федерального закона.

Статья 21. Переходные положения

Удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать требованиям настоящего Федерального закона, за исключением требования предварительно представлять сертификаты ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позднее чем через три месяца со дня вступления в силу настоящего Федерального закона.

Задания

1. Зайти на сайт Национального удостоверяющего центра РФ *http://www.nucrf.ru/#* и установить процедуру получения сертификата ЭЦП (по Регламенту услуг). Составить отчет в форме инструкции для пользователя, желающего получить сертификат ЭЦП.

2. Повторить Задание 1 для удостоверяющего центра *http://www.ekey.ru/*.

3. Повторить Задание 1 для удостоверяющего центра *http://www.nwudc.ru/*.

4. Повторить Задание 1 для удостоверяющего центра *http://www.cryptopro.ru/cryptopro/services/ca-service.htm*

5. Повторить Задание 1 для удостоверяющего центра *http://www.mruc.ru/*.

Приложение 2. Закон о государственной тайне (выписка)

Статья 2. Основные понятия, используемые в настоящем Законе

В настоящем Законе используются следующие основные понятия:

- государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;
- допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;
- доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;
- перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Статья 5. Перечень сведений, составляющих государственную тайну

Государственную тайну составляют:

1) сведения в военной области:

• о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

• о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

• о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

• о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

• о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

• о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

• о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизацион-

ных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

• об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

• о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

• об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

• о достижениях науки и техники, о научно - исследовательских, об опытно - конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

• об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики:

• о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

• о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

• о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

• о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно - розыскную деятельность;

• об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

• о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

• о методах и средствах защиты секретной информации;

• об организации и о фактическом состоянии защиты государственной тайны;

• о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

• о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

• о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства

Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию (в ред. Федерального закона от 06.10.97 № 131-ФЗ)

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

• о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

• о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

• о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

• о фактах нарушения прав и свобод человека и гражданина;

• о размерах золотого запаса и государственных валютных резервах Российской Федерации;

• о состоянии здоровья высших должностных лиц Российской Федерации;

• о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суд.

Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Статья 10. Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее – собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации

Статья 12. Реквизиты носителей сведений, составляющих государственную тайну

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- о регистрационном номере;
- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Статья 16. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями

Взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ, с санкции органа государственной власти, в распоряжении которого в соответствии со статьей 9 настоящего Закона находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений. Их руководители несут персональную ответственность за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.

Статья 20. Органы защиты государственной тайны

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне. Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом Российской Федерации.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложен-

ными на них законодательством Российской Федерации (часть третья в ред. Федерального закона от 29.06.2004 № 58-ФЗ).

Статья 21. Допуск должностных лиц и граждан к государственной тайне

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;
- ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;
- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации. Целью проведения проверочных мероприятий является выявление оснований, предусмотренных статьей 22 настоящего Закона.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Устанавливаются три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным или секретным.

Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Статья 21.1. Особый порядок допуска к государственной тайне (введена Федеральным законом от 06.10.97 № 131-ФЗ)

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных статьей 21 настоящего Закона.

Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:

- признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения Российской Федерации;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;
- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Прекращение допуска к государственной тайне не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Статья 28. Порядок сертификации средств защиты информации

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны.

Задания

1. Зайти на сайт Федеральной службы по техническому и экспортному контролю РФ (*http://www.fstec.ru/)* и найти там информацию, относящуюся к охране государственной тайны.

2. Выполнить п.1 для сертификации средств защиты информации.

3. Выполнить п.1 по лицензионной деятельности ФСТЭК в области информационной безопасности.

4. Выполнить п.1 по экспортному контролю ФСТЭК в области информационной безопасности.

По всем заданиям составить отчет в форме инструкции для пользователя.

Приложение 3. Выписка из УК РФ в сфере информационной и компьютерной безопасности

Статья 146. Нарушение авторских и смежных прав.

1. Незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб, – наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, – наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного го-

да до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Статья 275. Государственная измена

Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином Российской Федерации,– наказывается ли-

шением свободы на срок от двенадцати до двадцати лет с конфискацией имущества или без таковой.

Примечание. Лицо, совершившее преступления, предусмотренные настоящей статьей, а также статьями 276 и 278 настоящего Кодекса, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления.

Статья 276. Шпионаж

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства, – наказываются лишением свободы на срок от десяти до двадцати лет.

Статья 283. Разглашение государственной тайны

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены – наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 284. Утрата документов, содержащих государственную тайну

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную

тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, – наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 292. Служебный подлог

Служебный подлог, то есть внесение должностным лицом, а также государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершены из корыстной или иной личной заинтересованности, – наказываются штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до двух лет.

