Глава 10. Информационная безопасность

10.1. Основные понятия

Зависимость современных организаций от компьютерных технологий стала настолько сильной, что вывод из строя компьютерной сети или программного обеспечения может остановить работу предприятия. Чтобы этого не произошло, нужно соблюдать правила *информационной безопасности*.

Информационная безопасность — это защищенность информации от любых действий, в результате которых информация может быть искажена или утеряна, а владельцам или пользователям информации нанесен *недопустимый* ущерб.

Прежде всего, в защите нуждается государственная и военная тайна, коммерческая тайна, юридическая тайна, врачебная тайна. Необходимо защищать личную информацию: паспортные данные, данные о банковских счетах, логины и пароли на сайтах, а также любую информация, которую можно использовать для шантажа, вымогательства и т.п.

Конечно, невозможно защититься от любых потерь, поэтому задача состоит в том, чтобы исключить именно *недопустимый* ущерб. С точки зрения экономики, средства защиты не должны стоить больше, чем возможные потери.

Защита информации – это меры, направленные на то, чтобы не потерять информацию, не допустить ее искажения, а также не допустить, чтобы к ней получили доступ люди, не имеющие на это права. В результате нужно обеспечить

- *доступность* информации – возможность получения информации за приемлемое время;
- *целостность* (отсутствие искажений) информации;
- *конфиденциальность* информации (недоступность для посторонних).

Доступность информации нарушается, например, когда оборудование выходит из строя, или веб-сайт не отвечает на запросы пользователей в результате массовой атаки вредоносных программ через Интернет.

Нарушения *целостности* информации – это кража или искажение информации, например, подделка сообщений электронной почты и других цифровых документов.

Конфиденциальность нарушается, когда информация становится известной тем людям, которые не должны о ней знать (происходит перехват секретной информации).

В компьютерных сетях защищенность информации снижается в сравнении с отдельным компьютером, потому что

- в сети работает много пользователей, их состав меняется;
- есть возможность незаконного подключения к сети;
- существуют уязвимости в сетевом программном обеспечении;
- возможны атаки взломщиков и вредоносных программ через сеть.

В России вопросы, связанные с защитой информации, регулирует закон «Об информации, информационных технологиях и о защите информации».

Технические средства защиты информации – это замки, решетки на окнах, системы сигнализации и видеонаблюдения, другие устройства, которые блокируют возможные каналы утечки информации или позволяют их обнаружить.

Программные средства обеспечивают доступ к данным по паролю, шифрование информации, удаление временных файлов, защиту от вредоносных программ и др.

Организационные средства включают

- распределение помещений и прокладку линий связи таким образом, чтобы злоумышленнику было сложно до них добраться;
- политику безопасности организации.

Сервера, как правило, находятся в отдельном (охраняемом) помещении и доступны только администраторам сети. Важная информация должна периодически копироваться на резервные носители (диски или магнитную ленту), чтобы сохранить ее в случае сбоев. Обычные сотрудники (не администраторы)

- имеют право доступа только к тем данным, которые им нужны для работы;
- не имеют права устанавливать программное обеспечение;
- раз в месяц должны менять пароли.

Самое слабое звено любой системы защиты – это человек. Некоторые пользователи могут записывать пароли на видном месте (чтобы не забыть) и передавать их другим, при этом возможность незаконного доступа к информации значительно возрастает. Поэтому очень важно обучить пользователей основам информационной безопасности.

Большинство утечек информации связано с «инсайдерами» (англ. *inside* – внутри) – недобросовестными сотрудниками, работающими в фирме. Известны случаи утечки закрытой информации не через ответственных сотрудников, а через секретарей, уборщиц и другого вспомогательного персонала. Поэтому ни один человек не должен иметь возможности причинить непоправимый вред (в одиночку уничтожить, украсть или изменить данные, вывести из строя оборудование).

? *Вопросы и задачи*

1. Что такое информационная безопасность?
2. Что входит в понятие «защита информации»?
3. На какие группы делятся средства защиты информации?
4. Какие меры безопасности обычно применяются в организациях?
5. Почему при объединении компьютеров в сеть безопасность снижается?
6. Кто такие «инсайдеры»?

10.2.Вредоносные программы

10.2.1. Что такое компьютерный вирус?

Компьютерный вирус – это программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы и системные области компьютера. При этом копии могут распространяться дальше.

Как следует из этого определения, основная черта компьютерного вируса – это способность распространяться при запуске.

Вирус – это один из типов вредоносных программ. Однако очень часто вирусами называют любые вредоносные программы (англ. *malware*).

Вредоносные программы — это программы, предназначенные для незаконного доступа к информации, для скрытого использования компьютера или для нарушения работы компьютера и компьютерных сетей.

Зачем пишут такие программы? Во-первых, с их помощью можно получить управление компьютером пользователя и использовать его в своих целях. Например, через зараженный компью-

тер злоумышленник может взламывать сайты и переводить на свой счет незаконно полученные деньги. Некоторые программы блокируют компьютер и для продолжения работы требуют отправить платное SMS-сообщение.

Зараженные компьютеры, подключенные к сети Интернет, могут объединяться в сеть специального типа – *ботнет* (от англ. *robot* – робот и *network* – сеть). Такая сеть часто состоит из сотен тысяч компьютеров, обладающих в сумме огромной вычислительной мощностью. По команде «хозяина» ботнет может организовать атаку на какой-то сайт. В результате огромного количества запросов сервер не справляется с нагрузкой, сайт становится недоступен, и бизнесмены несут большие денежные потери. Такая атака называется *DoS*-атакой[1] (англ. *DoS* = *Denial of Service*, отказ в обслуживании). Кроме того, ботнеты могут использоваться для подбора паролей, рассылки *спама* (рекламных электронных сообщений) и другой незаконной деятельности.

Во-вторых, некоторые вредоносные программы предназначены для шпионажа – передачи по Интернету секретной информации с вашего компьютера: паролей доступа к сайтам, почтовым ящикам, учетным записям в социальных сетях, банковским счетам и электронным платежным системам. В результате таких краж пользователи теряют не только данные, но и деньги.

В-третьих, иногда вирусы пишутся ради самоутверждения программистами, которые по каким-то причинам не смогли применить свои знания для создания полезного ПО. Такие программы нарушают нормальную работу компьютера: время от времени перезагружают его, вызывают сбои в работе операционной системы и прикладных программ, уничтожают данные.

Наконец, существуют вирусы, написанные ради шутки. Они не портят данные, но приводят к появлению звуковых или зрительных эффектов (проигрывание мелодии; искажение изображения на экране; кнопки, убегающие от курсора и т.п.).

