РИИТ БНТУ

Белорусский национальный технический университет
Республиканский институт инновационных технологий

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Учебно-методическое пособие

В.А. Ганжа
В.В. Сидорик
О.И. Чичко

Информационные технологии в образовании

Министерство образования Республики Беларусь
БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Республиканский институт инновационных технологий

В.А. Ганжа
В.В. Сидорик
О.И. Чичко

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ НАДЁЖНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Учебно-методическое пособие
для слушателей системы повышения квалификации
и переподготовки

Рекомендовано учебно-методическим объединением высших учебных заведений Республики Беларусь по образованию в области приборостроения

Минск
БНТУ
2010

УДК 378.046:004 (075)
ББК 65.240я7
Г 19

Рецензенты:
С.Ф. Липницкий, главный научный сотрудник ОИПИ НАН Беларуси, д-р техн. наук;
В.М. Лутковский, старший преподаватель кафедры системного анализа БГУ

Ганжа, В.А.

Г 19 Безопасность информации и обеспечение надёжности компьютерных систем: учебно-методическое пособие для слушателей системы повышения квалификации и переподготовки / В.А. Ганжа, В.В. Сидорик, О.И. Чичко. – Минск: БНТУ, 2010. – 67 с.

ISBN 978-985-525-399-1.

В учебно-методическом пособии рассматриваются проблемы информационной безопасности при переподготовке по специальности «Программное обеспечение информационных систем». Проблемы информационной безопасности решаются на примерах защиты накопленных информационных ресурсов, обусловленных критической зависимостью нашей деятельности от информационных технологий. Разбираются некоторые аспекты использования пакета PGP для практической работы с обучаемыми.

Данное издание предназначено для слушателей системы повышения квалификации и переподготовки, преподавателей.

УДК 378.046:004 (075)
ББК 65.240я7

ISBN 978-985-525-399-1

Содержание

Введение 5
1. Теоретическая часть 8
1.1. Законодательный уровень 8
1.2. Нормативные документы и стандарты 8
1.2.1. Оценочный стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» 8
1.2.2. Информационная безопасность распределённых систем. Рекомендации Международного союза телекоммуникаций (ITU) X.800 9
1.2.3. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» 10
1.3. Административный уровень 12
1.3.1. Политика безопасности 12
1.3.2. Программа безопасности 15
1.3.3. Синхронизация программы безопасности с жизненным циклом систем 15
1.4. Процедурный уровень. Основные классы мер процедурного уровня 17
1.4.1. Управление персоналом 17
1.4.2. Физическая защита 19
1.4.3. Поддержание работоспособности 20
1.4.4. Реагирование на нарушения режима безопасности 21
1.4.5. Планирование восстановительных работ 22
1.5. Программно-технический уровень 23
1.5.1. Основные понятия программно-технического уровня информационной безопасности 23
1.5.2. Особенности современных информационных систем, существенные с точки зрения безопасности 24
1.5.3. Архитектурная безопасность 24
1.6. Основные понятия криптографии 26
1.6.1. Основные понятия 26
1.6.2. Криптоанализ 27
1.6.3. Алгоритмы традиционного симметричного шифрования 28
1.6.4. Шифрование с открытым ключом. Основные требования к алгоритмам асимметричного шифрования 29
1.6.5. Основные способы использования алгоритмов с открытым ключом 32
1.6.6. Аутентификация сообщений 34
1.6.7. Цифровые подписи и протоколы аутентификации 36
2. Практическая часть 41
2.1. Основные понятия и применение стеганографии 41
2.1.1. Внедрение данных в файл-носитель программой wbStego4 41
2.1.2. Извлечение данных из файла носителя программой wbStego4 47
2.2. Вычисление хэш-функции по алгоритму MD5 50
2.2.1. Использование хэш-функции для контроля целостности данных 50
2.2.2. Создание файла с хэш-функцией, на основе данных произвольной длины 50
2.2.3. Проверка целостности данных программой MD5summer 52
2.2.4. Сбой проверки целостности данных 53
2.3. Практическая работа с пакетом PGP 54
2.3.1. Шифрование данных симметричным ключом. Алгоритм IDEA 55

2.3.2. Создание пары ключей для осуществления метода асимметричного шифрования 56
2.3.3. Создание зашифрованного сообщения с помощью открытого ключа 59
2.3.4. Декодирование принятого зашифрованного сообщения с помощью private-ключа 60
2.3.5. Кодирование и декодирование сообщения с помощью произвольного ключа 61
2.3.6. Аутентификация сообщения. Создание простой цифровой подписи в пакете PGP 62
2.3.7. Создание цифровой подписи и сообщения единым файлом 63
2.3.8. Создание цифровой подписи отдельным файлом 63
2.3.9. Верификация цифровой подписи 64
2.3.10. Сбой верификации цифровой подписи 64
Список использованных источников 66

Введение

При подготовке инженеров-программистов учебным планом предусмотрено изучение курса «Безопасность информации и обеспечение надёжности компьютерных систем». Для успешного изучения этого курса следует обратить внимание на несколько существенных аспектов знаний обучаемых: социологический, гуманитарный, юридический и правовой. Для понимания и овладения этим предметом недостаточно только технических знаний, поскольку в проблемах безопасности информации и в различных её нарушениях в малой степени повинна аппаратура, но в значительно большей степени люди, персонал, их взаимоотношения, их отношение к аппаратуре, оборудованию, к материальным и информационным ценностям.

Если в обработке информации участвует только аппаратура, как правило, никаких коллизий с ней не происходит, только в случае сбоя в аппаратуре кое-какие биты могут потеряться или перепутаться. Для этого случая существуют различные методы контроля, например, дополнительные разряды для контроля чётности. Другой причиной для беспокойства могут являться шумы, попавшие в информационный поток. Однако с шумами также можно бороться, следуя каноническим предписаниям классика теории информации К. Шеннона:

- увеличить мощность передатчика;
- уменьшить скорость передачи информации;
- изменить метод модуляции;
- применить помехоустойчивое кодирование информации.

Перечисленные проблемы лежат в плоскости синтаксической и семантической адекватности информации.

В этой работе будет рассматриваться несколько другой круг проблем: преобразование и обработка информации в информационных системах.

В классическом определении «информационная система» рассматривается как комплекс двух компонентов: аппаратуры, осуществляющей обработку информации, и персонала. Вот почему в курсе «Безопасность информации и обеспечение надёжности компьютерных систем» наряду с техническими аспектами рассматриваются нормативно-правовые аспекты, законодательные, международные стандарты, поскольку аппаратуру всегда обслуживает персонал, постольку всегда будут присутствовать риски «сбоя» персонала и «человеческий» фактор.

И проблемы из синтаксической адекватности информации переходят в плоскость прагматической адекватности, то есть в случае «сбоя» мы оцениваем ущерб не в байтах и битах, а пытаемся оценить его в денежном, материальном эквиваленте.

Под информационной безопасностью обычно понимают защищённость информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений: владельцам информации, пользователям информации и оборудованию. Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. Поэтому трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «пусть лучше все сломается, чем враг узнает хоть один секретный бит», во втором – «да нет у нас никаких секретов, лишь бы учебный процесс не останавливался».

Важность курса «Безопасность информации и обеспечение надёжности компьютерных систем» объясняется двумя основными причинами: ценностью

накопленных информационных ресурсов и критической зависимостью от информационных технологий. Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – всё это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей. Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учёта активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать, нести убытки, получить моральный ущерб не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих организаций защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте, например, в вузах, в электронных средствах массовой информации.

Правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений.

Принято выделять основные составляющие информационной безопасности (ИБ) – это обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов:

- **доступность** – возможность за приемлемое время получить требуемую информационную услугу;
- **целостность** – актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения;
- **конфиденциальность** – защита от несанкционированного доступа к информации.

Превалирующая роль доступности проявляется в системах управления производством, транспортом. Весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей: продажа железнодорожных и авиабилетов, банковские услуги; web-сайты организаций, резервирование мест в гостиницах.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – всё это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Средства контроля целостности применяются при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Неприятно и искажение официальной информации, если это текст закона или страница Web-сервера государственной структуры.

Конфиденциальность – самый понятный аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьёзные

трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Для всех субъектов информационных отношений, реально использующих ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искажённые сведения? Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

Полную защиту информации осуществить невозможно, всегда останутся неучтённые бреши, непредвиденные факторы и обстоятельства. Возможно лишь стремиться к такому идеалу. К тому же полная защита информационной системы масштаба предприятия требует огромных капиталовложений, поэтому идут на компромиссы в зависимости от решаемых задач. Если стоимость информационных ценностей невелика, то создание дорогой системы защиты – обременительная роскошь. Если же речь идёт о защите важных информационных объектов, то и вложение средств здесь оправдано. Система защиты информации эффективна, если задействованы и участвуют все компоненты информационной безопасности:

- **законодательный** (стандарты, нормативно-правовые документы);
- **административный**;
- **процедурный**;
- **программно-технический**.

Проблема ИБ – не только техническая; без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить её невозможно. Комплексность также усложняет проблематику ИБ, требуется взаимодействие специалистов из разных областей.

1. Теоретическая часть

1.1. Законодательный уровень

Основным для обеспечения информационной безопасности является законодательный уровень. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается или наказывается обществом, потому, что так поступать не принято. На этом уровне выделяют две группы мер:

- создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности; разрушение романтического ореола существующего вокруг слова «хакер» и осознание, что хакер – это преступник, с которым Вы также можете столкнуться;
- повышение общей культуры и образованности общества в области информационной безопасности, помогающее в разработке и распространении средств обеспечения информационной безопасности.

На законодательном уровне должен работать механизм, согласующий процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но разрыв между ними и практикой не должен быть значительным, иначе этот законодательный «вакуум» будет заполнен криминалом.

В Республике Беларусь существуют законодательные акты регламентирующие вопросы информации, информатизации и защиты информации. Это прежде всего:

- ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З;
- ПОСТАНОВЛЕНИЕ СОВЕТА МИНИСТРОВ РЕСПУБЛИКИ БЕЛАРУСЬ «О некоторых вопросах защиты информации» от 26 мая 2009 г. № 675;
- УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ «О мерах по совершенствованию использования национального сегмента сети Интернет» от 1 февраля 2010 г. № 60.

Эти законодательные акты можно найти по ссылке: http://www.pravo.by/.

1.2. Нормативные документы и стандарты

Особое место в этом вопросе принадлежит стандартам и нормативным техническим документам. Эти документы рассматривают проблемы информационной безопасности с очень близких позиций под несколько разным ракурсом. Это оценочные стандарты, классифицирующие информационные системы и средства защиты по требованиям безопасности, и технические спецификации, предписывающие различные пути реализации средств защиты.

1.2.1. Оценочный стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем»

Исторически первым оценочным стандартом, получившим широкое распространение во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем», называемый по цвету обложки «Оранжевой книгой», впервые опубликованный в августе 1983 года. Этот документ описывает не безопасные, а доверенные системы, то есть системы, которым можно оказать определенную степень доверия.

«Оранжевая книга» определяет понятие безопасной системы, которая «управляет с помощью соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять инфор-

мацию». Поскольку безопасных систем не существует, оценивается лишь степень доверия, которую можно оказать той или иной системе.

Доверенная система. В «Оранжевой книге» доверенная система определяется как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

Степень доверия оценивается по **активному аспекту защиты** – политике безопасности и **пассивному аспекту защиты** – уровню гарантированности. Политика безопасности – правила и нормы поведения, определяющие, как организация обрабатывает и защищает информацию. Чем выше степень доверия системе, тем строже и многообразнее политика безопасности. Политика безопасности – это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации информационной системы. Доверие безопасности основано на анализе результатов тестирования и проверки общего замысла и реализации системы. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это – пассивный аспект защиты.

Механизмы безопасности. Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Классы безопасности. «Критерии» Министерства обороны США допускают ранжирование информационных систем по степени доверия безопасности. Определяется четыре уровня доверия – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жёсткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности – C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, её политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям.

Для своего времени публикация «Оранжевой книги» стала эпохальным событием в области безопасности информации. Появился общепризнанный понятийный базис, без которого обсуждение проблем информационной безопасности было бы затруднительным. Конечно, на момент публикации (1983 год) компьютерные сети были ещё в зачаточном состоянии и, поэтому, в «Оранжевой книге» вопросы безопасности распределённых систем не рассматриваются.

1.2.2. Информационная безопасность распределённых систем. Рекомендации Международного союза телекоммуникаций (ITU) X.800

Документ X.800 является технической спецификацией, предписывающей различные способы реализации информационной безопасности и защиты компьютерных сетей. Документ описывает следующие сетевые функции безопасности, сервисы безопасности:

аутентификация – проверка подлинности партнёров по общению;

управление доступом – обеспечение защиты от несанкционированного использования ресурсов, доступных по сети;

- конфиденциальность данных – обеспечение защиты от несанкционированного получения информации;
- целостность данных – защита данных от несанкционированного изменения;
- неотказуемость – подтверждение подлинности данных и невозможность отказа от совершённых действий.

Документ X.800 широко использует стандарт семиуровневой модели открытых систем OSI, на которых реализуются перечисленные выше сервисы безопасности. Поддержку всех сервисов можно реализовать на уровне приложений.

1.2.3. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»

«Критерии оценки безопасности информационных технологий» (изданы в 1999 году) является оценочным стандартом. Этот международный стандарт – итог многолетней работы специалистов нескольких стран, он охватывает документы национального и межнационального масштаба. По историческим причинам данный стандарт часто называют «Общими критериями».

«Общие критерии» (ОК) на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от «Оранжевой книги», ОК не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

Как и «Оранжевая книга», «Общие критерии» содержат два основных вида требований безопасности:

- функциональные, соответствующие **активному аспекту защиты**, предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия, соответствующие **пассивному аспекту защиты**, предъявляемые к технологии, процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки – аппаратно-программного продукта или информационной системы. Безопасность в «Общих критериях» рассматривается в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте **среды безопасности**, которая характеризуется определенными условиями и угрозами (рис.1).

Собственник определяет множество **информационных ценностей**, которые должны быть защищены от различного рода атак. Атаки осуществляются противниками или оппонентами, использующими различные уязвимости в защищаемых ценностях. Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря конфиденциальности), их неавторизованная модификация (потеря целостности) или неавторизованная потеря доступа к этим ценностям (потеря доступности).

Собственники информационных ценностей анализируют уязвимости защищаемых ресурсов и возможные атаки, которые могут иметь место в конкретном окружении. В результате такого анализа определяются риски для данного набора информационных ценностей. Этот анализ определяет выбор контрмер, который задается политикой безопасности и обеспечивается с помощью механизмов и сервисов безопасности. Следует учитывать, что отдельные

уязвимости могут сохраниться и после применения механизмов и сервисов безопасности. Политика безопасности определяет согласованную совокупность механизмов и сервисов безопасности, адекватную защищаемым ценностям и окружению, в котором они используются.

В «Общих критериях» используются следующие определения.

Уязвимость – слабое место в системе, с использованием которого может быть осуществлена атака.

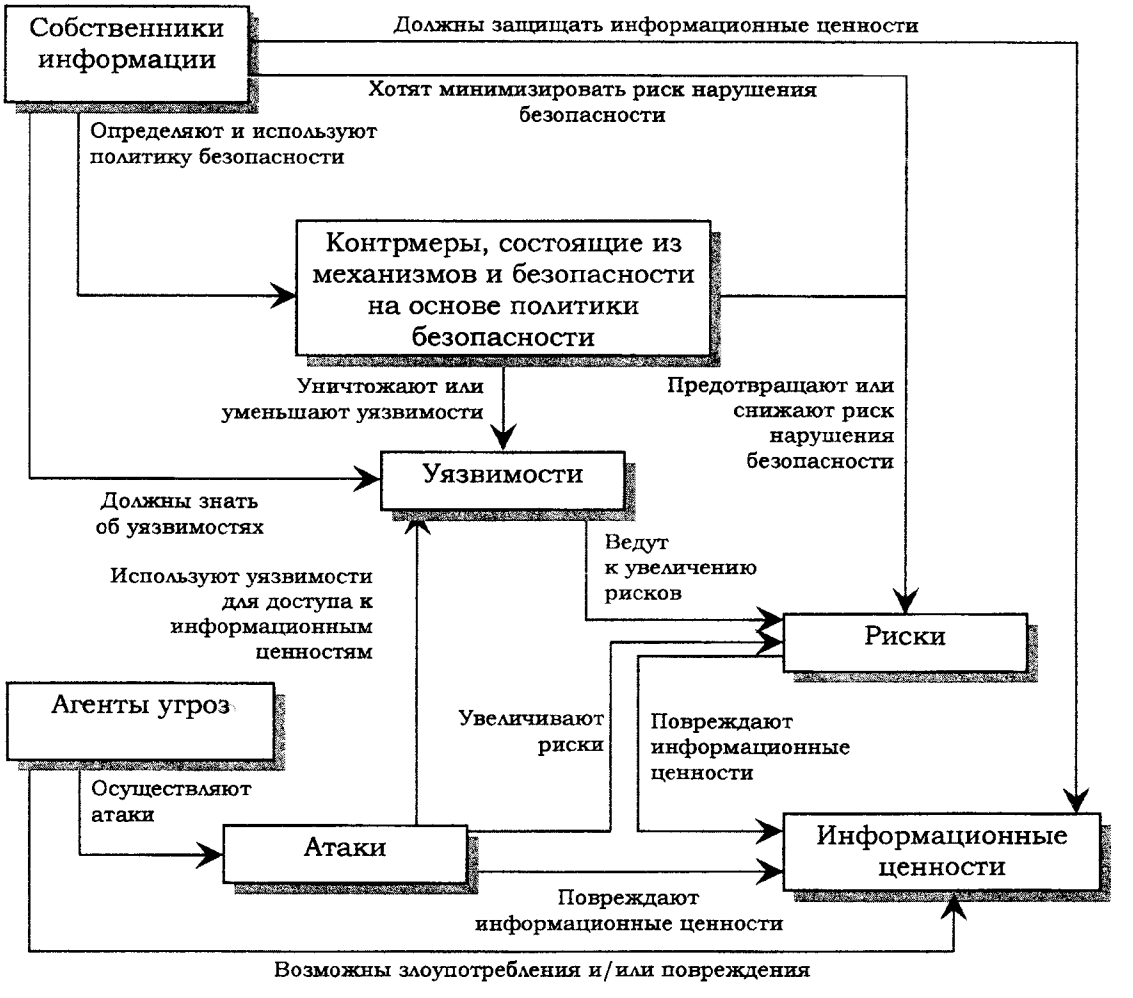


Рис. 1. Связи концепций безопасности по стандарту ISO/IEC 15408

Риск – вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости. В конечном счете, каждая организация должна принять решение о допустимом для нее уровне риска. Это решение должно найти отражение в политике безопасности, принятой в организации.

Политика безопасности – правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления сервисов безопасности.

Атака – любое действие, нарушающее безопасность информационной системы. Более формально можно сказать, что атака – это действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности.

Механизм безопасности – программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.

Сервис безопасности – сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление атаки. Сервис использует один или более механизмов безопасности.

1.3. Административный уровень

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации. Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы.

1.3.1. Политика безопасности

Политика безопасности – это совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации. С практической точки зрения политика безопасности рассматривается на трёх уровнях. К **верхнему уровню** относятся решения, затрагивающие организацию в целом. Они носят общий характер и исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать комплексную программу обеспечения информационной безопасности, назначение ответственных за её осуществление;
- формулировка целей организации в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по вопросам реализации программы безопасности.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности. Политика

верхнего уровня должна чётко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике определяются обязанности должностных лиц по выработке программы безопасности и претворению её в жизнь. Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определённую степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

На верхний уровень следует выносить минимум вопросов. Это целесообразно в случае экономии средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп, отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К **среднему уровню** можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов – отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы.

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, поль-

зующихся портативными и домашними компьютерами и вынужденных переносить информацию на компьютеры своих рабочих мест?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности, в разных организациях может сильно отличаться.

Роли и обязанности. В «политический» документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности **нижнего уровня** относится к конкретным информационным сервисам. Она включает в себя два аспекта – цели и правила их достижения, поэтому её порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- Кто имеет право доступа к объектам, поддерживаемым сервисом?
- При каких условиях можно читать и модифицировать данные?
- Как организован удалённый доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Её цели должны быть более конкретными. Например, если речь идёт о системе расчёта заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

1.3.2. Программа безопасности

После того, как сформулирована политика безопасности, можно приступать к составлению программы её реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, её нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней – верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. Главные цели программы следующие:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, поэтому необходимо иметь чёткую политику контроля и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать меры защиты с учётом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определённое место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определённый штат и бюджет.

Цель программы нижнего уровня – обеспечить надёжную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест. Обычно за программу нижнего уровня отвечают администраторы сервисов.

1.3.3. Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы.

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- Какого рода информация предназначается для обслуживания новым сервисом?
- Каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- Каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- Есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?
- Каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?
- Каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки – один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоёмким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей. После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации – самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные

изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось, на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

1.4. Процедурный уровень. Основные классы мер процедурного уровня

На процедурном уровне рассматриваются меры безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания.

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

1.4.1. Управление персоналом

Управление персоналом начинается с приёма нового сотрудника на работу и даже раньше – с составления должностной инструкции. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить од-

ному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоём, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить её критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять её. В то же время, неразумно и совсем отказываться от предварительной проверки.

