Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

А. Н. Поликанин

ИСТОРИЯ И СОВРЕМЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Утверждено редакционно-издательским советом университета
в качестве учебного пособия для обучающихся
по направлению подготовки 10.03.01 Информационная безопасность
(уровень бакалавриата)

Новосибирск
СГУГиТ
2022

УДК 007
П501

Рецензенты: доктор технических наук, зав. кафедрой безопасности информации и технологий СибГУТИ *С. Н. Новиков*

Ph. D., доцент СГУГиТ *А. В. Троеглазова*

Поликанин, А. Н.

П501 История и современные системы информационной безопасности : учебное пособие / А. Н. Поликанин. – Новосибирск : СГУГиТ, 2022. – 44 с. – Текст : непосредственный.

ISBN 978-5-907513-90-7

Учебное пособие подготовлено старшим преподавателем А. Н. Поликаниным на кафедре информационной безопасности СГУГиТ.

В настоящем пособии рассматриваются вопросы истории развития средств информационной безопасности с древности и до наших времен.

Учебное пособие по дисциплине «История систем защиты информации» предназначено для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

Рекомендовано к изданию кафедрой информационной безопасности, Ученым советом Института оптики и технологий информационной безопасности СГУГиТ.

Печатается по решению редакционно-издательского совета СГУГиТ

УДК 007

ISBN 978-5-907513-90-7

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Историю систем защиты информации можно разделить на 10 основных этапов:

1) понимание полезности введения противника в заблуждение, VI в. до н. э.;

2) понятие о сокрытии самого факта передачи информации, V в. до н. э.;

3) понятие о шифровании информации, IV в. до н. э.;

4) понятие о сохранении трактов передачи информации, XIII в.;

5) появление целенаправленной информационной разведки – прослушивание телефонных и перехват телеграфных сообщений, XIX в.;

6) развитие радио и появление радиоразведки, начало XX в.;

7) появление промышленного шпионажа, первая половина XX в.;

8) механические шифровальные машины, середина XX в.;

9) появление электронной вычислительной техники, 50-е гг. XX в.;

10) появление новых средств передачи информации – спутниковой связи (1960-е гг.), оптоволоконных линий (1970-е гг., наше время).

1. ЗАЩИТА ИНФОРМАЦИИ В ДРЕВНЕЕ ВРЕМЯ. ВВЕДЕНИЕ ПРОТИВНИКА В ЗАБЛУЖДЕНИЕ. ДЕЗИНФОРМАЦИЯ

Еще до начала эпохи развития средств информационной безопасности появилось понимание о том, что дезинформация – это тоже оружие. Первый письменный источник, в котором описано использование информации как средства ведения боевых действий, относится к VI в. до н. э.

Китайский военачальник Сунь Цзы в своем труде «Трактат о правилах ведения боевых действий» описывает использование информации как средство введения противника в заблуждение [1]. Это первый письменный источник, который вводит само понятие дезинформации. Трактат относительно небольшой – всего несколько страниц из деревянных реек (рис. 1).

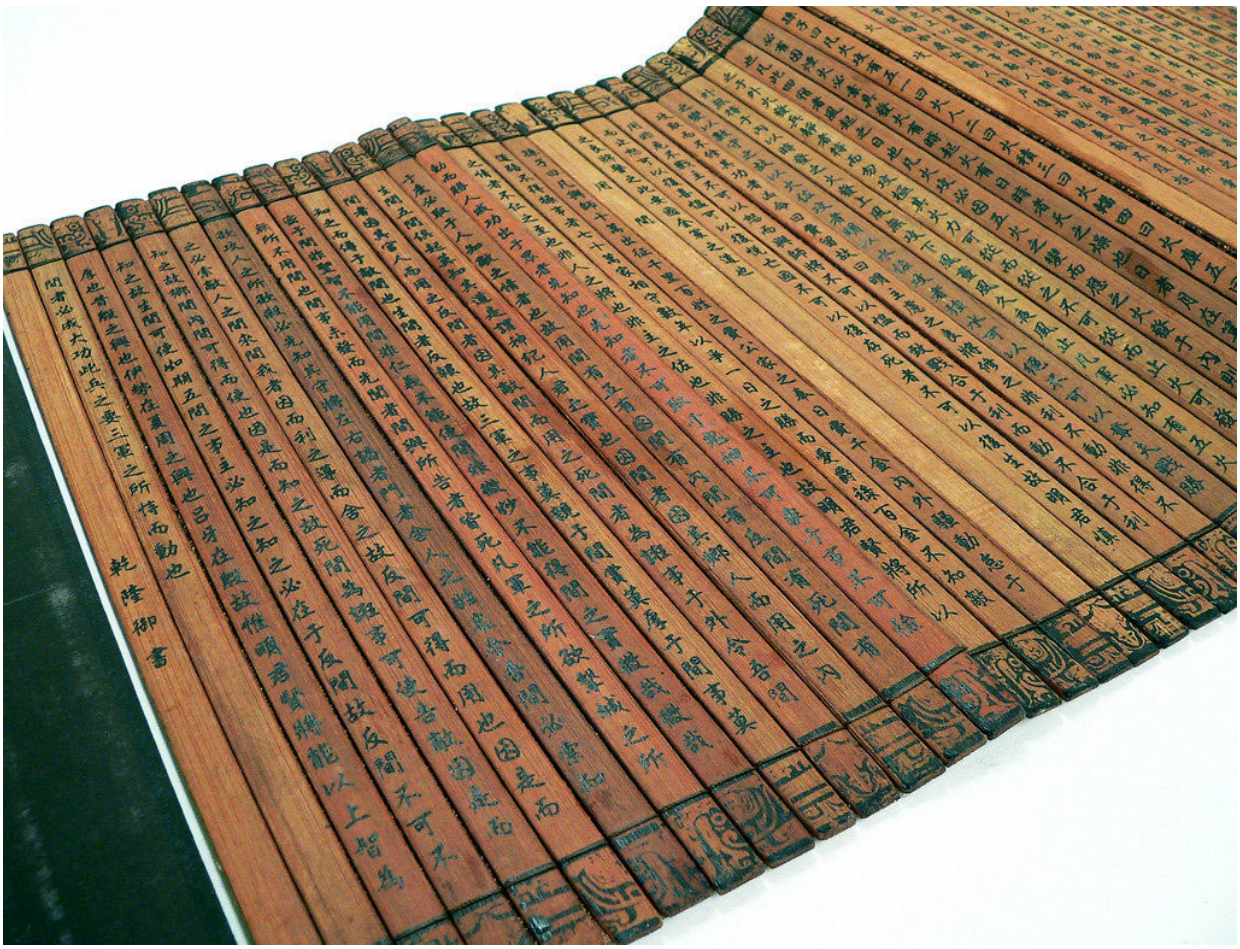

Рис. 1. Трактат о правилах ведения боевых действий

Однако даже сегодня он не потерял своей актуальности, и современные переводы трактата изучаются в ведущих военных академиях стран мира, в том числе во многом благодаря пониманию значения информации в военном противостоянии.

Вот несколько основных тезисов Сунь Цзы, которые касаются действий с информацией:

− если ты можешь что-нибудь, показывай противнику, будто не можешь;

− если ты пользуешься чем-нибудь, показывай ему, будто у тебя этого нет;

− хотя ты и близко, показывай, будто ты далеко;

− хотя ты и далеко, показывай, будто ты близко;

− заманивай его выгодой, а потом обмани;

− если он силен – жди и уклоняйся от него;

− вызови в нем гнев, приведи его в состояние расстройства; приняв смиренный вид, вызови в нем самомнение; если его силы свежи, утоми его; если они дружны, разъедини; нападай на него, когда он не готов; выступай, когда он не ожидает…

По сути, это первый труд, в котором описана информационная война. Большая часть этих правил посвящена искусству введения противника в заблуждение. В наше время, в эпоху переизбытка информации, мы привыкли иметь дело с недостоверными сведениями, и эти правила кажутся нам достаточно простыми. Однако в те времена, когда информационный обмен был ограничен и получение любой новой информации занимало большое количество времени, сил и ресурсов, такие приемы, как описанные в трактате, позволяли получить большое преимущество над врагом.

Некоторые исследователи считают, что Сунь Цзы не является реальным персонажем, а представляет собой собирательный образ, сам же трактат – это обобщение опыта информационных войн политиков и военачальников древнего Китая [2].

Тем не менее память о знаменитом китайском военачальнике до сих пор живет, его трактат пережил века, а самому Сунь Цзы установлены многочисленные памятники в самом Китае и в других странах (рис. 2).

Рис. 2. Памятник Сунь Цзы, Китай

2. ПОНЯТИЕ О СОКРЫТИИ ФАКТА ПЕРЕДАЧИ ИНФОРМАЦИИ

В Древней Греции в V в. до н. э. родилось понятие стеганографии от греческого «стеганос» – «покрытый» и «графиен» – «писать».

Сейчас это известный термин, определяющий способ защиты информации путем сокрытия самого факта передача информации адресату. Первый случай применения стеганографии относится к периоду греко-персидских войн, описанных Геродотом [3]. В те времена послания записывались на глиняных табличках или на пергаменте. Случай, о котором рассказывает Геродот, произошел на территории Греции в то время, когда в нее вторглись войска персидского царя Дария. Они осадили один из городов на севере Греции и сумели перехватить гонцов греческого полководца с просьбой о помощи к другим греческим городам. Для этого они останавливали всех путников, шедших по дороге в сторону греческих городов, обыскивали их в поисках писем и если что-то подозревали, отправляли их обратно или убивали. Для передачи послания греки пошли на хитрость. Одному из рабов обрили голову и записали послание на кожу его головы виде татуировки (рис. 3).