Создание и распространение компьютерных вирусов и вредоносных программ – это уголовные преступление, которое предусматривает (в особо тяжких случаях) наказание до 7 лет лишения свободы (Уголовный кодекс РФ, статья 273).

Признаки заражения вирусом:

- замедление работы компьютера;
- уменьшение объема свободной оперативной памяти;
- зависание, перезагрузка или блокировка компьютера;
- ошибки при работе ОС или прикладных программ;
- изменение длины файлов, появление новых файлов (в том числе «скрытых»);
- рассылка сообщений по электронной почте без ведома автора.

Для того, чтобы вирус смог выполнить какие-то действия, он должен оказаться в памяти в виде программного кода и получить управление компьютером.

Поэтому вирусы **заражают** не любые данные, а только программный код, который может выполняться. Например:

- исполняемые программы (с расширениями **`.exe`**, **`.com`**);
- загрузочные сектора дисков;
- пакетные командные файлы (**`.bat`**);
- драйверы устройств;
- библиотеки динамической загрузки (**`.dll`**), функции из которых вызываются из прикладных программ;

[1] Здесь речь идет, строго говоря, о распределенной *DoS*-атаке (англ. *DDoS* = *Distributed DoS*), которая проводится сразу со многих компьютеров.

- документы, которые могут содержать *макросы* – небольшие программы, выполняющиеся при нажатии на клавиши или выборе пункта меню; например, макросы нередко используются в документах пакета *Microsoft Office*;
- веб-страницы (в них можно внедрить программу-*скрипт*, которая выполнится при просмотре страницы на компьютере пользователя).

В отличие от кода программ, файлы с данными (например, тексты, рисунки, звуковые и видеофайлы) только обрабатываются, но не выполняются, поэтому заложенный в них код никогда не должен получить управление компьютером. Однако из-за ошибок в программном обеспечении может случиться так, что специально подобранные некорректные данные вызовут сбой программы обработки и выполнение вредоносного кода[2]. Таким образом, существует некоторый шанс, что вредоносная программа, «зашитая» в рисунок или видеофайл, все-таки запустится.

Сейчас существуют два основных источника заражения вредоносными программами – флэш-диски и компьютерные сети. Компьютер может быть **заражен** при:

- запуске зараженного файла;
- загрузке с зараженного CD(DVD)-диска или флэш-диска;
- автозапуске зараженного CD(DVD)-диска или флэш-диска (вирус автоматически запускается из файла **`autorun.inf`** в корневом каталоге диска);
- открытии зараженного документа с макросами;
- открытии сообщения электронной почты с вирусом или запуске зараженной программы, полученной в приложении к сообщению;
- открытии веб-страницы с вирусом;
- установке активного содержимого для просмотра веб-страницы.

Кроме того, есть вирусы-черви, которые распространяются по компьютерным сетям без участия человека. Они могут заразить компьютер даже тогда, когда пользователь не сделал никаких ошибочных действий.

10.2.2. Типы вредоносных программ

К вредоносным программам относятся компьютерные вирусы, черви, троянские программы и др. По «среде обитания» обычно выделяют следующие типы вирусов:

- **файловые** – внедряются в исполняемые файлы, системные библиотеки и т.п.;
- **загрузочные** – внедряются в загрузочный сектор диска или в главную загрузочную запись винчестера (англ. *MBR = Master Boot Record*); опасны тем, что загружаются в память раньше, чем ОС и антивирусные программы;
- **макровирусы** – поражают документы, в которых могут быть макросы;
- **скриптовые вирусы** – внедряются в командные файлы или в веб-страницы (записывая в них код на языке *VBScript* или *JavaScript*);
- **сетевые вирусы** – распространяются по компьютерным сетям.

Некоторые вирусы при создании новой копии немного меняют свой код, для того чтобы их было труднее обнаружить. Такие вирусы называют «полиморфными» (от греч. *πολυ* — много, *μορφη* — форма, внешний вид).

Червь — это вредоносная программа, которая распространяется по компьютерным сетям. Наиболее опасны *сетевые черви*, которые используют «дыры» (ошибки в защите, уязвимости) операционных систем и распространяются очень быстро без участия человека. Червь посылает по

[2] В 2002 г. был обнаружен вирус, которые внедрялся в рисунки формата JPEG. Однако он получал управление только из-за ошибки в системной библиотеке *Windows*, которая была быстро исправлена.

сети специальный пакет данных (*эксплойт*, от англ. *exploit* – эксплуатировать), который позволяет выполнить код на удаленном компьютере и внедриться в систему.

Как правило, вскоре после обнаружения уязвимости выпускается обновление программного обеспечения («заплатка», «патч»); если его установить, то червь становится неопасен. К сожалению, системные администраторы не всегда вовремя устанавливают обновления. Это приводит к эпидемиям сетевых червей, которые по статистике вызывают наибольшее число заражений[3]. Зараженные компьютеры используются для рассылки *спама* или массовых *DoS*-атак на сайты в Интернете.

Почтовые черви распространяются как приложения к сообщениям электронной почты. Они представляют собой программы, которые при запуске заражают компьютер и рассылают свои копии по всем адресам из адресной книги пользователя. Из-за этой опасности многие почтовые серверы (например, *mail.google.com*) не разрешают пересылку исполняемых файлов.

Чтобы заставить пользователя запустить червя, применяются методы *социальной инженерии*: текст сообщения составляется так, чтобы заинтересовать человека и спровоцировать его на запуск программы, приложенной к письму. В некоторых случаях программа-вирус упакована в архив и защищена паролем, но находится немало людей, которые распаковывают его (пароль указывается в письме) и запускают программу. Часто в почтовых сообщениях содержится только ссылка на сайт, содержащий вирус.

Иногда файл, пришедший как приложение к письму, имеет двойное расширение, например,

«**СуперКартинка.jpg .exe**»

В самом деле, это программа (расширение имени файла **.exe**), но пользователь может увидеть только первые две части имени и попытаться открыть такой «рисунок».

Существуют черви, которые могут распространяться через файлообменные сети, чаты и системы мгновенных сообщений (например, ICQ), но они мало распространены.