Когда кандидат определён, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до создания его учётной записи в системе с входным именем, паролем и привилегиями.

С момента заведения учётной записи начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности. Всё это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация учётной записи пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно. Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное «хозяйство» и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту. В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения «внешние» сотрудники будут администрировать «местных», а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнёров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удалённом режиме. Вообще говоря, это создаёт в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удалённого доступа или обучением собственных сотрудников.

Проблема обучения – одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Не зная мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

1.4.2. Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных. Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как «непрерывность защиты в пространстве и времени».

Мы кратко рассмотрим следующие направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может всё здание организации, а также отдельные помещения. Нужно сделать так, чтобы посетители, по возможности, не имели непосредственного доступа к компьютерам или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят «без опознавательных знаков», злоумышленнику достаточно снять карточку, чтобы его считали «своим». Очевидно, соответствующие карточки нужно выдавать всем.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального средства целесообразно провести анализ рисков.

Необходимо установка противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, что защитные меры могут создавать новые слабые места. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам нарушает рабочий режим, то ввиду повышенной пожароопасности подобная мера защиты может только навредить.

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но могут нанести огромный ущерб. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок. Необходимо повсеместно использовать криптографию, стараться максимально расширить контролируемую территорию, разместившись поодаль, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероят-

но, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. Необходимо шифровать данные на жёстких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией, характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий. В то же время, во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но все же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

1.4.3. Поддержание работоспособности

Существует ряд рутинных мероприятий, направленных на поддержание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе – ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Поддержка пользователей подразумевает, прежде всего, консультирование и оказание помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный «справочный стол», но чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

Поддержка программного обеспечения – одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что «самодеятельность» пользователей постепенно приведёт к хаосу на их компьютерах, а исправлять ситуацию придётся системному администратору.

Второй аспект поддержки программного обеспечения – контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум, сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами. Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь, таким образом, от крупных аварий и аналогичных инцидентов.

Документирование – неотъемлемая часть информационной безопасности. В виде документов оформляется почти всё – от политики безопасности до журнала учёта носителей. К хранению одних документов применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий – требования целостности и доступности.

Регламентные работы – очень серьёзная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно контролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

1.4.4. Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки, который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить, и что делать до приезда пожарной команды.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, на наш взгляд, в первую очередь следует заботиться о минимизации ущерба.

Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие

пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

1.4.5. Планирование восстановительных работ

Ни одна организация не застрахована от серьёзных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время, у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объёме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчёт в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет своё лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

- персонал;
- информационная инфраструктура;
- физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдёт с критичными ресурсами? Например,

смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение. Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий – те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах). Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или заключать соглашения с несколькими поставщиками.

1.5. Программно-технический уровень

1.5.1. Основные понятия программно-технического уровня информационной безопасности

Программно-технические меры, то есть меры, направленные на контроль оборудования, программ и данных, образуют последний и один из самых важных рубежей информационной безопасности. Как показывает статистика, ущерб наносят, в основном, действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные «враги» – некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

С одной стороны, быстрое развитие информационных технологий предоставляет обороняющимся новые возможности, но с другой стороны затрудняет обеспечение надёжной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет взламывать, ранее казавшиеся неприступными барьеры;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых информационных сервисов ведёт и к образованию новых уязвимых мест;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надёжных, апробированных конфигураций.

Для программно-технического уровня основным является понятие сервиса безопасности, в который входят:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

1.5.2. Особенности современных информационных систем, существенные с точки зрения безопасности

Информационная система современной организации является весьма сложным образованием, которое пользуется многочисленными внешними сервисами и, в свою очередь, предоставляет собственные сервисы вовне.

Следует учитывать еще, по крайней мере, два момента. Во-первых, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются посвоему. Целостность с точки зрения системы управления базами данных и с точки зрения почтового сервера – вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует анализировать защищенность сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному.

Во-вторых, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников.

В силу изложенных причин далее будут рассматриваться распределённые, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

1.5.3. Архитектурная безопасность

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;

- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.

Кратко смысл перечисленных принципов заключается в следующем.

Если **непрерывность** нарушена, тогда у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает.

Следование **признанным стандартам** и использование апробированных решений повышает надежность ИС и уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет неуправляемой и, следовательно, обеспечить ее безопасность будет невозможно.

Надёжность любой обороны определяется самым **слабым звеном**. Злоумышленник не будет бороться против силы, он предпочтёт легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности **перехода в небезопасное состояние** означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

Применительно к программно-техническому уровню принцип **минимизации привилегий** предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Этот принцип позволяет уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип **разделения обязанностей** предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. В частности, соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип **эшелонированности обороны** предписывает не полагаться на один защитный рубеж, каким бы надёжным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, – протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а благодаря наличию такого рубежа, как протоколирование и аудит, его действия не останутся незамеченными.

Принцип **разнообразия защитных** средств предполагает создание различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками.

Очень важен **принцип простоты и управляемости** информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование.

1.6. Основные понятия криптографии

1.6.1. Основные понятия

Здесь мы обсудим принципы, на которых основаны современные методы традиционного шифрования. Рассмотрим общую схему симметричной, или традиционной, криптографии (рис. 2).

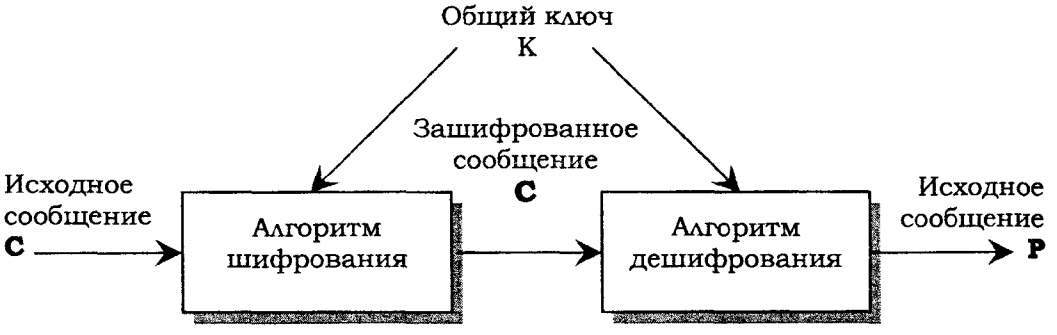


Рис. 2. Общая схема симметричного шифрования

В процессе шифрования используется определённый алгоритм шифрования, по которому обрабатываются входные незашифрованные данные. Математический алгоритм обычно является открытым и описание его доступно в открытой печати, например, в математических журналах. Однако, в процессе шифрования используется ключ – вот он-то является закрытым и им владеют только отправитель и получатель. Результатом работы алгоритма является зашифрованное сообщение. Ключ является значением, не зависящим от шифруемого сообщения. Изменение ключа должно приводить к изменению зашифрованного сообщения.

Зашифрованное сообщение передается получателю. Получатель преобразует зашифрованное сообщение в исходное незашифрованное сообщение с помощью алгоритма дешифрования и того же самого ключа, который использовался при шифровании, или ключа, легко получаемого из ключа шифрования.

Незашифрованное сообщение будем обозначать **P** или **M** (от слов plaintext и message). Зашифрованное сообщение будем обозначать **C** (от слова ciphertext).

Безопасность, обеспечиваемая традиционной криптографией, зависит от нескольких факторов. Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Описание стойкости алгоритма шифрования при статистическом анализе потока зашифрованных сообщений использует понятия диффузии и конфузии, введенные Клодом Шенноном.

Суть диффузии заключается в рассеянии статистических особенностей незашифрованного текста в широком диапазоне статистических характеристик зашифрованного текста. Это достигается тем, что значение каждого элемента незашифрованного текста влияет на значения многих элементов зашифрованного текста или, что то же самое, любой элемент зашифрованного текста зависит от многих элементов незашифрованного текста.

Конфузия усложняет статистическую взаимосвязь между зашифрованным текстом и ключом с целью противостояния попыткам определить ключ. Это достигается использованием сложных подстановочных алгоритмов – простые линейные подстановочные функции увеличивают беспорядок лишь в незначительной степени.

Если X – это исходное сообщение и K – криптографический ключ, то зашифрованный передаваемый текст Y можно записать в виде

$$Y = E_K(X), \tag{1}$$

где E – функция, осуществляющая алгоритм шифрования.

Получатель, используя тот же ключ, расшифровывает сообщение

$$X = D_K(Y), \tag{2}$$

где D – функция, осуществляющая алгоритм дешифрования.

Противник, не имея доступа к K и X, пытается узнать X, K.

Алгоритмы симметричного шифрования различаются способом, которым обрабатывается исходный текст. Возможно шифрование блоками или шифрование потоком. Поточными называются шифры, в которых поток цифровых данных шифруется последовательно бит за битом. Блочными называются шифры, в которых логической единицей шифрования является некоторый блок открытого текста, после преобразований которого получается блок шифрованного текста такой же длины.

Блочные шифры изучены гораздо лучше. Считается, что они обладают более широкой областью применения, чем поточные. Блок текста рассматривается как неотрицательное целое число. Длина блока всегда выбирается равной степени двойки. Обычно используют блоки размером 64 бита. В большинстве блочных алгоритмов симметричного шифрования используются следующие типы операций:

- табличная подстановка, при которой группа битов отображается в другую группу битов. Это, так называемые, S-box;
- перемещение, с помощью которого биты сообщения переупорядочиваются;
- операция сложения по модулю 2, обозначаемая XOR или $\oplus$;
- операция сложения по модулю 2^{32} или по модулю 2^{16};
- циклический сдвиг на некоторое число битов.

Эти операции циклически повторяются в алгоритме, образуя так называемые раунды. Входом каждого раунда является выход предыдущего раунда и ключ, который получен по определенному алгоритму из ключа шифрования K. Ключ раунда называется подключом.

1.6.2. Криптоанализ

Процесс воссоздания значений X, K из Y (1, 2), называется криптоанализом. Используемая стратегия зависит от схемы шифрования. Одной из возможных атак на алгоритм шифрования является лобовая атака, то есть простой перебор всех возможных ключей. Если множество ключей достаточно большое, то подобрать ключ маловероятно. При длине ключа n бит количество возможных

ключей равно 2^n. Таким образом, чем длиннее ключ, тем более стойким считается алгоритм для лобовой атаки.

Существуют различные типы атак, основанные на том, что противнику известно определенное количество пар «незашифрованное сообщение – зашифрованное сообщение». При анализе зашифрованного текста противник часто применяет статистические методы анализа текста. При этом он может иметь общее представление о типе текста, например, английский или русский текст, исполняемый файл, исходный текст на языке программирования. Во многих случаях криптоаналитик имеет достаточно много информации об исходном тексте. Криптоаналитик может иметь возможность перехвата одного или нескольких незашифрованных сообщений вместе с их зашифрованным видом. Или криптоаналитик может знать основной формат или основные характеристики сообщения. Говорят, что криптографическая схема абсолютно стойкая, если зашифрованное сообщение не содержит информации достаточной для однозначного восстановления соответствующего открытого текста, какой бы большой по объёму шифрованный текст не имелся у противника. К сожалению, среди алгоритмов шифрования нет абсолютно стойких. И поэтому говорят, что криптографическая схема **вычислительно безопасна**, если:

- стоимость взлома шифра превышает стоимость расшифрованной информации;
- время, которое требуется для того чтобы взломать шифр, превышает время, в течение которого информация актуальна.

1.6.3. Алгоритмы традиционного симметричного шифрования

Рассмотрим несколько наиболее известных и популярных алгоритмов симметричного шифрования. Требования, предъявляемые к алгоритмам симметричного шифрования, обычно сводятся к следующим:

- иметь размер блока 64 или 128 бит;
- иметь масштабируемый ключ до 256 бит;
- использовать простые операции, эффективные на микропроцессорах, то есть, сложение, сложение по модулю 2, табличные подстановки, умножение по модулю;
- алгоритм должен работать на 8-битном процессоре с минимальными требованиями к памяти;
- алгоритм должен использовать заранее вычисленные подключи; всегда должна быть возможность шифрования данных без каких-либо предварительных вычислений;
- алгоритм должен состоять из переменного числа итераций;
- алгоритм не должен иметь слабых ключей, если это невозможно, то количество слабых ключей должно быть минимальным;
- алгоритм должен использовать простую для понимания структуру, это уменьшает закрытость алгоритма.

При построении большинства алгоритмов симметричного шифрования используются блочные алгоритмы, основанные на использовании сети Файстеля. Они удовлетворяют всем требованиям к алгоритмам симметричного шифрования, а с другой стороны, достаточно просты и компактны.

Одним из самых распространённых и наиболее известных алгоритмов симметричного шифрования является DES (Data Encryption Standard – стандарт шифрования данных). Алгоритм был разработан в 1977 году, в 1980 году был принят NIST (National Institute of Standards and Technolody США) в качестве стандарта.

DES является классической сетью Файстеля с двумя ветвями. Данные шифруются 64-битными блоками, используя 56-битный ключ. Алгоритм преобразует

за несколько раундов 64-битный вход в 64-битный выход. Длина ключа равна 56 битам.

При такой длине ключа существует 256 возможных комбинаций. На сегодня такая длина ключа недостаточна, поскольку допускает успешное применение лобовых атак. Альтернативой DES можно считать тройной DES, IDEA, а также алгоритм Rijndael, принятый в качестве нового стандарта на алгоритмы симметричного шифрования.

Ещё одним интересным алгоритмов симметричного шифрования является IDEA (International Data Encryption Algorithm). Это блочный симметричный алгоритм шифрования, разработанный в швейцарском федеральном институте технологий в 1990 году.

IDEA является одним из нескольких симметричных криптографических алгоритмов, которыми первоначально предполагалось заменить DES. IDEA является блочным алгоритмом, который использует 128-битовый ключ для шифрования данных блоками по 64 бита. Целью разработки IDEA было создание относительно стойкого криптографического алгоритма с достаточно простой реализацией.

Алгоритм Blowfish является сетью Файстеля, у которой количество итераций равно 16. Длина блока равна 64 битам, ключ может иметь любую длину в пределах 448 бит. Перед началом шифрования выполняется сложная фаза инициализации, но само шифрование данных выполняется достаточно быстро.

Алгоритм предназначен в основном для приложений, в которых ключ меняется нечасто, во время фазы инициализации происходит аутентификация сторон и согласование общих параметров и секретов. Классическим примером подобных приложений является сетевое взаимодействие. При реализации на 32-битных микропроцессорах с большим кэшем данных Blowfish значительно быстрее DES.

Алгоритм ГОСТ 28147 является российским стандартом для алгоритмов симметричного шифрования. ГОСТ 28147 разработан в 1989 году, является блочным алгоритмом шифрования, длина блока равна 64 битам, длина ключа равна 256 битам, количество раундов равно 32. Алгоритм представляет собой классическую сеть Файстеля.

В рамках американского института стандартов (NIST) была сделана попытка разработать продвинутый стандарт шифрования (Advanced Encryption Standard – AES). Основная цель состояла в создании федерального стандарта, который бы описывал алгоритм шифрования, используемый для защиты информации как в государственном, так и в частном секторе.

В 1998 году NIST объявил несколько кандидатов на алгоритм AES. Эти алгоритмы были разработаны промышленными и академическими кругами двенадцати стран. В 1999 году были представлены выбранные NIST пять финалистов. Ими стали MARS, RC6, Rijndael, Serpent и Twofish.

1.6.4. Шифрование с открытым ключом. Основные требования к алгоритмам асимметричного шифрования

Создание алгоритмов асимметричного шифрования является величайшим достижением в истории криптографии. Алгоритмы шифрования с открытым ключом разрабатывались для того, чтобы решить две наиболее трудные задачи, возникшие при использовании симметричного шифрования.

Первой задачей является распределение ключа. При симметричном шифровании требуется, чтобы обе стороны уже имели общий ключ, который каким-то образом должен быть им заранее передан. Диффи, один из основоположников шифрования с открытым ключом, заметил, что это требование отрицает

всю суть криптографии, а именно – возможность поддерживать всеобщую секретность при коммуникациях.

Второй задачей является необходимость создания таких механизмов, при использовании которых невозможно было бы подменить кого-либо из участников, то есть нужна цифровая подпись. При использовании коммуникаций для решения широкого круга задач, например в коммерческих и частных целях, электронные сообщения и документы должны иметь эквивалент подписи, содержащейся в бумажных документах. Необходимо создать метод, при использовании которого все участники будут убеждены, что электронное сообщение было послано конкретным участником. Это более сильное требование, чем аутентификация.

Диффи и Хеллман предложили способ решения обеих задач, который радикально отличается от всех предыдущих подходов к шифрованию. Рассмотрим общие черты алгоритмов шифрования с открытым ключом и требования к этим алгоритмам. Определим требования, которым должен соответствовать алгоритм, использующий один ключ для шифрования, другой ключ – для дешифрования.

В некоторых алгоритмах асимметричного шифрования, например RSA, имеется интересная особенность: каждый из двух ключей может использоваться как для шифрования, так и для дешифрования.

При описании симметричного шифрования и шифрования с открытым ключом будем использовать следующую терминологию. Ключ, используемый в симметричном шифровании, будем называть секретным ключом. Два ключа, используемые при шифровании с открытым ключом, будем называть открытым ключом и закрытым ключом. Закрытый ключ держится в секрете, но называть его будем закрытым ключом, а не секретным, чтобы избежать путаницы с ключом, используемым в симметричном шифровании. Закрытый ключ пользователя *A* будем обозначать KR_a, открытый ключ – KU_a.

Предполагается, что все участники имеют доступ к открытым ключам друг друга, а закрытые ключи создаются локально каждым участником и распределяться не должны.

В любое время участник может изменить свой закрытый ключ и опубликовать составляющий пару открытый ключ, заменив им старый открытый ключ.

Диффи и Хеллман описывают требования, которым должен удовлетворять алгоритм шифрования с открытым ключом:

1) для стороны *B* процесс генерирования пары ключей (открытый ключ KU_b, закрытый ключ KR_b) не должен вызывать вычислительных трудностей;

2) для отправителя *A* вычислительно легко, имея открытый ключ получателя *B* (KU_b) и незашифрованное сообщение *M*, создать для *B* соответствующее зашифрованное сообщение:

$$C = E_{KU_b}(M); \tag{3}$$

3) для получателя *B* не должно вызывать вычислительных трудностей дешифрование сообщения, если использовать свой закрытый ключ KU_b:

$$M = D_{KR_b}(C) = D_{KR_b}(E_{KU_b}(M)); \tag{4}$$

4) для противника должно быть вычислительно невозможно восстановить личный ключ KR_b из имеющегося открытого ключа KU_b:

$$KR_b = F(KU_b), \tag{5}$$

функция F не вычисляется;

5) для противника должно быть вычислительно невозможно восстановить оригинальное сообщение M, зная открытый ключ KU_b и зашифрованное сообщение C:

$$M = F_{KUb}(C), \tag{6}$$

функция F_{KUb} не вычисляется.

Можно добавить ещё одно требование, выполняющееся не для всех алгоритмов с открытым ключом;

6) шифрующие и дешифрующие функции могут применяться в любом порядке:

$$M = E_{KUb}(D_{KRb}(M)). \tag{7}$$

Перечисленные требования достаточно сложны для выполнения, что подтверждается тем, что за несколько десятилетий, прошедших со времени открытия метода криптографии с открытым ключом, только один такой алгоритм получил широкое признание. Эти требования сводятся к необходимости нахождения односторонней функции с секретом. Односторонней функцией называется такая функция, у которой каждый аргумент имеет единственное обратное значение, при этом вычислить саму функцию легко, а вычислить обратную функцию трудно:

$Y = f(X)$ – легко,

$X = f^{-1}(Y)$ – трудно,

или другими словами – равенство (3) вычисляется легко, а обратное равенство

$$M = E^{-1}{}_{KU}(C) \tag{8}$$

вычисляется трудно.

Термин «вычислительно легко» означает, что проблема может быть решена за полиномиальное (линейное) время от длины вводимого значения. Так, если длина вводимого значения n бит, то время, требуемое для вычисления функции пропорционально n^a, где a – фиксированная константа. Термин «вычислительно трудно» означает более сложное понятие. В общем случае можно сказать, что функция является практически невычислимой, если усилия по её вычислению возрастают быстрее, чем n^a (полиномиального времени от величины входа). Например, если длина входа n битов, а время вычисления функции пропорционально 2^n, то такая функция считается практически невычислимой.

Вернёмся к определению односторонней функции с секретом, которую, подобно односторонней функции, легко вычислить в одном направлении и трудно вычислить в обратном направлении до тех пор, пока недоступна некоторая дополнительная информация. При наличии этой дополнительной информации инверсию можно вычислить за полиномиальное время. Таким образом, односторонняя функция с секретом принадлежит семейству односторонних функций f_k таких, что

$Y = f_k(X)$ – легко, если k и X известны;

$X = f_k^{-1}(Y)$ – легко, если k и Y известны;

$X = f_k^{-1}(Y)$ – трудно, если Y известно, но k неизвестно.

Видно, что разработка конкретного алгоритма с открытым ключом зависит от открытия соответствующей односторонней функции с секретом.

1.6.5. Основные способы использования алгоритмов с открытым ключом

Основными способами использования алгоритмов с открытым ключом являются шифрование/дешифрование, создание и проверка подписи и обмен ключа (рис. 3).

