Содержание

О книге 7
Предисловие 10
Введение 14

Глава I
Общие сведения по классической криптографии 21

1.1. Общие сведения 21
1.1.1. Стойкость алгоритмов шифрования 23
1.1.2. Типы алгоритмов шифрования 28
1.1.3. Аппаратная и программная реализация алгоритмов шифрования 31
1.2. Алгоритмы блочного шифрования 34
1.2.1. Общие сведения 34
1.2.2. Алгоритм DES 40
1.2.3. Алгоритм блочного шифрования 46
1.2.4. Применение алгоритмов блочного шифрования 51
1.3. Асимметричные алгоритмы шифрования 53
1.3.1. Общие сведения 53
1.3.2. Стандарт асимметричного шифрования RSA 55
1.3.3. Стойкость алгоритма RSA 57
1.3.4. Методы ускорения вычислений, применяемых в асимметричных алгоритмах 59
1.3.5. Практическое применение 62
1.4. Электронно-цифровая подпись 65
1.4.1. Общие положения 65
1.4.2. Атаки на ЭЦП 68
1.4.3. Алгоритм DSA 70
1.4.4. Стандарт на процедуры выработки и проверки ЭЦП 72
1.4.5. Практическое применение ЭЦП 74
1.4.6. Арбитраж ЭЦП 76
1.5. Хэш-функции 78
1.5.1. Общие сведения 78
1.5.2. Типы хэш-функций 79
1.5.3. Требования к хэш-функциям 83
1.5.4. Стойкость хэш-функций 84

1.6. Ключевая информация ... 85
1.6.1. Общие сведения ... 85
1.6.2. Генерация ключевой информации ... 86
1.6.3. Хранение ключей ... 88
1.6.4. Распределение ключей ... 89
1.6.5. Минимальная длина ключа ... 90

Глава II
Теоретические аспекты создания и применения криптографических протоколов ... 93
2.1. Общие сведения ... 93
2.1.1. Область применения ... 93
2.1.2. Вопросы безопасности криптопротоколов ... 95
2.1.3. Формальные методы анализа криптопротоколов ... 99
2.2. Протоколы аутентификации ... 104
2.2.1. Общие сведения ... 104
2.2.2. Простая аутентификация ... 109
2.2.3. Строгая аутентификация ... 113
2.2.4. Протоколы аутентификации, обладающие свойством доказательства с нулевым знанием ... 121
2.3. Протоколы распределения и управления ключевой информацией ... 124
2.3.1. Протоколы распределения ключевой информации ... 124
2.3.2. Управление ключевой информацией ... 139
2.4. Специфические криптографические протоколы ... 157
2.4.1. Безопасные выборы ... 157
2.4.2. Совместная подпись контракта ... 159
2.4.3. Групповая подпись ... 160
2.4.4. Доверенная подпись ... 161
2.4.5. Неоспариваемая подпись ... 162
2.4.6. Слепая подпись ... 163
2.4.7. Забывающая передача ... 165
2.4.8. Подбрасывание монеты по телефону ... 166
2.4.9. Разделение знания секрета ... 167

Глава III
Компьютерная безопасность и практическое применение криптографии ... 169
3.1. Общие сведения ... 169
3.1.1. Физический и канальный уровни ... 176
3.1.2. Сетевой уровень ... 177
3.1.3. Транспортный уровень ... 179