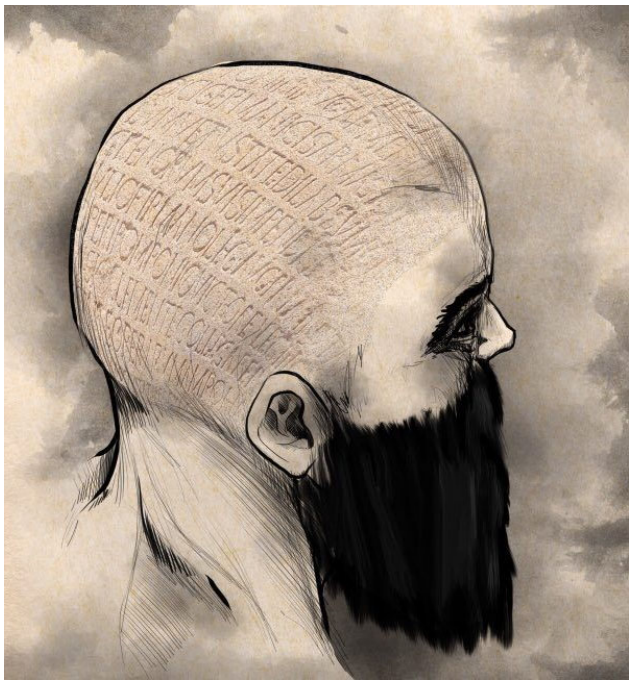

Рис. 3. Послание на голове раба

После того как его волосы немного отросли, они отправили его через позиции персидских войск. Конечно, персы сразу же остановили раба, обыскали его, при этом увидели, что раб немой, у него нет языка, значит, он не может говорить; у него нет никаких посланий при себе, значит, он не может ничего передать. Рабы в те времена были неграмотны, также, как и большинство населения, и представить, что он мог что-то написать позже и передать тем самым информацию, было практически невозможно. Поэтому раба отпустили, он преодолел позиции персидской армии и благополучно достиг ближайшего греческого города. Добравшись до места назначения, он попросил снова обрить ему голову и послание было прочитано. Трудно сказать, насколько правдива эта история, но, как можно понять из нее, основной недостаток стеганографии заключается в том, что при обнаружении скрытой информации противником он легко сможет ее прочитать. Именно это происходило впоследствии, когда в Грецию вторглись римские войска. Когда греки применяли этот прием для передачи посланий, римляне уже знали о нем и обривали головы в поисках записей. Так были пойманы и обнаружены несколько курьеров, несших информацию на своей голове (рис. 4).

Рис. 4. Обнаружение послания

Другие случаи применения стеганографии были описаны греческим историком Плинием [4]. В своих трудах он упоминал применение сока растений в качестве чернил для записи сообщений на пергаменте. Прозрачный сок растений после застывания оставался прозрачным и невидимым, однако при обжигании пергамента над огнем свечей сок растений темнел и проявлялись буквы текста. При этом скрытая запись выполнялась между строк обычного открытого текста. Таким образом при нахождении его противником, он предполагал, что в нем содержится только та информация, которую он мог прочитать. Обычно для этого использовалась смесь лимонного сока с водой. Такой способ сокрытия информации на бумаге используется даже сейчас (рис. 5).

Рис. 5. Стеганография соком растений

В дальнейшем, с развитием техники, стеганография получила широкое распространение для доставки тайных сообщений. Например, во время Второй мировой войны использовался способ сокрытия сообщений с помощью оптической техники. Для этого применялся фотоувеличитель, который использовался в обратном режиме, уменьшая исходное послание до микроскопических размеров, а оно, в свою очередь, фотографировалось и распечатывалось, добавляясь в открытое письмо в виде точек или других декоративных элементов.

Одна из таких применявшихся схем представлена на рис. 6. Способ был использован немецкой агентурой для отправки сообщений в Соединенные Штаты Америки.

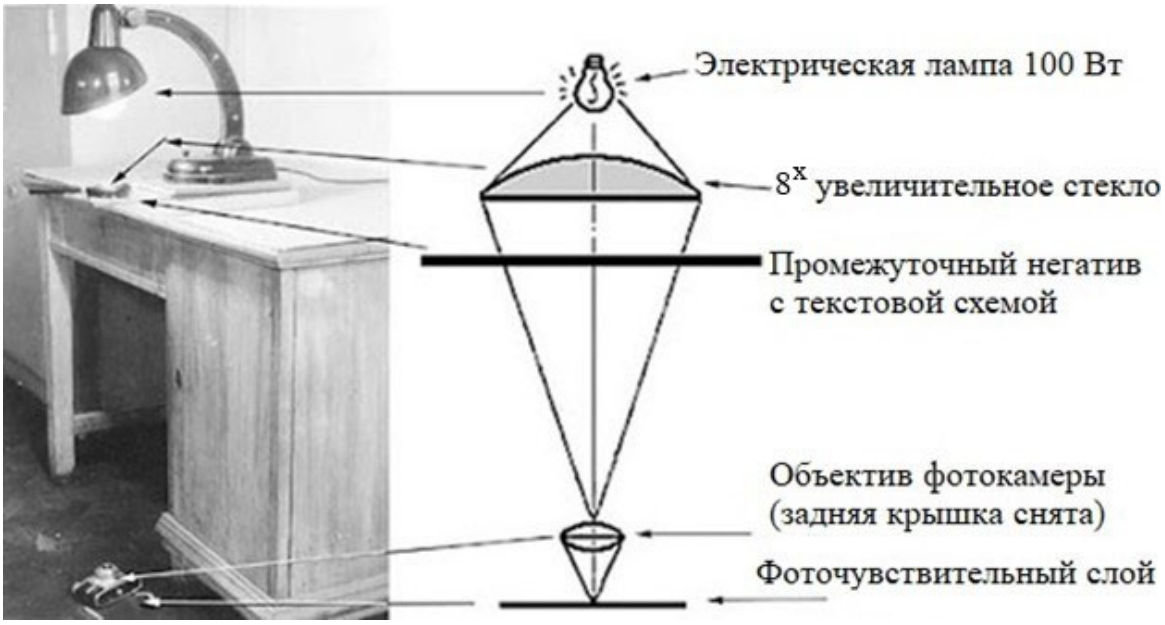

Рис. 6. Схема создания скрытого сообщения

При этом конечный объект послания выглядел как одна из точек, образующих декоративный фон конверта. То есть скрытое сообщение нанесено не на само послание, а на сопутствующие предметы. Это тоже одна из форм обеспечения сохранения в секрете факта передачи сообщения (рис. 7).

Для того чтобы прочитать этот текст, необходимо было провести обратное оптическое преобразование с помощью фотоувеличителя. Однако для этого, конечно, необходимо было знать, что это послание там имеется.

Сегодня для применения стеганографии достаточно использовать простую программу, позволяющую объединить текстовый файл с файлом изображения. При этом текст сообщения равномерно распределяется среди символов гипертекста, образующих код изображения. Не зная алгоритма распределения текста, выявить его в результирующем файле изображения очень трудно. Интерфейс одной из таких программ, а также результат преобразования представлен на рис. 8.

Внешне фото никак не изменяется, файл становится лишь немного «тяжелей», на размер вписанного в него текста.

Рис. 7. Конверт с микроточкой, отправленной в 1941 г. немецкому агенту в США

Рис. 8. Слияние текста с картинкой

3. ПОНЯТИЕ О ШИФРОВАНИИ ИНФОРМАЦИИ

Примерно к IV в. до н. э. родилось понимание того, что информацию нужно не только скрывать, но и изменять ее так, чтобы противник, даже получив конфиденциальное послание и узнав о его существовании, просто не сумел его прочитать. Такой способ защиты информации получил название «криптография» («криптос» (греч.) – «тайный»).

Цель криптографии – скрыть не наличие сообщения, а его смысл.

Тогда же родились основные способы криптографического сокрытия информации. Таких способов было два: перестановка и замена [5].

Способ шифрования методом перестановки заключается в следующем: все буквы каждого слова перемешивались согласно определенному алгоритму. Если послание было достаточно большим, восстановить его после перемешивания крайне трудно. В качестве примера рассмотрим слово «код». Это слово состоит из трех букв и имеет шесть вариантов написания после перестановки символов.

«КОД»: КДО, ДОК, ДКО, ОКД, ОДК.

Таким образом, можно констатировать, что число вариантов перестановки какого-либо текста, состоящего из n символов равно $n!$. В данном случае $3! = 6$.

Для примера посмотрим на следующий текст: «Рассмотрим данное короткое предложение». Это предложение имеет 35 символов, $35! = 1 \cdot 10^{40}$. Последнее число 40-й степени – это и есть число вариантов перестановки предложения. Как мы видим, перебрать все варианты без применения вычислительной техники было невозможно.

Конечно, мало провести подобную перестановку в хаотичном порядке; необходимо, чтобы адресат смог прочитать это послание. Для этого адресат должен знать алгоритм, по которому происходила перестановка. Такой алгоритм носит название «ключ». Зная ключ, всегда можно восстановить зашифрованное послание до исходного варианта.

Рассмотрим самый простой пример метода перестановки под названием «штакетник». Для этого возьмем то же самое предложение из примера выше, но уберем из него все пробелы:

рассмотримданноекороткоепредложение.

Следующим этапом необходимо выписать в ряд все нечетные символы предложения, а в другой ряд – все четные символы:

– рсмтиднокртопелжне – *все нечетные;*

– асорманеоокердоеи – *все четные.*

После этого обе строки необходимо совместить:

рсмтиднокртопелжнеасорманеоокердоеи.

Получившийся в итоге текст невозможно прочитать и понять, если не знать механизма обратного преобразования, то есть ключа. Для обратной операции нужно разделить текст пополам, при этом первая половина включает в себя нечетные символы, а вторая половина – четные. Расположив их поочередно, мы получим исходный текст.

Для реализации алгоритма перестановки применялись специальные приспособления. Одним из таких была изображенная на рисунке греческая скитала (рис. 9).

Рис. 9. Скитала

Скитала представляла собой многогранный деревянный брусок, на который наматывалась лента из кожи или пергамента. После этого на ленте записывалось сообщение, каждая строчка которого соответствовала грани

бруска. Каждая буква послания записывалась на следующем отрезке ленты. Когда лента разматывалась, получившийся ряд символов представлял собой хаотичный набор, который невозможно было прочитать без применения такой же по размеру и конфигурации скиталы.

В данном примере роль ключа играет специальное приспособление, которое задает алгоритм прямого и обратного преобразования.

Следующий способ шифрования носит название «замена». При таком способе все символы остаются на своих местах и не перемешиваются, но при этом изменяется их написание.

Один из примеров способа шифрования заменой описан в рассказе Артура Конан Дойла «Пляшущие человечки». По сюжету рассказа главный герой получал зашифрованные послания, которые он не мог расшифровать. Каждый символ послания представлял собой изображение пляшущего человечка (рис. 10).