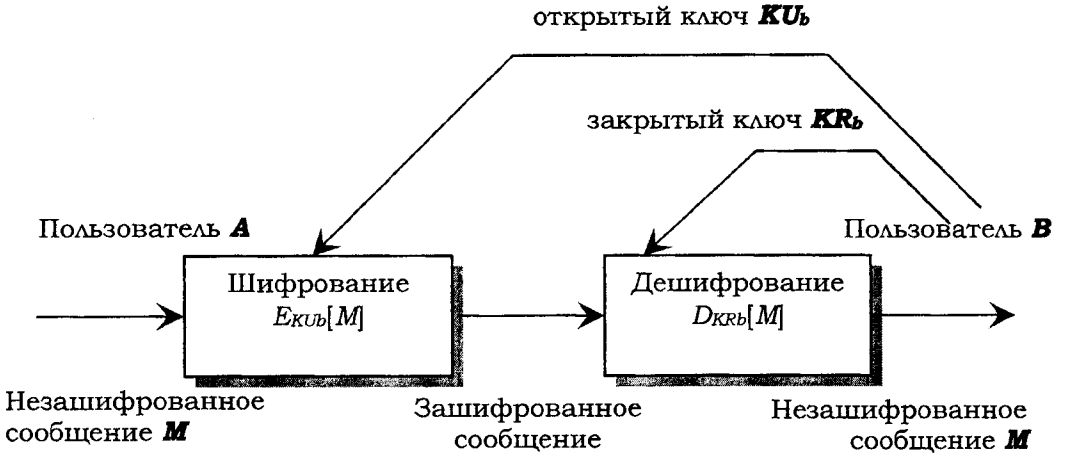


Рис. 3. Криптосистема с открытым ключом: защита

Шифрование с открытым ключом состоит из следующих шагов.

1. Пользователь *B* создает пару ключей KU_b и KR_b, используемых для шифрования и дешифрования передаваемых сообщений.

2. Пользователь *B* делает доступным некоторым надёжным способом свой ключ шифрования, то есть открытый ключ KU_b. Составляющий пару закрытый ключ KR_b держится в секрете.

3. Если *A* хочет послать сообщение *B*, он шифрует сообщение, используя открытый ключ *B* – KU_b .

4. Когда *B* получает сообщение, он дешифрует его, используя свой закрытый ключ KR_b. Никто другой не сможет дешифровать сообщение, так как этот закрытый ключ знает только *B*.

Если пользователь (конечная система) надежно хранит свой закрытый ключ, то никто не сможет подсмотреть передаваемые сообщения (рис. 4).

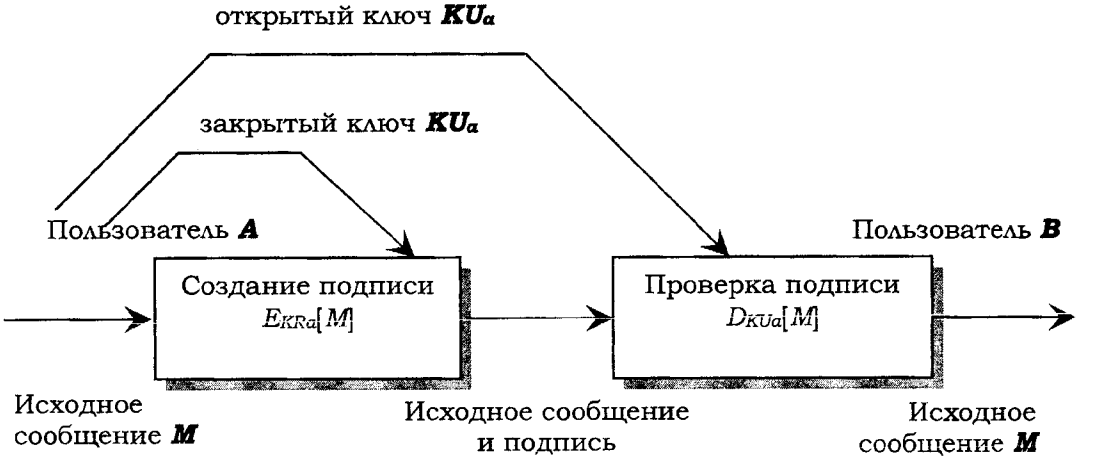


Рис. 4. Криптосистема с открытым ключом: аутентификация

Создание и проверка подписи состоит из следующих шагов.

1. Пользователь *A* создает пару ключей KR_a и KU_a, используемых для создания и проверки подписи передаваемых сообщений.

2. Пользователь *A* делает доступным некоторым надёжным способом свой ключ проверки, то есть открытый ключ KU_a. Составляющий пару закрытый ключ KR_a держится в секрете.

3. Если *A* хочет послать подписанное сообщение *B*, он создает подпись $E_{KRa}(M)$ для этого сообщения, используя свой закрытый ключ KR_a.

4. Когда *B* получает подписанное сообщение, он проверяет подпись $D_{KUa}(M)$, используя открытый ключ *A* – KU_a. Никто другой не может подписать сообщение, так как этот закрытый ключ знает только *A*.

До тех пор, пока пользователь или прикладная система надёжно хранит свой закрытый ключ, их подписи достоверны.

Кроме того, невозможно изменить сообщение, не имея доступа к закрытому ключу *A*, обеспечивая тем самым аутентификацию и целостность данных.

В этой схеме все сообщение подписывается, причем для подтверждения целостности сообщения требуется много памяти. Каждое сообщение должно храниться в незашифрованном виде для использования в практических целях. Кроме того, копия сообщения также должна храниться в зашифрованном виде, чтобы можно было проверить в случае необходимости подпись. Более эффективным способом является шифрование небольшого блока битов, который является функцией от сообщения. Такой блок, называемый аутентификатором, должен обладать свойством невозможности изменения сообщения без изменения аутентификатора. Если аутентификатор зашифрован закрытым ключом отправителя, он является цифровой подписью, с помощью которой можно проверить исходное сообщение. Далее эта технология будет рассматриваться в деталях.

Важно подчеркнуть, что описанный процесс создания подписи не обеспечивает конфиденциальность. Это означает, что сообщение, посланное таким способом, невозможно изменить, но можно подсмотреть. Это очевидно в том случае, если подпись основана на аутентификаторе, так как само сообщение передается в явном виде. Но даже если осуществляется шифрование всего сообщения, конфиденциальность не обеспечивается, так как любой может расшифровать сообщение, используя открытый ключ отправителя.

Обмен ключей: две стороны взаимодействуют для обмена ключом сессии, который в дальнейшем можно использовать в алгоритме симметричного шифрования.

Некоторые алгоритмы можно задействовать тремя способами, в то время как другие могут использоваться одним или двумя способами.

Перечислим наиболее популярные алгоритмы с открытым ключом и возможные способы их применения (табл.).

Таблица

Алгоритм	Шифрование/дешифрование	Цифровая подпись	Обмен ключей
RSA	Да, непригоден для больших блоков	Да	Да
DSS	Нет	Да	Нет
Диффи-Хеллман	Нет	Нет	Да

Алгоритм RSA. Диффи и Хеллман определили новый подход к шифрованию, что вызвало к жизни разработку алгоритмов шифрования, удовлетворяющих требованиям систем с открытым ключом. Одним из первых результатов был алгоритм, разработанный в 1977 году Роном Ривестом, Ади Шамиром и Леном

Адлеманом и опубликованный в 1978 году. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом.

Алгоритм основан на использовании того факта, что задача факторизации является трудной, т.е. легко перемножить два числа, в то время как не существует полиномиального алгоритма нахождения простых сомножителей большого числа.

Алгоритм RSA представляет собой блочный алгоритм шифрования, где зашифрованные и незашифрованные данные являются целыми между 0 и (n – 1) для некоторого n.

1.6.6. Аутентификация сообщений

Рассмотрим основные понятия, относящиеся к обеспечению целостности и аутентификации сообщений с помощью MAC-кода и хэш-функций. Аутентификация сообщений представляет собой процедуру проверки того, что полученное сообщение пришло от указанного источника и не было изменено в пути следования. Цифровая подпись является средством аутентификации и включает меры противодействия возможности оспорить источником или адресатом факт отправки и получения сообщения.

Функции, которые могут служить для создания аутентификатора, делятся на три типа:

- шифрованное сообщение, когда в качестве аутентификатора используется сам шифрованный текст всего сообщения;
- код аутентичности сообщения (Message Authentication Code – MAC), когда в качестве аутентификатора выступает значение фиксированной длины, создаваемое некоторой открытой функцией сообщения и секретным ключом;
- функция хэширования, когда в качестве аутентификатора используется значение фиксированной длины, создаваемое некоторой открытой функцией от сообщения произвольной длины.

Хэш-функции. Хэш-функцией называется односторонняя функция, предназначенная для получения сообщения или некоторого блока данных постоянной длины при обработке входного сообщения переменной длины.

Хэш-код создается функцией H:

$$h = H(M),$$

где M является сообщением произвольной длины и h является фиксированным значением функции (хэш-кодом).

Рассмотрим требования, которым должна соответствовать хэш-функция для того, чтобы она могла использоваться в качестве аутентификатора сообщения. Начнём с простого примера хэш-функции и проанализируем несколько подходов к построению хэш-функции.

Хэш-функция H, которая используется для аутентификации сообщений, должна обладать следующими свойствами:

1. Аргументом хэш-функции H может быть блок данных любой длины.
2. Значение, принимаемое хэш-функцией H, всегда фиксированной длины.
3. Значение функции $H(M)$ относительно легко (за полиномиальное время) вычисляется для любого аргумента M.
4. Для любого полученного значения хэш-кода h вычислительно невозможно найти X такое, чтобы $H(X) = h$. Такое свойство называется односторонностью.
5. Для любого данного X вычислительно невозможно найти $Y \neq X$, что $H(X) = H(Y)$.

6. Должно быть практически невозможно найти произвольную пару значений ($Y \neq X$) такую, что $H(X) = H(Y)$.

Первые три свойства требуют, чтобы хэш-функция создавала хэш-код для любого сообщения.

Четвертое свойство определяет требование односторонности хэш-функции: легко создать хэш-код по данному сообщению, но невозможно восстановить сообщение по данному хэш-коду. Это свойство важно, если аутентификация с использованием хэш-функции включает секретное значение. Само секретное значение может не посылаться, тем не менее, если хэш-функция не является односторонней, противник может легко раскрыть секретное значение следующим образом. При перехвате передачи атакующий получает сообщение M и хэш-код $C = H(S_{AB} \,||\, M)$. Если атакующий может инвертировать хэш-функцию, то, следовательно, он может получить $S_{AB} \,||\, M = H^{-1}(C)$. Так как атакующий теперь знает и M и $S_{AB} \,||\, M$, получить S_{AB} совсем просто.

Пятое свойство гарантирует, что невозможно найти другое сообщение, чьё значение хэш-функции совпадало бы со значением хэш-функции данного сообщения. Это предотвращает подделку аутентификатора при использовании зашифрованного хэш-кода.

Хэш-функция MD5. Одним из распространённых алгоритмов получения хэш-функции от сообщения произвольной длины является алгоритм MD5, разработанный Роном Ривестом.

Алгоритм, обрабатывая сообщение произвольной длины, создаёт фиксированную хэш-функцию длиной 128 бит.

Алгоритм MD5 разработан на основе более раннего алгоритма MD4 того же автора – Рона Ривеста. Первоначально данный алгоритм MD4 был опубликован в октябре 1990 года.

Хэш-функция SHA-1. На основе алгоритма MD4 в настоящее время национальным институтом стандартов и технологии (NIST) разработан ещё один алгоритм получения хэш-функции – безопасный хэш-алгоритм (Secure Hash Algorithm – SHA-1). Алгоритм SHA-1 может обработать сообщение максимальной длины 264 бит и создаёт хэш-функцию сообщения длиной 160 бит.

Алгоритм ГОСТ 3411 является российским стандартом для хэш-функций. Его структура довольно сильно отличается от структуры алгоритмов SHA-1,2 или MD5, в основе которых лежит алгоритм MD4. Длина хэш-кода, создаваемого российским алгоритмом ГОСТ 3411, равна 256 битам.

Коды аутентификации сообщений (MAC) и требования к ним. Напомним, что обеспечение целостности сообщения – это невозможность изменения сообщения так, чтобы получатель этого не обнаружил. Под аутентификацией понимается подтверждение того, что информация получена от законного источника, и получателем является тот, кто нужно. Один из способов обеспечения целостности – это вычисление MAC (Message Authentication Code). В данном случае под MAC понимается некоторый аутентификатор, являющийся определённым способом вычисленным блоком данных, с помощью которого можно проверить целостность сообщения. В некоторой степени симметричное шифрование всего сообщения может выполнять функцию аутентификации этого сообщения. Но в таком случае сообщение должно содержать достаточную избыточность, которая позволяла бы проверить, что сообщение не было изменено. Избыточность может быть в виде определённым образом отформатированного сообщения, текста на конкретном языке. Если сообщение допускает произвольную последовательность битов (например, зашифрован ключ сессии), то симметричное шифрование всего сообщения не может обеспечивать его целостность, так как при дешифровании в любом случае получится последовательность битов, правильность которой проверить нельзя. Поэтому гораздо чаще

используется криптографически созданный небольшой блок данных фиксированного размера – аутентификатор, так называемая криптографическая контрольная сумма, с помощью которого проверяется целостность сообщения. Этот блок данных и есть MAC. Он может создаваться с помощью секретного ключа, который используют отправитель и получатель. MAC вычисляется в тот момент, когда известно, что сообщение корректно. После этого MAC присоединяется к сообщению и передаётся вместе с ним получателю. Получатель вычисляет MAC, используя тот же самый секретный ключ, и сравнивает вычисленное значение с полученным. Если эти значения совпадают, то с большой долей вероятности можно считать, что при пересылке изменения сообщения не произошло:

$$MAC = C_K(M).$$

Хочется заметить, что MAC-код не обеспечивает цифровую подпись, так как и отправитель, и получатель используют один и тот же общий ключ.

1.6.7. Цифровые подписи и протоколы аутентификации

Требования к цифровой подписи. Аутентификация защищает двух участников, которые обмениваются сообщениями, от воздействия некоторой третьей стороны, но не обеспечивает защиту участников друг от друга, тогда как и между ними тоже могут возникать определённые формы споров.

Например, предположим, что адресат *A* посылает адресату *B* аутентифицированное сообщение, и аутентификация осуществляется на основе общего ключа. Рассмотрим возможные недоразумения, которые могут при этом возникнуть:

- адресат *B* может подделать сообщение и утверждать, что оно пришло от адресата *A*. Адресату *B* достаточно просто создать сообщение и присоединить аутентификационный код, используя совместный ключ, который имеется у адресата *A* и адресата *B*;
- адресат *A* может отрицать, что он посылал сообщение адресату *B*. Так как адресат *B* может подделать сообщение, у него нет способа доказать, что адресат *A* действительно посылал его.

В ситуации, когда обе стороны не доверяют друг другу, необходимо нечто большее, чем аутентификация. Возможным решением подобной проблемы является использование цифровой подписи. Цифровая подпись должна обладать следующими свойствами:

- должна быть возможность проверить автора, дату и время создания подписи;
- должна быть возможность установить достоверность содержимого сообщения (аутентифицировать) на время создания подписи;
- подпись должна быть проверяема третьей стороной в случае возникновения спора.

Таким образом, функция цифровой подписи включает, в частности, функцию аутентификации. На основании этих свойств можно сформулировать следующие требования к цифровой подписи.

1. Подпись должна быть двоичным кодом, который зависит от подписываемого сообщения.

2. Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки (фальсификации) или отказа (отрицания авторства).

3. Создавать цифровую подпись должно быть относительно легко.

4. Цифровую подпись должно быть относительно просто распознать и проверить.

5. Должно быть вычислительно невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием ложной цифровой подписи для некоторого сообщения.

6. Цифровые подписи должны быть компактны для удобного хранения в запоминающем устройстве.

Хэш-функции, описанные в разделе 6.1, и зашифрованные закрытым ключом отправителя, удовлетворяет перечисленным требованиям.

Существует несколько подходов к использованию функции цифровой подписи. Все они могут быть разделены на две категории: прямые и арбитражные.

Прямая и арбитражная цифровые подписи. При использовании **прямой** цифровой подписи взаимодействуют только сами участники, то есть отправитель и получатель. Предполагается, что получатель знает открытый ключ отправителя. Цифровая подпись может быть создана шифрованием всего сообщения или его хэш-кода закрытым ключом отправителя.

Конфиденциальность может быть обеспечена дальнейшим шифрованием всего сообщения вместе с подписью открытым ключом получателя (асимметричное шифрование) или совместным секретным ключом (симметричное шифрование). Заметим, что обычно функция подписи выполняется первой, и только после этого выполняется функция конфиденциальности. В случае возникновения спора некая третья сторона должна просмотреть сообщение и его подпись. Если функция подписи выполняется над зашифрованным сообщением, то для разрешения споров придется хранить сообщение как в незашифрованном виде (для практического использования), так и в зашифрованном (для проверки подписи). Если цифровая подпись выполняется над незашифрованным сообщением, получатель может хранить только сообщение в незашифрованном виде и соответствующую подпись к нему.

Все прямые схемы, рассматриваемые далее, имеют общее слабое место. Действенность схемы зависит от безопасности закрытого ключа отправителя. Если отправитель впоследствии не захочет признать факт отправки сообщения, он может утверждать, что закрытый ключ был потерян или украден, и в результате кто-то подделал его подпись. Можно применить административное управление, обеспечивающее безопасность закрытых ключей, для того чтобы хоть в какой-то степени ослабить эти угрозы. Один из возможных способов состоит в требовании в каждую подпись сообщения включать отметку времени (дату и время) и сообщать о скомпрометированных ключах в специальный центр.

Другая угроза состоит в том, что закрытый ключ может быть действительно украден у отправителя X в момент времени T. Нарушитель может затем послать сообщение, подписанное подписью X и помеченное временной меткой, которая меньше или равна T.

Проблемы, связанные с прямой цифровой подписью, могут быть частично решены с помощью арбитра. Существуют различные схемы с применением **арбитражной** подписи. В общем виде арбитражная подпись выполняется следующим образом. Каждое подписанное сообщение от отправителя X к получателю Y первым делом поступает к арбитру A, который проверяет подпись для данного сообщения. После этого сообщение датируется и посылается к Y с указанием того, что оно было проверено арбитром. Присутствие A решает проблему схем прямой цифровой подписи, при которых X может отказаться от сообщения.

В таких схемах арбитр играет исключительно важную роль, и все участники должны ему доверять. Рассмотрим несколько примеров схем арбитражной цифровой подписи.

I. Симметричное шифрование, при котором арбитр может видеть сообщение

Обозначим:
X – отправитель,
Y – получатель,
A – арбитр,
M – открытое сообщение,
E – алгоритм шифрования,
K_{Xa} – совместный ключ X и A,
K_{aY} – совместный ключ Y и A,
K_{XY} – совместный ключ X и Y,
H – функция хэширования,
$||$ – операция конкатенации,
T – метка времени.

В этих обозначениях последовательность действий участников цифровой подписи можно описать следующими формулами:

$$X \rightarrow A: \quad M \,||\, E_{KXa}(ID_X \,||\, H(M)). \tag{9}$$

Предполагается, что отправитель X и арбитр A используют общий секретный ключ K_{Xa} и что A и Y используют общий секретный ключ K_{aY}. X создаёт сообщение M и вычисляет его хэш-значение $H(M)$. Затем X передаёт сообщение с добавленной к нему подписью арбитру A. Подпись складывается из идентификатора X и хэш-значения, всё это зашифровано с использованием ключа K_{Xa}. Арбитр A дешифрует подпись и проверяет хэш-значение:

$$A \rightarrow Y: \quad E_{KaY}(ID_X \,||\, M \,||\, E_{KXa}(ID_X \,||\, H(M)) \,||\, T). \tag{10}$$

Затем A передает сообщение к Y, шифруя его K_{aY}. Сообщение включает IDX, первоначальное сообщение от X, подпись и отметку времени. Получатель Y может дешифровать его для получения сообщения и подписи. Отметка времени информирует Y о том, что данное сообщение не устарело и не является повтором. Y может сохранить M и подпись к нему. В случае спора Y, который утверждает, что получил сообщение M от X, посылает следующее сообщение к арбитру A:

$$E_{KaY}(ID_X \,||\, M \,||\, E_{KXa}(ID_X \,||\, H(M)) \,||\, T). \tag{11}$$

Арбитр использует K_{aY} для получения ID_X, M и подписи, а затем, используя K_{Xa}, может дешифровать подпись и проверить хэш-код. По этой схеме Y не может прямо проверить подпись X; подпись используется исключительно для разрешения споров. Y считает сообщение от X аутентифицированным, потому что оно прошло через A. В данном сценарии обе стороны должны иметь высокую степень доверия к A:

- X должен доверять A в том, что тот не разгласит K_{Xa} и не будет создавать фальшивые подписи вида $E_{KXa}(ID_X \,||\, H(M))$;
- Y должен верить, что A будет посылать $E_{KaY}(IDX \,||\, M \,||\, E_{KXa}(IDX \,||\, H(M)) \,||\, T)$ только в том случае, если хэш-значение является корректным и подпись была создана X;
- обе стороны должны быть уверены, что A будет честно разрешать спорные вопросы.

