Посвящается
моим школьным друзьям,
Алексею Титову и Юрию Кретинину,
выпускникам средней школы № 11
г. Калининграда (ныне г. Королев)
Московской области

Содержание

От автора

Уважаемые читатели!
Прежде чем вы начнете читать данную книгу, считаю необходимым ознакомить вас со следующей информацией.

Любые оценки, мнения, рекомендации, высказанные в этой книге, являются личными оценками, мнениями автора и не могут рассматриваться как реклама или антиреклама.

Автор старался предоставлять точную и проверенную информацию, однако не может гарантировать полной достоверности изложенных в книге материалов, рисунков и таблиц в связи со спецификой тематики рассматриваемых вопросов.

Ссылки, а также иные сведения даются исключительно в информационных целях.

Вся информация, изложенная в данной книге, приводится «как есть» (as is) с возможными ошибками, без гарантий любого вида, прямо выраженных или подразумеваемых. Поэтому ни автор, ни издательство не несут ответственности за возможные последствия, вызванные использованием приведенных в данной книге материалов, рисунков, схем и иной информации, в том числе за любые прямые или косвенные убытки, возникшие в результате практического или теоретического применения сведений, изложенных в этой книге.

Использование рисунков, таблиц и схем, приводимых в данной книге, а также иной изложенной в ней информации осуществляется читателем на собственный страх и риск с возложением на него ответственности за все возможные последствия, в том числе за возникшие у него или у третьих лиц прямые или косвенные убытки.

С уважением и наилучшими пожеланиями,
М. В. Адаменко

Предисловие

На протяжении всей многовековой истории человечества многих людей всегда интересовала возможность обмениваться сообщениями, содержащими какую-либо информацию. Поэтому наши изобретательные предки постоянно придумывали разнообразные способы и средства для передачи и сохранения определенных сведений. При этом для отображения или фиксирования информации, для ее передачи и приема, а также для хранения данных человечество с древних времен использует всевозможные системы условных обозначений, знаков, символов и сигналов. Главными требованиями, предъявляемыми к таким системам кодирования, начиная от возникновения письменности, являются не только обеспечение возможности отображения, передачи и сохранения сведений, но и сравнительно легкое понимание смысла и содержания информации, которую несет тот или иной символ или знак.

В то же время всегда существовал и существует определенный круг лиц, заинтересованных в том, чтобы с содержанием создаваемых ими сообщений могли ознакомиться только те люди, которым эти сообщения предназначены. Для создания таких секретных сообщений и были нужны шифры. Поэтому шифры стары как сам мир. Люди начали придумывать шифры с незапамятных времен, с тех самых пор, когда впервые захотели что-то утаить.

Короли и королевы, законные и незаконные наследники и претенденты на престол, президенты и главы правительств, высокопоставленные чиновники и предприниматели – все они зашифровывали и зашифровывают свою личную, государственную, дипломатическую и деловую почту с той целью, чтобы об их замыслах не узнали их недруги, шпионы из других государств или, например, конкуренты. Великие полководцы и флотоводцы отдавали и отдают зашифрованные приказы, чтобы важная военная информация не оказалась в руках противника. Влюбленные договаривались и договариваются о своих тайных встречах с помощью писем, содержание которых скрыто шифром.

Необходимость использования шифров и в нашей повседневной жизни весьма высока, поскольку дипломатические, военные и промышленные секреты обычно передаются или хранятся не в исходном, а в зашифрованном виде. Помимо этого, с развитием современ-

ных технологий стремительно возрастает потребность в надежных шифрах для сохранения не только государственных или военных тайн, коммерческих секретов фирм и компаний, но также, безусловно, сведений, имеющих непосредственное отношение к нашей личной жизни.

Следует признать, далеко не всегда высокопоставленные особы и простые смертные для скрытия истинного смысла своего сообщения использовали собственноручно созданные ими шифры. Для создания надежных шифров чаще всего нанимались талантливые люди, ученые и изобретатели. Способность и умение создать шифр для сообщения, которое смогут прочитать только друзья, а не враги, всегда ценилась очень высоко.

В то же время всегда существовало немалое число заинтересованных лиц, которые многое отдали бы за то, чтобы прочитать секретные послания, им не предназначенные. Они также никогда не жалели сил и средств для того, чтобы раскрыть шифр и прочитать интересующее их сообщение. Для достижения своих целей они также нанимали не менее талантливых и способных специалистов.