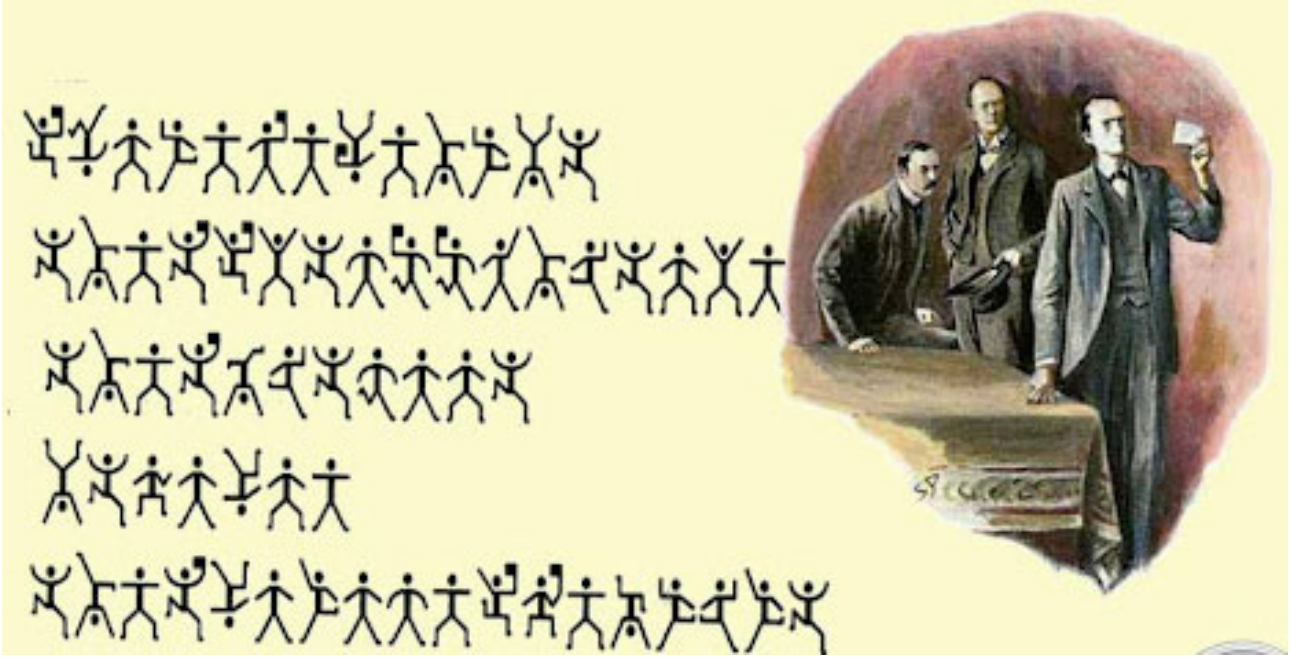

Рис. 10. Пример шифротекста с заменой

Расшифровать такое послание можно в том случае, если знаешь соответствие каждого символа зашифрованного текста символу исходного алфавита. Таблица с подобным алфавитом соответствия должна была находиться как у отправителя, так и у получателя сообщения.

Главный герой был вынужден обратиться к сыщику Шерлоку Холмсу за помощью в расшифровке. Метод расшифровки сообщений, зашифрованных способом «замена», был описан еще арабским исследователем Аль-Кинди в IX в. и получил название «частотный метод». Его идея заключается в том, что в каждом языке существуют символы, которые встречаются чаще других, и символы, которые встречаются реже. При этом можно составить статистику частоты встреч разных символов. Зная статистику, мы можем произвести подсчет частоты встречи зашифрованных символов и заменить их на соответствующие по частоте символы обычного алфавита.

Например, для английского алфавита эта статистика выглядит так, как показано в таблице [6].

Статистика частотности латинского алфавита

Буква	E	T	A	O	I	N	S	H	R	D	L	C	U
Частота, %	12,7	9,1	8,2	7,5	7	6,8	6,3	6,1	6	4,3	4	2,8	2,8
Буква	M	W	F	G	Y	P	B	V	K	X	J	Q	Z
Частота, %	2,4	2,4	2,2	2	2	1,9	1,5	1	0,8	0,2	0,2	0,1	0,1

Далее, применив статистику, сыщик определил, какие символы зашифрованного послания соответствуют буквам английского алфавита (рис. 11).

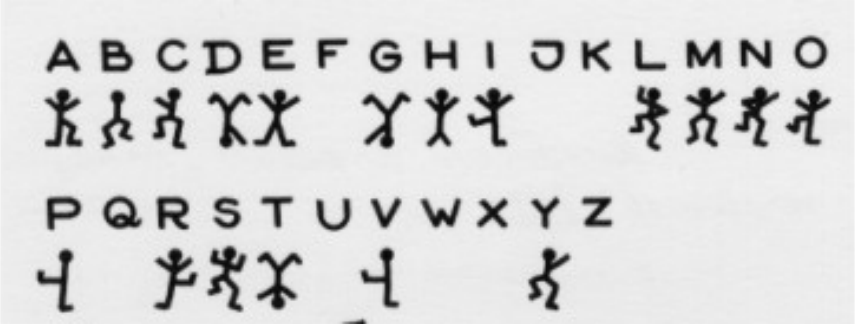

Рис. 11. Расшифровка шифротекста с заменой

В результате сообщение было успешно расшифровано.

Другой известный сегодня шифр методом замены – шифр Цезаря, также известный как шифр сдвига, код Цезаря – один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря представляет собой вид шифра замены, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее [7].

Шифр назван в честь римского полководца Гая Юлия Цезаря, якобы использовавшего его для секретной переписки со своими генералами (рис. 12).

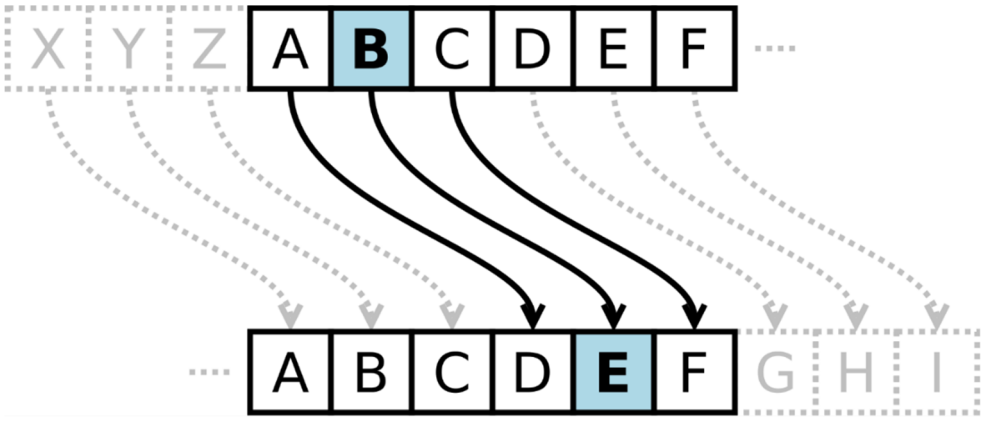

Рис. 12. Шифр Цезаря

4. ЗАЩИТА ИНФОРМАЦИИ В СРЕДНИЕ ВЕКА. ПОНЯТИЕ О СОХРАНЕНИИ ТРАКТОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

Понимание того, что сохранять нужно не только саму информацию, но и способ ее передачи, получило широкое распространение примерно к Средним векам. В монгольской империи XIII в. появились хорошо охраняемые почтовые тракты. Несмотря на отсутствие хороших дорог, для движения курьеров, несших государственные сообщения, создавалась сеть пунктов отдыха, замены лошадей и охраны. Это был пример первой охраняемой почтовой сети, действовавшей на тысячи километров [8]. Для беспрепятственного перемещения курьеров и получения ими любой возможной помощи на пути почтового тракта каждый из них получал специальный знак – тамгу (рис. 13).

Рис. 13. Монгольская тамга

При предъявлении этого знака каждый пункт почтового тракта обязан был оказать курьеру любое содействие, включая сопровождение охраны.

Еще одним примером уязвимости тракта передачи сообщений в эпоху до появления электросвязи был так называемый оптический телеграф, получивший широкое распространение в Западной Европе в конце XVIII в. Каждый пункт этого тракта представлял собой башню с установленной на ее крыше конструкцией, с помощью которой можно было создавать символы определенной конфигурации. Следующая башня этого тракта располагалась

в пределах прямой видимости и позволяла обмениваться сообщениями, кодируя информацию различными положениями конструкции (рис. 14).

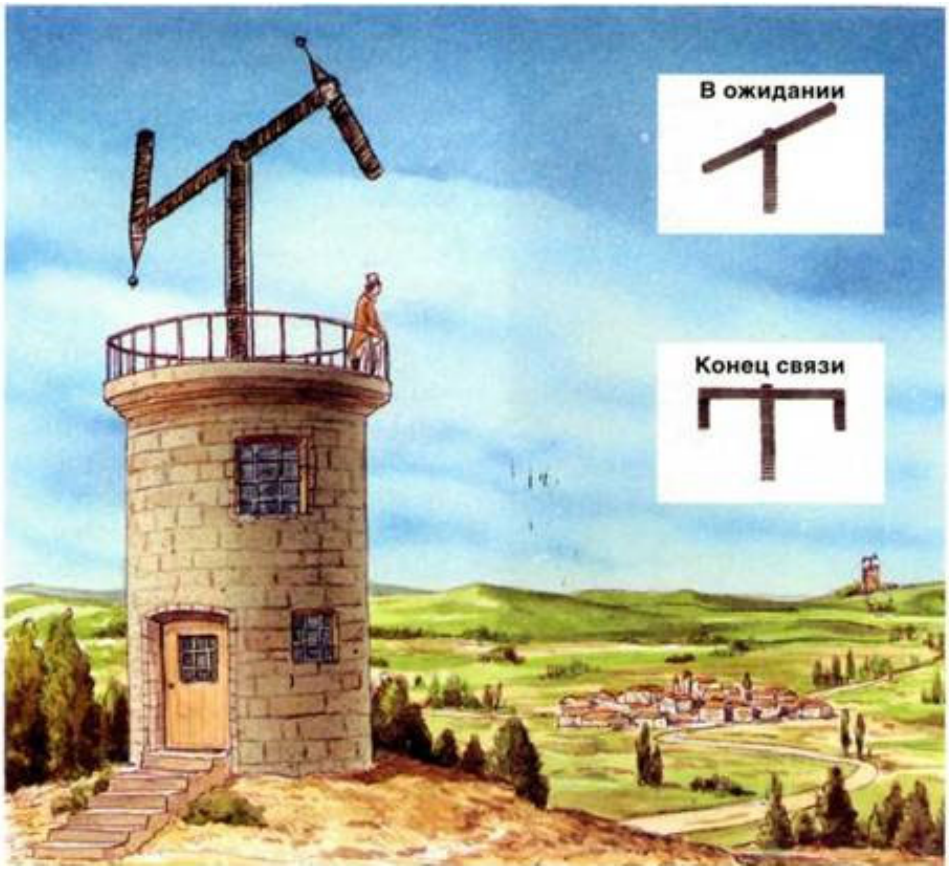

Рис. 14. Оптический телеграф

Через некоторое время после начала применения этой сети ее владельцы стали получать свидетельства о том, что в некоторых случаях передаваемые сообщения не соответствовали исходным. После проведенного расследования выяснилось, что некоторым злоумышленникам удавалось подкупить или запугать служащих, управлявших работой конструкции. В результате важные сообщения искажались, терялись или перехватывались злоумышленниками в корыстных целях. Такой случай с подобной сетью был даже описан в художественном произведении Александра Дюма «Граф Монте-Кристо».