II. Симметричное шифрование, при котором арбитр не видит сообщение

Если арбитр не является такой доверенной стороной, то *X* должен добиться того, чтобы никто не мог подделать его подпись, а *Y* должен добиться того, чтобы *X* не мог отвергнуть свою подпись.

Предыдущий сценарий также предполагает, что *A* имеет возможность читать сообщения от *X* к *Y* и что возможно любое подсматривание. Рассмотрим сценарий, который, как и прежде, использует арбитраж, но при этом ещё гарантируется конфиденциальность. В таком случае также предполагается, что *X* и *Y* используют общий секретный ключ K_{XY}:

$$X \rightarrow A: \quad ID_X \,||\, E_{KXY}(M) \,||\, E_{KXa}(ID_X \,||\, H(E_{KXY}(M))). \tag{12}$$

X передает *A* свой идентификатор, сообщение, зашифрованное K_{XY}, и подпись. Подпись состоит из идентификатора и хэш-значения зашифрованного сообщения, которые зашифрованы с использованием ключа K_{Xa}. *A* дешифрует подпись и проверяет хэш-значение. В данном случае *A* работает только с зашифрованной версией сообщения, что предотвращает его чтение.

Следующий шаг в этой схеме – *A* после проверки передаёт адресату *Y*

$$A \rightarrow Y: \quad E_{KaY}(ID_X \,||\, E_{KXY}(M) \,||\, E_{KXa}(ID_X \,||\, H(E_{KXY}(M))) \,||\, T). \tag{13}$$

Арбитр *A* передает *Y* всё, что он получил от *X* плюс отметку времени, шифруя всё с использованием ключа K_{aY}.

Хотя арбитр и не может прочитать сообщение, он в состоянии предотвратить подделку любого из участников – *X* или *Y*. Остаётся проблема, как и в первом сценарии, что арбитр может сговориться с отправителем, отрицающим подписанное сообщение, или с получателем для подделки подписи отправителя.

III. Шифрование открытым ключом, при котором арбитр не видит сообщение

Все упомянутые сложности могут быть решены с помощью открытого ключа по следующей схеме

$$X \rightarrow A: \quad ID_X \,||\, E_{KRx}(ID_X \,||\, (E_{KUy}(E_{KRx}(M)))). \tag{14}$$

В этом случае *X* осуществляет двойное шифрование сообщения *M*, сначала своим закрытым ключом KR_X, а затем открытым ключом *Y* – KU_Y. Получается подписанная секретная версия сообщения. Теперь это подписанное сообщение вместе с идентификатором *X* шифруется KR_X и вместе с ID_X посылается *A*. Внутреннее, дважды зашифрованное сообщение недоступно арбитру (и всем, исключая *Y*). Однако *A* может дешифровать внешнюю шифрацию, чтобы убедиться, что сообщение пришло от *X* (так как только *X* имеет KR_X). Проверка даёт гарантию, что пара «закрытый/открытый ключ» законна, и тем самым верифицирует сообщение:

$$A \rightarrow Y: \quad E_{KRa}(ID_X \,||\, (E_{KUy}(E_{KRx}(M)) \,||\, T). \tag{15}$$

Затем *A* передаёт сообщение *Y*, шифруя его KR_a. Сообщение включает ID_X, дважды зашифрованное сообщение и отметку времени.

Эта схема имеет ряд преимуществ по сравнению с предыдущими двумя схемами. Во-первых, в совместном распоряжении сторон до начала обмена данными нет никакой информации, что предотвращает возможность сговора с

целью обмана. Во-вторых, некорректные данные не могут быть посланы, даже если KR_X скомпрометирован, при условии, что не скомпрометирован KR_a. В заключение, содержимое сообщения от X к Y неизвестно ни A, ни кому бы то ни было ещё.

Стандарты цифровой подписи. Национальный институт стандартов и технологии США (NIST) разработал федеральный стандарт цифровой подписи DSS. Для создания цифровой подписи используется алгоритм DSA (Digital Signature Algorithm). В качестве хэш-алгоритма стандарт предусматривает использование алгоритма SHA-1 (Secure Hash Algorithm). DSS первоначально был предложен в 1991 году и пересмотрен в 1993.

DSS использует алгоритм, который разрабатывался для использования только в качестве цифровой подписи. В отличие от RSA, его нельзя использовать для шифрования или обмена ключами. Тем не менее, это технология открытого ключа.

В российском стандарте ГОСТ 3410, принятом в 1994 году, используется алгоритм, аналогичный алгоритму, реализованному в стандарте DSS. Оба алгоритма относятся к семейству алгоритмов ElGamal.

В стандарте ГОСТ 3410 используется хэш-функция ГОСТ 3411, которая создаёт хэш-код длиной 256 бит. Это во многом обуславливает требования к выбираемым простым числам p и q.

Еще раз обратим внимание на отличия DSS и ГОСТ 3410:

- используются разные хэш-функции: в ГОСТ 3410 применяется российский стандарт на хэш-функции ГОСТ 3411, в DSS используется SHA-1, которые имеют разную длину хэш-кода. Отсюда и разные требования на длину простого числа q: в ГОСТ 3410 длина q должна быть от 254 бит до 256 бит, а в DSS длина q должна быть от 159 бит до 160 бит;
- по-разному вычисляется компонента s подписи.

Подписи, созданные с использованием стандартов ГОСТ 3410 или DSS, называются **рандомизированными**, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи (r, s), поскольку каждый раз будет использоваться новое значение k. Подписи, созданные с применением алгоритма RSA, называются **детерминированными**, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будет создаваться одна и та же подпись.

2. Практическая часть

Одним из основных компонентов организации безопасности информационной системы является криптозащита и шифрование данных, использующее методы криптографии. Авторы, читая этот курс несколько лет, отказались от изложения серьезной математической базы и математических основ криптографии и ограничились кратким обзором методов симметричного шифрования и методов шифрования с открытым ключом. Но сделали акцент на практическом использовании и освоении этих методов на примере конкретных программных продуктов. Далее предлагается выполнить ряд несложных практических заданий, иллюстрирующих изложенный в первой части теоретический материал.

Практические задания выполняются с использованием несложных бесплатных программных пакетов, которые любой читатель без труда загрузит по приведенным в надлежащем месте ссылкам.

2.1. Основные понятия и применение стеганографии

В большинстве случаев в практике обмена и передачи данных и сообщений нужно не столько зашифровать данные, сколько просто скрыть сам факт обмена и передачи сообщений. Этой темой полна литература ещё докомпьютерной эпохи. Практика написания текста молоком между строк, с целью дальнейшего проявления и визуализации сообщения, тоже восходит к тем временам. Методы использующие маскировку и сокрытие самого факта наличия сообщения и его передачи изучает стеганография.

Что изменилось в стеганографии с появлением компьютеров, и как всё это работает с использованием компьютерных программ и данных? Принципы стеганографии в компьютерную эру подверглись минимальным изменениям и остались такими же простыми. Файл с данными, факт передачи которого вы хотите скрыть, может быть любым: это может быть текст, изображение, бинарный файл, мультимедийный объект. С другой стороны, эти данные специальным образом внедряются в так называемый файл-носитель (carrier file). Естественно, файл-носитель внешне должен быть совершенно безобидным и не вызывать никаких подозрений у хакеров, нацеленных вас атаковать, – это рекламная картинка, текст песенки-шлягера, нейтральные фотографии цветов и домашних животных.

Второе требование к файлу-носителю – он должен быть «рыхлым», то есть содержать достаточное количество избыточных данных. Такие файлы обычно очень хорошо упаковываются архиваторами. Форматы таких файлов известны – это `*.bmp`, `*.txt`, `*.html`, `*.pdf`. Именно такие файлы используются в качестве файлов-носителей. Программа, осуществляющая все эти функции, подходит для нашей задачи. Такие программы обычно небольшие и имеются в свободном доступе в Интернете. Стоит вам набрать в любой поисковой системе «program steganography» и вы получите список из сотен названий.

Выполним некоторые практические задания. Используем программу `wbStego4`, которая написана программистом `Werner Bailer` и загружена с его web-странички `http://wbstego.wbailer.com/`. В дистрибутивном пакете автор любезно предоставил регистрационное имя и регистрационный ключ.

2.1.1. Внедрение данных в файл-носитель программой wbStego4

Работа с программой состоит из ряда этапов.

Первый этап. На первом этапе запускаем программу и видим интерактивное окно (рис. 5). Программа информирует о своих возможностях и предла-

гает сделать выбор режима работы. По умолчанию предлагается пошаговый режим. Программа сообщает основные сведения: кодирование/декодирование, режимы работы, типы файлов-носителей.

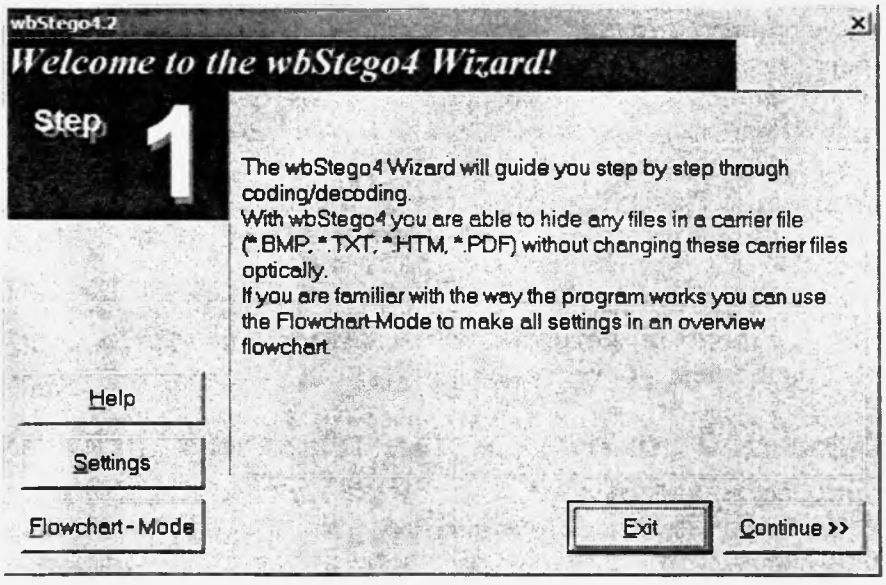


Рис. 5. Первый шаг работы с программой wbStego4

Для продвинутых пользователей имеется другой, альтернативный режим. Выбор режима работы и переход к другому стилю интерфейса осуществляется нажатием на Flowchart-Mode (режим блок-схемы).

При щелчке по кнопке Help программа предлагает некоторые сведения из стеганографии и справку по интерфейсу управления программой.

Упражнение для самостоятельной работы 1. Нажмите кнопку Help и просмотрите сведения, которые хочет сообщить вам программа.

Упражнение для самостоятельной работы 2. Нажмите кнопку Flowchart-Mode и перейдите в этот режим. Проделайте приведенное ниже упражнение в режиме «Блок-схема».

Упражнение для самостоятельной работы 3. Нажмите кнопку Setting и просмотрите, доступ к каким настройкам разрешает программа wbStego4.

Если вы передумали, хотите «откатить назад» и выйти из программы, для этого нажимаем Exit. Переход к следующему этапу – кнопка Continue.

Второй этап. На втором этапе делаем выбор: отправлять данные (внедрять – encode) или получать (извлекать – decode) (рис. 6).

Для извлечения данных из файла-носителя выставляем флажок у команды Decode. Если требуется внедрить туда данные, то выставляем флажок у команды Encode. Выбираем Encode и нажимаем кнопку Continue.

Третий этап. Программа просит указать, где расположены ваши конфиденциальные данные.

На этом этапе вы должны выбрать и указать полный путь в файловой системе для файла с вашими конфиденциальными данными, которые вы хотите скрыть. На рис. 7 указан файл secret.txt.

Четвёртый этап. Программа просит указать файл-носитель (рис. 8). Во-первых, из списка File Type, приведенного в диалоговом окне, необходимо указать тип файла-носителя (у нас выделен тип *.bmp), если у пользователя возникли затруднения, можно попытаться активировать поиск файла-носителя с помощью самой программы, нажимая Find carrier file.

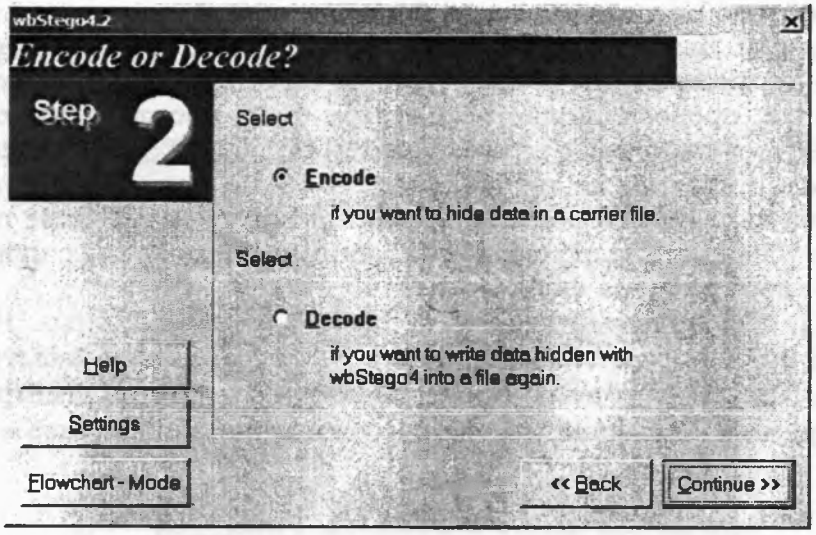


Рис. 6. Выбор режима работы программы wbStego4

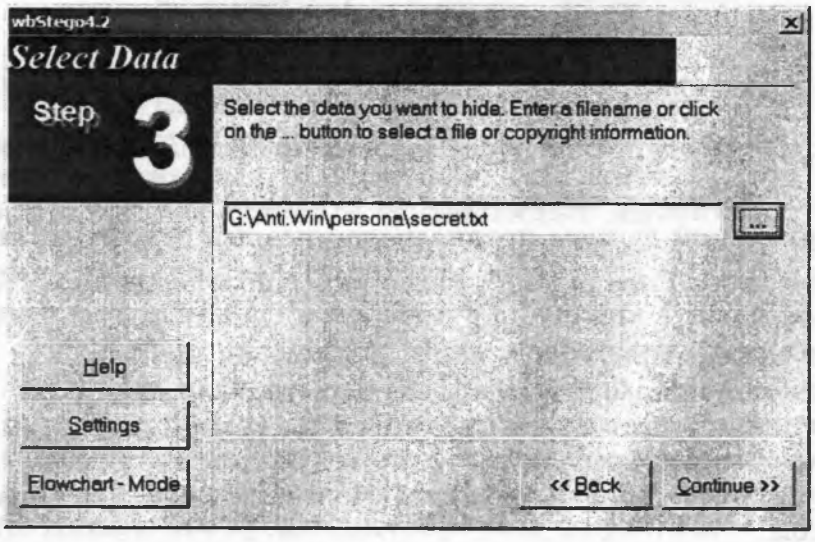


Рис. 7. Указание пути к файлу с конфиденциальными данными

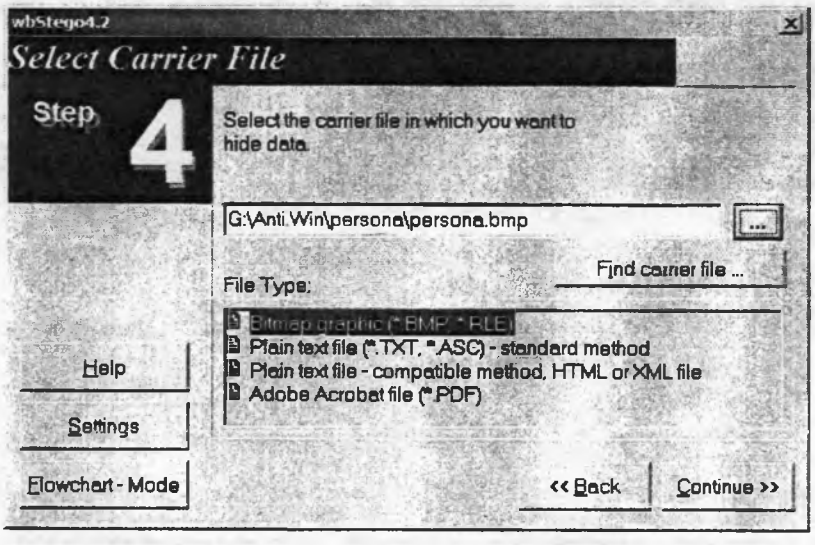


Рис. 8. Указание пути к файлу-носителю

Во-вторых, необходимо учесть, что размеры файла-носителя и данных, которые вы хотели бы туда внедрить, коррелируют. Файл-носитель, конечно, «рыхлый», но не «резиновый» и естественное ограничение – это его собственный размер. Данные, превосходящие по размеру файл-носитель, внедрить туда никак нельзя. Речь может идти только о какой-то части, о какой-то доле размера файла-носителя, обычно, не превышающей 50 %. Точных рецептов и точных аналитических формул для расчёта этого параметра нет. Общее правило такое: для сокрытия большого массива конфиденциальных данных нужен соответствующего большего размера файл-носитель.

В-третьих, обсуждаемый параметр зависит от типа данных: Наиболее «рыхлые» – это чёрно-белые картинки формата `*.bmp`, минимум избыточных данных в формате `*.pdf`. В-четвёртых, проверку обсуждаемого параметра осуществляет сама программа и вы можете увидеть сообщение, показанное на рис. 9.

Рис. 9. Предупреждающее сообщение программы `wbStego4`

Сообщение означает, что программа `wbStego4` сама произвела проверку и определила, что ваши данные предназначенные для сокрытия, не поместятся в файл-носитель. Для исправления необходимо вернуться в поле `Select the carrier file`, нажать кнопку [...] и выбрать файл-носитель подходящего размера. Можно также вернуться к шагу 3, нажимая кнопку `Back` (см. рис. 8.) и подобрать конфиденциальные данные меньшего размера.

Пятый этап. Следует заметить, что метод стеганографии не предполагает никакого кодирования данных и то, что мы видим на рис. 10 – это дополнительная функция пакета `wbStego4`, реализованная разработчиком-программистом.

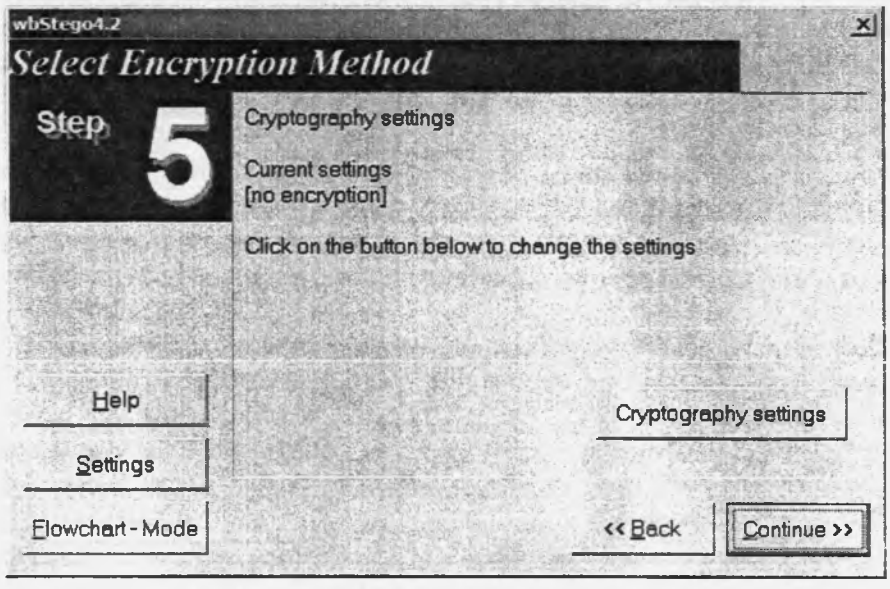


Рис. 10. Установка криптографических параметров программы `wbStego4`

Нажав кнопку Cryptography setting, переходим к следующему окну, выбрав криптографический алгоритм (рис. 11). В этом окне мы видим предлагаемые алгоритмы шифрования.

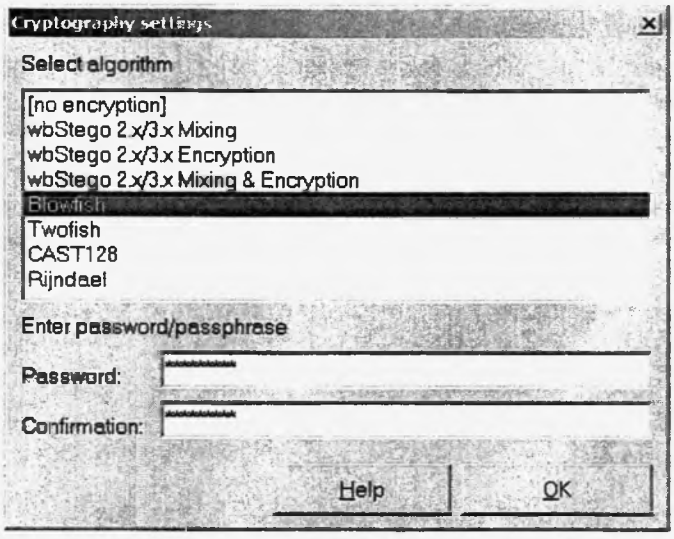


Рис. 11. Выбор криптографического алгоритма в программе wbStego4

Можно отказаться от шифрования, выбрав [no encryption], а можно выбрать один из предложенных стандартных алгоритмов: Blowfish, Twofish, Cast128, Rijndael. Это популярные традиционные алгоритмы симметричного шифрования, упомянутые в данной работе в подразделе 1.6.3 и разработанные математиками двенадцати стран. При выборе шифрования, необходимо дважды ввести пароль (см. рис. 11).