3.1.4. Прикладной уровень ... 179
3.1.5. Обзор стандартов в области защиты информации ... 180
3.1.6. Подсистема информационной безопасности ... 185
3.2. Защита локальной рабочей станции ... 189
3.2.1. Угрозы и задачи информационной безопасности для локальных рабочих станций ... 190
3.2.2. Методы и средства обеспечения информационной безопасности локальных рабочих станций ... 196
3.2.3. Организационно-технические меры защиты локальной рабочей станции ... 216
3.2.4. Штатные средства защиты современных операционных систем на примере Windows NT ... 221
3.2.5. Аудит ... 229
3.3. Защита в локальных сетях ... 231
3.3.1. Общие вопросы безопасности в ЛВС ... 232
3.3.2. Безопасность в сетях Novell NetWare ... 237
3.3.3. Безопасность в сетях Windows NT ... 241
3.3.4. Система Secret Net NT ... 257
3.4. Защита информации при межсетевом взаимодействии ... 260
3.4.1. Общие сведения ... 260
3.4.2. Обеспечение защиты информации при построении VPN ... 270
3.5. Защита технологии «клиент-сервер» ... 292
3.5.1. Типовые угрозы и обеспечение информационной безопасности при использовании технологии «клиент-сервер» ... 294
3.5.2. Подходы, применяемые к обеспечению информационной безопасности в клиент-серверных ИВС ... 300
3.5.3. Криптографические протоколы, используемые для защиты технологии «клиент-сервер» ... 302
3.5.4. Решения по защите информации в Web-технологиях ... 312
3.6. Применение межсетевых экранов ... 317
3.6.1. Пакетные фильтры ... 318
3.6.2. Шлюзы сеансового уровня ... 320
3.6.3. Шлюзы уровня приложений ... 321
3.6.4. Использование межсетевых экранов для создания VPN ... 323
3.6.5. Proxy-серверы ... 324
3.6.6. Виды подключения межсетевых экранов ... 326
3.6.7. Использование межсетевых экранов ... 328
3.6.8. Применение криптографии в межсетевых экранах на примере CheckPoint Firewall-1 ... 329

3.7. Защита электронной почты ... 336
3.7.1. Принципы защиты электронной почты ... 337
3.7.2. Средства защиты электронной почты ... 340
3.7.3. Защита в архитектуре X.400 ... 351
3.8. Корпоративные системы и опыт обеспечения информационной безопасности в них ... 361
3.8.1. Система S.W.I.F.T. ... 361
3.8.2. Технология SmartCity ... 372
3.8.3. Система UEPS ... 380
3.9. Электронные платежные системы и Internet ... 382
3.9.1. Классификация платежных систем ... 383
3.9.2. Теоретические основы электронных денег ... 393
3.9.3. Смарт-карты ... 397
3.9.4. Средства обеспечения безопасности электронных платежных систем ... 401
Приложение 1. Сравнительные характеристики отечественных средств построения VPN ... 407
Приложение 2. Система санкционированного доступа к ресурсам корпоративной информационной системы ... 418
Приложение 3. Ресурсы в Internet, посвященные вопросам компьютерной безопасности ... 433
Список рекомендуемой литературы ... 437

О книге

В настоящее время издано много руководств, справочников, пособий по проблемам защиты информации. Это и переводные книги, и оригинальные работы отечественных авторов, и вузовские учебники. У подавляющего большинства авторов книги либо чересчур «теоретичны», либо предельно популярны. И то, и другое отпугивает читателей-практиков, которым понимание теории необходимо для ее конкретного применения.

Монография А. Петрова «Компьютерная безопасность. Криптографические методы защиты» является в этом смысле приятным исключением. Наряду с описанием шифрующих преобразований и цифровой подписи в книге содержатся и актуальные сведения о современных криптографических протоколах, и практическая информация, посвященная принципам применения имеющихся на рынке сертифицированных криптографических средств («Криптон», «Верба», «Шип», «Игла» и др.).

Нельзя не отметить и те разделы книги, в которых излагаются теоретические основы компьютерной безопасности. Здесь впервые систематизированы и всесторонне рассмотрены атаки на современные компьютерные системы и различные способы защиты от них.

Монография, несомненно, представляет интерес для широкого круга читателей, в том числе обучающихся по типовым программам специальностей «Введение в криптографию», «Компьютерная безопасность», «Программно-аппаратные средства обеспечения информационной безопасности».

А. Ю. Щербаков,
доктор технических наук, научный консультант подразделения ФАПСИ,
руководитель группы систем защиты от информационного оружия,
почетный член Европейской ассоциации хакеров,
профессор кафедры «Информационная безопасность»
Московского государственного института электроники и математики

Разработчикам информационных систем повышенной сложности, таких как корпоративные информационные системы или информационные системы масштаба крупного предприятия, в последнее время приходится решать задачи, удачное решение которых полностью зависит от точного соблюдения основополагающих и общепринятых правил проектирования и эксплуатации виртуальных конструкций, как-то:

- поддержка стандартов, подразумевающая соответствие общепринятым технологическим стандартам, которыми руководствуются фирмы-производители программного обеспечения;
- масштабируемость, означающая, что программное обеспечение должно работать с приемлемой производительностью без внесения в него существенных изменений при увеличении мощности и количества используемого оборудования;
- многозвенность, где требуется, чтобы каждый уровень системы (клиент, Web-сервер, сервер приложений, сервер баз данных) отвечал и реализовывал только те функции, которые ему наиболее присущи;
- обеспечение (по возможности) аппаратно-платформенной независимости программного обеспечения, используемого при разработке системы;
- коммуникативность и интегрированность, что означает возможность различных уровней системы взаимодействовать между собой, как по данным, так и по приложениям;
- защищенность.