Поэтому от момента появления первой буквы и до настоящего времени изобретатели шифров постоянно совершенствуют свое мастерство. Но и те, кто пытался и пытается прочитать тайные сообщения, тоже не сидят сложа руки. И в наше время это незримое соревнование между создателями шифров и теми, кто их желает раскрыть, продолжается. При этом невидимые поля ожесточенных сражений переместились на экраны компьютерных мониторов.

Необходимо признать, что большинство людей не может преодолеть искушение попробовать разгадать какую-либо головоломку, кроссворд, ребус или шифр. И нет ничего удивительного в том, что тайные шифры принадлежат к наиболее притягательным головоломкам современности. Поэтому всегда были, есть и будут весьма одаренные люди, которые ради собственного удовольствия занимались, занимаются и будут заниматься созданием и, естественно, разгадкой разных головоломок, в том числе очень замысловатых и на сегодняшний день практически не поддающихся разгадке шифров. К сожалению, довольно часто усилия некоторых из них направлены для достижения весьма неблаговидных целей.

Увлекаясь разгадкой чужих шифрованных посланий, не следует забывать о том, что тайна переписки охраняется законом. В конце концов, читать чужие письма просто неприлично. Более того, многие действия, связанные с вскрытием чужой корреспонденции, а также

с противоправным получением и незаконным использованием информации, преследуются в уголовном порядке.

Однако истории известна масса примеров, когда для того, чтобы избежать больших бед для огромного количества ничего не подозревающих людей, было просто необходимо получить определенные сведения, мягко выражаясь, не совсем законными средствами. В том числе и с помощью разгадки шифров секретных сообщений. Так, например, немалую роль в победе во Второй мировой войне сыграли талантливые специалисты Советского Союза, США, Великобритании и их союзников, разгадывая шифры фашистской Германии и милитаристской Японии, предоставляя руководителям государств самую достоверную информацию о намерениях противника.

Поэтому при создании, использовании и особенно при разгадке всевозможных шифров читатель всегда должен четко представлять себе границы дозволенного. Эти границы определяются не только нормами действующего гражданского и уголовного законодательства, но и нравственными устоями, моральными принципами и ответственностью, сознанием и совестью каждого отдельного человека.

При работе над предлагаемой книгой автор ставил перед собой несколько задач. Среди них были ознакомление читателей как с историей возникновения и развития кодов и шифров, так и с наиболее интересными и заметными событиями из истории криптологии. Автор также попытался рассказать о самых сложных для своего времени шифрах и кодах, которые были изобретены за всю многовековую историю человечества, а также о гениях, которые смогли их разгадать.

Естественно, для того чтобы читатель имел хотя бы общее представление, о чем написана эта книга, перед кратким изложением исторических фактов автор постарался в простой и доступной форме разъяснить значение основных понятий, терминов и определений, используемых при работе с шифрами и кодами.

Не менее важной являлась и задача научить заинтересованных читателей самостоятельно составлять простейшие шифры для использования в повседневной жизни. Без сомнения, овладение навыками работы с шифрами способствует развитию наблюдательности, сосредоточенности, терпеливости и последовательности в суждениях, не говоря уже об аналитических способностях и логическом мышлении.

В предлагаемой книге рассматриваются простые шифры и особенности их практического применения даже неподготовленными пользователями в повседневной жизни. Такие шифры обычно используются для защиты личных данных, позволяя значительно ограничить

возможность несанкционированного получения и использования пароля или кода доступа, например, к банковской карте, к банковскому счету, а также в других случаях.

Для подавляющего большинства людей удержать в памяти даже несколько паролей и кодов доступа (например, пароли к банковским картам или PIN-коды к SIM-картам мобильных телефонов и т. п.) весьма сложно. И желание иметь эти данные всегда под рукой вполне закономерно и оправдано. Для этого используются различные технические средства. Например, программное обеспечение многих моделей мобильных телефонов содержит специальные приложения, предназначенные для хранения паролей и кодов доступа.

Однако не всегда и не все пользователи для хранения соответствующих сведений и данных могут и желают воспользоваться техническими средствами, по-прежнему доверяя листу бумаги. В этом случае значительно ограничить возможность использования пароля или кода доступа, например, к той же банковской карте, можно весьма простым способом. Для этого достаточно зашифровать пароль или код с помощью одного из рассматриваемых в этой книге шифров, после чего его можно хранить вместе с банковской картой. Конечно же, после нескольких неудачных попыток преступник может разгадать шифр и узнать пароль. Однако количество таких неудачных попыток практически всегда будет многократно превышать допустимый для банковской карты лимит. В результате после определенного числа неправильно введенных паролей карта будет заблокирована.

