ГЛАВА 2
ИСТОРИЯ РАЗВИТИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема защиты информации имеет многовековую историю. С момента возникновения человечества всегда существовали сведения, которые человеку или группе людей необходимо было скрыть от своих недругов. Даже в первобытных племенах утечка информации об убитом мамонте могла оставить без пищи охотников. С развитием общества совершенствовались и способы добывания необходимой информации. К 400 году до н.э. Восток значительно опередил Запад в искусстве разведки. Сунь Цзы писал: «То, что называют предвидением, не может быть получено ни от духов, ни от богов, ни посредством расчетов. Оно должно быть добыто от людей, знакомых с положением противника».

С этого начался шпионаж, в том числе промышленный. Очень преуспели в нем многие государи и частные лица. Прекрасно поставленная служба разведки помогала купцам Венеции и банкирскому дому Фуггеров, фирме Круппа и дому Ротшильдов. Методы практически не менялись столетиями: подкупали, шантажировали, посылали послов-шпионов, перехватывали письма, читали пергаменты (позже книги и газеты) в библиотеках и монастырях. Когда удавалось, подсматривали и подслушивали. Трудности возникали и тогда, надо было передавать полученную информацию в центр сбора и обработки. Для этого приходилось гнать не всегда надежных гонцов, лично пробегать марафонскую дистанцию или пользоваться голубиной почтой. А чтобы не забыть по дороге, о чем шла речь, содержание перехваченных переговоров записывали, а иногда и шифровали. Таким образом, мы видим прообраз технической системы съема информации:

- микрофон, фотоаппарат, камера – ухо или глаза шпиона;
- диктофон или система накопления информации – записки;

– радиоканал, провода и т.д. – гонец;

– приемник – лицо, принявшее сообщение у гонца.

Что касается анализа полученной информации, то все осталось без изменений – нужен человек или группа людей, умеющих думать. Их работу сейчас несколько облегчила вычислительная машина. Развитие техники вплоть до начала XX века не влияло на средства несанкционированного съема информации: сверлили дырки в стенах и потолках, использовали потайные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30–40 годы появились диктофоны, действительно миниатюрные фотоаппараты и микрофоны. В дальнейшем все большее значение приобретает перехват данных, обрабатываемых в компьютерах, но совершенствуются и традиционные средства.

Желание добывать конфиденциальную информацию всегда сопровождалось не меньшим желанием противоположной стороны защитить эту информацию. Поэтому история развития средств и методов разведки – это также и история развития средств и методов защиты информации. Причем, появившиеся в древние времена способы защиты информации по сути своей не изменились до настоящего времени, совершенствовалась лишь техника их реализации. Например, такой способ защиты, как маскировка содержания информации, прошел в своем развитии несколько этапов. В древнем Риме сообщение, написанное на доске, заливали от посторонних глаз воском. В древней Греции обривали раба, писали на его голове и, когда волосы отрастали, отправляли с поручением к адресату. В средние века придумали тайнопись и сообщения скрывали с помощью невидимых химических средств. Параллельно развивались методы шифрования и кодирования, история возникновения которых начинается со времен возникновения письменности в древнем Египте и Китае.

Наиболее интенсивное развитие этих методов приходится на период массовой информатизации общества. Поэтому история наиболее интенсивного развития проблемы защиты информации связывается с внедрением автоматизированных систем обработки информации и измеряется периодом в 30 с лишним лет. В 60-х годах на Западе стало появляться большое количество открытых публикаций по различным аспектам защиты информации. Такое внимание к этой проблеме вызвано было в первую очередь все возрастающими финансовыми потерями фирм и государственных организаций от преступлений в компьютерной сфере.

В нашей стране также давно и небезуспешно стали заниматься проблемами защиты информации. И не зря советская криптографическая школа до сих пор считается лучшей в мире. Однако чрезмерная закрытость всех работ по защите информации, сконцентрированных главным образом в отдельных силовых ведомствах, в силу отсутствия регулярной системы подготовки профессионалов в этой области и возможности широкого обмена опытом привела к некоторому отставанию в отдельных направлениях информационной безопасности, особенно в обеспечении безопасности компьютерной. Тем не менее, к концу 80-х годов бурный рост интереса к рассматриваемым проблемам не обошел и нашу страну. В данное время есть все основания утверждать, что в России сложилась отечественная школа защиты информации. Ее отличительной особенностью является то, что в ней наряду с решением сугубо прикладных проблем защиты большое внимание уделяется формированию развитого научно-методологического базиса, создающего объективные предпосылки для решения всей совокупности соответствующих задач на регулярной основе.