Безусловно, существуют и другие, менее важные задачи, но здесь хотелось бы отметить, что любая из перечисленных проблем внедрения корпоративных информационных систем на базе технологий Internet/intranet может быть успешно реализована только при наличии хорошо организованных средств защиты информации, централизованного управления информационными ресурсами и разграничения доступа к ним. Особенно это важно при обеспечении доступа пользователей из внешних сетей к ресурсам корпоративной ИС по так называемой extranet-технологии.

Как раз одному из этих направлений – защите информации в распределенных сетях – и посвящена книга А. Петрова «Компьютерная безопасность. Криптографические методы защиты», которую мне особенно приятно представить коллегам и читателям.

На сегодняшний день обеспечение безопасности потоков данных является одним из самых перспективных направлений науки и техники, имеющих большое теоретическое и практическое значение.

Автору удалось собрать в книге солидный фактический материал, систематизировать его, изложить свою точку зрения по конкретным вопросам, касающимся практического использования не только отечественных, но и зарубежных криптографических методов и средств защиты информации.

В приложениях, написанных сотрудниками ЦБ России, приведен список известных серверов по проблемам защиты информации. Эти сведения, безусловно, позволят читателям расширить свои знания в данной области.

Я надеюсь, что после знакомства с представляемой книгой моим коллегам станут ближе и понятнее проблемы защиты информации, в том смысле, что работа начинается с проектирования архитектуры информационной системы и заканчивается выбором средств на уровне шифрования.

Занимаясь вопросами создания реальных информационных систем, нам часто не хватает времени познакомиться и тем более сравнить различные варианты реализации средств защиты информации. Надеюсь, что данная книга и приложения к ней позволят уважаемым читателям и коллегам различить новые направления в такой широкой и в то же время такой специальной теме, как проблема построения защищенных информационных систем.

В. С. Лаптев,
кандидат технических наук,
президент Фонда развития программной инженерии

Предисловие

В настоящее время первостепенным фактором, влияющим на политическую и экономическую составляющие национальной безопасности, является степень защищенности информации и информационной среды. Вот почему важное значение приобретают вопросы обеспечения безопасности информационных и телекоммуникационных технологий и гарантированной защиты данных в компьютерных сетях экономически значимых структур. О необходимости надежной защиты свидетельствуют многочисленные компьютерные преступления, совершаемые как в кредитно-финансовой сфере, так и в государственных органах. При этом заметно увеличилось число противоправных деяний, совершенных путем удаленных атак с использованием территориально-распределенных сетей передачи данных. Подобные правонарушения опасны тем, что на сегодняшний день устоявшейся практики борьбы с ними не существует.

Вместе с тем необходимо отметить, что, несмотря на резкое возрастание интереса к проблемам защиты информации, в отечественной научно-технической литературе данная тема освещена слабо, и автор в меру своих сил попытался заполнить этот пробел. В предлагаемой книге рассматриваются вопросы применения криптографии для защиты информации в современных информационно-телекоммуникационных системах, отражающие только одну из областей компьютерной безопасности, однако, на взгляд автора, на сегодняшний день наиболее значимую. В книге освещаются как теоретические аспекты применения классической криптографии (глава 1) и современных криптографических протоколов (глава 2), так и практические вопросы (глава 3), которые возникают при осуществлении защиты информации криптографическими методами и средствами.

В данной книге также затрагиваются проблемы защиты платежных систем в Internet, безопасность современных операционных систем (Windows NT и Novell NetWare) и ряд других актуальных вопросов компьютерной безопасности.

Во введении обсуждается терминология, а также цели и задачи, возникающие при обеспечении информационной безопасности. Здесь определяется роль криптографических протоколов как наиболее перспективного

средства защиты в общей задаче сохранения конфиденциальности, целостности и достоверности информационных потоков.