В Библии сказано: «Благоразумный видит беду, и укрывается; а неопытные идут вперед, и наказываются» (Книга Притчей Соломоновых, 22:3). В современном мире каждый человек, желая оградить себя от кражи и мошенничества, должен, по меньшей мере, проявить определенную предусмотрительность, постоянно задавая себе вопросы о том, насколько надежно он защитил свои личные данные и каким образом он может улучшить их защиту. Предлагаемая книга поможет читателям найти ответы на эти вопросы.

Глава 1

Основные понятия и определения

Перед тем как начать знакомство с историей возникновения и развития кодов и шифров, не будет лишним разобраться, а что же обозначают эти таинственные слова «шифр» и «код». Есть ли между этими понятиями разница? И если есть, то в чем именно? Сразу следует признать, что в настоящее время даже среди специалистов, занимающихся шифрами и кодами, проходят оживленные дискуссии и даже споры, касающиеся формулировки точных определений этих терминов.

Тем не менее в этой главе попробуем дать объяснение тому, что именно на страницах предлагаемой книги мы будем называть «кодом», а что – «шифром».

Чтобы правильно определить истинное значение указанных слов, надо довольно точно и четко понимать, для чего нужны эти самые шифры и коды. Естественно, мы попытаемся дать определения и некоторым другим терминам и выражениям, используемым при работе с кодами и шифрами. Необходимо отметить, что предлагаемые далее разъяснения и определения не претендуют на академическую точность, поскольку отражают значение отдельных понятий и терминов в упрощенном виде, удобном для восприятия неподготовленными читателями.

Но сначала немного поговорим о другом.

1.1. Отрывки из теории информации

Когда разговор заходит о кодах и шифрах, большинство наших сограждан сразу вспоминают шпионские боевики и детективные романы. Именно из фильмов и литературных произведений многие из нас знают, что всевозможная секретная информация обычно передается с помощью зашифрованных сообщений. Однако далеко не все могут

внятно объяснить, что означают слова «информация» или, например, «сообщение».

Информация об информации

Не секрет, что в наше время иностранное слово «информация» известно каждому. Но постоянно употреблять его начали всего лишь несколько десятков лет назад. Именно тогда были опубликованы так называемые основы теории связи и передачи кодов. Эта теория и стала называться «теорией информации».

Однако сейчас смысл, вкладываемый в термин «информация» нашими современниками, значительно расширился. Для многих не владеющих специальными знаниями людей понимание значения этого слова во многом остается интуитивным и поэтому получает различные смысловые наполнения в различных отраслях человеческой деятельности. Более того, можно утверждать, что значение слова «информация» в строго научном смысле значительно отличается от того, как его понимает большинство окружающих нас людей.

Известный советский филолог Сергей Иванович Ожегов, составивший Словарь русского языка, считал, что информация – это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами, а также сообщения, осведомляющие о положении дел или о состоянии чего-нибудь.

Так, например, исходя из данного определения, любые сведения о космосе или о микроорганизмах, о кораблях или о растениях, о вулканах или о президентах – все это является информацией. Любые новости, о которых нам сообщают в радио- и телевизионных передачах или в газетах и журналах, – это информация. Любые знания, которые мы получаем из учебников или из книг, на уроках или лекциях, – это информация. Любые сообщения от друзей или знакомых – это информация. Даже в том случае, когда мы просто смотрим вокруг себя, мы получаем какие-либо сведения о тех объектах, на которые смотрим, то есть информацию о них.

Следует отметить, что приведенное выше определение не является классическим или общепризнанным. Ученые, работающие в разных областях науки, дают свои определения значения слова «информация».

Так, например, некоторые из них считают, что под информацией следует понимать любые сведения о каких-либо ранее неизвестных

объектах. Другие предлагают называть информацией результат отражения реальности в сознании человека, представленный на его внутреннем языке. Третьи убеждены, что информация – это содержательное описание объекта или явления. Для четвертых информация – содержание сигнала или сообщения, а для пятых – атрибут материи.

И на этом перечень предлагаемых определений не заканчивается. Весьма широкое распространение получила точка зрения многих ученых, считающих, что информация является одним из первичных понятий мироздания наряду с материей и энергией. Некоторые наши современники вполне обоснованно считают, что иностранному термину «информация» достаточно близко соответствует русское слово «смысл». В результате слово «информация» является одним из тех терминов, которые достаточно часто можно встретить не только в научных трудах, но и в разговорной речи. И значение этого слова интуитивно понятно каждому человеку.

Тем не менее особенности рассматриваемых в предлагаемой книге вопросов требуют однозначного понимания того, что же именно в последующих главах и разделах будет подразумеваться под информацией.