Шестой этап. Здесь возможны некоторые манипуляции с файлом-носителем. Мы выбрали persona.bmp (см. рис. 8, рис. 15, *а*). После этого программа модифицирует файл-носитель, внедрив туда наши данные и изменяя его (при необходимости сохраняя зарезервированную копию файла). Чтобы исходный файл не изменять, файл-носитель после внедрения туда данных лучше переименовать. Именно это продемонстрировано на рис. 12.

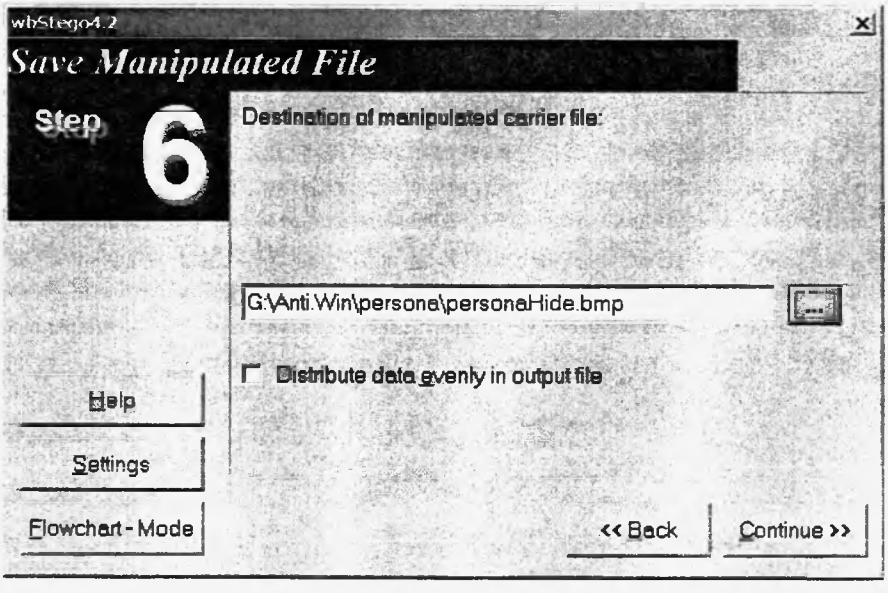


Рис. 12. Указание пути к модифицированному файлу-носителю с внедрёнными в него данными

Мы переименовали и указали полный путь в файловой системе для файла-носителя, куда программа внедрит ваши конфиденциальные данные. Переименованный файл-носитель – это `personaHide.bmp` (рис. 15, *б*).

На этом этапе программа предоставляет ещё одну возможность – распределять внедрённые данные в выходной файл равномерно (`Distribute data evenly in output file`). Если вы уверены в структуре распределения данных этого файла – отметьте флажок, но лучше положиться на программу, она разберётся, как распределить внедрённые данные в файле-носителе. Для продолжения нажимает кнопку `Continue`.

Седьмой этап. На этом итоговом этапе программа завершила подготовительную работу: собрала все сведения и приготовила все данные. Итоговые данные выводятся пользователю в специальном диалоговом окне (рис. 13). Окно содержит пользовательские установки (`current setting`):

- файл-носитель (`carrier file`) — `persona.bmp`;
- шифруемые данные (`encode data`) — `secret.txt`;
- выходной файл (`manipulated file`) — `personaHide.bmp`;
- метод кодирования (`encryption method`) — `Blowfish`.

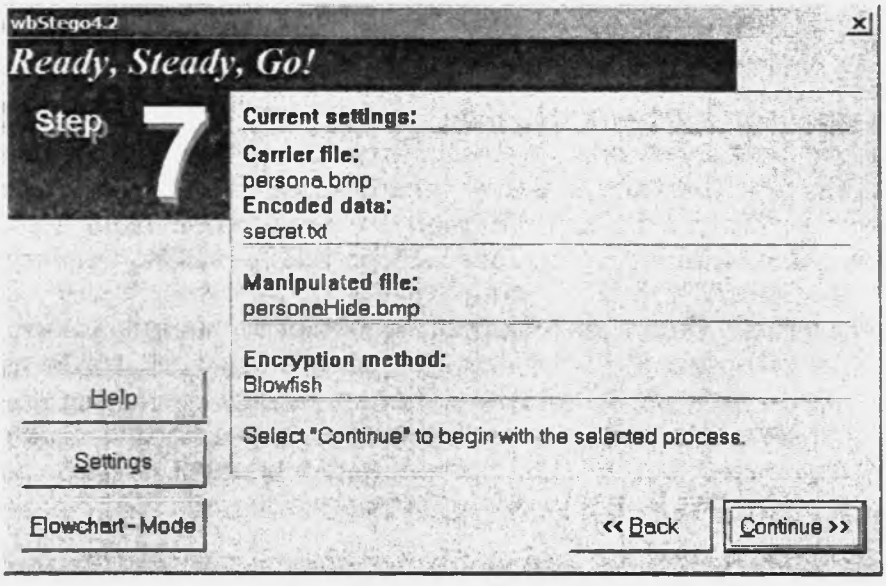


Рис. 13. Завершение этапа работы программы `wbStego4` и краткий отчёт о завершённом кодировании

При необходимости внесения изменений используется кнопка `Back` для «отката» на предыдущий этап. Для продолжения работы нажимаем кнопку `Continue`.

После нажатия `Continue` программа обработает все данные и в случае успешного завершения процесса подтвердит это сообщением, представленным на рис. 14. На этом этапе работа с программой завершена. Программа информирует, что процесс шифрования данных и их внедрение в файл-носитель успешно завершён.

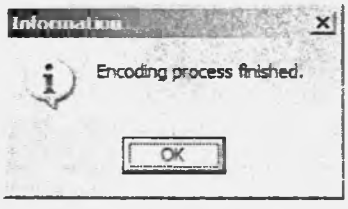
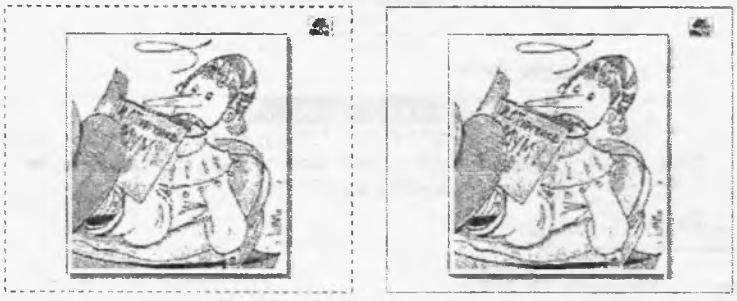


Рис. 14. Завершающее сообщение программы `wbStego4`

Восьмой этап. На этом этапе проводится мониторинг файла-носителя и его визуальный контроль.

Парадигма метода стеганографии заключается в скрытии факта внедрения данных в файл-носитель. На рис. 15 приведены два изображения файла-носителя: а) до внедрения данных; б) после внедрения. Отличия вы не найдёте, более того, размеры у этих файлов одинаковы.



а) persona.bmp б) personaHide.bmp

Рис. 15. Фрагмент окна программы просмотрщика ACDSee с файлом-носителем:
а) пустой файл-носитель (persona.bmp);
б) файл-носитель с внедрёнными данными (personaHide.bmp)

2.1.2. Извлечение данных из файла носителя программой wbStego4

Для решения обратной задачи – извлечения данных из файла-носителя – последовательно выполняем несколько этапов работы.

Первый этап. Запускаем программу (см. рис. 5) и нажимаем кнопку Continue.

Второй этап. Для извлечения данных из файла-носителя выставляем флажок у команды Decode (рис. 16) и нажимаем кнопку Continue.

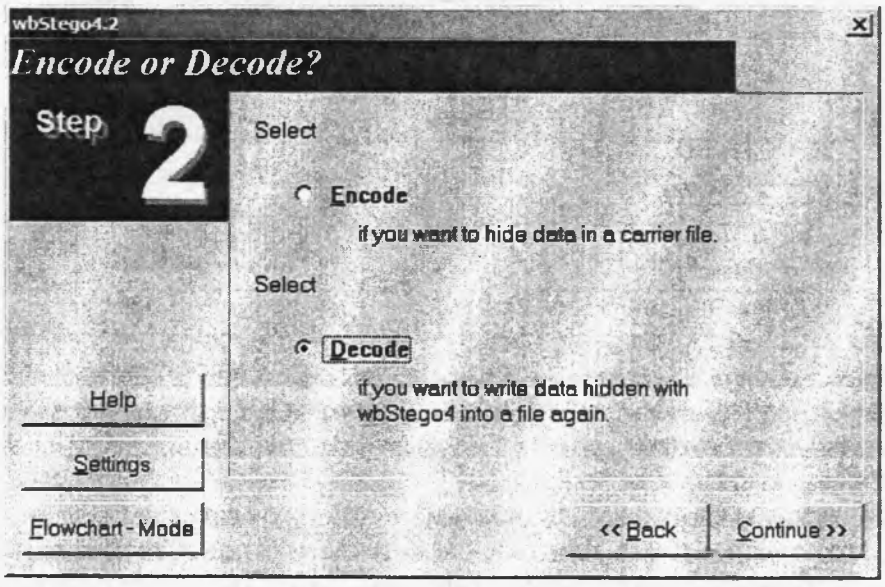


Рис. 16. Выбор режима работы программы wbStego4 для извлечения данных

Третий этап. На этом этапе, воспользовавшись кнопкой [...], в поле ввода данных указываем полный путь к файлу-носителю (рис. 17) и из списка File Type выбираем тип файла-носителя. Нажимаем кнопку Continue.

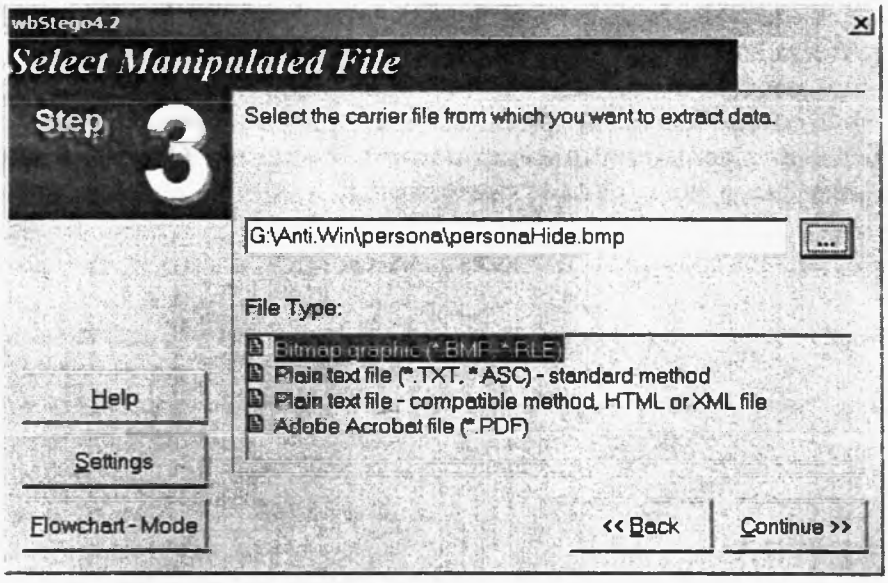


Рис. 17. Указание пути к файлу-носителю

Четвёртый этап. На этом этапе программа просит ввести пароль (рис. 18). Выполняем ввод пароля и нажимаем кнопку Continue.

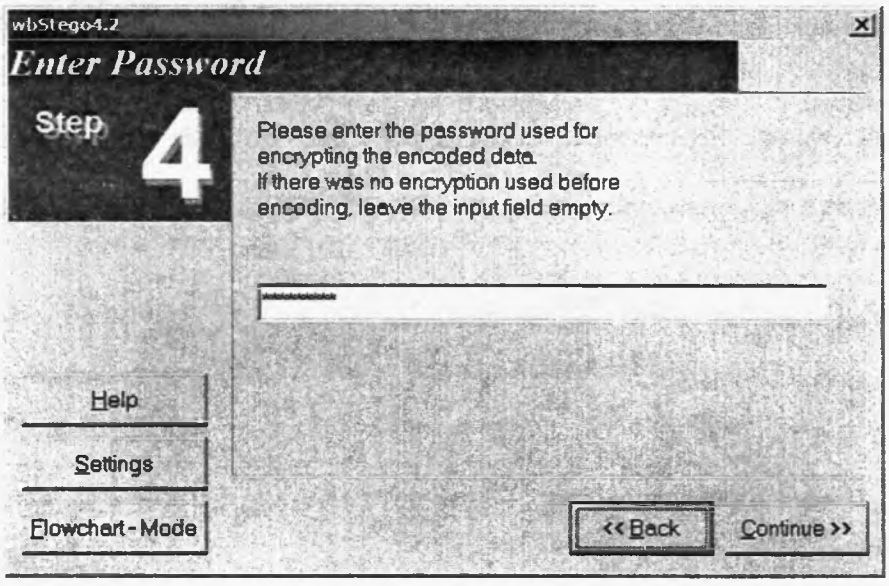


Рис. 18. Указание пароля для начала процесса декодирования

Пятый этап. На этом этапе программа предлагает присвоить имя файлу конфиденциальных данных, которые она извлечёт из файла-носителя (рис. 19). Рекомендуется дать файлу данных другое имя, отличающееся от первоначального. Нажимаем кнопку Continue.

Шестой этап. Программа завершила подготовительный этап, собрала все сведения и приготовила все данные. Эти итоговые данные она выводит пользователю в специальном диалоговом окне (рис. 20). Окно содержит пользовательские установки (`current setting`):

- выходной файл (`manipulated file`) — `personaHide.bmp`;
- извлечённый файл (`result`) — `secret2.txt`;
- метод кодирования (`encryption method`) — `automatic decoding`.

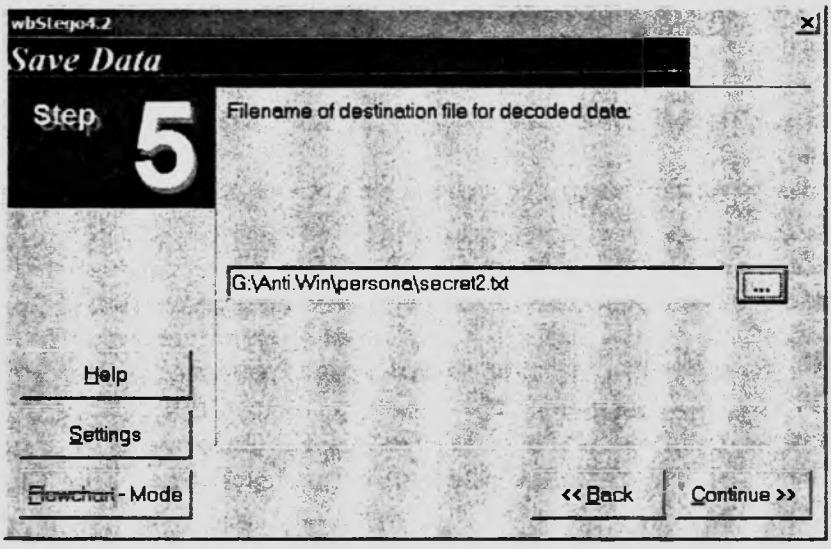


Рис. 19. Указание пути к файлу с конфиденциальными данными

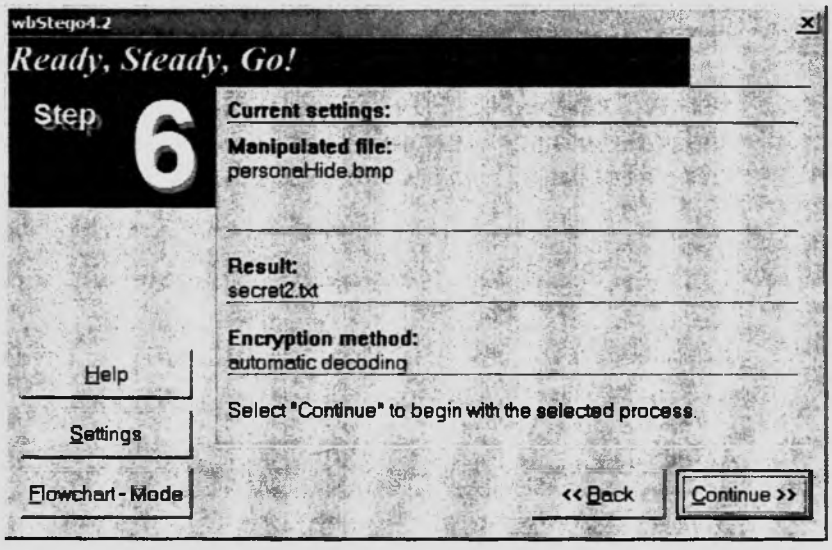


Рис. 20. Завершение этапа работы программы `wbStego4` и краткий отчёт о завершённом декодировании

Программа автоматически определяет метод шифрования (`automatic decoding`) и пользователь избавлен от необходимости заполнять это вручную. Обычно пользователь-получатель не знает метода шифрования, который употребил пользователь-отправитель. Ему достаточно знать пароль.

Нажав Continue, завершаем работу программы и получаем завершающее сообщение (рис. 21): `Decoding process finished` (процесс декодирования завершён).

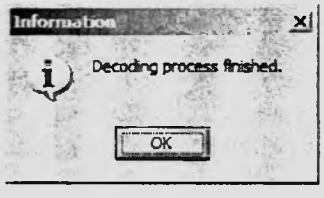


Рис. 21. Завершающее сообщение программы `wbStego4` об успешном извлечении данных и декодировании

Упражнение для самостоятельной работы 4. Сравните содержимое файлов `secret.txt` и `secret2.txt`. В каком случае может возникнуть несовпадение?

2.2. Вычисление хэш-функции по алгоритму MD5

2.2.1. Использование хэш-функции для контроля целостности данных

О важности и значимости функции хэширования достаточно подробно изложено в разделе 1.6.6 этого пособия. Здесь в практической части мы рассмотрим, как можно реализовать идею использования хэш-функции для контроля целостности ваших данных.

Для реализации этой идеи рассмотрим решение нескольких примеров с помощью несложной программы `MD5summer`, вычисляющей хэш-функцию по алгоритму `MD5`. Эта программа (`http://www.md5summer.org/`) распространяется бесплатно и не требует инсталляции, поместив её в отдельный каталог, можно приступать к работе.

Допустим, Persona нашёл мультимедийные данные на одном из `ftp`-серверов о своих друзьях Coach и Actor. Он загрузил эти данные на свой компьютер и теперь озабочен вопросом, не произошёл ли какой-либо сбой при передаче по компьютерным сетям таких больших файлов. Этика предоставления `ftp`-сервиса клиентам требует, чтобы разместивший свои данные (файлы) на `ftp`-сервере снабжал их контрольными значениями хэш-функций. Это даёт возможность пользователям при загрузке файлов проверить их целостность. Продемонстрируем эту историю на простейших примерах на локальном компьютере.

2.2.2. Создание файла с хэш-функцией, на основе данных произвольной длины

После запуска `MD5summer` программа требует определить каталог с данными и тип действия (рис. 22): создание суммы `MD5` или её проверка.

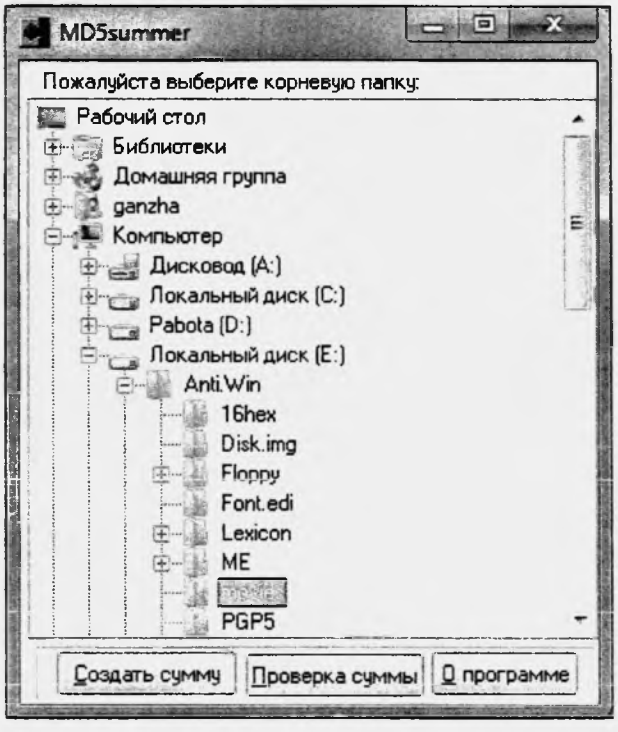


Рис. 22. Определение рабочего каталога программы `MD5summer`

Для начала мы хотим создать хэш-функцию. Нажав кнопку «Создать сумму», переходим к диалоговому окну (рис. 23), в котором приведен список папок с песнями и кинофильмами, которые загрузил Persona. Данная программа может вычислить значение хэш-функции для произвольного количества файлов в отмеченном каталоге. Выберем сначала один, к примеру, persona.avi.