Еще одна группа вредоносных программ – **троянские программы** или «троянцы» (трояны). «Троянский конь» — это огромный деревянный конь, которого древние греки подарили жителям Трои во время Троянской войны. Внутри него спрятались воины, которые ночью выбрались, перебили охрану и открыли ворота города. Троянские программы проникают на компьютер под видом «полезных» программ, например, кодеков для просмотра видео или экранных заставок (которые включаются, если некоторое время не работать на компьютере). В отличие от вирусов и червей, они не могут распространяться самостоятельно и часто «путешествуют» вместе с червями. Среди «троянцев» встречаются

- *клавиатурные шпионы* – передают «хозяину» все данные, вводимые с клавиатуры (в том числе коды доступа к банковским счетам и т.п.);
- *похитители паролей* – передают пароли, запомненные, например, в браузерах;
- *утилиты удаленного управления* – позволяют злоумышленнику управлять компьютером через Интернет (например, загружать и запускать любые файлы);
- *логические бомбы* – при определенных условиях (дата, время, команда по сети) уничтожают информацию на дисках.

Большинство существующих вирусов написано для ОС *Windows*, которая установлена более чем на 90% персональных компьютеров.

Известны также вирусы для *Mac OS* X и *Linux*, но не каждому удается их запустить. Дело в том, что обычный пользователь (не администратор) в этих операционных системах не имеет права на изменение системных файлов, поэтому *Mac OS* X и *Linux* считают защищенными от вирусов.

[3] http://www.securelist.com/ru/analysis

Кроме того, вирусы часто полагаются на то, что системные функции размещаются в памяти по определенным адресам. При сборке ядра *Linux* из исходных кодов эти адреса могут меняться, поэтому вирус, работающий на одном дистрибутиве, может не работать на других.

Вопросы и задачи

1. Что такое компьютерный вирус? Чем он отличается от других программ?
2. Что такое вредоносные программы? Какие вредоносные программы вы знаете?
3. Перечислите признаки заражения компьютера вирусом.
4. Какие вредные действия могут совершать вредоносные программы?
5. Какие объекты могут быть заражены вирусами?
6. Какие объекты не заражаются вирусами?
7. При каких действиях пользователя возможно заражение вирусом?
8. Является ли создание и распространение вирусов уголовным преступлением?
9. Какие типы вирусов вы знаете?
10. Что означает сокращение «MBR»?
11. Чем опасны загрузочные вирусы?
12. Что такое макровирусы? Какие файлы они поражают?
13. Что могут заражать скриптовые вирусы?
14. Что такое полиморфные вирусы? Почему их сложно обнаруживать?
15. Что такое сетевой червь?
16. Что такое эксплойт?
17. Почему необходимо сразу устанавливать обновления для операционных систем?
18. С какими целями могут быть использованы компьютеры, зараженные сетевым червем?
19. Почему многие почтовые сервера запрещают пересылку исполняемых файлов?
20. Что такое социальная инженерия? Как она используется авторами вирусов?
21. Что такое троянские программы? Какие типы троянских программ вы знаете?
22. Какие операционные системы лучше защищены от вирусов? Почему?

10.3.Защита от вредоносных программ

10.3.1. Антивирусные программы

Антивирус – это программа, предназначенная для борьбы с вредоносными программами.

Антивирусы выполняют три основные задачи:

1) не допустить заражения компьютера вирусом;
2) обнаружить присутствие вируса в системе;
3) удалить вирус без ущерба для остальных данных.

Код большинства вирусов содержит характерные цепочки байт – *сигнатуры* (от лат. *signare* – «подписать»). Если в файле обнаруживается сигнатура какого-то вируса, можно предположить, что файл заражен. Такой подход используется всеми антивирусными программами. Сигнатуры известных вирусов хранятся в базе данных антивируса, которую нужно регулярно обновлять через Интернет.

Современные антивирусы – это программные комплексы, состоящие из нескольких программ. Чаще всего они включают антивирус-сканер (иногда его называют антивирус-доктор) и антивирус-монитор.

Для того, чтобы **антивирус-сканер** начал работу, пользователь должен его запустить и указать, какие файлы и папки нужно проверить. Это «защита по требованию». Сканеры используют два основных метода поиска вирусов:

- *поиск в файлах сигнатур вирусов*, которые есть в базе данных; после обнаружения файл с вирусом можно вылечить, а если это не получилось – удалить;
- *эвристический анализ* (греч. *ευρηκα* – «нашёл!»), при котором программа ищет в файле код, похожий на вирус.

Эвристический анализ часто позволяет обнаруживать полиморфные вирусы (изменяющие код с каждым новым заражением), но не гарантирует это. Кроме того, случаются ложные срабатывания, когда «чистый» файл попадает под подозрение.

Главный недостаток сканеров состоит в том, что они не могут предотвратить заражение компьютера, потому что начинают работать только при ручном запуске.

Антивирусы-мониторы – это программы постоянной защиты, они находятся в памяти в активном состоянии. Их основная задача – не допустить заражения компьютера и получения зараженных файлов извне. Для этого мониторы

- проверяют «на лету» все файлы, которые копируются, перемещаются или открываются в различных прикладных программах;
- проверяют используемые дискеты и флэш-диски;
- перехватывают действия, характерные для вирусов (форматирование диска, замена и изменение системных файлов) и блокируют их;
- проверяют весь поток данных, поступающий из Интернета (сообщения электронной почты, веб-страницы, сообщения ICQ).

Мониторы ведут непрерывное наблюдение, блокируют вирус в момент заражения. Иногда они могут перехватить и неизвестный вирус (сигнатуры которого нет в базе), обнаружив его подозрительные действия.

Главный недостаток антивирусов-мониторов – значительное замедление работы системы, особенно на маломощных компьютерах. Кроме того, мониторы фактически встраиваются в операционную систему, поэтому ошибки разработчиков антивируса могут привести к печальным последствиям (вплоть до вывода ОС из строя). Бывает и так, что при запущенном мониторе некоторые программы работают неправильно или вообще не работают. Тем не менее, не рекомендуется отключать монитор, особенно если вы работаете в Интернете или переносите файлы с помощью флэш-дисков.

Кроме вредоносных программ, современные антивирусы частично защищают компьютер от

- *фишинга* – выманивания паролей для доступа на сайты Интернета с помощью специально сделанных веб-страниц, которые внешне выглядят так же, как «официальные» сайты;
- *рекламных баннеров и всплывающих окон* на веб-страницах;
- *спама* – рассылки нежелательных рекламных сообщений по электронной почте.

Большинство антивирусных программ – условно-бесплатные (*shareware*), пробные версии с ограниченным сроком действия можно свободно загрузить из Интернета. Наиболее известны антивирусы *AVP* (*www.kaspersky.ru*), *DrWeb* (*www.drweb.com*), *Nod32* (*www.eset.com*), *McAfee* (*home.mcafee.com*).