В главе 1 рассматриваются некоторые теоретические аспекты криптографии и описаны способы построения часто используемых на сегодняшний день криптографических алгоритмов. Раздел 1.1 посвящен теоретическим основам применения и реализации криптографических алгоритмов в современных информационно-телекоммуникационных системах. В разделе 1.2 представлены традиционные блочные алгоритмы шифрования; здесь же изложены принципы блочного шифрования и виды применения подобных алгоритмов, а также конкретные алгоритмы – DES и ГОСТ 28147-89. Раздел 1.3 знакомит с асимметричными алгоритмами шифрования; в нем уделяется внимание математическим идеям, а также получившему широкое распространение алгоритму RSA (с точки зрения уязвимости и возможности проведения на него теоретических атак и с точки зрения эффективности его реализации). В разделе 1.4 рассказывается об электронно-цифровой подписи (ЭЦП); при этом разбираются не только конкретные схемы (ГОСТ Р 34.10-94 и DSA), но и атаки на схемы ЭЦП, а также вопросы, связанные с арбитражем ЭЦП. В разделе 1.5 описываются хэш-функции, используемые совместно с алгоритмами ЭЦП, и затрагиваются вопросы их стойкости. В разделе 1.6 излагаются вопросы, связанные с генерацией, хранением и распределением ключей. Здесь также рассматривается актуальный на сегодняшний день вопрос о минимальной длине ключа, необходимой для обеспечения адекватного уровня безопасности.

Вторая глава посвящена интересным и острым на сегодняшний день проблемам построения, реализации и применения криптографических протоколов, таких как протоколы аутентификации, протоколы распределения и управления ключевой информацией и специфические протоколы. В разделе 2.1 излагаются основные принципы их построения и безопасного использования, а также формальные методы их анализа. Несмотря на то что подобные протоколы до сих пор считаются мощным средством обеспечения безопасности в современных информационно-телекоммуникационных системах, в настоящий момент в хорошо известных протоколах уже найдено немало уязвимых мест. В разделе 2.2 обсуждаются различные схемы аутентификации, начиная с простой аутентификации и заканчивая аутентификацией, обладающей свойством нулевого знания. В разделе 2.3 рассматривается недостаточно освещенная в отечественной литературе проблема распределения и управления ключевой информацией, причем описываются протоколы с использованием симметричных и асимметричных алгоритмов. Одной из главных трудностей, возникающих при построении криптографической системы защиты информации в распределенных

системах, как раз является распределение ключевой информации, поэтому данный раздел в современном контексте развития Internet особенно актуален. Кроме этих проблем в разделе 2.3 затронуты вопросы сертификатов открытых ключей, центров сертификации, междоменные отношения и т.д. Раздел 2.4 посвящен интересным, но малоизученным на практике специфическим криптографическим протоколам, призванным решать вопросы безопасности легитимного голосования, группового разделения знания секрета. Приведенные в этом разделе результаты можно активно использовать как в кредитно-финансовой сфере, так и в повседневной жизни.

В главе 3 рассматриваются практические вопросы применения криптографических средств защиты информации для решения типовых задач информационной безопасности. Обсуждение ведется на основе анализа проблемных вопросов информационной безопасности и средств защиты информации, применяемых на сегодняшний день в России и за рубежом. В качестве законченных решений для конкретных задач приводятся некоторые корпоративные решения. В данной главе также затронута область электронной коммерции в Internet, так как эта сфера в последние годы становится наиболее активным потребителем новых идей и средств криптографической защиты информационных потоков. Раздел 3.1 представляет собой своеобразный путеводитель по этой специфической области переработки и накопления данных; здесь также описывается общая проблематика и подходы к решению задач обеспечения информационной безопасности в современных информационно-телекоммуникационных системах. Приведен обзор стандартов в области криптографической защиты обрабатываемых и передаваемых сведений. Раздел 3.2 посвящен проблемам защиты информации локальных рабочих станций (не подключенных к каналам передачи данных). В качестве конкретных средств криптографической защиты информации рассматриваются семейство «Верба», программно-аппаратные комплексы «Аккорд», «Криптон» и др. Также затрагиваются вопросы и задачи информационной безопасности, возникающие при использовании современных операционных систем (на примере Windows NT). Раздел 3.3 посвящен защите информации в локальных сетях передачи данных на примере сетей Windows NT (в том числе и Windows NT 5.0) и Novell NetWare, широко распространенных на отечественном рынке. В данной части анализируются уязвимости протоколов PPTP и CIFS (от Microsoft). В качестве средства, позволяющего решить большинство задач информационной безопасности в локальных сетях передачи данных, рассмотрена система Secret Net NT. В разделе 3.4 освещаются вопросы, связанные с защитой информации в сетях, имеющих выход в другие сети передачи данных. Здесь приводятся общие сведения об угрозах