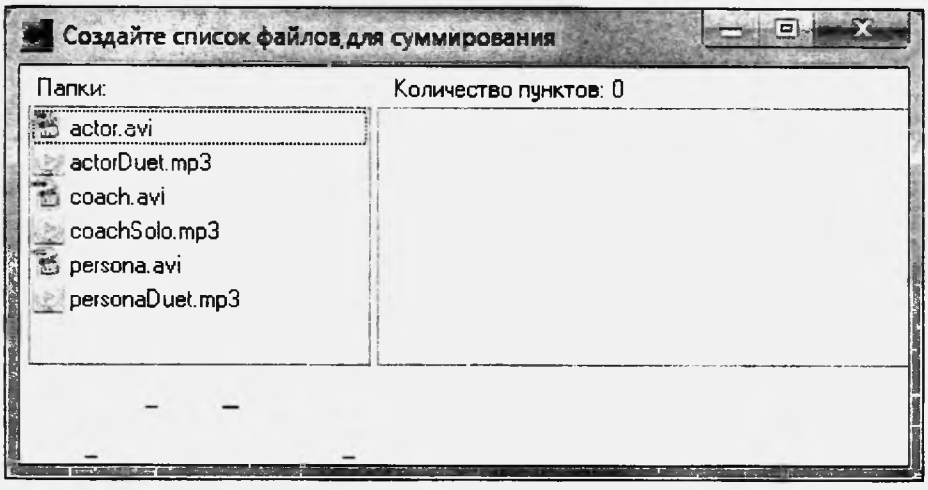


Рис. 23. Окно выбора данных программы MD5summer

Выбрав файл persona.avi и нажав кнопку «Добавить» видим появление ссылки на этот файл в правом списке (рис. 24).

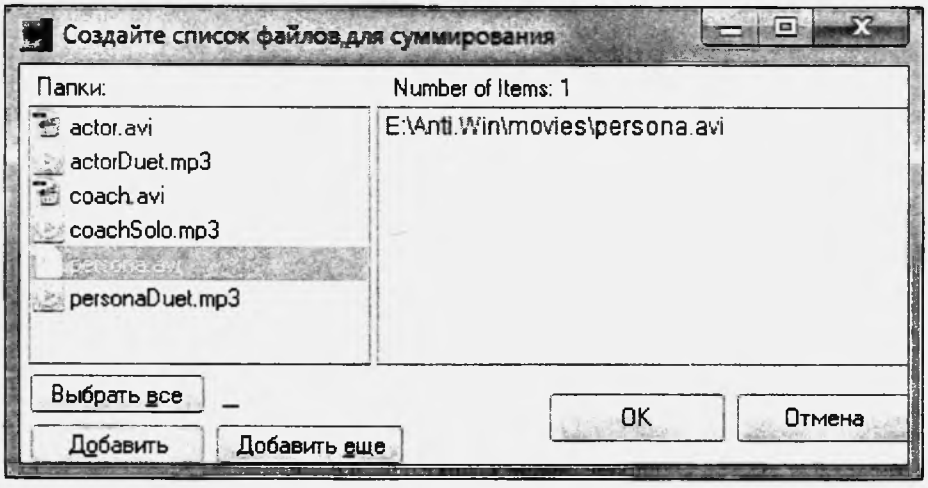


Рис. 24. Указание файлов с данными для вычисления хэш-суммы

Выделив этот файл в правом списке и подтвердив этот выбор кнопкой OK, открываем окно, представленное на рис. 25. В окне представлена информация об имени файла (слева) и значение хэш-функции в виде 16-ричного 32-разрядного числа (справа). Один разряд такого числа состоит из четырёх бит, значит, полное значение хэш-функции составляет 32 × 4 = 128 бит, в полном соответствии с алгоритмом MD5. В левом нижнем углу указано время, которое программа затратила на вычисление хэш-функции. В данном случае на файл persona.avi (94 Мб) затрачена 1 секунда.

Упражнение для самостоятельной работы 5. Создайте для каждого мультимедийного файла в каталоге Anti.Win с помощью программы MD5summer файл с хэш-суммой, с расширением *.md5.

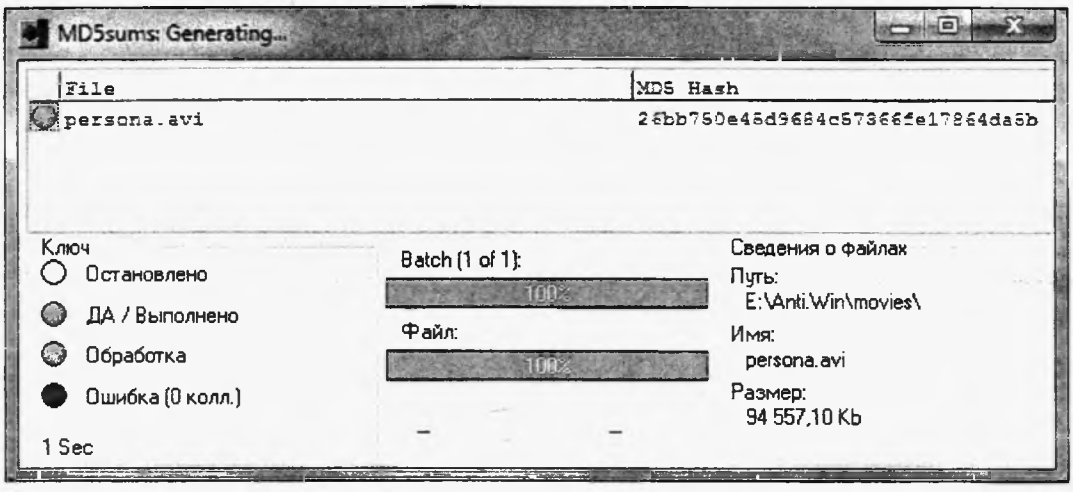


Рис. 25. Рабочее окно программы MD5summer

Упражнение для самостоятельной работы 6. Доступными вам средствами найдите 128-битовое значение хэш-функции в файле persona.md5. Проверьте, соответствует ли это значение приведенному на копии экрана (см. рис. 25) выше. Если 128 бит перевести в байты, то получится 16 байт, почему тогда все размеры файлов (рис. 26) с расширением *.md5 значительно превышают этот размер?

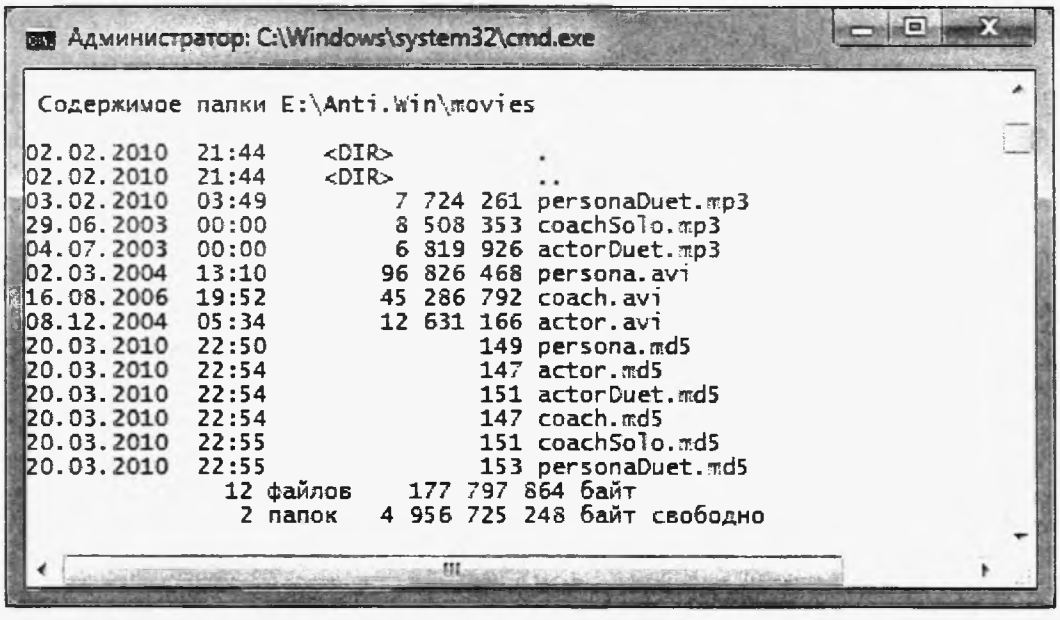


Рис. 26. Копия экрана со списком файлов рабочего каталога программы MD5summer

2.2.3. Проверка целостности данных программой MD5summer

Программа MD5summer позволяет проверить, не нарушена ли целостность данных в файлах, для которых предварительно была рассчитана хэш-сумма по алгоритму MD5. Убедимся в этом. Теперь, запустив программу и отыскав каталог с данными, нажимаем кнопку «Проверка суммы» (рис. 27). В окне появляется список всех файлов с контрольными суммами *.md5.

Необходимо указать, какую сумму мы хотим проверить. Для данного примера это persona.md5. Нажимаем кнопку «Открыть» и программа производит проверку. Получаем такой же экран, как на рис. 25. Слева от имени файла

появится зелёный флажок (кружочек), что говорит об успешном завершении проверки.

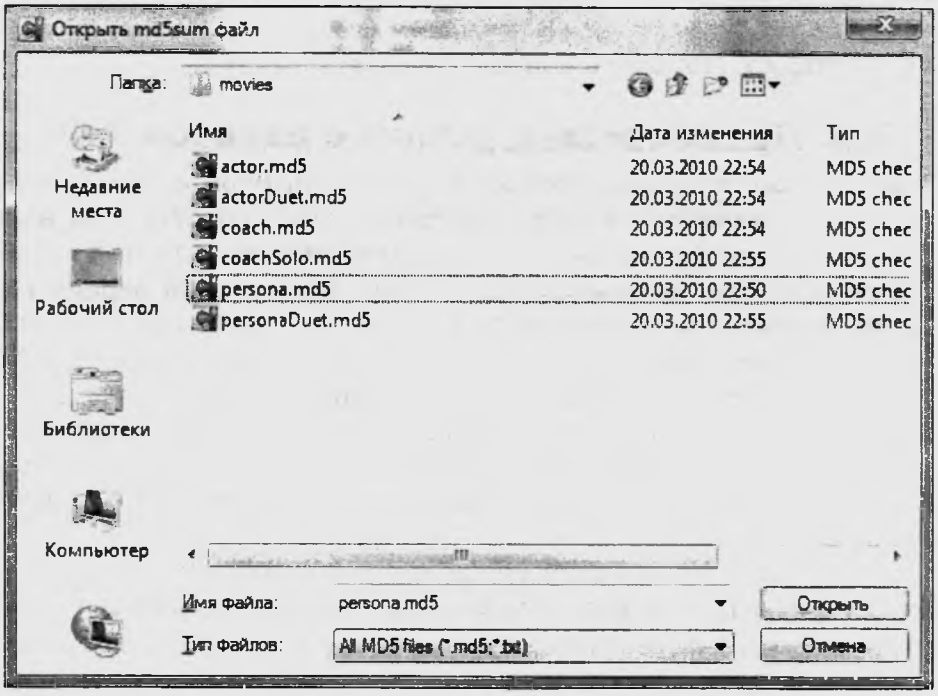


Рис. 27. Копия экрана со списком отфильтрованных файлов рабочего каталога программы `MD5summer`

2.2.4. Сбой проверки целостности данных

При передаче данных по сетям вполне вероятны сбои и ошибки. В этом случае хэш-функция, вычисленная до передачи данных и после, конечно же не совпадает. Как реагирует программа `MD5summer` в этом случае? Выясним на следующем примере.

Упражнение для самостоятельной работы 7. Доступными вам средствами измените один бит данных в файле `personaDuet.mp3`.

Запустив программу `MD5summer` и получив диалоговое окно как на рис. 22, нажмите кнопку «Проверка суммы». Укажите программе, что вы хотите проверить файл `personaDuet.md5`. Программа произведёт вычисления и выведет сообщение (рис. 28).

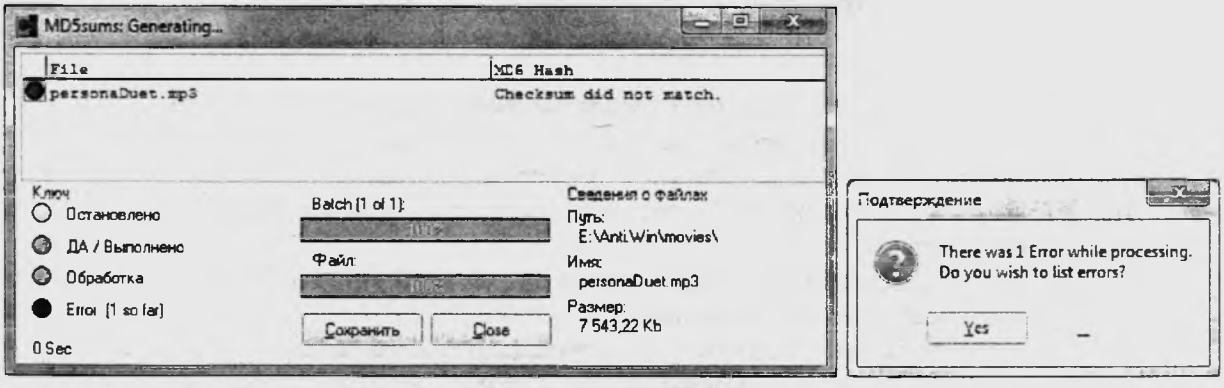


Рис. 28. Рабочее окно программы в процессе обнаружения несоответствия хэш-функции. Отчёт программы `MD5summer` об обнаружения несоответствия

В этом случае мы получим, во-первых, диалоговое окно с красным флажком (кружком) и с надписью «Checksum did not match» (Несоответствие контрольной суммы), а, во-вторых, дополнительное сообщение «There was 1 Error while processing. Do you wish to list errors?» (В процессе обработки обнаружена 1 ошибка. Показать список ошибок?).

2.3. Практическая работа с пакетом PGP

В настоящей работе приводится несколько примеров использования пакета PGP (Pretty Good Privacy – вполне надёжная секретность). Для иллюстрации различных методов шифрования используется пакет PGP 5.0, управляемый текстовым интерфейсом из командной строки. Выбор этой версии пакета объясняется не консерватизмом автора (в настоящее время существуют и продаются коммерческие версии PGP 8.0–9.0), а тем, что последние версии, используя графический интерфейс, прячут и скрывают «кухню» работы алгоритмов шифрования. Быть может это удобно для конечного пользователя, работающего с электронной почтой и шифрующего поток своих конфиденциальных данных, но совершенно недопустимо для будущих программистов, обучающихся навыкам защиты информации.

Пакет PGP 5.0 в 32-разрядной среде Windows может работать только в текстовой консоли виртуальной машины MS DOS. Методическая цель упражнений с этим пакетом, во-первых, напомнить слушателям работу с текстовым интерфейсом, что совершенно необходимо будущим инженерам-программистам, поскольку работа с конфигурационными файлами, с различными тонкими настройками системы чаще всего предполагает работу с текстовым интерфейсом командной строки. Во-вторых, только так можно увидеть и понять все детали работы пакета PGP и различные аспекты криптографической защиты.

Обучаемые «в живую» могут увидеть и воспользоваться функциями симметричного шифрования, закодировав файлы, предлагаемые им в методическом задании, используя для этого алгоритм симметричного шифрования IDEA. Пакет PGP обеспечивает также все функции асимметричного шифрования, которыми могут воспользоваться обучаемые:

- создание пары ключей для организации шифрованной переписки с корреспондентом (для генерации случайной последовательности при создании ключей используются индивидуальные биометрические особенности пользователя);
- передача сообщений, зашифрованных публичным ключом по алгоритму RSA, по открытым каналам связи, в том числе по электронной почте;
- передача секретного ключа симметричного шифрования по алгоритму DSS/Diffie-Hellman по открытым каналам связи, включая электронную почту;
- приём зашифрованных сообщений и их раскодирование private-ключом;
- создание с помощью private-ключа аутентифицированного сообщения и цифровой подписи между двумя корреспондентами;
- организация арбитражной цифровой подписи в случае отсутствия доверия у корреспондентов.

Вот неполный перечень возможностей этого небольшого пакета PGP, который может быть успешно использован.

Пакет PGP5 работает только в шестнадцатиразрядном окне (консоли), в формате записи файлов 8.3 (восемь_точка_три). Терминал (консоль текстовой строки) для работы с интерфейсом текстовой строки и ввода команд в операционных системах Microsoft можно открыть сочетанием клавиш [⊞+R]. После чего в появившемся текстовом поле набираем cmd.

Используя команды dir и cd, перейдите в каталог, где у вас установлен пакет PGP и сделайте его текущим.

2.3.1. Шифрование данных симметричным ключом. Алгоритм IDEA

Это задание необходимо выполнить до создания пары «открытый/закрытый ключ», иначе приложение будет конфликтовать с вами, пытаясь использовать имеющийся ключ в текущем каталоге.

Создание зашифрованного файла

В окне терминала введите команду:

```
pgpe -c file_name.
```

После ввода команды программа спросит пароль, который потребуется ввести два раза, после чего происходит шифрование по стандартному алгоритму IDEA и параллельно архивация (рис. 29). Следует иметь в виду, что при вводе пароля приложение не показывает ни «звёздочек», ни «пробелов» и курсор остаётся на месте.

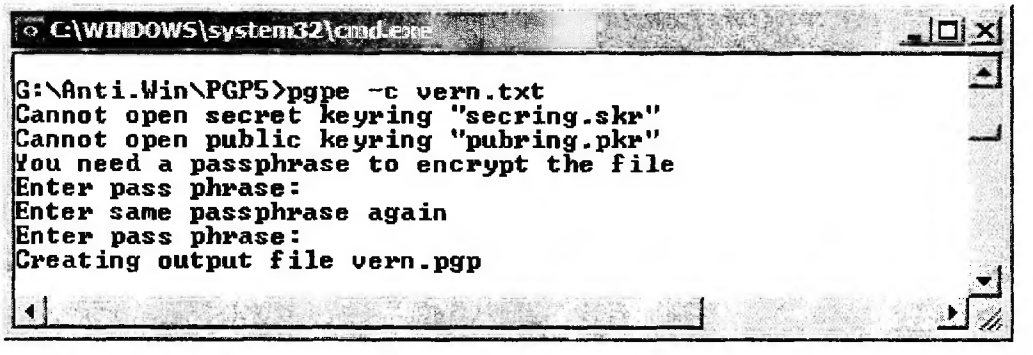


Рис. 29. Сообщения, выводимые на терминал программой PGP в процессе шифрования файла

Хочется отметить, что все команды программы, разбираемые здесь имеют полезный ключ –o, позволяющий присвоить выходному файлу любое пользовательское имя, например:

```
pgpe -c file_name -o output_file_name.
```

В противном случае по умолчанию пакет к имеющемуся имени файла добавляет своё расширение *.pgp как мы видим на копии экрана.

Декодирование зашифрованного файла

В окне терминала выполняем команду (рис. 30):

```
pgpv file_name -o output_file_name.
```

Для того чтобы сохранить существующий файл vern.txt, имя выходного файла изменено на vern1.txt. Естественно, что программа осуществит декодирование только в том случае, если введен соответствующий правильный пароль.

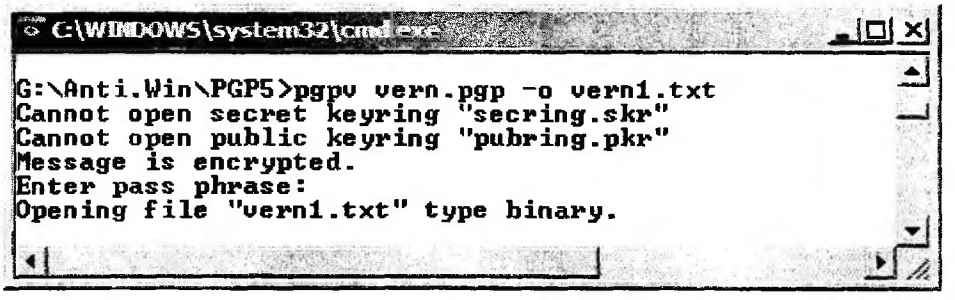


Рис. 30. Сообщения, выводимые на терминал программой PGP при декодировании зашифрованного файла

Упражнение для самостоятельной работы 8. Сравните размеры и содержимое файлов `vern.txt` и `vern1.txt` и сделайте соответствующие выводы.

2.3.2. Создание пары ключей для осуществления метода асимметричного шифрования

Для создания пары ключей в окно терминала вводится команда

```
pgpk -g.
```

После этого программа в интерактивном режиме вступает в диалог с пользователем и требует от него правильных ответов и дополнительных действий (рис. 31).

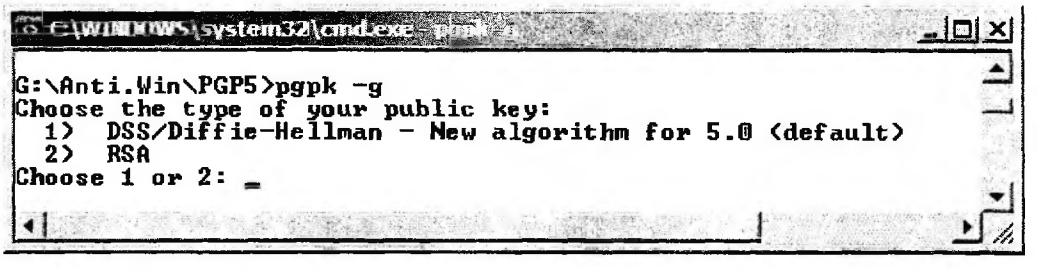


Рис. 31. Запрос программы алгоритма кодирования

Требуется выбрать алгоритм асимметричного шифрования. Программа предлагает нам два варианта: алгоритм DSS/Диффи-Хеллмана и – RSA. Алгоритм Диффи-Хеллмана используется только для кодированной передачи ключа сессии симметричного шифрования и не пригоден для кодирования обычных сообщений, поэтому выбираем RSA, для чего набираем цифру 2 (рис. 32).