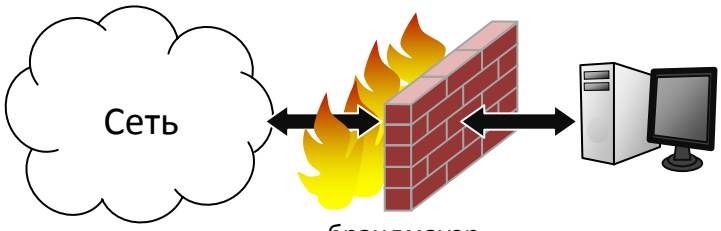
На многих сайтах (*www.kaspersky.ru*, *www.freedrweb.com*) доступны для скачивания лечащие программы-сканеры, которые бесплатны для использования на домашних компьютерах. В отличие от полных версий, в них нет антивируса-монитора, и базы сигнатур не обновляются.

Существуют бесплатные антивирусы, например, *Microsoft Security Essentials* (*www.microsoft.com*), *Avast Home* (*www.avast.com*), *Antivir Personal* (*free-av.com*), *AVG Free* (*free.grisoft.com*). Антивирус *ClamAV* (*www.clamav.net*) – бесплатный и поставляется с исходным кодом.

На сайтах некоторых компаний можно найти *онлайновые антивирусы* (например, *http://www.kaspersky.ru/virusscanner*). Они устанавливают на компьютер специальный сканирующий модуль и проверяют файлы и оперативную память. Как правило, онлайновые антивирусы могут обнаружить вирусы, но не удаляют их, предлагая приобрести коммерческую версию.

10.3.2. Брандмауэры

Для защиты отдельных компьютеров и сетей от атак из Интернета (в том числе и вирусных) используются **брандмауэры** (нем. *Brandmauer* – стена между зданиями для защиты от распространения огня). Их также называют «сетевые экраны» или «фаейрволы» (от англ. *firewall*). Брандмауэры запрещают передачу данных по каналам связи, которые часто используют вирусы и программы для взлома сетей.



брандмауэр

На рисунке показана защита одного компьютера с помощью брандмауэра, точно так же защищаются от угроз из Интернета локальные сети.

Брандмауэр входит в состав современных версий ОС *Windows*, в ядро *Linux* также включен встроенный брандмауэр *Netfilter*. Иногда устанавливают дополнительные брандмауэры, например, *Agnitum Outpost* (*www.agnitum.com*), *Kerio Winroute Firewall* (*kerio.ru*) или бесплатную программу *Comodo Personal Firewall* (*www.personalfirewall.comodo.com*).

10.3.3. Меры безопасности

Главные вред, который могут нанести вредоносные программы – это потеря данных или паролей доступа к закрытой информации.

Чтобы уменьшить возможный ущерб, рекомендуется регулярно делать резервные копии важных данных на CD(DVD)-дисках или флэш-дисках.

Если вы работаете в сети, желательно включать антивирус-монитор и брандмауэр. Монитор также сразу сообщит об опасности, если вставленный флэш-диск содержит вирус. Все новые файлы (особенно программы!) нужно проверять с помощью антивируса-сканера.

Не рекомендуется открывать подозрительные сообщения электронной почты, полученные с неизвестных адресов, особенно файлы-приложения (помните про методы социальной инженерии – заинтересовать жертву и заставить запустить программу). Опасно также переходить по ссылкам в тексте писем, с большой вероятностью они ведут на сайты, зараженные вирусами.

Если компьютер заражен, нужно отключить его от сети и запустить антивирус-сканер. Очень часто это позволяет удалить вирус, если его сигнатура есть в базе данных. Если антивирус не был установлен раньше, можно попробовать установить его на зараженный компьютер, но это не всегда приводит к успеху (вирус может блокировать установку антивируса).

Если антивирус-сканер не обнаруживает вирус или не может его удалить, можно попытаться (желательно с другого компьютера) найти в Интернете бесплатную утилиту для лечения с новыми базами сигнатур. Например, утилита *CureIt* (*www.freedrweb.com*) не требует установки и может быть запущена с флэш-диска. Даже если удалить вирус не удалось, скорее всего, он будет обнаружен, и программа покажет его название. Следующий шаг – искать в Интернете утилиту для удаления именно этого вируса (например, ряд утилит можно найти на сайте *support.kaspersky.ru*).

В особо тяжелых случаях для уничтожения вирусов приходится полностью форматировать жесткий диск компьютера, при этом все данные теряются.

? *Вопросы и задачи*

1. Что такое антивирус? Какие задачи он решает?
2. Что такое сигнатура?
3. Почему нужно регулярно обновлять базы сигнатур антивирусов?
4. Чем отличается антивирус-сканер от антивируса-монитора?
5. Что значит «защита по требованию»?
6. Что такое эвристический анализ? В чем его достоинства и недостатки?
7. Что делает антивирус-монитор? Каковы его недостатки?
8. Что такое фишинг?
9. Что такое спам?
10. Какие ограничения есть у пробных версий коммерческих антивирусов?
11. Что такое онлайновый антивирус?
12. Что такое брандмауэр? Зачем он нужен?
13. В чем заключается основной вред, наносимый вирусами? Как можно уменьшить возможные потери?
14. Как можно улучшить безопасность компьютера при работе в сети Интернет?
15. Какие меры безопасности необходимы при работе с электронной почтой?
16. Какие действия можно предпринять, если компьютер заражен вирусом?

10.4. Что такое шифрование?

Один из методов защиты информации от неправомерного доступа – это *шифрование*, то есть кодирование специального вида.

Шифрование – это преобразование (кодирование) открытой информации в зашифрованную, недоступную для понимания посторонних.

Шифрование применяется, в первую очередь, для передачи секретной информации по незащищённым каналам связи. Шифровать можно любую информацию – тексты, рисунки, звук, базы данных и т.д.

Человечество применяет шифрование с того момента, как появилась секретная информация, которую нужно было скрыть от врагов. Первый известное науке шифрованное сообщение – египетский текст, в котором вместо принятых тогда иероглифов были использованы другие знаки.

Методы шифрования и расшифровывания сообщения изучает наука *криптология*, история которой насчитывает около четырех тысяч лет. Она состоит из двух ветвей: *криптографии* и *криптоанализа*.

Криптография – это наука о способах шифрования информации.
Криптоанализ – это наука о методах и способах вскрытия шифров.

Обычно предполагается, что сам алгоритм шифрования известен всем, но неизвестен его *ключ*, без которого сообщение невозможно расшифровать. В этом заключается отличие шифрования от простого кодирования, при котором для восстановления сообщения достаточно знать только алгоритм кодирования.