Итак, далее при упоминании о какой-либо информации или о сообщениях, содержащих какую-либо информацию, будем считать, что **информация** – это прежде всего какие-либо сведения об окружающем мире, содержащиеся в этих сообщениях, а также смысловое содержание таких сообщений. При этом указанные сведения являются объектом преобразования, передачи и хранения.

Конечно же, получаемая нами из всевозможных источников информация может быть неполной или, наоборот, исчерпывающей, она может быть правдивой или ложной. В конце концов, какая-либо информация нам может быть жизненно необходима или вовсе не нужна. Но, независимо от указанных признаков, такая информация остается информацией.

Преобразование, передача и хранение информации

В наше время преобразование или отображение информации, ее передача и хранение могут осуществляться самыми различными способами с применением не только хорошо известных, но и весьма непривычных средств. Однако так было далеко не всегда.

С древних времен человек искал средства и способы сначала для обмена информацией с соплеменниками, а затем для ее отображения и сохранения. И одними из первых таких способов были звуковые сигналы и жесты.

Нетрудно представить ситуацию, когда собирающийся на охоту древний человек, выглянув из пещеры, увидел, что идет дождь или ливень. Скорее всего, охота была отложена, а наш далекий предок вернулся в пещеру. Но как объяснить своим соплеменникам, почему они остались без обеда? Возможно, древний охотник набрал в ладони немного дождевой воды и, вернувшись в пещеру, выплеснул ее на своих сородичей. Как говорится, для полноты ощущений. Или же, издавая звуки определенной громкости и тональности, жестами передал сородичам информацию о плохой погоде. В рассмотренном случае информация о наличии дождя была преобразована нашим сообразительным предком в жесты и звуки.

Со временем у людей появилась потребность отображать или фиксировать определенную информацию. Так, например, после удачной охоты на мамонта переполняемые положительными эмоциями соплеменники высекали на стенах пещеры наиболее впечатляющие эпизоды этой охоты. Естественно, в те далекие времена древний человек и не предполагал, что одновременно с отображением определенных сцен он, высекая фигуру охотника или мамонта, сохраняет их на века, то есть фиксирует и сохраняет информацию.

Постепенно люди придумывали все новые возможности для обмена информацией, а также для ее отображения и сохранения. Появились речь и письменность, на смену стенам пещеры пришли папирус, а затем и бумага. В конце концов, человечество пришло к тому, что наши современники не могут представить себе окружающий мир без радиоволн и квантовой механики. Поэтому всю историю человечества можно считать историей поиска способов и средств для обмена и сохранения информации.

Для подавляющего большинства современных людей не существует проблем с отображением, передачей или с сохранением информации. Вопрос может быть лишь в правильном выборе нужных средств и способов.

Так, например, записать сведения об оценках, полученных учеником за полугодие обучения, можно в его дневнике. Но эти оценки также можно зафиксировать и в школьном компьютере. Информацию о новостях корреспондент может передать в редакцию с помощью телефона, телеграфом или просто письмом. При этом корреспонденты разных

стран передают одну и ту же информацию на разных языках. Сохранить какие-либо сведения можно, например, с помощью наскальных рисунков, как это делали наши предки. А можно записать необходимые данные на компакт-диск, карту памяти или флэш-диск. Такими данными могут быть не только результаты научных исследований, но и, например, любимые компьютерные игры или музыкальные записи.

Сообщение, сигнал, система связи

Всевозможная секретная информация обычно передается с помощью зашифрованных сообщений. Однако, как и в случае со словом «информация», не все наши современники могут объяснить, что понимается под словом «сообщение».

Напомним, что, строго говоря, теория информации является одной из ветвей теории связи. А само слово «связь» подразумевает обмен сообщениями. Таким образом, не углубляясь в рассмотрение теоретических вопросов, можно считать, что информация передается и хранится в виде сообщений.

Сообщение может иметь различный вид и форму. Так, например, сообщением является какой-либо текст. При этом такой текст может быть напечатан в газете, на бланке телеграммы или отображен на экране монитора. Сообщение может быть звуковым, например слова и предложения при разговоре, музыка, записанная на аудиокассету. Записанные на компакт-диск или флэш-карту музыкальные произведения или программы – это тоже сообщения.

Итак, **сообщение** – это знаки или сигналы, содержащие какую-либо информацию. Именно такое весьма упрощенное определение наиболее полно подходит при рассмотрении в данной книге вопросов шифрования и кодирования.