Естественно, что за истекшее после возникновения проблемы защиты информации время, существенно изменилось как представление о сущности, так и методологические подходы к решению. Указанные изменения происходили постепенно и непрерывно, поэтому всякая периодизация этого процесса в значительной мере будет носить искусственный характер [32].

2.1. Организация защиты информации в Древней Руси

В IX в. в результате объединения новгородских и киевских земель образовалось единое русское государство – Киевская Русь. Эффективное управление весьма обширной территорией было невозможно без организации надежной связи между столицей Киевом с подчиненными территориями и войсками, несущими сторожевую службу на границах Руси, а также находящимися в походе. Основным средством связи в то время были специальные княжеские гонцы – «люди пешие и конные» – и «верные головы» (люди из княжеской дружины), которые со скоростью 200 и более верст в сутки передвигались от одного пункта до другого, передавая как устные, так и письменные сообщения. Использовались и другие способы связи: оптическая сигнализация с помощью костров и дымов, почтовые голуби, на поле боя управление осуществлялось с помощью сигнальных труб и свистков.

Для обеспечения конфиденциальности передаваемой информации использовались различные методы. Наиболее важные сообщения заучивались гонцом наизусть. При этом часто использовались намеки, иносказания условные слова. Суть данного метода заключается в том, что смысл передаваемого сообщения мог понять только посвященный человек. В последствии в криптографии такой способ обеспечения секретности получил название «жаргонного кода» и применяется до сих пор. Использовался и так называемый «тарабарский язык», когда в устное сообщение вставлялись частицы-паразиты так фраза «возьми суму» звучала так: «тараВОбараЗЬМИтараСУбараМУ». Причем фраза произносилась как можно быстрее, человеку непривычному к такому способу общения понять смысл сказанного было крайне затруднительно. Подобные способы защиты информации с древних времен были распространены не только у государственных служб, но и среди представителей криминального мира в различных странах, в том числе и в России.

Для защиты письменных сообщений использовалась физическая защита, стеганография и шифрование. В качестве гонцов использовались физически крепкие люди, они были хорошо вооружены, нередко гонец следовал в сопровождении охраны. Сами письма скручивались в свитки, которые опечатывались специальными печатями, содержащими надпись « ДЬНЕСЛОВО», что переводится как «скрытое, тайное слово». Такие печати были у многих русских князей, в том числе и у Александра Невского.

Стеганографический метод заключался в запрятывании сообщений. Депеши зашивались в одежду, помещались в подошвы и каблуки обуви и другие места.

2.2. Организация защиты информации в Средневековье

Во время царствования Ивана IV Грозного (1530–1584 гг.) осуществлялись крупные дипломатические и военные акции – покорение Астраханского и Казанского ханств, Ливонская война, установление торговых связей с Англией и некоторыми другими государствами, присоединение Сибири. Все это, естественно, оказало влияние на дальнейшее развитие конфиденциальной государственной и военной связи.

Этой же цели служило и упорядочение несения службы на границах Московского государства. 16 февраля 1571 г. был утвержден Приговор (устав) «О станичной и сторожевой службе», установивший расписание доставки гонцами и сторожами имеющих государственное значение вестей из столицы на места и обратно.

Доставка ратных вестей в большие города и центры государства кроме гонцов и сторож осуществлялась также с помощью ямской гоньбы, которая получила дальнейшее развитие и была независима от разведки и сторож. В 1550 г. был основан Ямской приказ – центральное учреждение в России, ведавшее почтовыми сообщениями. К важным центрам государства и пограничным городам были проложены ямские тракты.