Впоследствии владельцы сети были вынуждены установить охрану для каждого пункта тракта передачи данных. Это существенно увеличило расходы на функционирование сети и с появлением проводного телеграфа она прекратила свое существование, не выдержав конкуренции.

5. НОВЫЕ КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ. СЕТИ ЭЛЕКТРОСВЯЗИ – ПЕРЕХВАТ ТЕЛЕГРАФНЫХ СООБЩЕНИЙ

Следующий этап развития средств разведки и защиты информации относится к эпохе появления сетей электросвязи. Первой такой глобальной сетью по передаче информации на большие расстояния был телеграф.

Длительное время телеграфный тракт передачи данных никак не защищался. С момента изобретения первых телеграфных аппаратов в 30–40-х гг. и до 60-х гг. XIX в. случаев перехвата телеграфных сообщений было крайне мало, и они были несистемными. Первый такой массовый случай произошел в 1862 г. в США во время Гражданской войны. Примечательно то, что перехватом сообщений занималась сама компания – владелец телеграфной сети Western Union. К моменту начала гражданской войны Western Union заняла лидирующее положение на рынке телеграфной связи всех Соединенных Штатов, практически речь шла о монополии. Услугами связи этой компании пользовались как северные штаты, так и южные, однако офисы и главное представительство Western Union находились на территории северных штатов, в городе Вашингтоне. Североамериканское правительство сумело надавить на руководство компании и заставило их перехватывать все сообщения, идущие в южной части телеграфной сети. Таким образом, Северное командование получило возможность перехватывать конфиденциальные сообщения Южного командования. Данный факт стал известен уже после войны и, возможно, он был одним из важных факторов поражения Южной Конфедерации в Гражданской войне.

После этого случая правительство Соединенных Штатов, а затем и правительства европейских держав озаботились созданием способов защиты телеграфных сообщений. Кроме физической защиты тракта передачи данных, начали применять шифрование сообщений. В Российской империи шифрование телеграфных сообщений биграммным шифром началось в 1873 г. [9].

6. РУССКО-ЯПОНСКАЯ ВОЙНА. ПОЯВЛЕНИЕ РАДИОРАЗВЕДКИ

После изобретения радио Александром Степановичем Поповым в 1895 г. развитие данного средства связи получило широкое распространение в армиях и флотах ведущих держав. В первую очередь это касалось именно флота, так как к концу XIX в. скорости перемещения и маневра кораблей были таковыми, что передача сообщений семафором и флажковой азбукой существенно затрудняли действия флотов. Появившееся средство беспроводной связи сразу же получило широкое распространение во флоте Российской империи, а затем и других европейских стран.

В 1902 г. в Великобритании был опубликован рассказ Редьярда Киплинга «Беспроволочный телеграф», в котором описывались опыты по перехвату радиосигналов [10]. Таким образом, уже через 7 лет после изобретения радио разведка Великобритании заинтересовалась способами перехвата радиосообщений. И уже в 1904–1905 гг. в ходе Русско-японской войны британские корабли систематически перехватывали радиопередачи русских боевых кораблей, передавая информацию своим союзникам японцам.

Итоги Русско-японской войны были всесторонне проанализированы во флотах и армиях ведущих держав мира. Было констатировано решающее значение как радиоразведки, так и защиты радиосообщений для ведения боевых действий. В русской армии это нашло отражение в создании специализированных подразделений радиоразведки и радиосвязи. Службы радиоразведки появились как в российском императорском флоте, так и в полевой армии.

Российская армия была первой, в которой применялись подразделения по пеленгации, поиску и борьбе с источниками радиоизлучений противника. Для этого при армиях создавались специальные роты радиопеленгации, снабженные мощными мобильными радиостанциями, которые базировались на грузовых автомобилях. Одна из таких радиостанций изображена на фотографии тех лет (рис. 15).

Рис. 15. Машина с пеленгационной установкой
в подразделении радиоразведки

Самый простой метод радиопеленгации – это использование триангуляции [11]. Триангуляция – это буквально с английского «три угла». Метод основан на способе регистрации направления распространения радиоволн с помощью антенны. Для определения направления на источник радиосигнала подразделение радиоразведки использовало вращение плоскости антенны с целью поиска наиболее высокого уровня сигнала, находясь в точке 0 (рис. 16).

После нахождения наиболее вероятного направления на источник сигнала *A* командир подразделения рисует линию направления от места своего расположения в сторону источника. Также происходит измерение угла между направлением на источник сигнала и произвольной линией, например, линией «восток – запад» (угол α), после чего подразделение меняет свою дислокацию и снова замеряет уровень сигнала из другой точки. Направление из этой точки на сигнал также отмечается на карте. Одновременно происходит отметка направления на предыдущую точку и замеряется угол между направлением на источник из второй точки и линией «восток – запад». В результате построения этих линий получается треугольник с двумя известными углами и одной известной стороной, которая называется базой измерения. Базу подразделение замеряет по спидометру, перемещаясь во вторую точку измерения – *B* (рис. 17).

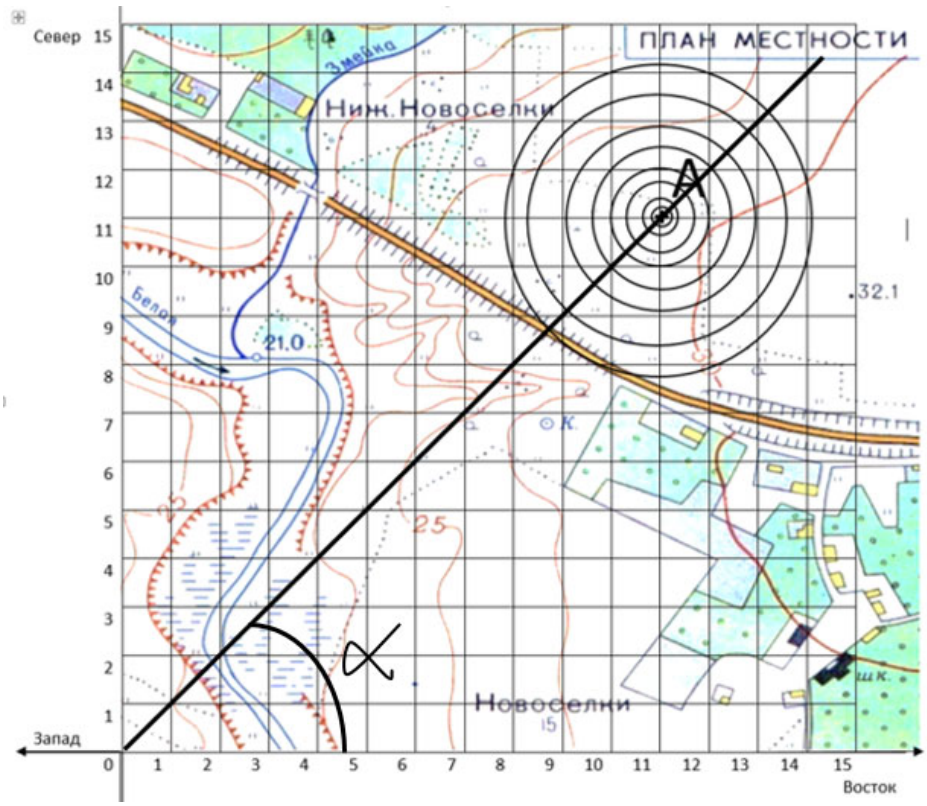

Рис. 16. Первый этап радиопеленгации

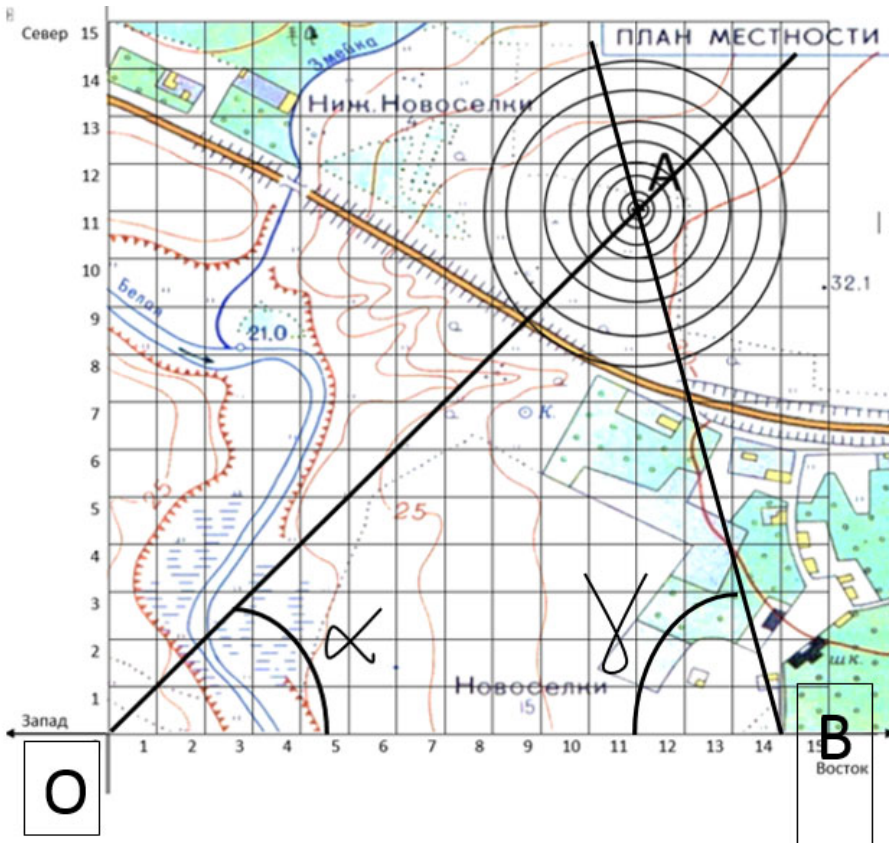

Рис. 17. Второй этап радиопеленгации

В итоге расстояние между первоначальной точкой и источником радиосигнала легко определяется из решения треугольника.

В целях радиосвязи и радиоразведки в российской армии использовались радиостанции меньшего размера, базировавшиеся на лошадиных упряжках (рис. 18).