Задания

Составить перечень жизненных ситуаций (связанных с информационными объектами), подпадающих под каждую статью УК РФ, перечисленные выше. Например: купил пиратский диск для собственного использования (ст. 146), без разрешения преподавателя вставил флешку в государственный компьютер и скопировал и скопировал файл (ст. 272), записал на чужой компьютер свой файл, зараженный вирусом (ст. 273), стер системный файл в компьютерном классе (ст. 274), сознательно выдал государственную тайну другу-студенту, гражданину другой страны (ст. 275), собирал информацию в Интернете о ТТХ оружия РФ (ст. 276) неосторожно выдал государственную тайну соседу-студенту, гражданину КНР (ст. 283), потерял ноутбук с государственными тайнами (ст. 284), подменил экзаменационный лист на сайте преподавателя (ст. 292). В отчете привести анализ ситуации (*case study*).

Приложение 4. Перечень государственных стандартов в сфере информационной безопасности

- ГОСТ Р 34.10-94. «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
- ГОСТ Р 34.11-94. «Информационная технология. Криптографическая защита информации. Функция хэширования».
- ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
- ГОСТ Р 51188-98. «Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство».
- ГОСТ Р 51275-99. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
- ГОСТ Р 51898-2002. «Аспекты безопасности. Правила включения в стандарты».
- ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью».

Этот стандарт устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями.

- ГОСТ Р 50922-2006. «Национальный стандарт РФ. Защита информации. Основные термины и определения».
- ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».

- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».
- ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности».
- ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств».
- ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
- ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
- ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки».
- ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца».
- ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица».
- ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза».
- ГОСТ Р ИСО/МЭК 15408-1-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». Данная часть ИСО/МЭК 15408 устанавливает две формы представления функциональных требований и требований доверия к безопасности ИТ. Конструкция «профиль защиты» (ПЗ) предусматривает создание обобщенного, предназначенного для многократного использования набора этих требований безопасности. ПЗ может быть использован предполагаемыми потребителями для спецификации и идентификации продуктов с характеристиками безопасности ИТ, которые будут удовлетворять их потребностям. Задание по безопасности (ЗБ) содержит требования безопасности и специфицирует функции безопасности для конкретного продукта или системы, подлежащих оценке и называемых

объектом оценки (ОО). ЗБ используется оценщиками в качестве основы для оценки, проводимой в соответствии с ИСО/МЭК 15408.

- ГОСТ Р ИСО/МЭК 15408-2-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».
- ГОСТ Р ИСО/МЭК 15408-3-2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».
- ГОСТ Р ИСО/МЭК 15408. «Общие критерии оценки безопасности информационных технологий» – стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности, благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» – защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
- ГОСТ Р ИСО/МЭК 27001-2006 – «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Прямое применение международного стандарта *ISO*/*IEC* 27001:2005. Этот стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). Внедрение СМИБ является стратегическим решением организации. На проектирование и внедрение СМИБ влияют потребности и цели организации, требования безопасности, используемые процессы, а также масштабы деятельности и структура организации. Предполагается, что вышеуказанные факторы и поддерживающие их системы будут изменяться во времени. Предполагается также, что СМИБ будет изменяться пропорционально потребностям организации, т. е. для простой ситуации потребуется простое решение по реализации СМИБ.

Задания

По названию ГОСТ найти в Интернете сайт с его содержанием (официальный) и сделать его краткий обзор в форме инструкции для пользователя. Название ГОСТ задается преподавателем.

Оглавление

Учебное издание

Практикум по информационной безопасности

Учебное пособие

ХАМУХИН Александр Анатольевич

Научный редактор кандидат технических наук,
зав кафедрой информационных систем ЮТИ
доцент А.А. Захарова

Издано в авторской редакции

Отпечатано в Издательстве ТПУ в полном соответствии
с качеством предоставленного оригинал-макета

Подписано к печати 01.01.2011. Формат 60x84/16. Бумага «Снегурочка».
Печать XEROX. Усл.печ.л. 12,25. Уч.-изд.л. 11,09.
Заказ XXX. Тираж 100 экз.

Национальный исследовательский Томский политехнический университет
Система менеджмента качества
Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту ISO 9001:2000

ИЗДАТЕЛЬСТВО ТПУ. 634050, г. Томск, пр. Ленина, 30.
Тел./факс: 8(3822)56-35-35, www.tpu.ru