Следует подчеркнуть, что ямская гоньба в Российском государстве была учреждена исключительно для нужд правительства и для проезда послов иностранных государств. Право пользования ямскими подводами определялось особыми грамотами, называвшимися подорожными, которые появились еще до учреждения ямской гоньбы и выдавались обычно только княжеским гонцам или другим должностным лицам, выполнявшим аналогичные поручения. Наличие подорожных грамот у гонцов способствовало более успешному выполнению возложенных на них обязанностей по срочной доставке особо важной правительственной корреспонденции. Тем более, что подписывались такие грамоты, как правило, великими князьями, а в дальнейшем царями. Роль правительственных гонцов в рассматриваемый период могли выполнять не только ответственные должностные лица ямского приказа, но и военные курьеры военного ведомства (разрядного приказа).

Кроме основных ямских направлений в X VI в. существовали и другие, второстепенные направления к городам, имевшим политическое, военное и экономическое значение.

Ямская гоньба использовалась также для связи с появившимися в середине XIV в. на восточной и юго-восточной окраинах государства казачьими войсками (запорожскими, донскими, кубанскими, терскими).

Ко времени правления Ивана Грозного, понимавшего, что ведение «большой политики» немыслимо без соблюдения государственной тайны, относится и начальный этап становления криптографии в России как явления государственного.

Образованный в 1549 г. Посольский приказ, отвечавший, в числе прочего, за организацию посольской и внутриполитической шифрованной переписки, обеспечивал весьма высокий уровень ее конфиденциальности.

Таким образом, в XVI в. в России впервые сложилась довольно стройная система связи высших органов управления централизованным

государством, обеспечивавшаяся специальными категориями служилых людей следующих структур исполнительной власти:

– ямского приказа (почтового ведомства) – организационное обеспечение системы ямской гоньбы и доставка корреспонденции второстепенного значения;

– разрядного приказа (военного ведомства) – доставка особо важно правительственной корреспонденции военными курьерами (гонцами);

– посольского приказа (внешнеполитического ведомства) – организация и обеспечение криптографической защиты внешне- и внутригосударственной переписки.

При царе Алексее Михайловиче, втором царе из династии Романовых, был создан приказ тайных дел (1654 г.). В ведении Приказа находилась и шифровальная служба государя. При Алексее Михайловиче бежал за границу один из служащих, имевших доступ к материалам тайного приказа. Он кормился за рубежом за счет продажи своих сенсационных «откровений». В частности, он сообщил следующее: «А устроен тот приказ при нынешнем царе для того, чтобы его царская мысль и дела исполнялись все по его хотению, а бояре б и думные люди о том ничего не ведали». Таким образом, шифровальное дело находилось под личным контролем царя, и никто из его окружения доступ к нему не мог иметь. Так сохранялась тайна секретной переписки государства. К ней не допускались даже члены боярской думы. И это было вполне оправдано.

В это же время была организована система регулярного перехвата и перлюстрации (тайное вскрытие и копирование) корреспонденции зарубежных представителей, находившихся в России. Здесь стоит высказать гипотезу, что уничтожались как раз шифрованные письма, которые в приказе тайных дел прочитать не могли и действовали по принципу: «так не доставайся ж ты никому».

После кончины царя Алексея Михайловича в 1676 г., тайный приказ, ведавший секретной перепиской, был упразднен. По вполне понятным

причинам среди бояр было немало людей, которые спешили ликвидировать и его архив.

Тем не менее, один из бывших руководителей приказа дьяк Д. Башмаков сумел сохранить для потомков мешок с «тайными азбуками» – шифрами. Он передал его наследнику – будущему царю Петру I. Петр I очень внимательно отнесся к этим бумагам. Опыт отца в защите информации он эффективно использовал.

Петр сам изобретал шифрсистемы, заставлял заниматься этим своих соратников, и даже лично проводил криптоанализ некоторых русских шифров для оценки их стойкости.

Заметим, что Петр I считал шифры монополией царя российского. Он строго наказывал своих подданных за использование «негосударственных» шифров («цифирей»). Однако частные лица все же пользовались собственными шифрами. Среди них можно указать царевну Софью Алексеевну, которая использовала шифр в переписке со своим фаворитом князем В. В. Голицыным.