Рис. 18. Малые радиостанции в русской армии

Применение таких подразделений в российской армии было несистемным явлением, они работали на отдельных участках фронта во время Первой мировой войны. Однако в других частях работа радиоразведки могла отсутствовать полностью, а в ряде случаев не соблюдались даже элементарные меры предотвращения утечки информации.

Один из таких случаев произошел с армией Самсонова, в которой служба шифрования радиосообщений была полностью развалена, и сообщения отправлялись открытым текстом. В результате немецкое командование перехватывало приказы генерала Самсонова и сумело упредить его действия на своем участке фронта, что в итоге привело к разгрому армии и пленению большого числа русских солдат [12].

Иногда радиоразведка оказывала решающее влияние на весь ход боевых действий. Так произошло в самом начале войны, когда благодаря службе радиоразведки императорского российского флота 1 августа 1914 г.

было получено сообщение о помощи от севшего на мель немецкого крейсера «Магдебург». В тот же час российский флот в составе нескольких кораблей был отправлен к месту бедствия «Магдебурга» с целью его захвата. Капитан «Магдебурга» Густав Хабенихт приказал подготовить крейсер ко взрыву, чтобы не допустить его захвата, однако благодаря смелым и быстрым действиям русских моряков взрыв крейсера не состоялся и он был захвачен (рис. 19).

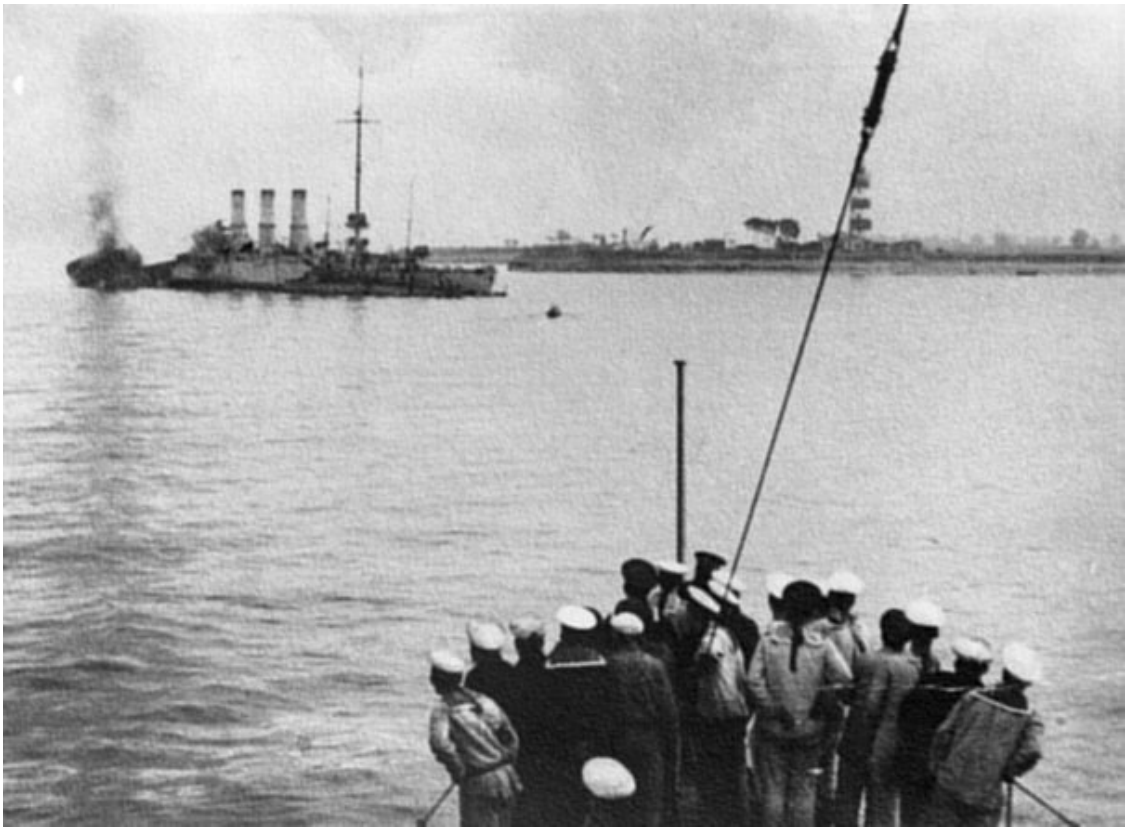

Рис. 19. Русские моряки готовятся к абордажу крейсера «Магдебург»

На борту крейсера были найдены ценные документы, среди которых была «Сигнальная книга императорского флота» Германии. Книга являлась документом, определяющим организацию и функционирование военно-морской связи. Также она являлась кодовой книгой для криптографической службы военно-морского флота Германии. Она была настолько ценной, что британское правительство срочно организовало миссию из военно-морских специалистов в Санкт-Петербург с целью снятия копии с этой книги [13].

Потеря книги уже через три месяца обернулась катастрофой для флота Германии во время сражения у Фолклендских островов, когда была разгромлена Дальневосточная эскадра адмирала Шпее. Британский флот подстерег ее и устроил засаду благодаря перехваченным и быстро расшифрованным сообщениям немецких кораблей.

Успехи радиоразведки и ее влияние на геополитические события в годы Первой мировой войны также ярко проявились в работе британской секретной службы. В ее составе действовало подразделение, занимавшееся дешифровкой перехваченных радиосообщений противника, – «Комната 40» (рис. 20).

Рис. 20. Отдел «Комната 40»

При формировании этого подразделения в него были набраны в том числе гражданские люди, профессора математики университетов. Благодаря им работа по дешифровке сообщений происходила очень быстро. Один из самых известных успехов «Комнаты 40» – это расшифровка телеграммы от 17 января 1917 г. министра иностранных дел Германии Артура

Циммермана в немецкое посольство в Вашингтоне. В этой телеграмме он давал разъяснение немецкому послу о его действиях по склонению Мексики к войне с США для предотвращения вступления Штатов в Первую мировую войну на стороне Великобритании и России. После расшифровки телеграммы она была опубликована в британских газетах. Факт таких инструкций и возможных действий Германии против США привел в возмущение американское общество, и под давлением общественного мнения Конгресс США уже 6 апреля объявил Германии войну, хотя до этой истории правительство и Конгресс США склонялись к решению не вмешиваться в европейский конфликт [14].

7. ПРОМЫШЛЕННЫЙ ШПИОНАЖ

Начало XX в. по праву считается временем расцвета технического прогресса. Ни один период технической истории человечества не может похвастаться таким количеством изобретений в самых разных отраслях: строительство (появление небоскребов), энергетика (все виды электростанций, кроме ядерных), транспорт (стремительное развитие авиации и автомобилей)... Одновременно эти изобретения давали возможность их владельцам получить преимущество на конкурентном рынке. Спрос на патенты, инновации и ноу-хау породил явление, получившее название «промышленный шпионаж».

Основное предназначение промышленного шпионажа – экономия средств и времени, которые требуется затратить, чтобы догнать конкурента, занимающего лидирующее положение, либо не допустить в будущем отставания от конкурента, если тот разработал или разрабатывает новую перспективную технологию, а также чтобы выйти на новые для предприятия рынки [15].

В России одним первых случаев классического промышленного шпионажа считается история изобретения бездымного пороха Дмитрием Ивановичем Менделеевым. В конце XIX в. Россия отставала от развитых стран Европы в создании современных боеприпасов по причине невозможности производства у себя так называемого бездымного пороха, имевшего существенно лучшие характеристики температуры и скорости сгорания по сравнению с традиционным черным порохом. Это сдерживало развитие военной промышленности Российской империи, подрывая ее обороноспособность. Осознавая это, российское правительство поручило Д. И. Менделееву выяснить секрет бездымного пороха, который производился на заводах Англии и Франции.

Выяснить это можно было лишь на месте – в Англии или во Франции. Дмитрий Иванович понадеялся на свой авторитет и предполагал выяснить секрет пороха из разговоров с коллегами. Самому ученому на тот момент было уже 56 лет (рис. 21).

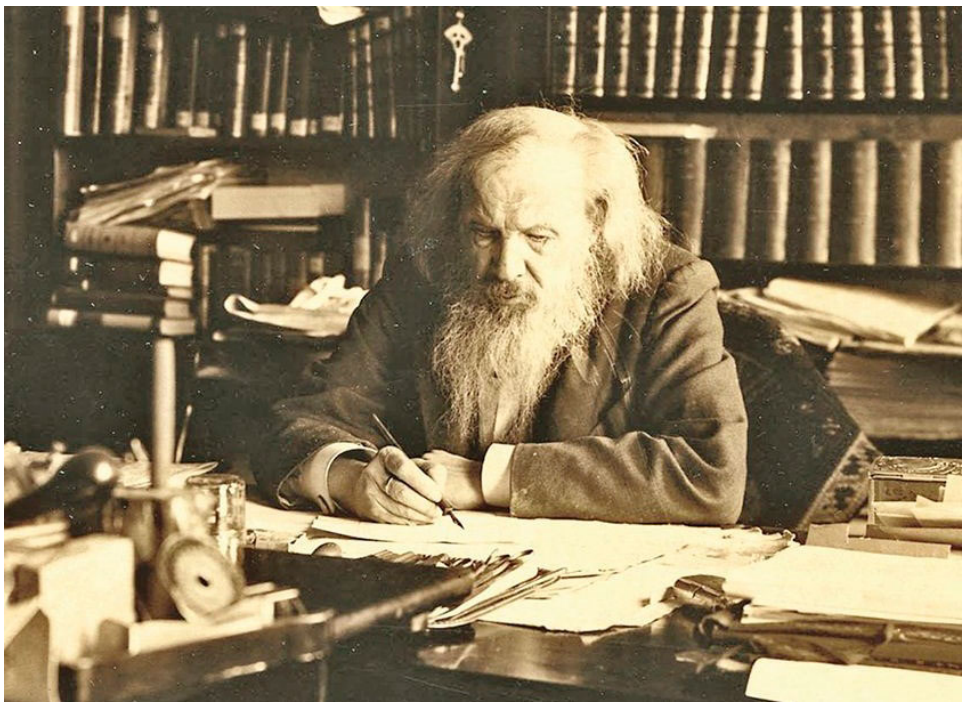

Рис. 21. Д. И. Менделеев

Совершив поездку в Англию и посетив английские лаборатории и заводы, Менделеев так и не смог добиться от англичан секрета формулы пороха, точнее, пироксилина, который был в его основе. Англичане с удовольствием демонстрировали ученому цеха и оборудование, но только не состав и пропорции выпускаемой продукции. Не добившись успеха в Англии, ученый отправился во Францию, где встретил точно такой же прием. Никто не собирался делиться секретами.