Ключ – это параметр алгоритма шифрования (шифра), позволяющий выбрать одно конкретное преобразование из всех вариантов, предусмотренных алгоритмом. Знание ключа позволяет свободно зашифровывать и расшифровывать сообщения.

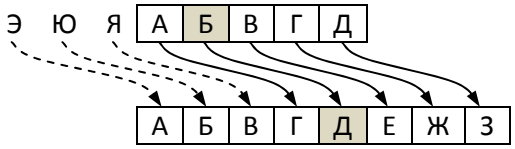
Все шифры (системы шифрования) делятся на две группы – *симметричные* и *несимметричные* (с открытым ключом).

Симметричный шифр означает, что и для шифрования, и для расшифровывания сообщений используется один и тот же ключ. В системах **с открытым ключом** используются два ключа – открытый и закрытый, которые связаны друг с другом с помощью некоторых математических зависимостей. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптостойкость шифра – это устойчивость шифра к расшифровке без знания ключа.

Стойким считается алгоритм, который для успешного раскрытия требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных сообщений, или такого времени, что по его истечению защищённая информация будет уже не актуальна.

Шифр Цезаря[4] – один из самых известных и самых древних шифров. В этом шифре каждая буква заменяется на другую, расположенную в алфавите на заданное число позиций k вправо от нее. Алфавит замыкается в кольцо, так что последние символы заменяются на первые. Вот пример шифра Цезаря (со сдвигом 3):



Знаменитая фраза «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ» при использовании шифра Цезаря со сдвигом 3 будет закодирована так:

ТУЛЫИО ЦЕЛЗИО ТСДИЗЛО

Если первая буква алфавита имеет код 0, вторая – код 1 и т.д, алгоритм шифрования может быть выражен формулой

$$y = (x + k) \mod n,$$

где x – код исходного символа, k – величина сдвига, y – код символа-замены, n – количество символов в алфавите, а запись $(x + k) \mod n$ обозначает остаток от деления $x + k$ на n. Операция взятия остатка от деления необходима для того, чтобы «замкнуть» алфавит в кольцо. Например, при использовании русского алфавита (33 буквы) для буквы «Я» (код 32) получаем код заменяющего символа $(32 + 3) \mod 33 = 2$, это буква «В».

Ключом для шифра Цезаря служит сдвиг k, если его знать, то сообщение легко расшифровать. Для этого используется формула

$$x = (y - k + n) \mod n.$$

Шифр Цезаря относится к шифрам *простой подстановки*, так как каждый символ исходного сообщения заменяется на другой символ из того же алфавита. Такие шифры легко раскрываются с

[4] Назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

помощью частотного анализа, потому что в каждом языке частоты встречаемости букв примерно постоянны для любого достаточно большого текста.

Значительно сложнее сломать *шифр Виженера*[5], который стал естественным развитием шифра Цезаря. Для использования шифра Виженера используется ключевое слово, которое задает переменную величину сдвига. Например, пусть ключевое слово – «ЗАБЕГ». По таблице определяем коды букв:

0	1	2	3	4	5	6	7	8	9	
А	Б	В	Г	Д	Е	Ё	Ж	З	И	…

Получаем: «З» – 8, «А» – 0, «Б» – 1, «Е» – 5, «Г» – 3. Это значит, что для кодирования первой буквы используется сдвиг 8, для кодирования второй – 0 (символ не меняется) и т.д. Для пятой буквы используется сдвиг 3, а для шестой – снова 8 (начали «проходить» кодовое слова с начала). Фраза «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ» при использовании шифра Виженера с ключом «ЛИМОН» будет закодирована в виде «ЪШФЖТЦ ЯРХПНЧ ЬЩЙСТХЦ».

Шифр Виженера обладает значительно более высокой криптостойкостью, чем шифр Цезаря. Это значит, что его труднее раскрыть – подобрать нужное ключевое слово. Теоретически, если длина ключа равна длине сообщения, и каждый ключ используется только один раз, шифр Виженера взломать невозможно.

? *Вопросы и задачи*

1. Чем отличаются понятия «шифрование» и «кодирование»?
2. Что такое ключ?
3. Как называется наука, изучающая методы шифрования?
4. Что такое симметричный шифр? Какая проблема возникает при использовании симметричного шифра, если участники переписки находятся в разных странах?
5. Что такое несимметричные шифры? На чем основана их надежность?
6. Что такое криптостойкость алгоритма? Какой алгоритм считается криптостойким?
7. Зашифруйте с помощью шифра Цезаря со сдвигом 6 высказывание «ЛЮДИ ОХОТНО ВЕРЯТ ТОМУ, ЧЕМУ ЖЕЛАЮТ ВЕРИТЬ».
   (Ответ: «СДКО ФЫФШУФ ИЛЦЕШ ШФТЩ, ЭЛТЩ МЛСЖДШ ИЛЦОШВ»).
8. *Попытайтесь расшифровать сообщение, закодированное шифром Цезаря с неизвестным сдвигом: «ХШЖНПУТ ФКХКОЙКТ». Для этого можно написать программу. (Ответ: «РУБИКОН ПЕРЕЙДЕН», сдвиг 5)
9. Используя шифр Виженера с ключом «ЛЕНА», зашифруйте сообщение «НЕЛЬЗЯ ОБИЖАТЬ ГОСТЯ».
   (Ответ: «ШКШЬТД ОМНУАЭБ ГЩЦЯЯ»)

10.5. Хэширование и пароли

В современных информационных системах часто используется вход по паролю. Если при этом где-то хранить пароли всех пользователей, система становится очень ненадежной, потому что «утечка» паролей позволит сразу получить доступ к данным. С другой стороны, кажется, что пароли обязательно где-то нужно хранить, иначе пользователи не смогут войти в систему. Однако, это не совсем так. Можно хранить не пароли, а некоторые числа, полученные в результате обработки паролей. Простейший вариант – сумма кодов символов, входящих в пароль. Для пароля «А123» такая сумма равна

215 = 65 (код «А») + 49 (код «1») + 50 (код «2») + 51 (код «3»).

[5] Назван по имени Блеза Виженера, швейцарского дипломата XVI века.

Фактически мы определили функцию $H(M)$, которая сообщение M *любой* длины превращает в короткий код m *заданной* длины. Такая функция называются *хэш-функцией* (от англ. *hash* – «мешанина», «крошить»), а само полученное число – *хэш-кодом*, *хэш-суммой* или просто *хэшем* исходной строки. Важно, что зная хэш-код, невозможно восстановить исходный пароль! В этом смысле хэширование – это *необратимое* шифрование.