Другим способом защиты информации было введение цензуры. Предпоследнее десятилетие XVII в. в России сложилась весьма тяжелая внутриполитическая обстановка. Три человека считались главой государства – царевна Софья и два царя (среди них – будущий император Петр I), наводили свои порядки стрельцы, поговаривали о будущей войне с Крымом. Все слухи могли проникнуть за границу и вызвать там нежелательный резонанс. Поэтому правительство приняло решение о введении гласной почтовой цензуры писем, отправленных в западноевропейские страны, цензуры явной, а не тайной перлюстрации, которая широко применялась на почтовых дворах Западной Европы.

XVII, XVIII и первая половина XIX вв. вошли в историю криптографии как эра «чёрных кабинетов» – специальных государственных органов по перехвату и дешифрованию переписки. В штат « чёрных кабинетов» входили криптографы-дешифровальщики, агенты по перехвату почты, специалисты

по вскрытию пакетов, писцы-копировальщики, переводчики, граверы, специализировавшиеся на подделке печатей, химики, их наличие было необходимо из-за активного использования стеганографических методов защиты информации, так называемых невидимых чернил, специалисты по имитации почерков и так далее.

Таким образом, чёрные кабинеты состояли из высококвалифицированных специалистов в различных областях деятельности. Первый «светский» «чёрный кабинет» (без криптоаналитической составляющей) был организован по приказу императора Священной Римской империи Максимилиана I в первом десятилетии XVI века, это была одна из первых в Европе служб перлюстрации почтовой корреспонденции, которую можно считать прародительницей всех европейских «черных кабинетов». Что касается Ватикана то подобные службы, работавшие на папский престол, в составе которых были и дешифровальщики, появились ещё ранее.

Во все времена дешифровальщики тесно сотрудничали со специалистами по перехвату и перлюстрации (тайное и безуликовое ознакомление с содержанием переписки), без перехвата нет дешифрования. До изобретения во второй половине XIX века электрических способов передачи информации (телеграф, телефон, радио) существовало два основных способа передачи сообщений – почта и специальные курьеры. Первый способ был дешевле и быстрее, но менее безопасным, «чёрные кабинеты» располагались, как правило, именно на почтамтах. Для защиты информации помимо шифрования использовались физические методы, конверты тщательно опечатывались сургучными и восковыми печатями, прошивались по контуру нитками, часто вместе с письмом в конверт вкладывался некий специальный знак (например волос) при вскрытии целостность этого знака нарушалась (тот же волос выпадал из конверта) и адресат мог понять что с письмом уже кто-то ознакомился. С курьерами было

ещё сложнее – их надо было подкупить, напоить, усыпить, а иногда даже убить, чтобы добыть секретную депешу.

Российские дипломаты имели некоторые сведения о возможностях «черных кабинетов» по перлюстрации дипломатической переписки и пускались на различные ухищрения, чтобы противодействовать этой деятельности. Так, например, посол России в Турции граф Н. П. Игнатьев (о нем упоминалось при описании примеров шифров, используемых во время русско-турецкой войны 1877–1878 гг .) знал о том, что посольская переписка перехватывается. Это было видно по внешним признакам получаемых пакетов. Кроме того, по внешним признакам письма, его объему, качеству пакета (конверта), почерку, запаху, можно было судить о важности корреспонденции. «Тонкий запах», высококачественный конверт, почерк посла вызывали настороженность специальных почтовых чиновников Турции. Поэтому посол прибегнул к следующему приему. Конверт был «простейшего» качества (очень дешевый), адресацию писал его лакей (якобы отправляя письмо своему знакомому или родственнику); само письмо несколько дней выдерживали рядом с открытой бочкой, в которой находилась соленая селедка. Запах от письма появлялся специфический, свойственный людям «низшего» сословия. Этот прием себя оправдал. Послания Игнатьева по внешним признакам не перехватывались.

В начале XIX в. в России была произведена реорганизация органов управления страной. Манифестом Александра I вместо коллегий учреждались министерства. В частности, было организовано МИД, руководителем которого был назначен граф А.Р. Воронцов. Канцелярия МИД содержала четыре основные экспедиции и три секретные. Первая секретная – цифирная (шифровальная), вторая – цифирная (дешифровальная), третья – газетная (служба перлюстрации). Позднее экспедиции стали называться отделениями.