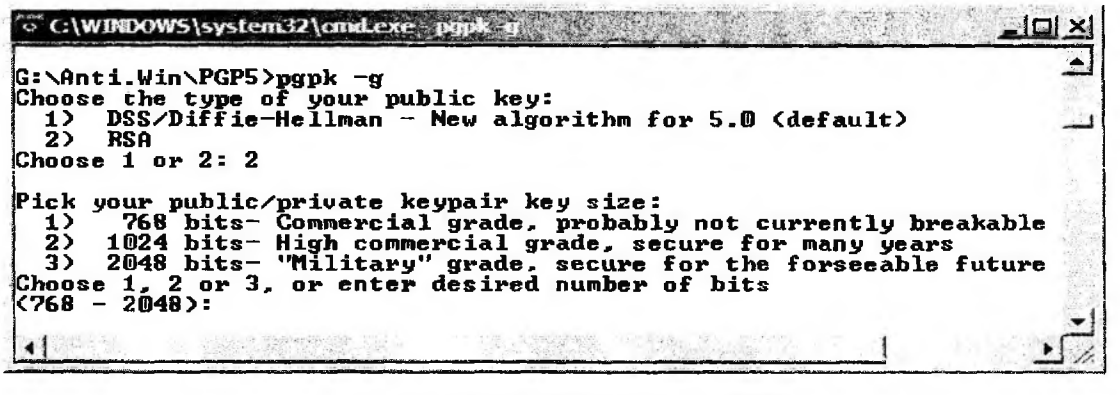


Рис. 32. Запрос размера ключа

Теперь программа спрашивает, какой длины ключ шифрования мы хотели бы выбрать? От длины ключа зависит криптостойкость зашифрованных данных, но с другой стороны шифрование с длинными ключами происходит медленнее. Для мощного компьютера выбираем третий вариант (рис. 33).

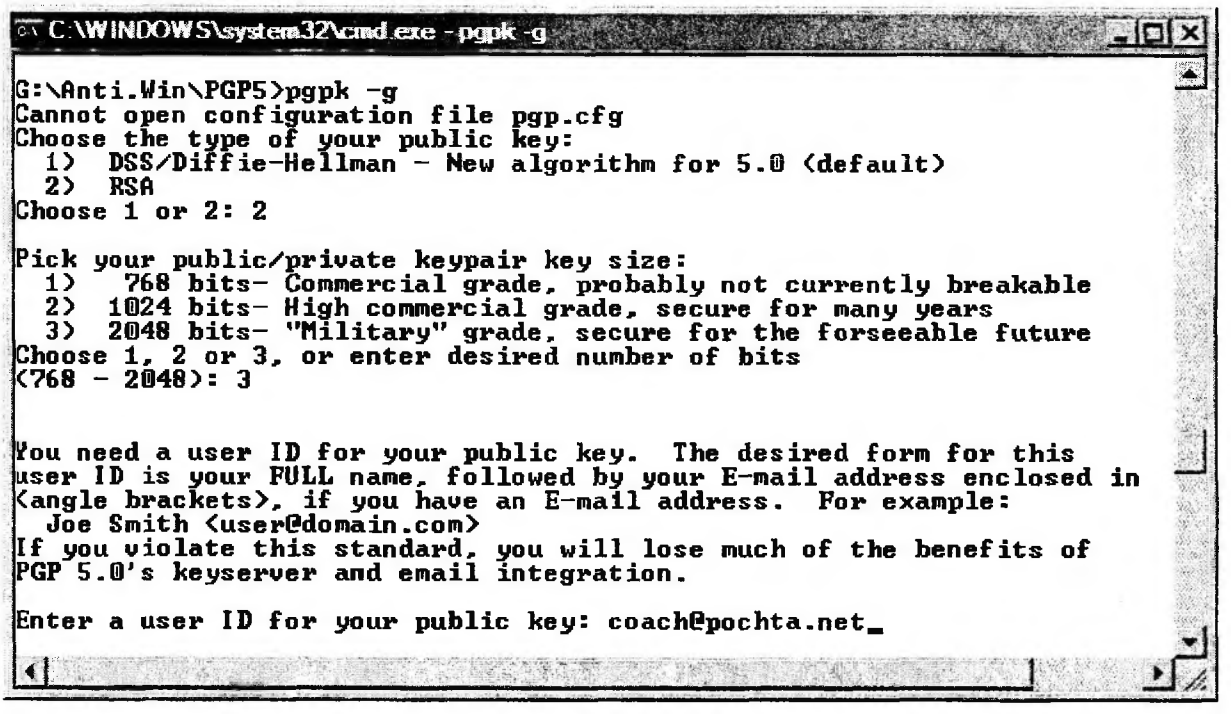


Рис. 33. Запрос открытого идентификатора пользователя

Далее программа спрашивает идентификатор пользователя, создающего ключи. Нет особых ограничений на длину и синтаксис этого идентификатора – это открытые данные, которые впоследствии могут использовать ваши корреспонденты по переписке. Чаще всего это адрес электронной почты пользователя, как показано на копии экрана.

Следующий шаг – программа спрашивает: «Сколько дней вы собираетесь пользоваться вашими ключами?». Принимаем решение – год (365 дней) (рис. 34).

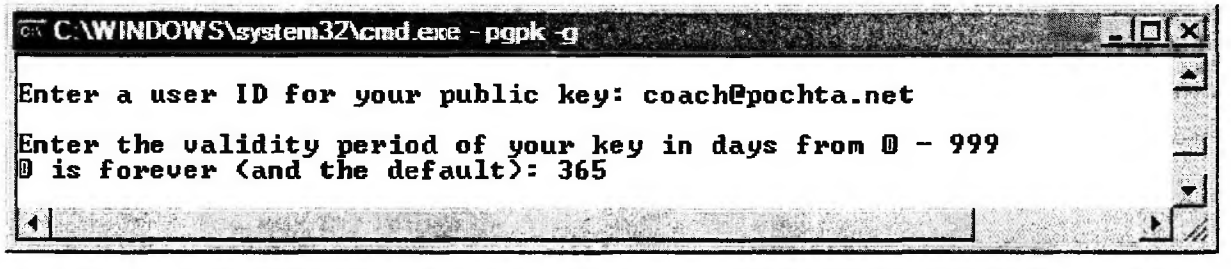


Рис. 34. Запрос срока действия пары создаваемых ключей

Дальше программа просит ввести пароль для private-ключа. Эти данные являются закрытыми, и никто кроме вас ключ этот знать не должен (рис. 35).

Пароль вводится два раза.

Для создания ключей программа просит выступить вас в роли генератора случайных чисел: путём случайного и беспорядочного постукивания по клавиатуре вы создаёте для программы набор случайных временных интервалов, создавая тем самым случайную последовательность. Сделайте это (только не разбейте клавиатуру!) (рис. 36).

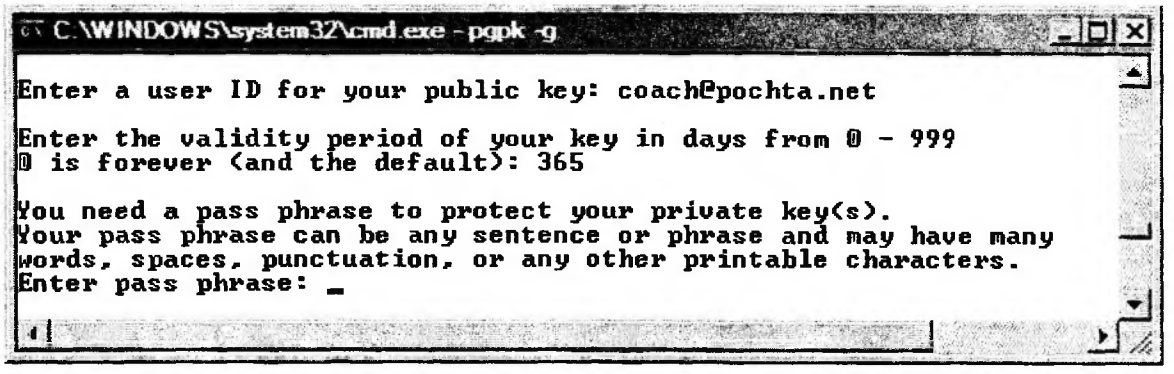


Рис. 35. Запрос на ввод закрытого пароля для private-ключа

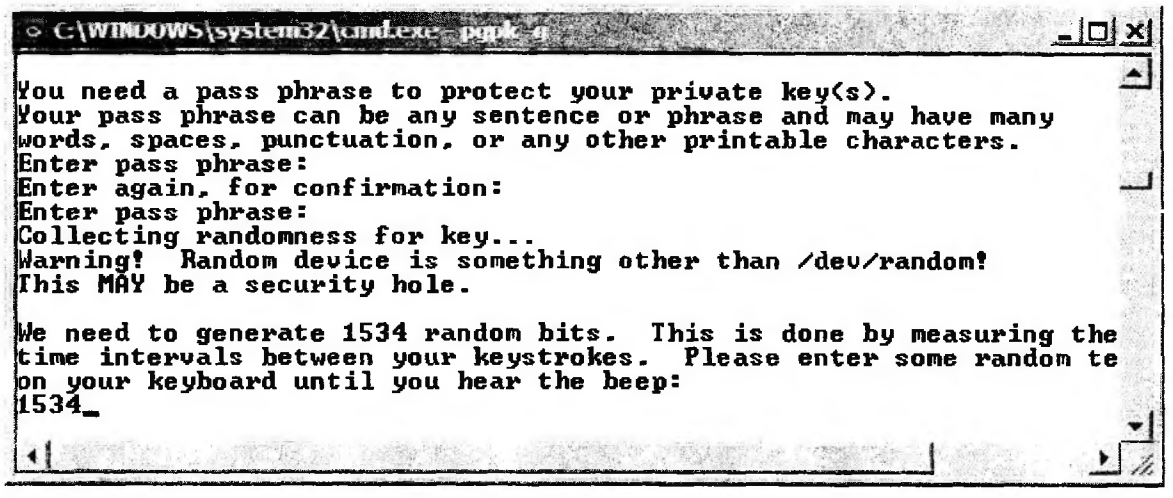


Рис. 36. Запрос активных действий пользователя для создания случайной последовательности

После информации об успешном создании ключей, программа вас с этим поздравляет, выходит из интерактивного режима, и вы вновь оказываетесь в режиме командной строки (рис. 37).

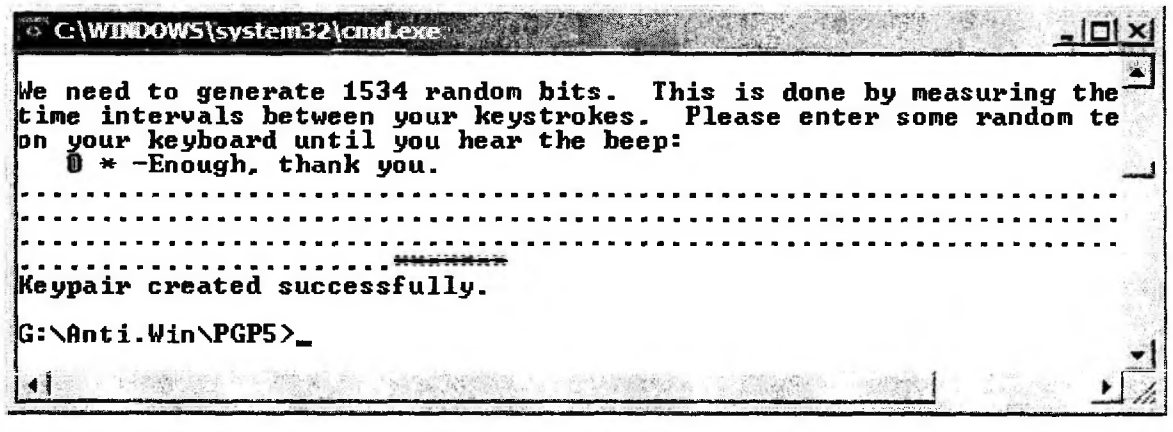


Рис. 37. Выведенное на терминал сообщение программы PGP об успешном создании пары ключей

Упражнение для самостоятельной работы 9. Проверьте доступными вам средствами, появились ли в текущем каталоге файлы пары ключей `pubring.pkr` и `secring.skr`?

Упражнение для самостоятельной работы 10. Как вы думаете, зачем программа создала в текущем каталоге ещё пару файлов - `pubring.bak` и

secring.bak – причём нулевой длины? Когда бы эти файлы были не нулевой длины? Сделайте выводы.

2.3.3. Создание зашифрованного сообщения с помощью открытого ключа

Теперь всё готово для кодирования сообщений методом асимметричного шифрования по алгоритму RSA. Закодируем файл vern.txt. Для этого в командной строке набираем (рис. 38):

```
pgpe -r ID file_name -o output_file_name.
```

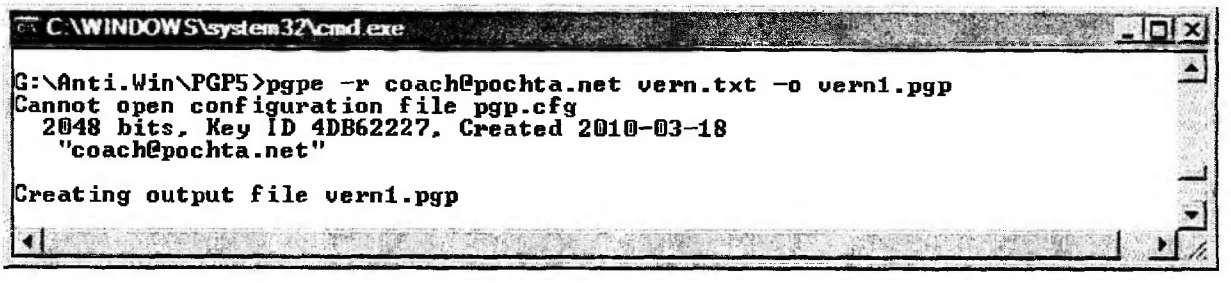


Рис. 38. Сообщение программы PGP об успешном кодировании данных

Все опции в командной строке вам уже знакомы за исключением ID – это тот самый открытый идентификатор вашего корреспондента, например, адрес его электронной почты. Свой публичный ключ pubring.pkr он уже выложил на почтовый сервер или прислал вам непосредственно и вы его заблаговременно положили в текущий каталог.

Зашифрованный файл vern1.pgp создан, можете его посылать своему корреспонденту по открытым сетям, пусть хакеры поломают голову над его криптоанализом. Только ваш корреспондент, имея private-ключ secring.skr, может декодировать и прочитать сообщение.

Здесь следует отметить ещё одну полезную опцию программы. На очередной копии экрана показана опция -a. Это позволяет провести шифрование, используя только первую половину кодовой таблицы ASCII, то есть используя не весь байт (восемь бит), а только младшие разряды байта – 7-битовую кодировку. Шифрованное сообщение будет состоять только из печатываемых символов. За такое «удобство» приходится расплачиваться более длинным (на 20–30 %) зашифрованным сообщением. Во-вторых, вы обезопасите себя, если ваше зашифрованное сообщение vern1a.pgp «забредёт» в старые дремучие компьютерные сети, поддерживающие только 7 младших бит и усекающие старший 8-й бит, то целостность сообщения нарушена не будет (рис. 39).

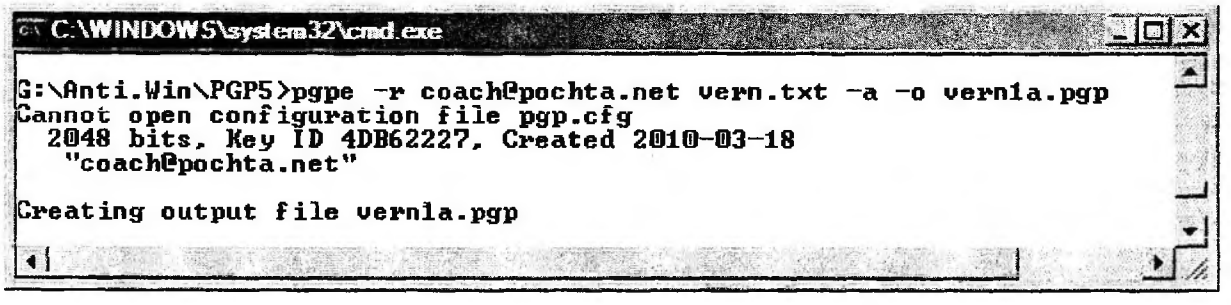


Рис. 39. Сообщение программы PGP об успешном кодировании данных первой половиной стандартной кодовой таблицы

Упражнение для самостоятельной работы 11. Сравните размеры полученных зашифрованных файлов: vern1.pgp и vern1a.pgp. Доступными вам средствами просмотрите файлы vern1.pgp и vern1a.pgp. Обратите внимание, что в файле vern1.pgp присутствуют все 256 символов, из всего диапазона кодовой таблицы (00 - FFhex), в то время как в файле vern1a.pgp только первые 128 символов (00 - 79hex). Сделайте выводы.

2.3.4. Декодирование принятого зашифрованного сообщения с помощью private-ключа

Ваш корреспондент получил зашифрованное сообщение. Для того, чтобы его прочитать, корреспондент должен декодировать (расшифровать) сообщение, используя свой private-ключ. Для этого в командной строке терминала он должен набрать

```
pgpv file_name -o output_file_name.
```

Теперь программа, прежде чем приступить к процессу декодирования, в интерактивном режиме попросит вас ввести пароль. Будьте аккуратны, имейте в виду, при вводе пароля эта программа никак не реагирует на ваши нажатия клавиш: не подает звуковых сигналов, курсор не перемещается, никаких символов-звёздочек не появляется. Завершение ввода пароля подтверждается клавишей [Enter].

Если вы сделали всё правильно, программа сообщит, что пароль правильный (Pass phrase is good) и декодирует зашифрованный файл (рис. 40).

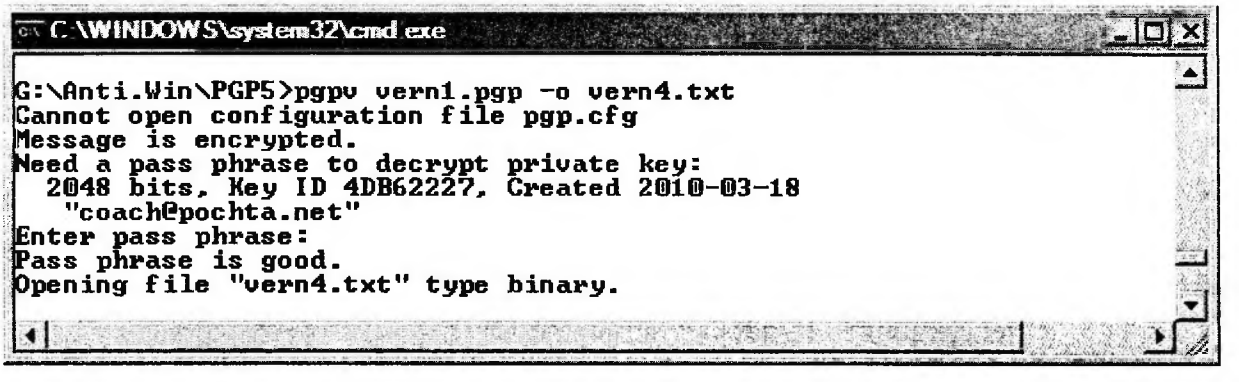


Рис. 40. Запрос пароля и сообщение программы PGP об успешном декодировании данных

В этой операции программа будет использовать private-ключ и спросит пароль (видно на копии экрана). В случае совпадения паролей будет проведено декодирование файла vern1.txt в файл vern4.txt.

Декодирование 7-битного файла vern1a.txt в файл vern4a.txt происходит аналогично, с теми же опциями командной строки, не надо указывать, что в файле присутствуют символы только первой половины кодовой таблицы, программа сама в этом разберётся. Это показано на следующей копии экрана (рис. 41).

Упражнение для самостоятельной работы 12. Сравните размеры и содержимое файлов vern.txt, vern4.txt и vern4a.txt. Одинаковое ли у них содержимое? Нарушена ли целостность файла vern.txt при кодировании/декодировании алгоритмом RSA? Сделайте соответствующие выводы.