в распределенных IP-сетях и протоколах, применяемых для защиты информации в Internet, а также описываются функциональные возможности и применение криптографических средств защиты информации для построения виртуальных частных сетей («Шип», «ФПСУ», «Игла-П» и «Застава»). Раздел 3.5 посвящен не менее актуальным вопросам защиты информации в распределенных сетях – защите технологий «клиент-сервер». Многообразие средств защиты данных и задачи информационной безопасности в клиент-серверных технологиях тоже представлены в этом разделе. Здесь читатель познакомится как с хорошо известными средствами защиты информации SSL и Kerberos, так и с их реализацией в виде законченного продукта – Trusted Web. В разделе 3.6 описывается применение межсетевых экранов, proxy-серверов, а также подробно излагается реализация криптографических средств защиты информации в Check Point Firewall-1. Следующий раздел посвящен принципам защиты электронной почты, в том числе таким известным протоколам защищенной электронной почты, как PEM (и его разновидности) и PGP. Отдельно представлена интересная проблема – защита информации в архитектуре X.400, и в качестве конкретной реализации данного вида электронной почты рассмотрен Messenger 400. Раздел 3.8 рассказывает об опыте обеспечения информационной безопасности в виде отдельных корпоративных решений. Причем на этих страницах рассматриваются системы перевода денежных средств и средства обеспечения финансовых операции – SWIFT и Smart City. Раздел 3.9 рассказывает об электронной коммерции в Internet и обеспечении информационной безопасности глобальной сети. Здесь читатель познакомится с понятием электронных денег и с проблемами информационной безопасности, возникающими при использовании смарт-карт.

В приложениях представлены результаты тестирования отечественных средств построения виртуальных частных сетей[1] и приведен общий обзор проблемы санкционированного доступа к ресурсам корпоративной информационной системы предприятия[2].

Автор надеется, что книга окажется полезной не только пользователям, начинающим осваивать данную область человеческих знаний, но и специалистам в сфере компьютерной безопасности.

[1] Авторы И. Гвоздев, В. Зайчиков, Н. Мошак, М. Пеленицин, С. Селезнев, Д. Шепелявый.

[2] Авторы В. С. Лаптев, С. П. Селезнев, М. Ю. Шувалов.

Введение

Задачи информационной безопасности

Стремительное развитие средств вычислительной техники и открытых сетей передачи данных обусловило их широкое распространение в повседневной жизни и предпринимательской деятельности. Мощные вычислительные возможности и оперативность передачи информации не только оказали большое влияние на принципы ведения бизнеса, сложившиеся в большинстве традиционных отраслей, но и открыли новые направления развития предпринимательской деятельности. В современных условиях автоматизация банковской деятельности и управления предприятиями является «modus vivendi», а такие слова, как «Internet-banking», «e-commerce» и «smart-cards», уже не вызывают всеобщего удивления и жарких дебатов.

Однако последние достижения человеческой мысли в области компьютерных технологий связаны с появлением не только персональных компьютеров, сетей передачи данных и электронных денег, но и таких понятий, как *хакер*, *информационное оружие*, *компьютерные вирусы* и т.п. Оказывается, что под *информационной безопасностью* подразумевается одно из ведущих направлений развития информационных технологий – круг задач, решаемых в этой области, постоянно расширяется как в количественном, так и в качественном отношении.

Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью потери, раскрытия, модификации данных, принадлежащих конечным пользователям.