«Черный кабинет» России, сосредоточенный в основном в МИД, совершенствовал методы, технику перехвата и перлюстрации сообщений

иностранных государств. На почтамтах были созданы профессиональные службы по перехвату и перлюстрации дипломатической переписки, разрабатывались методы быстрого копирования, перлюстрации без улик (подделка печатей и др.), оперативного ознакомления с содержанием сообщений и передачи их дешифровальным органам. За успехи в этой работе императоры щедро награждали подчиненных, так, например, один из чиновников «черного кабинета», который изобрел новый эффективный метод подделки печатей и аппарат для вскрытия конвертов паром, высочайшим указом был награжден орденом Святого Владимира 4-й степени «за полезные и применимые в деле открытия».

Обычно шифры классифицировались на общие и индивидуальные. Общие шифры предназначались для нескольких корреспондентов, как правило, расположенных в одном географическом регионе. Они обеспечивали им связь между собой и с «центром». Индивидуальный шифр предназначался исключительно для связи с центром. Идея такого разделения возникла еще при Екатерине II.

2.3.Организация защиты информации в XIX веке

Во второй половине XIX в. произошли революционные изменения средств передачи информации. Стали использовать телеграф, а с начала XXв. – радио.

Первая правительственная линия оптического телеграфа между Петербургом и Кронштадтом протяженностью 30 км бы-ла оборудована французским инженером Ж. Шато в 1833 г. Зимний дворец в 1835 г. получил прямую оптическую телеграфную связь с Царским Селом и Гатчиной. Тогда же международные события побудили русское правительство выделить средства для строительства линии оптического телеграфа от Петербурга до Варшавы. Линия протяженностью 1200 км, построенная в конце 1838 г., имела 149 промежуточных станций, через которые сигнал проходил за 15

мин. Правительственная шифрованная депеша, состоявшая из 45 сигналов, передавалась из Петербурга в Варшаву за 22 мин.

Оптический телеграф просуществовал в России около полувека примерно до середины 1850- х гг. Он сыграл значительную роль в развитии внутренних коммуникаций как средство оперативного управления исполнительными органами государства в мирное и военное время.

Однако более значительные перспективы давало использование электрического телеграфа. 21 октября 1832 г. в Петербурге состоялась публичная демонстрация электромагнитного телеграфного аппарата П. Л. Шиллинга фон Канштадта.

Увеличение количества линий связи приводило к необходимости разрабатывать новые шифры и коды, удобные для закрытия секретной информации, передаваемой с помощью телеграфа.

Следующий важнейший этап развития электрических средств связи начался с момента изобретения телефона. Его придумал американец А.Г. Белл в 1876 г. В России интерес к телефонной связи возник сразу после того, как стало известно об изобретении. Это было новое и эффективное средство управления. Первый телефонный разговор в России состоялся в ноябре 1879 г. между Петербургом и Малой Вишерой. В 1881 г. развернулось строительство телефонных станций в Петербурге.

К началу XX в. существовавшие электрические средства связи уже не в полной мере удовлетворяли потребности управления страной и вооруженными силами. Основная проблема заключалась в том, что для использования телеграфа и телефона необходимо протягивать кабель, по которому проходит сигнал. Впервые проблема передачи электрического сигнала без проводов была решена в России, где был создан беспроволочный телеграф – радио.

Таким образом, беспроволочный телеграф, несмотря на свою историческую молодость, еще до начала XX в. обратил на себя внимание

государственных и военных специалистов как наиболее перспективное средство связи с очень широкой предполагаемой областью применения.

Возможность быстрой передачи шифрованных сообщений на большие расстояния, а также возможность перехвата сообщений в пунктах передачи, приема и по пути следования депеш обусловливали рост криптографических отделов и отделений с привлечением на эту службу большого количества телеграфистов, радиотехников, лингвистов, математиков.

В конце XIX – начале XX вв. Россия активно использовала возможности подкупа иностранцев, имевших доступ к шифрам, кодам, шифрованной переписке. Особо важная корреспонденция иностранных дипломатов не отправлялась по почте, а обычно упаковывалась в специальные портфели с секретными замками и отправлялась к месту назначения с особыми курьерами. В результате она не попадала в «черный кабинет» и не могла быть перлюстрирована. В этих случаях приходилось прибегать к подкупу.