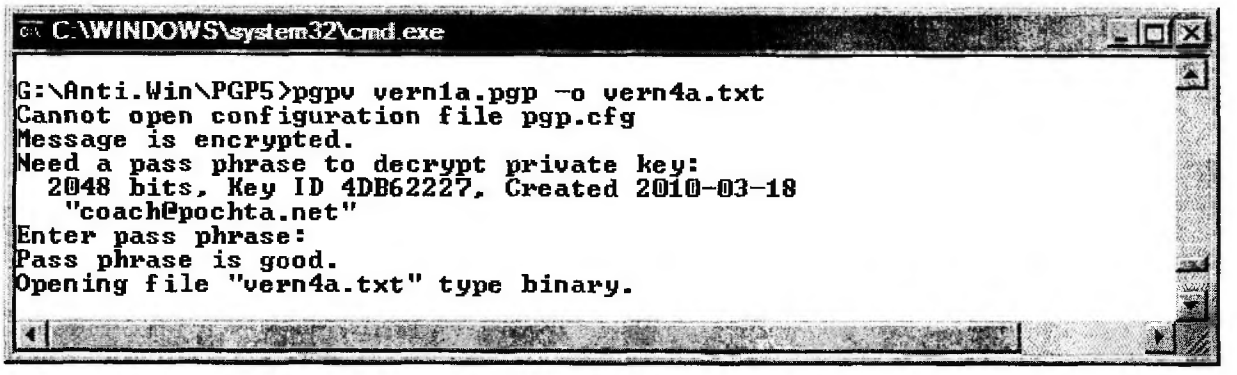


Рис. 41. Запрос пароля и сообщение программы PGP об успешном декодировании данных, использующих только первую половину кодовой таблицы

2.3.5. Кодирование и декодирование сообщения с помощью произвольного ключа

Вполне нормальна и типична ситуация, когда пакетом PGP и алгоритмом RSA захочет воспользоваться другой пользователь этого компьютера и создать свою пару ключей. Но программа по умолчанию создаст пару pubring.pkr и secring.skr и затрёт существующие ваши ключи. Для решения этой проблемы и однозначной идентификации, обычно, каждый пользователь переименовывает свою пару ключей в соответствии со своими вкусами. В командной строке пакету PGP необходимо указать, ключ какого пользователя вы хотите употребить. Новые ключи необходимо зафиксировать в файле pgp.cfg. Если этого не сделать, программа будет сообщать об отсутствии этого файла, что проиллюстрировано на рис. 42. Это не является ошибкой и не сказывается на работоспособности пакета, просто вы должны теперь каждый раз указывать эти параметры в командной строке.

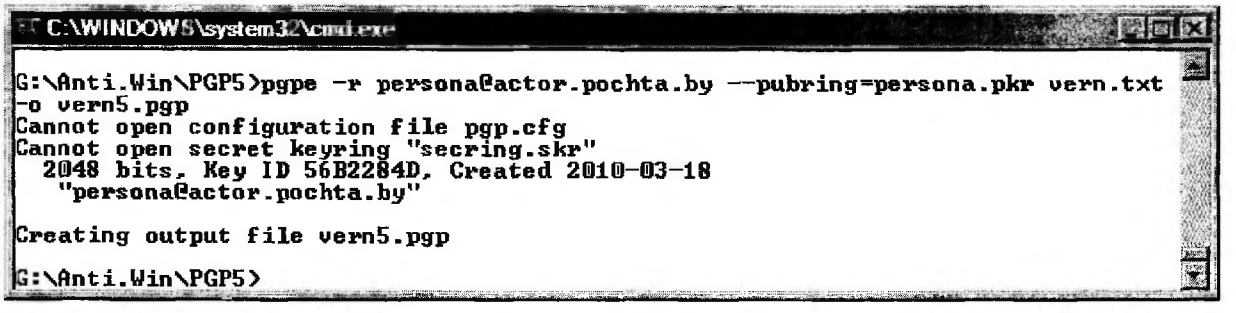


Рис. 42. Кодирование данных программой PGP произвольным публичным ключом пользователя

Это делается следующим образом. В командной строке терминала набираем:

```
pgpe -r ID --pubring=persona.pkr file_name -o output_file_name.
```

Идентификатор (ID) должен быть того пользователя, чей ключ вы используете, того, кому вы намереваетесь отправить сообщение, иначе получите от программы сообщение об ошибке. В данном примере пользователю Persona соответствует идентификатор его электронной почты persona@actor.pochta.by и пара ключей persona.pkr, persona.skr.

На приведенной копии экрана (см. рис. 42) видна работа программы и её сообщения.

Если ключи persona.pkr, persona.skr находятся не в текущем каталоге, то в соответствующей опции командной строки --pubring=.. указываем полный путь к файлу: --pubring=full_path\persona.pkr.

Аналогичная ситуация, если пользователь Persona получил закодированное сообщение и хочет его расшифровать, употребив свой не стандартно именованный private-ключ, тогда в командной строке он набирает

```
pgpv --secring=persona.skr file_name -o output_file_name.
```

Работа программы проиллюстрирована на рис. 43.

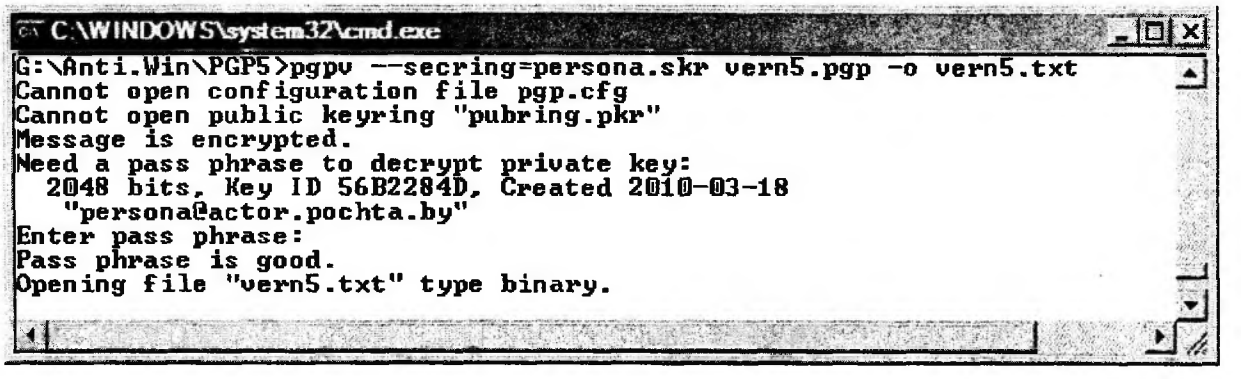


Рис. 43. Запрос пароля и декодирование данных программой PGP произвольным private-ключом пользователя

2.3.6. Аутентификация сообщения. Создание простой цифровой подписи в пакете PGP

Весьма важной является задача опознания, аутентификация пришедшего электронного сообщения, то есть, действительно ли пришедшее сообщение принадлежит тому лицу, подпись которого стоит под электронным сообщением? Здесь проблема конфиденциальности уходит на второй план, а на первый план выступает проблема целостности, то есть, не «лазил» ли кто в документ и не изменил ли его содержимое, и не приписал ли «лишний нолик» в цифре вашего платежа?

Описываемый пакет PGP предлагает несколько вариантов. Разберём их. Persona решил разослать своим корреспондентам важное сообщение, но шифрует сообщение private-ключом?! Наверно ошибся, переволновался и напутал! Нет, правильно. Алгоритм RSA работает в обе стороны, и кодировать сообщение можно private-ключом. Но тогда каждый имеющий публичный ключ Persona может легко расшифровать сообщение. И где же тут секретность, конфиденциальность? А она тут не нужна, гораздо важнее то, что декодировав сообщение Persona ключом persona.pkr вы убедились, что ключ подошёл, тем самым решаются две важнейшие вещи:

- это сообщение действительно от Persona (иначе этим ключом какое-либо иное сообщение декодировать бы не удалось), тем самым осуществлена аутентификация сообщения Persona;
- целостность сообщения в пути следования не нарушена, для этого злоумышленник должен бы был, во-первых, расшифровать сообщение (это он может сделать, имея persona.pkr – публичный ключ Persona), во-вторых, изменить данные и, в-третьих, снова их зашифровать (подписать) – но это невозможно, поскольку private-ключ вместе с паролем находится только у Persona.

2.3.7. Создание цифровой подписи и сообщения единым файлом

В командной строке терминала набираем

```
pgps -u ID --secring=persona.skr file_name -o output_file_name.
```

Эта команда кодирует файл vern.txt private-ключом и создаёт файл vern.pgp, содержащий цифровую подпись (рис. 44).

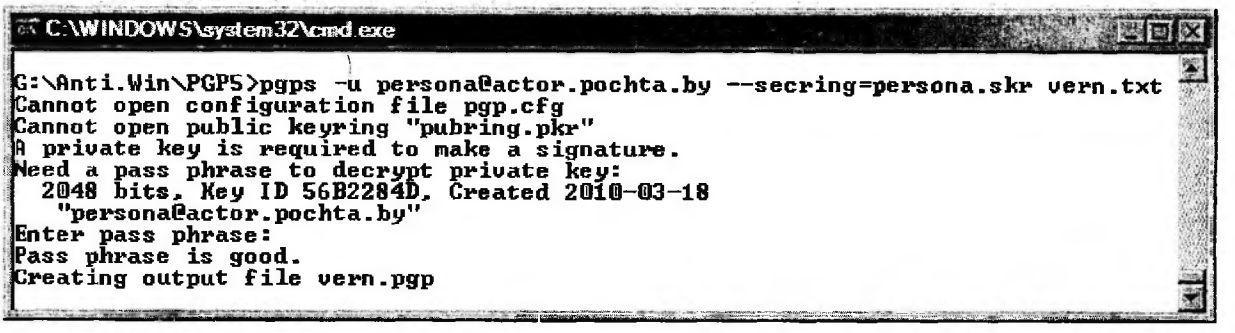


Рис. 44. Запрос на ввод пароля и создание цифровой подписи программой PGP произвольным private-ключом пользователя

На копии экрана (см. рис. 44) мы видим, что для этой операции программа PGP требует пароль.

2.3.8. Создание цифровой подписи отдельным файлом

Можно создать цифровую подпись отдельным файлом, а само сообщение оставить открытым и незашифрованным.

В командной строке терминала набираем предыдущую команду, указав дополнительную опцию -b (рис. 45):

```
pgps -u ID -b --secring=persona.skr file_name.
```

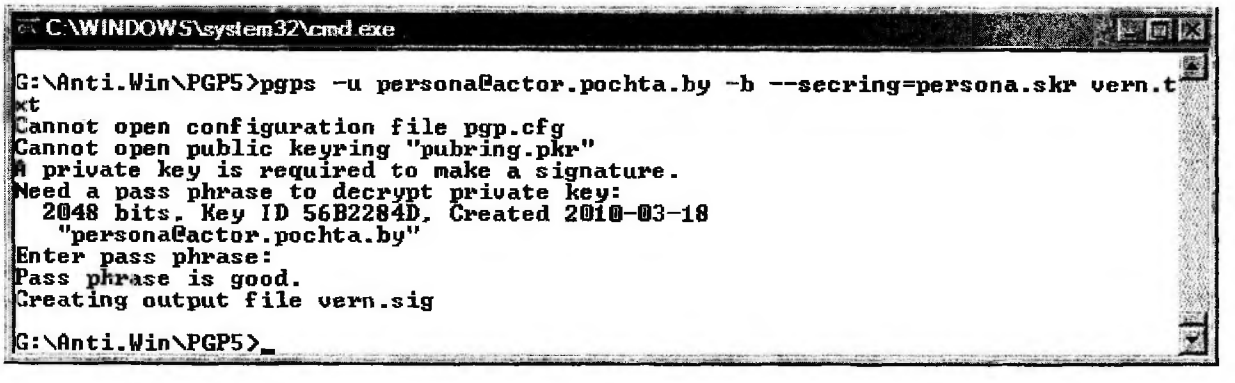


Рис. 45. Запрос на ввод пароля и создание цифровой подписи отдельным файлом

На копии экрана (см. рис. 45) мы видим, что программа создала файл цифровой подписи vern.sig. Изначальный файл vern.txt с данными не модифицировался.

Упражнение для самостоятельной работы 13. Посмотрите, какой размер у файла vern.sig. Много это или мало?

2.3.9. Верификация цифровой подписи

Вы получили файл `vern.txt` вместе с цифровой подписью `vern.sig` и хотите проверить (верифицировать), соответствует ли эта цифровая подпись полученным данным. Для этого нам нужен только лишь открытый, публичный ключ того лица, которое создало и подписало эти данные. Публичный ключ Persona у нас имеется. В командной строке набираем:

```
pgpv vern.sig --pubring=persona.pkr.
```

После запуска этой команды программа PGP переходит в интерактивный режим и просит вас ввести файл с данными, соответствующий цифровой подписи vern.sig. Мы набираем vern.txt, если файл с данными находится в другом каталоге, необходимо указать полный путь к файлу (рис. 46).

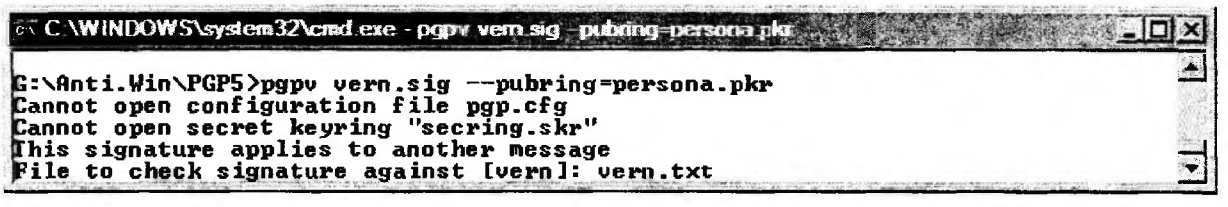


Рис. 46. Этап верификации цифровой подписи: запрос на ввод имени верифицируемого файла

Когда путь к файлу введен, программа продолжит работу: сообщит, во-первых, идентификатор пользователя, поставившего цифровую подпись и, во-вторых, результат верификации. Сообщение на копии экрана (рис. 47) «`Good signature`» означает, что верификация прошла успешно.

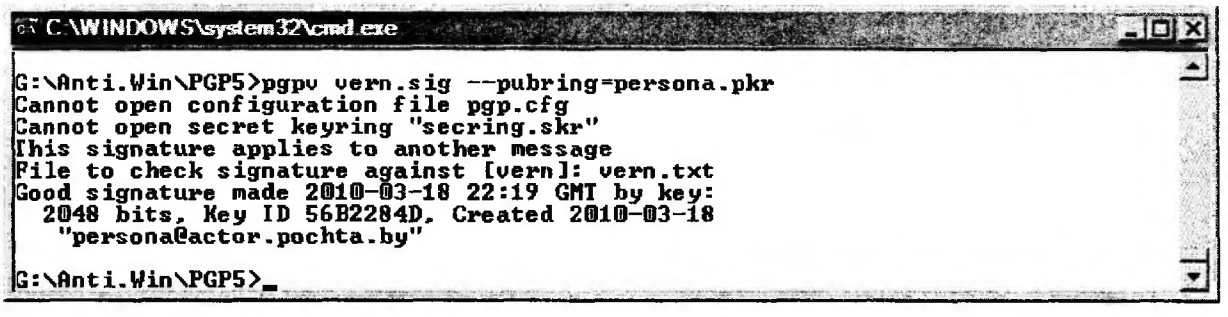


Рис. 47. Этап верификации цифровой подписи: завершение и сообщение об успешной верификации

Упражнение для самостоятельной работы 14. Измените хотя бы один бит в файле `vern.txt`. Постарайтесь не менять размер файла. Попытайтесь сделать верификацию так, как описано выше.

2.3.10. Сбой верификации цифровой подписи

Допустим, злоумышленник изменил подписанные данные (или вы старательно и правильно выполнили последнее самостоятельное упражнение). Как пройдёт верификация?

Осуществляем верификацию, как описано в предыдущем подразделе 2.3.9. Выполняем ту же команду:

```
pgpv vern.sig --pubring=persona.pkr.
```

Снова указываем путь к файлу с данными, но теперь, обратите внимание (рис. 48), программа вывела идентификатор лица, поставившего цифровую подпись и, во-вторых, вывела тревожное сообщение: «BAD signature» – это означает, что целостность файла с данными нарушена, данные кто-то менял и модифицировал, уже после того как была создана цифровая подпись.

Мы научились создавать и верифицировать простую цифровую подпись. Это механизм хорошо работает, если стороны доверяют друг другу. Однако, в жизни, в производственной деятельности, в бизнесе, к сожалению, возникают ситуации, когда мы с подозрением относимся к партнёру.

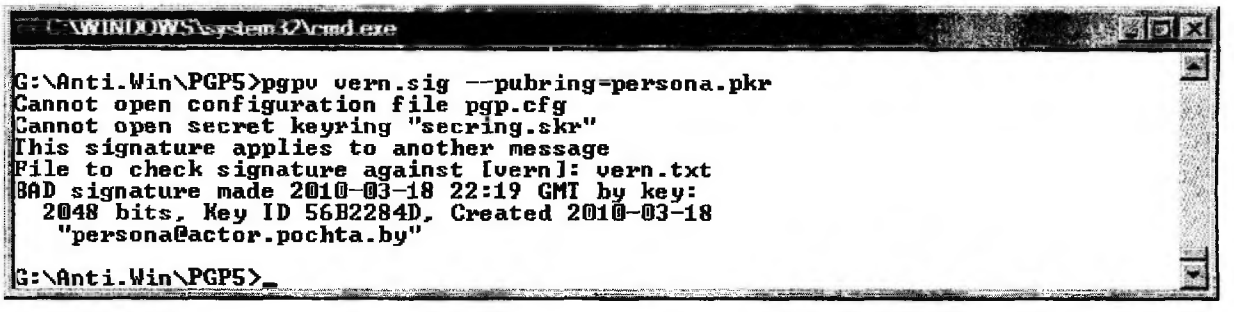


Рис. 48. Этап верификации цифровой подписи:
завершение и сообщение о сбое верификации

Типичный пример, вся финансовая работа банка видна из правильно составленного годового бухгалтерского баланса, тем не менее, в финансовых кругах не очень доверяют такому балансу. И администрация банка вынуждена, часто за значительные средства, привлекать независимую нейтральную организацию-арбитра, называемую аудиторской фирмой, которая составляет такой баланс. Баланс, составленный независимой аудиторской фирмой, имеет значительно более высокий рейтинг и может служить «доверительной» визитной карточкой финансового благополучия предприятия.

Так и с арбитражной цифровой подписью: если в своей переписке корреспонденты не доверяют друг другу, то они ищут третью, нейтральную доверительную сторону – арбитра. Механизм создания и использования арбитражной подписи подробно разобран в подразделе 1.6.7, поэтому практическое задание по созданию арбитражной подписи выносится в самостоятельное упражнение.

Упражнение для самостоятельной работы 15. Привлеките на помощь друга. Создайте ещё пару ключей. Выберите арбитра. Создайте арбитражную цифровую подпись, как описано в подразделе 1.6.7.

Список использованных источников

1. Баричев, С.Г. Криптография без секретов / С.Г. Баричев. – М.: Горячая Линия – Телеком, 2004. – 43 с.
2. Вишневский, А. Сетевые технологии Windows 2000 / А. Вишневский. – СПб.: Питер, 2000. – 591 с.
3. Домарёв, В.В. Защита информации и безопасность компьютерных систем / В.В. Домарёв. – Киев: Диалектика, 2004. – 670 с.
4. Касперски, К. Искусство дизассемблирования: наиболее полное руководство / К. Касперски, Е. Рокко. – СПб.: БХВ-Петербург, 2008. – 884 с.
5. Левин, М. Как стать хакером: интеллектуальное руководство по хакингу и фрикингу / М. Левин. – М.: Новый издательский дом, 2005. – 319 с.
6. Мак-Клар, С. Хакинг в Web. Атаки и защита / С. Мак-Клар, С. Шах, Ш. Шах. – М.: Вильямс, 2003. – 374 с.
7. Норткат, С. Обнаружение нарушений безопасности в сетях / С. Норткат, Д. Новак. – М.: Вильямс, 2003. – 447 с.
8. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие по специальности в области информационной безопасности / С.Н. Семкин [и др.]. – М.: Гелиос АРВ, 2005. – 185 с.
9. Скляров, Д.В. Искусство защиты и взлома информации / Д.В. Скляров. – СПб.: БХВ-Петербург, 2004. – 276 с.
10. Столингс, В. Криптография и защита сетей: принципы и практика / В. Столингс. – М.: Вильямс, 2001. – 669 с.
11. Хогланд, Г. Взлом программного обеспечения: анализ и использование кода / Г. Хогланд, Г. Мак-Гроу. – М.; СПб.; Киев: Вильямс, 2005. – 396 с.
12. Шнайер, Б. Секреты и ложь: безопасность данных в цифровом мире / Б. Шнайер. – СПб.: Питер, 2003. – 367 с.
13. Ярочкин, В.И. Информационная безопасность: учебник для вузов по гуманитарным и социально-экономическим специальностям / В.И. Ярочкин. – М.: Трикста; М.: Академический проект, 2005. – 543 с.

Учебное издание

ГАНЖА Виктор Александрович
СИДОРИК Валерий Владимирович
ЧИЧКО Ольга Ильинична

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ НАДЁЖНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Учебно-методическое пособие
для слушателей системы повышения квалификации
и переподготовки

Редактор Т.А. Подолякова

Подписано в печать 12.07.2010.
Формат 60×84 1/8. Бумага офсетная.
Отпечатано на ризографе. Гарнитура Bookman Old Style.
Усл. печ. л. 7,79. Уч.-изд. л. 3,05. Тираж 100. Заказ 489.

Издатель и полиграфическое исполнение:
Белорусский национальный технический университет.
ЛИ №02330/0494349 от 16.03.2009.
Проспект Независимости, 65. 220013, Минск.