Итак, вместо пароля «A123» мы храним число 215. Когда пользователь вводит пароль, мы считаем сумму кодов символов этого пароля и разрешаем вход в систему только тогда, когда она равна 215. И вот здесь возникает проблема: существует очень много паролей, для которых наша хэш-функция дает значение 215, например, «B023». Такая ситуация – совпадение хэш-кодов различных исходных строк – называется *коллизией* (англ. *collision* – «столкновение»). Коллизии будут всегда – ведь мы «сжимаем» длинную цепочку байт до числа. Казалось бы, ничего хорошего не получилось: если взломщик узнает хэш-код, то, зная алгоритм его получения, он сможет легко подобрать пароль с таким же хэшем и получить доступ к данным. Однако, это произошло потому, что мы выбрали плохую хэш-функцию.

Математики разработали надежные (но очень сложные) хэш-функции, обладающие особыми свойствами:

1) хэш-код очень сильно меняется при малейшем изменении исходных данных;
2) при известном хэш-коде m невозможно за приемлемое время найти сообщение M с таким хэш-кодом ($H(M) = m$);
3) при известном сообщении M невозможно за приемлемое время найти сообщение M_1 с таким же хэш-кодом ($H(M) = H(M_1)$).

Здесь выражение «невозможно за приемлемое время» (или «вычислительно невозможно») означает, что эта задача решается только перебором вариантов (других алгоритмов не существует), а количество вариантов настолько велико, что на решение уйдут сотни и тысячи лет. Поэтому даже если взломщик получил хэш-код пароля, он не сможет за приемлемое время получить сам пароль (или пароль, дающий такой же хэш-код).

Чем длиннее пароль, тем больше количество вариантов. Кроме длины, для надежности пароля важен используемый набор символов. Например, очень легко подбираются пароли, состоящие только из цифр. Если же пароль состоит из 10 символов и содержит латинские буквы (заглавные и строчные) и цифры, перебор вариантов (англ. *brute force* – метод «грубой силы») со скоростью 10 млн. паролей в секунду займет более 2000 лет.

Надежные пароли должны состоять не менее чем из 7-8 символов; пароли, состоящие из 15 символов и более взломать методом «грубой силы» практически невозможно. Нельзя использовать пароли типа «12345», «qwerty», свой день рождения, номер телефона. Плохо, если пароль представляет собой известное слово, для этих случаев взломщики используют подбор по словарю. Сложнее всего подобрать пароль, который представляет собой случайный набор заглавных и строчных букв, цифр и других знаков[6].

Сегодня для хэширования в большинстве случаев применяют алгоритмы MD5, SHA1 и российский алгоритм, изложенный в ГОСТ Р 34.11 94 (он считается одним из самых надежных). В криптографии хэш-коды чаще всего имеют длину 128, 160 и 256 бит.

Хэширование используется также для проверки правильности передачи данных. Различные контрольные суммы, используемые для проверки правильности передачи данных, – это не что иное, как хэш-коды.

[6] Однако такой пароль сложно запомнить.

? *Вопросы и задачи*

1. Что такое хэширование? хэш-функция? хэш-код?
2. Какую хэш-функцию вы используете, когда начинаете искать слово в словаре?
3. Что такое коллизии? Почему их должно быть как можно меньше?
4. Какие требования предъявляются к хэш-функциям, которые используются при хранении паролей?
5. Что значит «вычислительно невозможно»?
6. Взломщик узнал хэш-код пароля администратора сервера. Сможет ли он получить доступ к секретным данным на сервере?
7. Какие свойства пароля влияют на его надежность?
8. Как выбрать надежный пароль?
9. Какие алгоритмы хэширования сейчас чаще всего применяются?
10. *Предложите какой-нибудь свой метод хэширования. Подумайте, как часто при его использовании могут происходить коллизии.

10.6. Современные алгоритмы шифрования

Государственным стандартом шифрования в России является алгоритм, зарегистрированный как ГОСТ 28147-89. Он является *блочным* шифром, то есть шифрует не отдельные символы, а 64-битные блоки. В алгоритме предусмотрено 32 цикла преобразования данных с 256-битным ключом, за счет этого он очень надёжен (обладает высокой криптостойкостью). На современных компьютерах раскрытие этого шифра путем перебора ключей («методом грубой силы») займет не менее сотен лет, что делает такую атаку бессмысленной. В США используется аналогичный блочный шифр AES.

В Интернете популярен алгоритм RSA, названный так по начальным буквам фамилий его авторов – Р. Райвеста (R. Rivest), А. Шамира (A. Shamir) и Л. Адлемана (L. Adleman). Это алгоритм с *открытым* ключом, стойкость которого основанный на использовании свойств простых чисел. Для его взлома нужно разложить очень большое число на простые сомножители. Эту задачу сейчас умеют решать только перебором вариантов. Поскольку количество вариантов огромно, для раскрытия шифра требуется много лет работы современных компьютеров.

Для применения алгоритм RSA требуется построить открытый и секретный ключи следующим образом.

1. Выбрать два больших простых числа, p и q.
2. Найти их произведение $n = p \cdot q$ и значение $\varphi = (p-1)\cdot(q-1)$.
3. Выбрать число e ($1 < e < \varphi$), которое не имеет общих делителей с φ.
4. Найти число d, которое удовлетворяет условию $d \cdot e = k\varphi + 1$ для некоторого целого k.
5. Пара значений (e,n) – это открытый ключ RSA (его можно свободно публиковать), а пара (d,n) – это секретный ключ.

Передаваемое сообщение нужно сначала представить в виде последовательности чисел в интервале от 0 до $n-1$. Для шифрования используют формулу

$$y = x^e \bmod n,$$

где x – число исходного сообщения, (e,n) – открытый ключ, y – число закодированного сообщения, а запись $x^e \bmod n$ обозначает остаток от деления x^e на n. Расшифровка сообщения выполняется по формуле

$$x = y^d \bmod n.$$

Это значит, что зашифровать сообщение может каждый (открытый ключ общеизвестен), а прочитать его – только тот, кто знает секретный показатель степени d.

Для лучшего понимания мы покажем работу алгоритма RSA на простом примере. Возьмем $p = 3$ и $q = 7$, тогда находим $n = p \cdot q = 21$ и $\varphi = (p-1)\cdot(q-1) = 12$. Выберем $e = 5$, тогда равенство $d \cdot e = k\varphi + 1$ выполняется, например, при $d = 17$ (и $k = 7$). Таким образом, мы получили открытый ключ (5,21) и секретный ключ (17,21).