Подводя итог, отметим, что развитие криптографии и связи в России в XIX в. отвечало мировому уровню. Однако в организации шифровального дела имелись существенные недостатки, основными были длительные сроки действия ключей и использование ключей после их компрометации [33].

2.4.Организация защиты информации в XX веке

Уже в первые годы 20 века все крупные мировые державы начали подготовку к войне, напряжено наблюдая за тем, что делают потенциальные союзники и противники. В мирное время немногочисленные аппараты спецслужб «охотились» за мобилизационными планами, новинками военной техники и информацией о приготовление к будущей войне.

Как следствие этого, в военном ведомстве начались активные действия по созданию и совершенствованию системы по защите военной тайны. Работа велась по четырём направлениям:

1. Создание и совершенствование системы контрразведывательных органов. Их основной задачей являлось противодействие шпионажу противника в мирное и военное время.

2. Организация комплексной системы защиты информации, содержащей военную тайну.

3. Совершенствование системы фельдъегерской связи.

4. Организация военной цензуры.

2.4.1. Первая Мировая война.

Когда началась первая мировая война, то выяснилось, что армия и вместе с ней и государство, не способны обеспечить необходимый уровень защиты военной тайны. И как следствие этого, население не было готово активно помогать органам контрразведке.

И только 22 июня 1914 года газета “Русский инвалид” опубликовала обращение к гражданам Российской империи. Это было первая попытка выразить мнение властей об отношение к защите военной тайны в Российской империи. В нём власти призывали население хранить в тайне информацию о дислокации, перемещение и численности войск. Население призывали не верить различным слухам и сохранять спокойствие. Правительство обещало информировать о реальной обстановке на фронте.

К сожалению, время было упущено. Волна шпиономании, захлестнувшая Россию, как и другие европейские страны, не способствовало активизации мероприятий по защите военной тайны.

Самым опасным во время боевых действий считался перехват донесений и распоряжений противником. В качестве меры противодействия рекомендовалось посылать несколько экземпляров донесения для повышения вероятности доставки его адресату.

В отношение полевого телеграфа указывалось, что противник может только разрушить линии связи. О возможности съема информации с провода

или использование линий телеграфа противником в качестве средства оперативной связи ничего не говорилось.

В период первой мировой войны при Штабе верховного главнокомандующего, штабах фронтов и армий были сформированы специальные контрразведывательные отделения, которые развернули активную деятельность по выявлению и уничтожению вражеской агентуры.

В конце 1916 года во всех союзнических странах (Англия, Франция и Россия) были учреждены контрольные бюро, цель которых - обмен сведениями о лицах, заподозренных в военном шпионстве. Такое контрольное бюро в составе Особого Делопроизводства Отдела Генерал-Квартирмейстера в 1917 году называлось военно-регистрационным бюро.

До первой мировой войны, ни в одной стране мира, кроме Франции и Австро - Венгрии, не существовало военных дешифрованных органов. И созданное в ноябре 1911 года при Генштабе Австро-венгерской армии криптографическое бюро во главе с капитаном Андрашим Фиглем безуспешно пытались взломать русские дипломатические и военные криптосистемы.

Правда, ситуация резко изменилась в период первой мировой войны. Тогда дешифрованная служба Австро - Венгрии искусно вскрывало русские криптографические системы из за бесчисленных недоразумений связанных с военной мобилизацией в России.

Начальник армейского шифровального бюро полковник Андреев вплоть до последней минуты перед началом боевых действий воздерживался от рассылки копий новых шифров, предназначенных для использования в период войны. Эта мера привела к печальным последствиям.

К этому надо добавить, что материальное снабжение армий было налажено из рук вон плохо.

При таком беспорядке в начале войны неоднократно случалось, что радиостанции, прибывшие на фронт и принадлежавшие различным радиоподразделениям, не могли обменяться шифрованными сообщениями по

той простой причине, что отдельные радиороты снабжали свои радиостанции собственными шифрами.