Тогда Менделеев просто поселился поблизости от порохового завода под Парижем, рядом с железнодорожной веткой, по которой на завод поступало сырье. Все это время он наблюдал за вагонами, проходящими в сторону завода. Необходимо отметить, что организация железнодорожного движения Франции была по тем временам самой образцовой и передовой в мире. Все грузы на вагонах проходили обязательную маркировку и указание тоннажа для обеспечения своевременного учета и сортировки вагонов. Поэтому Дмитрий Иванович мог легко посчитать, сколько за определенное время на завод поступило азота, серной кислоты, спирта, кислорода и прочих сырьевых компонентов. А поскольку все сырье, поступившее на завод, так или иначе использовалось в производстве, на выходе из которого была

только одна продукция – порох, то выдающийся химик смог вычислить массовую долю компонентов, входивших в формулу производства, и определить ее доподлинно [16]. Это один первых и ярких примеров промышленного шпионажа с использованием оптического канала утечки информации.

Но наибольшее развитие промышленный шпионаж получил в США. Именно там рождалось самое большое количество изобретений, патентов и инноваций. Борьба за секреты приобретала подчас черты настоящей войны, когда конкуренты нанимали целые детективные агентства и даже криминальные структуры, которые занимались только поиском и кражей промышленных секретов.

Одним из таких примеров войны за секреты была история конкуренции трех основоположников американской и мировой электротехники – Томаса Эдисона и Джорджа Вестингауза, точнее, их технологических корпораций, а также известного ученого Николы Теслы (рис. 22).

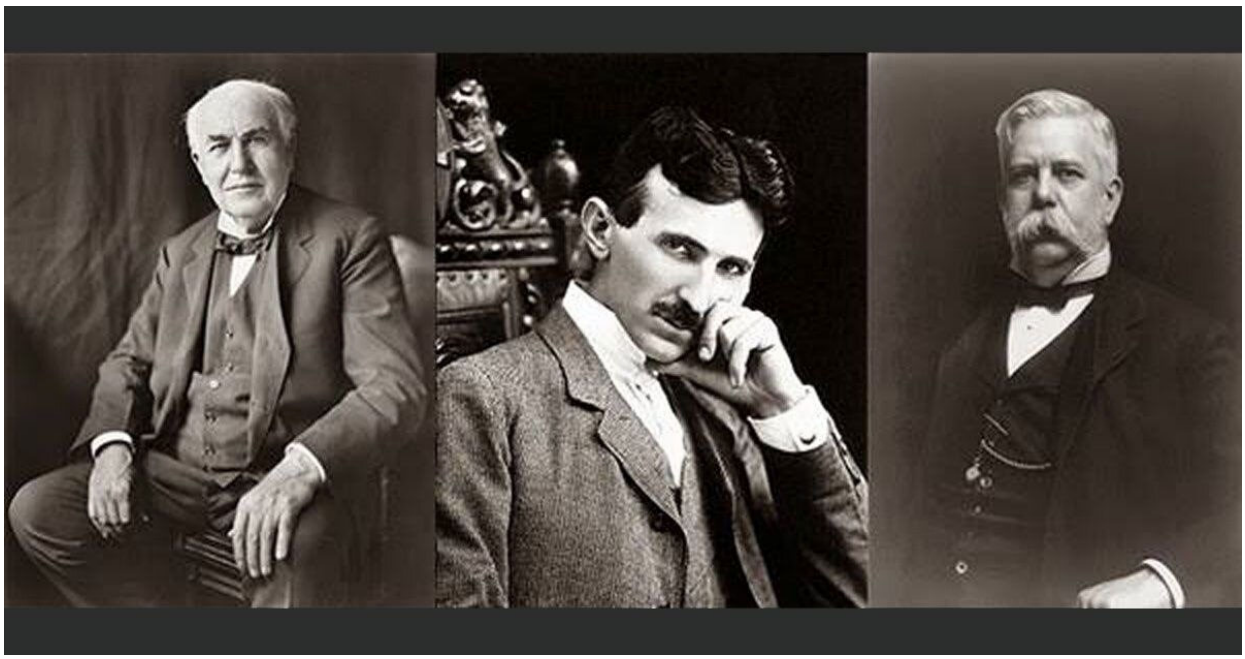

Рис. 22. Т. Эдисон, Н. Тесла, Д. Вестингауз

В результате этой борьбы и непрекращающихся краж секретов победителем стала корпорация Эдисона, электротехнические стандарты которой стали общемировыми, а лаборатория Теслы была уничтожена пожаром.

Тем не менее, промышленный шпионаж – это не только борьба коммерсантов за чужие секреты. Этим термином также называют и научно-техническую разведку стран. Одним из примеров таких успешных разведывательных операций в области промышленного шпионажа стало получение секретов производства атомной бомбы советскими разведчиками. Внедрение агентов – семьи Розенбергов – в Манхэттенский проект создания атомной бомбы позволило получить чертежи и основные технологические процессы производства бомбы, сброшенной на город Нагасаки, что позволило советским ядерщикам значительно сократить свое отставание в этой области и создать оружие, которое до сих пор защищает нашу страну от любой открытой агрессии.

8. ШИФРОВАЛЬНЫЕ МАШИНЫ

Этот этап отдельно выделен в истории развития средств защиты информации по причине своего огромного значения в деле развития средств криптографии.

К 1920-м гг. криптографические алгоритмы стали настолько сложны, что даже имея ключ, процесс ручной зашифровки и расшифровки сообщений требовал огромного количества времени и интеллектуальных усилий. В каждый штаб дивизии, полка или батальона нельзя посадить профессора математики, как в вышеупомянутую «Комнату 40». Однако опыт Первой мировой войны показал, что вопрос своевременной шифровки и обмена защищенными сообщениями является одним из самых важных в деле успешного проведения военных операций на суше и на море.

Выход был найден в создании механических вычислительных машин, позволявших реализовать сложные криптографические алгоритмы без привлечения высокоинтеллектуального персонала, силами простых рядовых шифровальщиков. Это позволило организовать криптографическую службу и систему обмена надежно зашифрованными сообщениями между низовыми структурами армии – на батальонном уровне.

Одним из самых известных примеров была «Энигма» – немецкая машина для шифрования и расшифровывания сообщений, внешний вид которой представлен на рис. 23.

Эта машина одновременно реализовывала оба основных способа шифрования – замену и перестановку. Конструктивно это была клавиатура, связанная через систему выбора алгоритма зашифровывания с тремя или четырьмя (в разных версиях) барабанами, имевшими 26 секторов – по числу букв латинского алфавита (рис. 24).

Печать происходила блоками по три или четыре символа (по числу барабанов). При наборе текста на клавиатуре каждое нажатие клавиши вызывало поворот соответствующего барабана на определенный угловой сектор в зависимости от заданного алгоритма [17].

Рис. 23. Внешний вид шифровальной машины «Энигма»

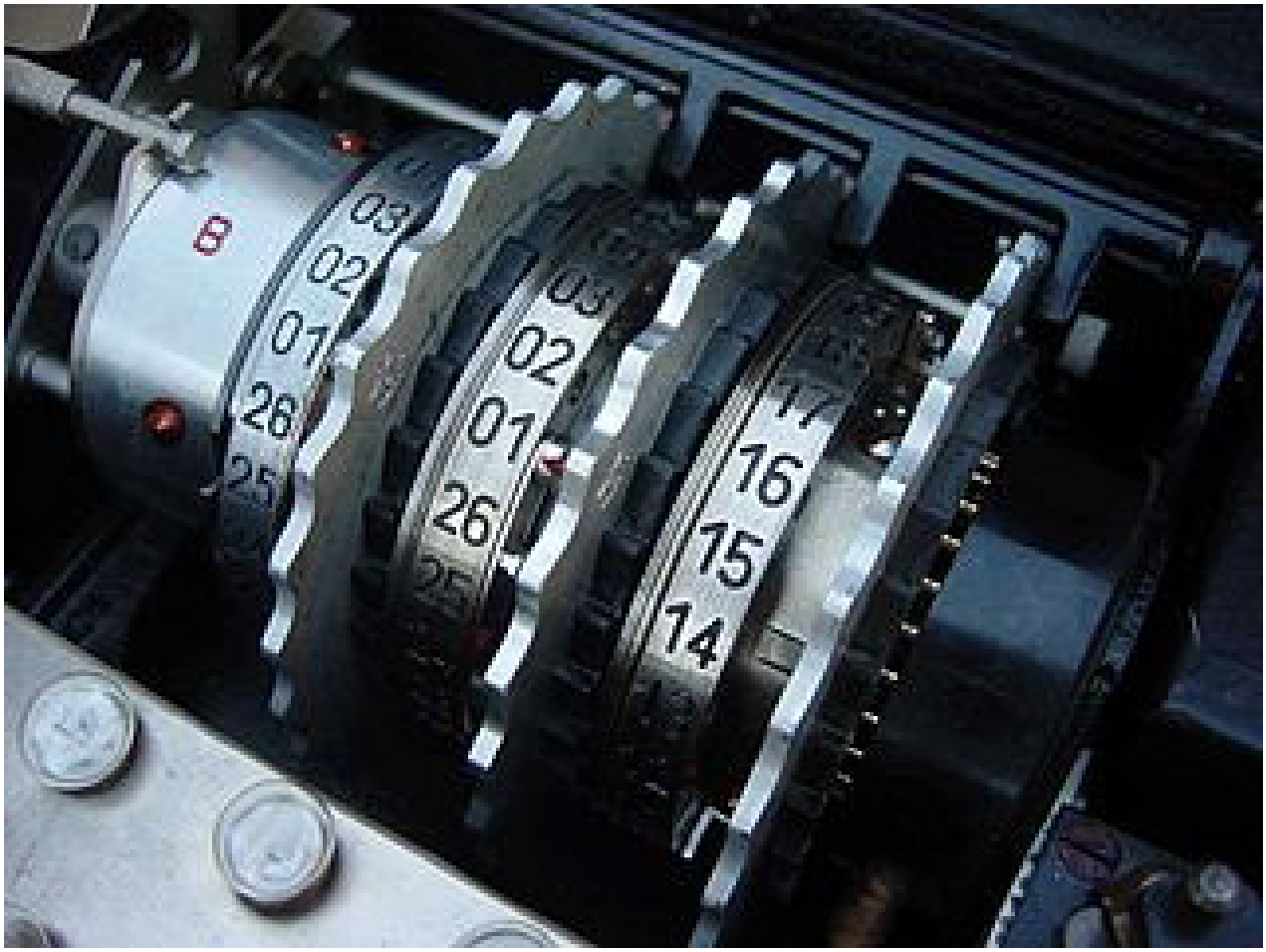

Рис. 24. Барабаны «Энигмы»

Таким образом происходила операция замены. Например, при алгоритме 3-11-5 при вводе слова kat должно было происходить перемещение первого барабана на три сектора и вместо символа «k» печать символа «n», второй барабан поворачивался на 11 секторов и вместо «a» должна печататься «l», а вместо «t», через пять секторов – «y». Итог замены – слово «nly».