На практике угрозы для *информационно-телекоммуникационных систем* (ИТС) могут быть реализованы непосредственным воздействием как на информацию, представляющую интерес для конечных пользователей подобных систем, так и на информационные ресурсы и телекоммуникационные службы, обеспечиваемые в рамках данной ИТС. Например, существует распространенный вид атаки через Internet – шторм ложных запросов на TCP-соединение, приводящий к тому, что система временно прекращает обслуживание удаленных пользователей. Перечень

подобного типа угроз достаточно обширен, и нередко такие проблемы необходимо решать путем защиты пользовательской информации как части ИТС.

Под *информационной безопасностью* в этой книге мы будем понимать состояние защищенности обрабатываемых, хранимых и передаваемых в ИТС данных от незаконного ознакомления, преобразования и уничтожения (как крайний случай модификации), а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Основными задачами защиты пользовательской информации являются:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение достоверности информации;
- обеспечение оперативности доступа к информации;
- обеспечение юридической значимости информации, представленной в виде электронного документа;
- обеспечение неотслеживаемости действий клиента.

Конфиденциальность – свойство информации быть доступной только ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.

Под *целостностью* понимается свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.

Здесь следует сделать пояснение. Рассматривая вопрос передачи информации в виде сообщений через сеть, можно прийти к заключению, что каждое сообщение по своему смысловому содержанию образует некоторый класс. Другими словами, смысл конечного сообщения останется таким же, как и начального, даже если форма представления информации в электронном виде существенно изменится. Таким образом, каждое сообщение на русском языке будет иметь свой класс эквивалентности, и для данного случая свойство сохранения целостности информации можно сформулировать следующим образом: переданное сообщение X считается сохранившим целостность, если полученное в результате передачи сообщение X1 принадлежит классу эквивалентности сообщения X.

Достоверность – свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.

Оперативность – способность информации или некоторого информационного ресурса быть доступным для конечного пользователя в соответствии с его временным потребностями.

Юридическая значимость означает, что документ обладает юридической силой. С этой целью субъекты, которые нуждаются в подтверждении юридической значимости передаваемого сообщения, договариваются о повсеместном принятии некоторых атрибутов информации, выражающих ее способность быть юридически значимой. Данное свойство информации особенно актуально в системах электронных платежей, где осуществляется операция по переводу денежных средств. Исходя из сказанного, можно сформулировать некоторые требования к атрибутам информации, выражающим ее свойство быть юридически значимой. Прежде всего ее необходимо сформировать таким образом, чтобы с формальной точки зрения было определенно ясно, что только отправитель, которому принадлежит данный платежный документ, мог его создать. О способах обеспечения юридической значимости платежных документов будет сказано ниже.

Неотслеживаемость – способность совершать некоторые действия в информационной системе незаметно для других объектов. Актуальность данного требования стала очевидной благодаря появлению таких понятий, как электронные деньги и Internet-banking. Так, для авторизации доступа к электронной платежной системе пользователь должен предоставить некоторые сведения, однозначно его идентифицирующие. По мере развития данных систем может появиться реальная опасность, что, например, все платежные операции будут контролироваться, тем самым возникнут условия для тотальной слежки за пользователями информационных систем.

Существует несколько путей решения проблемы неотслеживаемости:

- запрещение с помощью законодательных актов всякой тотальной слежки за пользователями информационных систем;
- применение криптографических методов для поддержания неотслеживаемости.

Как уже говорилось, информационная безопасность может рассматриваться не только по отношению к некоторым конфиденциальным сведениям, но и по отношению к способности информационной системы выполнять заданные функции.

Основные задачи, решаемые в рамках информационной безопасности по отношению к работоспособности ИТС, должны обеспечивать защиту от:

- нарушения функционирования телекоммуникационной системы, выражающегося в воздействии на информационные каналы, каналы сигнализации, управления и удаленной загрузки баз данных коммутационного оборудования, системное и прикладное программное обеспечение;

- несанкционированного доступа к информационным ресурсам и от попыток использования ресурсов сети, приводящих к утечке данных, нарушению целостности сети и информации, изменению функционирования подсистем распределения информации, доступности баз данных;
- разрушения встраиваемых и внешних средств защиты;
- неправомочных действий пользователей и обслуживающего персонала сети.

Приоритеты среди перечисленных задач информационной безопасности определяются индивидуально для каждой конкретной ИТС и зависят от требований, предъявляемых непосредственно к информационным системам.