Поскольку на один и тот же участок фронта могли попасть радиостанции разных рот, то в первые же дни войны выяснилось, что радиостанции, приданные одному и тому же армейскому корпусу или кавалерийской дивизии, говорят на разных шифроязыках.

А поскольку одна радиостанция не понимала другую, то при отсутствии надежной проволочно-телеграфной связи приходилось повторять шифрсообщение открытым текстом.

Но самый трагичный момент для русской армии наступил в августе 1914, когда в результате катастрофы у Мазурских озер из армии Раненкампфа сумело вырваться из окружения менее 2 тысяч человек.

Как писал Гофман, один из разработчиков этой операции в книги “Война упущенных возможностей”: “Русская радиостанция передала приказ в незашифрованном виде, и мы перехватили его. Это был первый из ряда других бесчисленных приказов, передававшихся у русских в первое время с невероятным легкомыслием ... Такое легкомыслие очень облегчало нам ведение войны на востоке, иногда лишь благодаря этому и вообще возможно было вести операции”. Сказано ясно. Перехват незашифрованных сообщений русских войск позволил немцам одержать победу в первой битве в мировой истории, на исход которой решающим образом повлияла несостоятельность в вопросах криптографии.

Хотя в начале войны Россия в начале войны испытывала большие трудности в обеспечение своих войск всем необходимым, в том числе и средствами связи, уже в первой половине сентября 1914 года ей удалось полностью снабдить их шифровальными средствами. 14 сентября 1914 года Ставка Верховного главнокомандующего отдала распоряжение о том, что все военные приказы подлежат зашифрованию.

Принятая шифросистема основывалась на многалфавитном шифре цифровой замены, в котором допускалась зашифрование несколько букв подряд по одному алфавиту.

Но уже 19 сентября молодой одаренный начальник русского отделения дешифрованной службы Австро - Венгрии капитан Герман Покорный вскрыл эту систему.

Дело в том, что такие шифросистемы не представляли непреодолимых преград для криптоаналитиков, поскольку в шифротексте зачастую сохранялась структура часто встречающихся в открытом тексте слов, таких как “атака”, “дивизия”, которые шифровали одной строкой таблицы.

К тому же поначалу русские связисты нередко вставляли открытый текст в шифрованный. Вскоре одновременное использование открытых и шифрованных текстов в сообщениях было запрещено, но было уже слишком поздно, и оно сыграло свою негативную роль.

И уже 25 сентября криптосистема была взломана окончательно.

О том, что криптосистема окончательно скомпрометирована русские догадались только 19 октября. До этого дня большинство приказов принимаемых германским командованием основывались на данных радиоперехвата. И это не случайно. Порой русские сами сообщали наиболее уязвимые места в своей обороне.

Чтение русских криптограмм позволило странам германского блока принимать время от времени такие меры, которые были единственно правильными тактическими решениями в данной ситуации. Российский Генеральный был озадачен прозорливостью противника.

Однажды немцы оставили занимаемые ими позиции за два дня до начало большого наступления русских войск. Одним из объяснений точного соответствия решений германского командование создавшиеся обстановке русские считали им аэрофотосъемки.

Но постепенно крепло убеждение, что противник читает русскую шифропереписку. Когда немецкое весеннее наступление второго года войны

достигло апогея, русские опять сменили шифр. Но эта смена доставила больше хлопот им самим. Почти все шифровки, переданные по радио в первые два дня после смены шифров, из - за допущенных ошибок, так и не были прочитаны адресатами.

В июне 1916 года вновь произошло изменение способа шифрования - русские ввели свой первый код. Возможно, это было сделано под влиянием Франции, которой из дешифрованных немецких криптограмм стало известно, что немцы читают русские шифрособщения, или под воздействием собственной службы радиоперехвата, которая начала функционировать в 1916 году.

Нарастающая дезорганизация русской армии оказывало отрицательное влияние и на службу связи. Пропорционально снижению дисциплины в войсках росла и болтливость радистов.

В начале 1917 года только в течение одного дня австрийская дешифровальная служба прочла более 300 русских шифротелеграмм, из чего следовало, что служба обеспечения связи России быстро развалилась.