Однако кроме операции замены «Энигма» выполняла еще и операцию перестановки, поэтому вторая часть алгоритма должна была задавать порядок печати этого трехсимвольного блока путем перемещения всего механизма роторов вдоль каретки на определенную позицию. Например, первый набранный символ должен был печататься не на первой позиции из трех, а на третьей, для печати второго символа каретка возвращалась в первое положение, а для печати третьего – в среднее между двумя предыдущими. Тогда итоговый алгоритм мог выглядеть как 3-11-5/2-3-1 и выдавал вместо слова «kat» слово «lyn». Шифр не поддавался обычному частотному анализу, поскольку даже если вы узнаете подлинное значение всех измененных символов, необходимо было вычислить еще и все варианты перестановки этих значений, причем начало печати сообщения могло происходить не с трехсимвольного блока, а с двухсимвольного или односимвольного. Таким образом, вы не можете доподлинно знать дальнейшего порядка повторений трехсимвольных блоков, тем более что трехроторной модификацией выпуск «Энигмы» не ограничивался. Например, для связи высших должностных лиц Рейха выпускалась стационарная восьмироторная версия «Энигмы».

Разумеется, подобный алгоритм не является невскрываемым и, затратив на это определенное время, его можно было расшифровать. Однако это время могло быть решающим в условиях ведения боевых действий, тем более что сообщения, отправляемые на тактическом уровне батальона или полка, могли устаревать уже в течение суток, а их количество было таковым, что расшифровывать вручную этот объем информации было бесперспективным занятием для противника. При неизвестной схеме машины общее количество возможных вариантов шифротекста составляло 10^{114}, при известной схеме роторов и настроек печати – 10^{23}. Невозможно было вручную перебрать все комбинации за разумное время.

Выход для противника мог быть только в определении точного устройства и алгоритма работы шифровальной машины для того, чтобы создать свой подобный экземпляр и использовать его для быстрой оперативной расшифровки. И такую задачу английская разведка успешно выполнила путем кражи одного из экземпляров «Энигмы», однако немецкая контрразведка, выяснив этот факт, просто рекомендовала выпустить новую модификацию, которая свела на нет успех британской спецслужбы.

9. СОЗДАНИЕ КОМПЬЮТЕРОВ

С появлением высокопроизводительной электронной вычислительной техники у криптоаналитиков появилась возможность вскрывать шифры методом простого перебора ключей. Как ответ, в 1960-х гг. начали появляться блочные шифры, которые обладали большей криптостойкостью по сравнению с результатом работы роторных машин.

Блочными называются шифры, в которых логической единицей шифрования является некоторый блок открытого текста, после преобразований которого получается блок шифрованного текста такой же длины. Обычно используются блоки размером 64 бита. Чем больше размер блока, тем выше надежность шифра (при прочих равных условиях), но тем ниже скорость выполнения операций шифрования и дешифрования. Разумным компромиссом является блок размером 64 бита, который является сегодня практически универсальным для всех блочных шифров. Также имеет значение размер ключа: чем длиннее ключ, тем выше надежность шифра, но большая длина ключа тоже может быть причиной слишком медленного выполнения операций шифрования и дешифрования [18].

Следующая идея состоит в том, что за один раунд шифровки данных обеспечивается недостаточно высокая надежность, но уровень надежности шифра повышается с каждым новым раундом обработки. Например, схема трехраундного шифрования выглядит следующим образом (рис. 25).

Шифр получает на вход блок и ключ и совершает несколько чередующихся раундов, состоящих из чередующихся стадий замены и перестановки. Для каждого раунда используется свой, получаемый из первоначального, ключ. Подобный ключ называется раундовым.

Таким образом, на сегодняшний день скорость работы вычислительных машин является решающим фактором в использовании криптоалгоритмов.

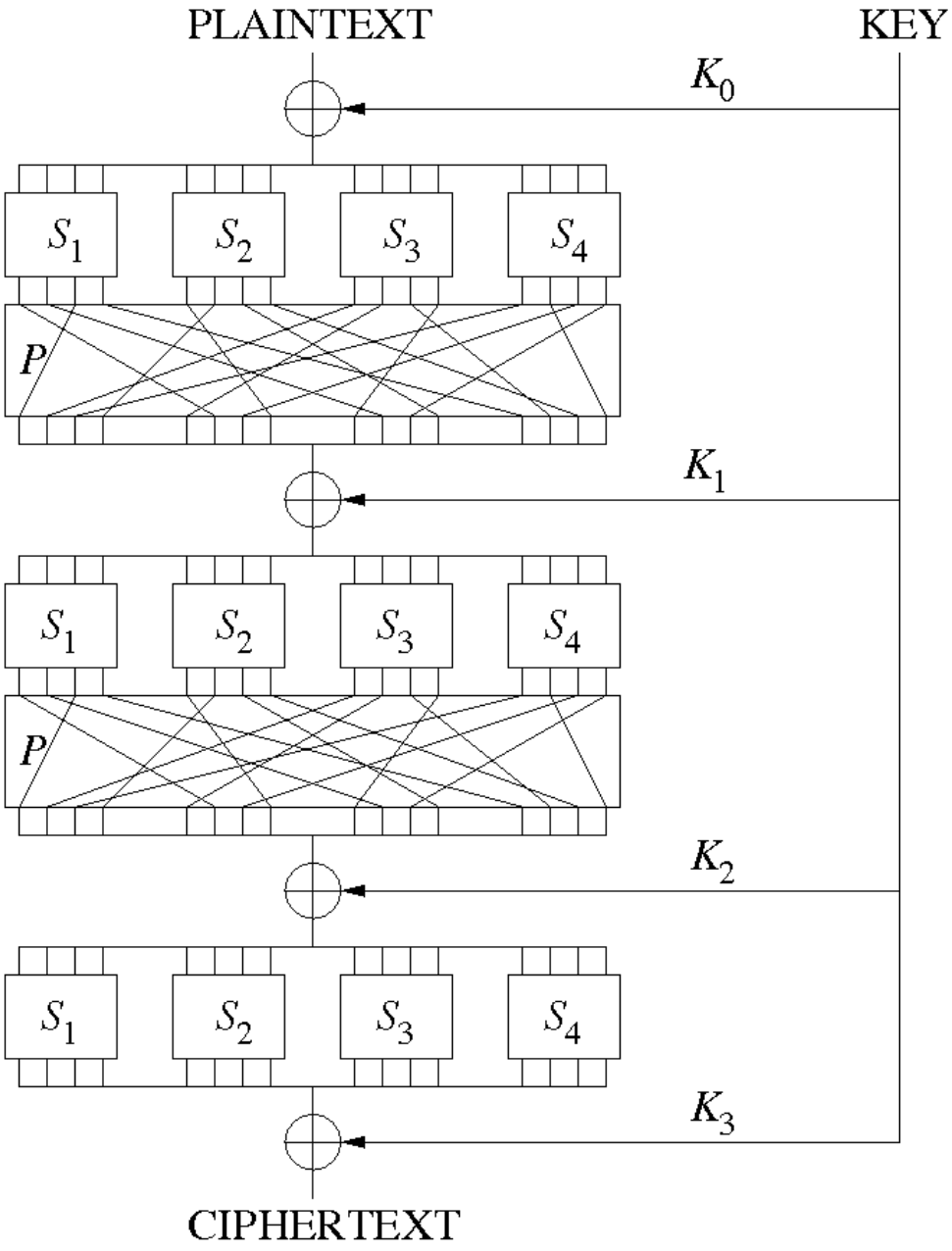

Рис. 25. Схема трехраундового блочного шифрования

10. ПОЯВЛЕНИЕ НОВЫХ СРЕДСТВ ПЕРЕДАЧИ ИНФОРМАЦИИ

Несмотря на повсеместное развитие радиосвязи и ее несомненное удобство, она имеет свои недостатки. С точки зрения защиты информации основной недостаток радиосвязи – ее широковещательность. И действительно, если для передачи радиособщения его необходимо выпустить в эфир, то получить его сможет не только ваш адресат, но и противник. В таких условиях единственной защитой информации может быть только шифрование канала.

Другой недостаток радиосвязи заключается в ограниченной пропускной способности радиоканала. Частота спутникового вещания – до 30 ГГц. Даже взяв чисто теоретическую пропускную способность радиоканала, основываясь на той идее, что каждый период колебания волны равен биту передаваемой информации, максимально возможная пропускная способность составит $3 \cdot 10^{10}$ бит в секунду. В то же время световая волна длиной 1 мкм способна задать теоретическую пропускную способность $3 \cdot 10^{14}$ бит в секунду – на четыре порядка больше.

Первые опыты по использованию стеклянных световодов для создания оптических кабелей относятся к 1950-м гг. Первые коммерческие оптоволоконные линии появились к концу 1970-х гг. На сегодняшний день практическая пропускная способность оптоволоконных DWDM-систем достигает 2 Тбит/с ($2 \cdot 10^{12}$) – все еще в сто раз меньше теоретической, но гораздо больше практической пропускной способности любого радиоканала.

Перехватить информационный канал, проходящий по кабелю, возможно, лишь получив к нему физический доступ. С точки зрения защиты информации это огромный плюс. Кроме того, оптоволоконный кабель не позволяет снимать сигнал удаленно, используя методы побочных электромагнитных излучений и наводок, как с обычными электрокабелями. Но и получив прямой физический доступ к оптоволоконному кабелю, все равно довольно сложно обеспечить съем сигнала таким образом, как это можно сделать через обычный медный электрокабель, – путем прямого со-

единения. Тем не менее, существуют способы снятия информации и с оптоволоконного кабеля.

Рассмотрим устройство обычного оптического кабеля на рис. 26.