Следует учесть, что с точки зрения государственных структур защитные мероприятия в первую очередь призваны обеспечить конфиденциальность, целостность и доступность информации. (Понятно, для режимных государственных организаций на первом месте всегда стоит конфиденциальность сведений, а целостность понимается исключительно как их неизменность.) Коммерческим структурам, вероятно, важнее всего целостность и доступность данных и услуг по их обработке. По сравнению с государственными, коммерческие организации более открыты и динамичны, поэтому вероятные угрозы для них отличаются не только количеством, но и качеством.

Для решения задачи обеспечения безопасности в информационно-телекоммуникационных сетях необходимо:

- защитить информацию при ее хранении, обработке и передаче по сети;
- подтвердить подлинность объектов данных и пользователей (аутентификация сторон, устанавливающих связь);
- обнаружить и предупредить нарушение целостности объектов данных;
- защитить технические устройства и помещения;
- защитить конфиденциальную информацию от утечки и от внедренных электронных устройств съема информации;
- защитить программные продукты от внедрения программных закладок и вирусов;
- защитить от несанкционированного доступа к информационным ресурсам и техническим средствам сети, в том числе и к средствам управления, чтобы предотвратить снижение уровня защищенности информации и самой сети в целом;
- организовать требующиеся мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

Конкретная реализация общих принципов обеспечения информационной безопасности может выражаться в организационных либо технических мерах защиты информации.

Следует отметить, что объем мероприятий по защите обрабатываемых и передаваемых данных зависит прежде всего от величины предполагаемого ущерба, который может выражаться в прямой (затраты на покупку нового программного обеспечения в случае нарушения целостности программного обеспечения) или в опосредованной (затраты от простоя информационной системы банка) форме. Правда, в некоторых ситуациях рассчитать величину ущерба затруднительно (например, в случае утечки государственного тайны).

Роль криптографических протоколов в общей задаче обеспечения информационной безопасности

Основу обеспечения информационной безопасности в информационно-телекоммуникационных системах составляют криптографические методы и средства защиты информации. Следует учесть, что наиболее надежную защиту можно обеспечить только с помощью комплексного подхода, то есть решение задачи должно представлять собой совокупность организационно-технических и криптографических мероприятий.

В основе криптографических методов лежит понятие *криптографического преобразования информации*, производимого по определенным математическим законам, с целью исключить доступ к данной информации посторонних пользователей, а также с целью обеспечения невозможности бесконтрольного изменения информации со стороны тех же самых лиц.

Применение криптографических методов защиты обеспечивает решение основных задач информационной безопасности. Этого можно добиться путем реализации следующих криптографических методов защиты как пользовательской и служебной информации, так и информационных ресурсов в целом:

- шифрование всего информационного трафика, передающегося через открытые сети передачи данных, и отдельных сообщений;
- криптографическая аутентификация устанавливающих связь разноуровневых объектов (имеются в виду уровни модели взаимодействия открытых систем);
- защита несущего данные трафика средствами *имитозащиты* (защиты от навязывания ложных сообщений) и электронно-цифровой подписи с целью обеспечения целостности и достоверности передаваемой информации;
- шифрование данных, представленных в виде файлов либо хранящихся в базе данных;

- контроль целостности программного обеспечения путем применения криптографически стойких контрольных сумм;
- применение электронно-цифровой подписи для обеспечения юридической значимости платежных документов; применение затемняющей цифровой подписи для обеспечения неотслеживаемости действий клиента в платежных системах, основанных на понятии электронных денег.

При реализации большинства из приведенных методов криптографической защиты возникает необходимость обмена некоторой информацией. Например, аутентификация объектов ИТС сопровождается обменом идентифицирующей и аутентифицирующей информации.

В общем случае взаимодействие объектов (субъектов) подобных систем всегда сопровождается соблюдением некоторых договоренностей, называемых *протоколом*. Формально протоколом будем считать последовательность действий объектов (субъектов) для достижения определенной цели. Она в данном случае определяет структуру и специфику применения протокола.

В свою очередь, *криптографическими протоколами* будем называть те, в которых участники для достижения определенной цели используют криптографические преобразования информации.