Зашифруем сообщение «123» с помощью открытого ключа (5,21). Получаем

$$1 \Rightarrow 1^5 \bmod 21 = 1, \quad 2 \Rightarrow 2^5 \bmod 21 = 11, \quad 3 \Rightarrow 3^5 \bmod 21 = 12,$$

то есть зашифрованное сообщение состоит из чисел 1, 11 и 12. Зная секретный ключ (17,21), можно его расшифровать:

$$1 \Rightarrow 1^{17} \bmod 21 = 1, \quad 11 \Rightarrow 11^{17} \bmod 21 = 2, \quad 12 \Rightarrow 12^{17} \bmod 21 = 3.$$

Мы получили исходное сообщение.

Конечно, вы заметили, что при шифровании и расшифровке приходится вычислять остаток от деления очень больших чисел (например, 12^{17}) на n. Оказывается, само число 12^{17} в этом случае находить не нужно. Достаточно записать в обычную целочисленную переменную, например, x, единицу, а потом 17 раз выполнить преобразование $x = 12 \cdot x \bmod 21$. После этого в переменной x будет значение $12^{17} \bmod 21 = 3$. Попробуйте доказать правильность этого алгоритма.

Для того, чтобы расшифровать сообщение, нужно знать секретный показатель степени d. А для этого, в свою очередь, нужно найти сомножители p и q, такие что $n = p \cdot q$. Если n велико, это очень сложная задача, ее решение перебором вариантов на современном компьютере займет сотни лет. В 2009 году группа ученых из разных стран в результате многомесячных расчетов на сотнях компьютеров смогла расшифровать сообщение, зашифрованное алгоритмом RSA с 768-битным ключом. Поэтому сейчас надежными считаются ключи с длиной 1024 бита и более. Если будет построен работающий квантовый компьютер, взлом алгоритма RSA будет возможен за очень небольшое время.

При использовании симметричных шифров всегда возникает проблема: как передать ключ, если канал связи ненадежный? Ведь получив ключ, противник сможет расшифровать все дальнейшие сообщения. Для алгоритма RSA этой проблемы нет, сторонам достаточно обменяться открытыми ключами, которые можно показывать всем желающим.

У алгоритма RSA есть еще одно достоинство: его можно использовать для цифровой подписи сообщений. Она служит для доказательства авторства документов, защиты сообщений от подделки и умышленных изменений.

Цифровая подпись – это набор символов, который получен в результате шифрования сообщения с помощью личного секретного кода отправителя.

Отправитель может передать вместе с исходным сообщением такое же сообщение, зашифрованное с помощью своего секретного ключа (это и есть цифровая подпись). Получатель расшифровывает цифровую подпись с помощью открытого ключа. Если она совпала с незашифрованным сообщением, можно быть уверенным, что его отправил тот человек, который знает секретный код. Если сообщение было изменено при передаче, оно не совпадет с расшифрованной цифровой подписью. Так как сообщение может быть очень длинным, для сокращения объема передаваемых данных чаще всего шифруется не всё сообщение, а только его хэш-код.

Во многих современных программах есть возможность шифровать данные с паролем. Например, офисные пакеты *OpenOffice.org* и *Microsoft Office* позволяют шифровать все создаваемые документы (для их просмотра и/или изменения нужно ввести пароль). При создании архива (на-

пример, в архиваторах 7ZIP, *WinRAR*, *WinZip*) также можно установить пароль, без которого извлечь файлы невозможно.

В простейших задачах для шифрования файлов можно использовать бесплатную программу *Шифровальщик* (*www.familytree.ru/ru/cipher.htm*), версии которой существуют для *Linux* и *Windows*. Программы *TrueCrypt* (*www.truecrypt.org*), *BestCrypt* (*www.jetico.com*) и *FreeOTFE* (*freeotfe.org*) создают логические диски-контейнеры, информация на которых шифруется. Свободно распространяемая программа *DiskCryptor* (*diskcryptor.net*) позволяет шифровать разделы жестких дисков и даже создавать шифрованные флэш-диски и CD/DVD диски.

Программа *GnuPG* (*gnupg.org*) также относится к свободному программному обеспечению. В ней поддерживаются симметричные и несимметричные шифры, а также различные алгоритмы электронной цифровой подписи.

? *Вопросы и задачи*

1. Какой алгоритм шифрования принят в России в качестве государственного стандарта?
2. Что такое блочный алгоритм шифрования?
3. К какому типу относится алгоритм RSA? На чем основана его криптостойкость?
4. *Напишите программу, которая строит открытый и секретный ключи RSA для небольших множителей p и q.
5. *Напишите программу, которая шифрует и расшифровывает сообщения с помощью алгоритма при небольших значениях открытого и секретного ключей.
6. Что такое цифровая подпись?
7. Как можно использовать алгоритм RSA для цифровой подписи?

10.7. Стеганография

При передаче сообщений можно не только применять шифрование, но и скрывать сам факт передачи сообщения.

Стеганография – это наука о скрытой передаче информации путем скрытия самого факта передачи информации.

Древнегреческий историк Геродот описывал, например, такой метод: на бритую голову раба записывалось сообщение, а когда его волосы отрастали, он отправлялся к получателю, который брил его голову и читал сообщение.

Классический метод стеганографии – *симпатические* (невидимые) *чернила*, которые проявляются только при определенных условиях (нагрев, освещение, химический проявитель). Например, текст, написанный молоком, можно прочитать при нагреве.

Сейчас стеганография занимается скрытием информации в текстовых, графических, звуковых и видеофайлах с помощью программного «внедрения» в них нужных сообщений.

Простейшие способ – заменять младшие биты файла, в котором закодировано изображение. Причем это нужно сделать так, чтобы разница между исходным и полученным рисунками была неощутима для человека. Например, если в черно-белом рисунке (256 оттенков серого), яркость каждого пикселя кодируется 8 битами. Если поменять 1-2 младших бита этого кода, «встроив» туда текстовое сообщение, фотография, в которой нет четких границ, почти не изменится. При замене 1 бита каждый байт исходного текстового сообщения хранится в младших битах кодов 8 пикселей. Например, пусть первые 8 пикселей рисунка имеют такие коды:

10101101	10010100	00101010	01010010	10101010	10101010	10101011	10101111

Чтобы закодировать в них код буквы «И» (11001000_2), нужно изменить младшие биты кодов:

10101101	10010101	00101010	01010010	10101011	10101010	10101010	10101110
1	1	0	0	1	0	0	0

Получателю нужно взять эти младшие биты и «собрать» их вместе в один байт.