Знаками могут быть жесты или движения, графические изображения, например буквы и цифры. Для того чтобы сохранить какое-либо сообщение, достаточно, например, нанести его на бумагу с помощью букв. Но для передачи сообщения на расстояние необходимо, говоря научным языком, воспользоваться некоторым физическим процессом в широком смысле этого слова, способным с той или иной скоростью распространяться от источника к получателю сообщения. Это могут быть, например, изменения электрического поля, радиоволны, это могут быть почтовая и даже визуальная связь.

Таким образом, **сигнал** можно представить как изменяющийся во времени физический процесс, отражающий передаваемое сообщение.

В современном мире для передачи сигналов используются всевозможные технические средства, которые в совокупности составляют **системы связи**. При этом система связи обычно состоит из нескольких составных частей.

Во-первых, в состав любой системы связи входят источник сообщений, непосредственно создающий сообщение, и передатчик, который определенным образом обрабатывает сообщение и преобразует его в сигналы определенного типа. Например, телеграфист создает сообщение в виде точек и тире азбуки Морзе, а специальный радиопередатчик преобразует эти точки и тире в радиосигналы и излучает в эфир.

Во-вторых, при передаче сообщений не обойтись без канала связи, под которым обычно подразумевается комплекс технических средств, обеспечивающих передачу сигналов от передатчика к приемнику. Неотъемлемой частью канала связи является так называемая линия связи, то есть среда, используемая для передачи сигнала от передатчика к приемнику. Это может быть, например, область распространения радиоволн, обычные электрические провода или коаксиальный кабель.

В-третьих, в системе связи не обойтись без приемника, который восстанавливает исходное сообщение из полученных сигналов, то есть выполняет операцию, обратную той, которую выполнил передатчик.

И наконец, от приемника исходное сообщение поступает к получателю, под которым обычно понимаются лицо или аппарат, для которого предназначено сообщение. Так, например, радиосигналы принимаются специальным приемником, который их преобразует в точки и тире. Из точек и тире телеграфист, знающий азбуку Морзе, восстанавливает исходное сообщение.

1.2. Коды вокруг нас

С кодами каждый из нас встречается практически ежедневно и на каждом шагу. Более того, определенные коды являются неотъемлемой частью нашей повседневной жизни. Однако чаще всего наши современники об этом даже не догадываются. Тем не менее без преувеличения можно утверждать, что без кодов в нашей жизни было бы больше беспорядка, хотя чаще всего мы их не замечаем или не обращаем на них никакого внимания.

Так, например, обычные буквы и цифры являются кодом, который используется для создания сообщений. Дорожные знаки также явля-

ются частью системы кодов, предназначенной для сообщения водителю автомобиля определенной информации. Каждый раз, когда мы работаем на компьютере, то пользуемся специальным кодом, поскольку компьютеры между собой объясняются с помощью специальной числовой системы, называемой бинарный код. В бинарном коде используются только цифры 1 и 0. Подобных примеров в окружающей нас действительности можно найти превеликое множество.

Однако следует признать, что в настоящее время даже среди специалистов нет однозначного мнения о том, что же следует называть кодом. Поэтому, учитывая особенности рассматриваемых в данной книге вопросов, попробуем определить, что именно в последующих главах и разделах мы будем подразумевать под кодом.

Язык как система звуков и знаков

Итак, для того чтобы передать какую-либо информацию, современные люди в первую очередь используют речевые сигналы.

Попробуем представить себя в ранее рассмотренной ситуации, когда первобытный человек не пошел на охоту из-за дождя. Конечно же, не владея речью, объяснить что-либо соплеменникам было довольно сложно. Любой из нас может попробовать, не издавая ни одного членораздельного звука, объяснить своим родным и близким, что на улице идет дождь. Вряд ли наше объяснение будет понято достаточно быстро. Если вообще будет правильно понято. Поэтому для общения между собой люди придумали речевые сигналы или просто речь. Таким образом, наши предки с помощью речи создали первую систему условных обозначений и сигналов. А для определения такого природного явления, когда с неба капает вода, было придумано слово «дождь», которое в русском языке и представляет собой условное обозначение дождя.

Необходимо отметить, что в разных частях земного шара, на разных континентах, у разных племен появлялись свои речевые сигналы, которые вместе с соответствующей письменностью впоследствии стали языком того или иного племени или народа. При этом чаще всего каждое племя или народ вырабатывали свой язык, отличающийся от языков людей, проживающих на других территориях.

Сначала это были примитивные звуковые сигналы, постепенно некоторые языки усложнились настолько, что их изучение даже для представителей коренных наций представляет определенные сложности и продолжается в течение нескольких лет. К примеру, вспомним,