Перечислим основные задачи обеспечения информационной безопасности, которые решаются с помощью криптографических протоколов:

- обмен ключевой информации с последующей установкой защищенного обмена данными. При этом не существует никаких предположений, общались ли предварительно между собой стороны, обменивающиеся ключами (например, без использования криптографических протоколов невозможно было создать системы распределения ключевой информации в распределенных сетях передачи данных);
- аутентификация сторон, устанавливающих связь;
- авторизация пользователей при доступе к телекоммуникационным и информационным службам.

На сегодняшний день благодаря повсеместному применению открытых сетей передачи данных, таких как Internet, и построенных на их основе сетей intranet и extranet криптографические протоколы находят все более широкое применение для решения разнообразного круга задач и обеспечения постоянно расширяющихся услуг, предоставляемых пользователям таких сетей.

Кроме вышеперечисленных классических областей применения протоколов существует широкий круг специфических задач, также решаемых с помощью соответствующих криптографических протоколов. Это прежде

всего раскрытие части сведений без обнародования самого секрета в его подлинном объеме, а также частичное раскрытие секрета. Так, например, участники могут для достижения какой-то общей цели сообщить друг другу часть своей информации или объединить усилия для раскрытия секрета, неизвестного каждому из них в отдельности.

Стремительное развитие криптографических протоколов в большей степени стимулируется развитием систем электронных платежей, интеллектуальных карточек, появлением электронных денег и т.д. По зарубежным оценкам, темпы развития электронной коммерции постоянно ускоряются. Например, судя по прогнозам, количество компаний, занимающихся этим видом коммерции во всем мире, вырастет с 111 тысяч в 1996 году до 435 тысяч в 2000 году. При этом суммарный объем продаж через Internet увеличится с 9,5 до 196 млрд долларов.

Что касается розничных продаж через Internet, то они, по тем же оценкам, с 500 млн долларов в 1996 году вырастут до 7 млрд в 2000 году. При этом более половины покупок будет оплачено с помощью новых средств платежей – электронных денег. Таким образом, прогнозируется не только увеличение числа компаний, занимающихся бизнесом в сети, и их общего оборота, но и резкое возрастание среднего дохода, приходящегося на одну такую компанию. Поскольку на сегодняшний день основным криптографическим средством защиты информации в Internet являются протоколы, можно констатировать, что развитие подобных средств защиты коммерческих тайн будет продолжаться и в количественном, и в качественном отношении.

Многогранность применения криптографических протоколов в решении задачи обеспечения информационной безопасности как в локальных информационных системах, так и в распределенных информационных системах приводит к необходимости детального рассмотрения их основных типов, вопросов практического применения таких протоколов и построения на их основе специальных информационных систем.

Учитывая, что основой любого криптопротокола являются так называемые *криптоалгоритмы*, в рамках данной книги рассматриваются вопросы построения и практического применения основных типов подобных механизмов. Кроме хорошо известных и повсеместно используемых зарубежных криптоалгоритмов, здесь уделяется достаточное внимание отечественным разработкам в области информационной безопасности и стандартов на криптоалгоритмы.

Глава 1

Общие сведения по классической криптографии

1.1. Общие сведения

Прежде чем перейти к рассмотрению криптографических протоколов, а также к их практическому применению, необходимо уделить внимание вопросам, которые в рамках криптографии давно признаются классическими, а именно – основам построения *систем засекреченной связи*.

Под системой засекреченной связи будем понимать систему передачи информации, в которой смысл передаваемой информации скрывается с помощью криптографических преобразований. При этом сам факт передачи информации не утаивается. В основе каждой системы засекреченной связи – использование алгоритмов шифрования как основного средства сохранения конфиденциальности.

Зашифрование – процесс криптографического преобразования множества открытых сообщений в множество закрытых сообщений.

Расшифрование – процесс криптографического преобразования закрытых сообщений в открытые.

Дешифрование – процесс нахождения открытого сообщения, соответствующего заданному закрытому при неизвестном криптографическом преобразовании.

Множество открытых сообщений может быть представлено в виде битового потока, сетевого фрейма, файла и т.д.

Абстрактно систему засекреченной связи можно описать как множество отображений множества открытых сообщений в множество закрытых. Выбор конкретного типа преобразования определяется *ключом* расшифрования (или зашифрования). Отображения должны обладать свойством взаимооднозначности, то есть при расшифровании должен получаться единственный результат, совпадающий с первоначальным открытым