Для звуков используются другие методы стеганографии, основанные на добавлении в запись коротких условных сигналов, которые обозначают 1 и 0 и не воспринимаются человеком на слух. Возможна также замена одного фрагмента звука на другой.

Для подтверждения авторства и охраны авторских прав на изображения, видео и звуковые файлы применяют *цифровые водяные знаки* – внедренную в файл информацию об авторе. Они получили свое название от старых водяных знаков на деньгах и документах. Для того чтобы установить авторство фотографии, достаточно расшифровать скрытую информацию, записанную с помощью водяного знака.

Иногда цифровые водяные знаки делают видимыми (текст или логотип компании на фотографии или на каждом кадре видеофильма). На многих сайтах, занимающихся продажей цифровых фотографий, видимые водяные знаки размещены на фотографиях, предназначенных для предварительного просмотра.

? *Вопросы и задачи*

1. Что такое стеганография?
2. Какие методы стеганографии существовали до изобретения компьютеров?
3. Как можно добавить текст в закодированное изображение?
4. На чем основаны методы стеганографии для звуковых и видеоданных?
5. Что такое цифровые водяные знаки? Зачем они используются?

10.8. Безопасность в Интернете

10.8.1. Угрозы безопасности

Если компьютер подключен к Интернету, появляются дополнительные угрозы безопасности. Атаку через сеть могут проводить злоумышленники и *боты* (программы-роботы), находящиеся в других городах и странах. Можно выделить три основные цели злоумышленников:

- *использование вашего компьютера* для взлома других компьютеров, атак на сайты, рассылки спама, подбора паролей и т.п.;
- *кража секретной информации* – данных о банковских картах, имен и паролей для входа на почтовые сервера, в социальные сети, платежные системы;
- *мошенничество* – хищение чужого имущества путем обмана.

Первые две угрозы связаны, главным образом, с вредоносными программами: вирусами, червями и «троянцами», которые позволяют злоумышленнику управлять компьютером через сеть и получать с него данные.

Мошенничество процветает потому, что многие пользователи Интернета очень доверчивы и неосторожны. Классический пример мошенничества – так называемые «нигерийские письма», приходящие по электронной почте. Пользователя от имени какого-то бывшего высокопоставленного лица просят принять участие в переводе крупных денежных сумм за границу, обещая выплачивать большие проценты. Если получатель соглашается, мошенники постепенно выманивают у него деньги.

Фишинг (англ. *phishing*, искажение слова *fishing* – рыбная ловля) – это выманивание паролей. Для этого чаще всего используются сообщения электронной почты, рассылаемые якобы от

имени администраторов банков, платежных систем, почтовых служб, социальных сетей. В сообщении говорится, что ваш счёт (или учетная запись) заблокирован, и дается ссылка на сайт, который внешне выглядит как настоящий, но расположен по другому адресу (это можно проверить в адресной строке браузера). Неосторожный пользователь вводит своё кодовое имя и пароль, с помощью которых мошенник получает доступ к данным или банковскому счету.

Антивирусы и последние версии браузеров содержат специальные модули для обнаружения подозрительных сайтов («*антифишинг*») и предупреждают о заходе на такой сайт. Кроме того, нужно помнить, что администраторы сервисов никогда не просят пользователя сообщить свой пароль по электронной почте.

Мошенничество может быть связано и с вредоносными программами. В 2010 году несколько миллионов компьютеров в России было заражено троянской программой *Winlock*, которая блокировала компьютер и требовала отправить платное SMS-сообщение для снятия блокировки.

10.8.2. Правила личной безопасности

Вредоносные программы, распространяющиеся через Интернет, представляю серьезную угрозу безопасности данных. Нужно помнить, что многих проблем можно избежать, если работать в Интернете только из-под ограниченной учетной записи (без прав администратора). Кроме того, желательно своевременно обновлять программное обеспечение; особенно важно устанавливать «заплатки», связанные с безопасностью.

Чтобы ваши пароли не украли, лучше не запоминать их в браузере (иногда они хранятся в открытом виде и могут быть украдены троянской программой). Заходя под своим именем в закрытую зону сайта с другого компьютера, нужно отмечать флажок «*Чужой компьютер*», иначе следующий человек, открывший эту страницу, сможет получить доступ к вашим данным.

На многих сайтах предусмотрена возможность восстановления пароля по секретному вопросу. Этот вопрос нужно выбирать так, чтобы никто другой не знал ответа на него и, самое важное, не мог его выведать. Например, ответы на вопросы «Как звали Вашу первую собаку?», «Какое Ваше любимое блюдо?» и т.п. часто можно найти на персональных страничках авторов в социальных сетях (в заметках, подписях к фотографиям и т.п.). Если мама автора имеет свою страничку, на ней, скорее всего можно найти ее девичью фамилию, поэтому вопрос «Какова девичья фамилия вашей матери?» тоже лучше не использовать.

Нужно понимать, что размещая какую-то информацию в Интернете, вы делаете ее доступной для широкого круга лиц, включая работодателей, милицию, официальные органы и даже преступников. Возможны ситуации, когда эта информация (личные данные, фотографии, высказывания на форумах и в блогах) может быть использована против вас, даже если она находится в закрытом разделе сайта.

Для передачи информации, которую необходимо сохранить в тайне, лучше применять шифрование (например, упаковать данные в архив с паролем).

Наибольший уровень безопасности обеспечивается при денежных расчетах через Интернет: вместо протокола *HTTP* используют защищенный протокол *HTTPS* (англ. *Hypertext Transfer Protocol Secure* – безопасный *HTTP*), который предусматривает шифрование данных (например, с помощью алгоритма *RSA*). Поэтому нужно проверять, чтобы адрес на странице ввода пароля в таких системах начинался с «**`https://`**», а не с «**`http://`**».

Современные молодые люди часто общаются в чатах, форумах и т.п., в том числе с теми, кого они не знают лично. Продолжение такого *виртуального* (компьютерного, электронного) знакомства в реальной жизни весьма опасно, потому что нередко участники чатов и форумов представляются не теми, кем они являются на самом деле.

? *Вопросы и задачи*

1. Какие угрозы безопасности существуют при подключении к Интернету?
2. Какие схемы интернет-мошенничества вам известны?
3. Какие меры безопасности нужно соблюдать при работе в Интернете?
4. Как обеспечивается безопасность обмена данными при денежных расчетах в Интернете?