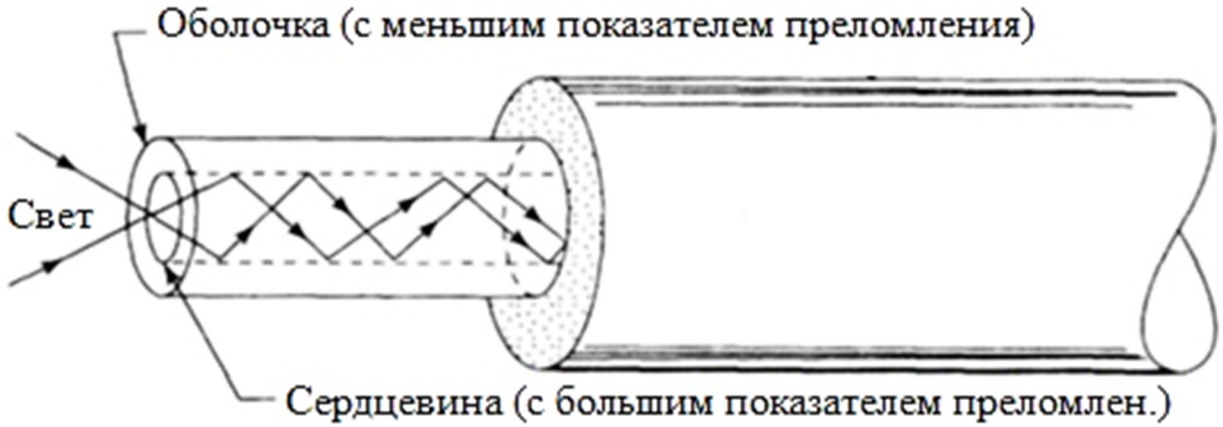

Рис. 26. Схема оптоволокна

Благодаря внутренней сердцевине с большим показателем преломления по сравнению с внешней оболочкой оптический луч, попавший в сердцевину под определенным углом, меньше угла полного внутреннего отражения. Он получает возможность пройти весь путь до другого конца волновода, отражаясь от границы раздела сердцевины и оболочки и не выходя за пределы кабеля.

Однако при создании определенных условий есть возможность заставить луч покинуть предназначенную ему траекторию и поймать его вне стенки кабеля, используя внешний фотоэлемент [19]. Это можно сделать локальным сжатием волновода, как показано на рис. 27.

Подобный способ снятия информации с оптоволокна был впервые применен в 1980-х гг. американскими спецслужбами, сумевшими снять информацию с оптоволоконной линии, проложенной между Дамаском и базой советского флота в порту Тартус в Сирии.

Сегодня устройства для снятия информации с оптоволокна вполне доступны даже для рядовых злоумышленников. В сети можно обнаружить объявления о продаже так называемых оптических прищепок, которые создают подобное локальное давление на световод и считывают выходящий из него оптический сигнал (рис. 28).

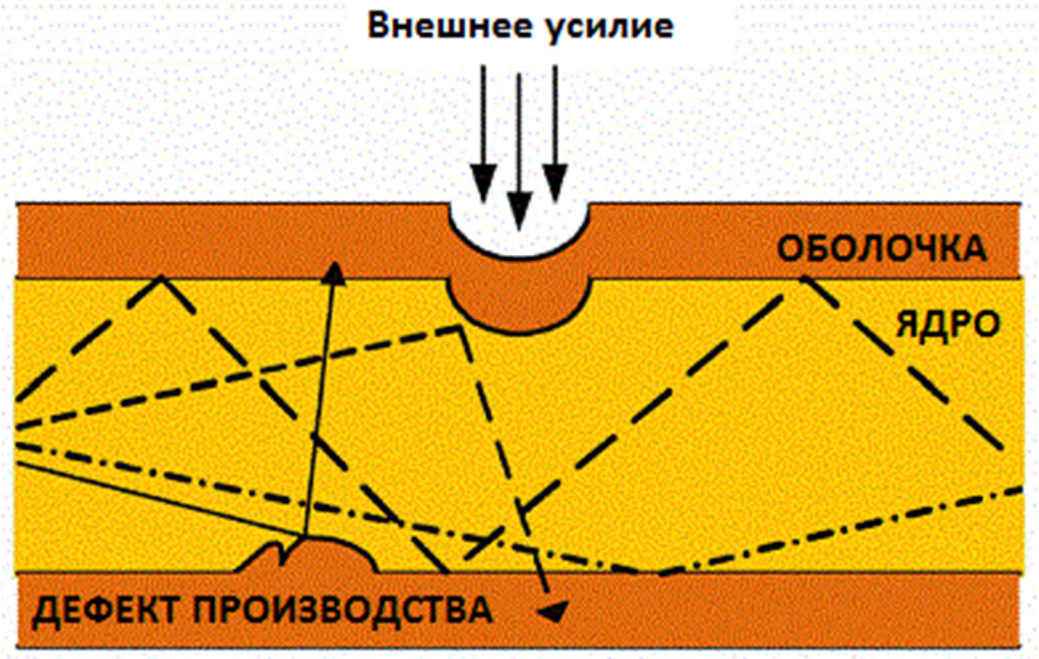

Рис. 27. Схема изменения хода луча в световоде

Рис. 28. Оптическая прищепка

Таким образом, мы можем констатировать, что средства защиты информации, как в древние времена, так и в современности находятся в постоянном соревновании со средствами несанкционированного доступа к информации. Новые возможности передачи сообщений тут же открывают и новые возможности их перехвата.

ЗАКЛЮЧЕНИЕ

В учебном пособии описаны основные этапы, которые, по мнению автора, можно выделить как основные вехи развития науки об информационной безопасности, средствах и методах защиты информации. Особо выделены и подробно описаны методы шифрования информации, применявшиеся с древнейших времен и являющиеся одним из самых действенных способов сохранения конфиденциальности передаваемых сведений. Также большое внимание уделено существующим и по сей день способам радиоразведки и истории развития этого вида информационной деятельности. Все факты, изложенные в пособии, подтверждены ссылками на научные издания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Клейменкин Д. В., Котлярова В. В. Анализ искусства войны в учении Сунь-цзы // Colloquium-Journal. – 2019. – № 25-6(49). – С. 62–63. – DOI 10.24411/2520-6990-2019-10901.

2. Туманова А. С. «Искусство войны» Сунь-цзы как исторический источник // Дни науки студентов Владимирского государственного ун-та им. А. Г. и Н. Г. Столетовых : сб. материалов науч.-практ. конф. (Владимир, 18 марта – 05 апреля 2019 г.). – Владимир : Владимирский государственный ун-т им. А. Г. и Н. Г. Столетовых, 2019. – С. 1949–1954.

3. Ермакова А. Ю., Лось А. Б. Краткий очерк истории криптографии. Древний мир, средние века // Тр. XIII междунар. Колмогоровских чтений : сб. ст. (Ярославль, 19–22 мая 2015 г.). – Ярославль : Ярославский государственный педагогический ун-т им. К. Д. Ушинского, 2015. – С. 278–286.

4. Запечников С. В. Из истории криптографии: тайнопись и тайные коммуникации в античном мире // Безопасность информационных технологий. – 2014. – Т. 21. – № 2. – С. 83–95.

5. Малаева А. Р. История криптографии. Шифр Марии Стюарт, королевы Шотландии // Гуманитарные науки в современном вузе: вчера, сегодня, завтра : материалы IV междунар. науч. конф. (Санкт-Петербург, 10 декабря 2021 г). – СПб. : Санкт-Петербургский государственный ун-т промышленных технологий и дизайна, 2021. – С. 92–96.

6. Рогожникова Т. М., Воронов Н. Н. Построение математической модели для оценки информационной избыточности текста // Теория и практика языковой коммуникации : материалы VIII междунар. науч.-метод. конф. (Уфа, 23–24 июня 2016 г.). – Уфа :УГАТУ, 2016. – С. 216–232.

7. Вдовенко С. Г., Ковачева К. А., Оленев А. А. Шифрование текста с использованием шифра Цезаря // Молодежный науч. форум: технические и математические науки. – 2017. – № 1 (41). – С. 125–128.

8. Исхаков Д. М. Исторические очерки. – Казань : Фэн АН РТ, 2009. – 164 с.

9. Ларин Д. А. Этапы криптографической деятельности в России / Д. А. Ларин // Вестник РГГУ. Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2011. – № 13 (75). – С. 11–37.

10. Ларин Д. А. Криптографическая деятельность во время Первой мировой войны // Защита информации. Инсайд. – 2014. – № 3 (57). – С. 76–87.

11. Головешкин В. Б. Особенности организации радиоэлектронной борьбы // Науч. вестник Вольского военного ин-та материального обеспечения : военно-научный журнал. – 2019. – № 4 (52). – С. 63–65.

12. Ларин Д. А. Первая мировая: трагедия армии Самсонова // Защита информации. Инсайд. – 2016. – № 5 (71). – С. 83–88.

13. Партала М. А. Рифы и мифы острова Оденсхольм. К истории захвата секретных документов германского флота на крейсере «Магдебург» в августе 1914 г. // Защита информации. Инсайд. – 2007. – № 1 (13). – С. 84–90.

14. Визавитин О. И., Варламова В. В., Таякин С. Д. Применение криптографии в период Первой мировой войны // Молодой ученый. – 2017. – № 12 (146). – С. 445–448.

15. Федотова Т. П., Иванова В. Б., Тимербулатова К. Ф. Промышленный шпионаж: история развития, виды, формы и методы борьбы // Актуальные проблемы социального, экономического и информационного развития современного общества : материалы II Ежегодной Всероссийской науч.-практ. конф. (Уфа, 26 апреля 2017 г.) ; гл. ред. А. И. Уразова. – Уфа : Башкирский государственный ун-т, 2017. – С. 510–515.

16. Изюмов И. А. Агент Д. И. М. // Химия в школе. – 2020. – № 8. – С. 63–66.

17. Тобольченко А. С., Тобольченко Д. Э. Шифровальная машина «Энигма»: технологическое описание и принцип работы // Актуальные проблемы морской энергетики : материалы Восьмой междунар. науч.-техн. конф. (Санкт-Петербург, 21–22 февраля 2019 г.). – СПб. : Санкт-Петербургский государственный морской технический ун-т, 2019. – С. 394–398.

18. Пестунов А. И. Блочные шифры и их криптоанализ // Вычислительные технологии. – 2007. – Т. 12. – № S4. – С. 42–49.

19. Горлов Н. И., Шайгараева Т. Н. Способы несанкционированных подключений к ВОЛС // Инновационные, информационные и коммуникационные технологии. – 2017. – № 1. – С. 192–195.

Учебное издание

Поликанин Алексей Николаевич

ИСТОРИЯ И СОВРЕМЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор *О. В. Георгиевская*

Компьютерная верстка *О. И. Голиков*

Изд. лиц. ЛР № 020461 от 04.03.1997.
Подписано в печать 27.12.2022. Формат 60 × 84 1/16.
Усл. печ. л. 2,55. Тираж 70 экз. Заказ 224.
Гигиеническое заключение
№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плахотного, 8.