Наличие слабых военных шифров, недостаточно продуманных инструкций к ним, большое количество нарушений шифродисциплины - все это в совокупности вело к тому, что русские шифры успешно раскрывались австрийскими и немецкими специалистами.

Правда проблемы с перехватом сообщений передавааемым по телеграфу возникли ещё в русско японскую войну. Если донесения в осажденный Порт-Артур шифровали, то по телеграфу информация передавалась в открытом виде.

И более того, уже в 1904 японские спецслужбы, впервые в истории радиотехнической разведки, реализовали на практики схему дистанционного съема акустической информации. Они использовали схему микрофон - кабель - приемник (наблюдатель).

Только в 1915 году в российской прессе прошло сообщение о том, что во время боевых действий в период русско-японской войны были случаи

перехвата телеграфных сообщений, которыми обменивалась Ставка главнокомандующего и войска.

2.4.2. Вторая мировая война.

К июню 1941, когда немецкие армии вторглись на территорию СССР, система защиты государственной тайны СССР была практически полностью сформирована. Она успешно выполняла целый ряд поставленных перед ней задач. От любых иностранных разведок надежно защищались все информационные ресурсы: мобилизационные, технические, военные, политические, идеологические и природные. Была организована бесперебойная поставка сведений о состоянии и положении военных, политических и экономических дел других государств. Производилась тотальная дезинформация противника о ситуации в СССР. Был установлен жесткий контроль над информацией, которая публиковалась в СМИ.

Уже 24-го июня, всего через 2 дня после начала Великой Отечественной войны, было создано «Совинформбюро», задачей которого было составление сводок для газет и радио о положение дел на фронте. Тогда же стала применяться практика «дезинформации населения», которая заключалась в замалчивании успехов противника на фронте и преувеличении результативности военных действий Рабоче-Крестьянской Красной Армии (РККА). Такой способ дезинформации способствовал сплочению населения СССР и уменьшал вероятность возникновения паники среди жителей прифронтовых районов.

Одна из важнейших ролей в информировании отводилась тогда проводному радио, по которому население и узнавало о достижениях армий на всех фронтах. В течение войны количество выпускаемых печатных изданий было сокращено практически в два раза, в печать выходило всего 18 газет. Был прекращен выпуск множества специализированных и отраслевых изданий, существенно сократился выпуск местной прессы. Тем не менее, все чаще стали появляться новые издания фронтовых газет всех уровней: бригадных, стрелковых и танковых.

Не стояло на месте и развитие технической защиты информации. Еще несколько лет назад повсеместно применялись ручные методы шифрования, которые занимали огромное количество времени и были недостаточно эффективны. Так, шифрование небольшого приказа занимало до 6 часов работы, примерно столько же требовалось на то, чтобы расшифровать полученное сообщение.

Однако, уже в 1937 году в Ленинграде на заводе «209», был образован комбинат техники особой секретности. Его основной задачей стало создание шифровальной техники для скрытого управления войсками. В этом же году на заводе были собраны первые опытные экземпляры шифровальной машины В-4, а в 1938 году началось серийное производство данных шифраторов. В 1939 году шифровальная машина была модернизирована, получила название М-100 и стала выпускаться параллельно с В-4. Основным недостатком этих машин был их огромный вес. Устройство весило 141 килограмм.

На смену М-100 пришла машина М-101, которая была в 6 раз меньше своей предшественницы и в несколько раз легче ее. Также были достигнуты успехи в разработке и выпуске компактных шифровальных машин.

В 1939 году была запущенна в серийное производство шифровальная машина К-37 «Кристалл», которая упаковывалась в ящик весом всего 19 килограмм. К началу войны на вооружение шифрорганов СССР было принято свыше 150 комплектов шифровальных устройств К-37. Это позволило значительно повысить скорость обработки шифрограмм, и к тому же улучшить криптостойкость.

В годы войны на машинную шифросвязь легли огромные нагрузки. Только шифровальной службой РККА (8-й отдел) за период войны было отработано 1,5 миллиона шифротелеграмм и кодограмм. Очень часто сотрудникам управления приходилось обрабатывать до 1500 шифрограмм в день, тогда как суточная норма составляла всего 400 шифрограмм. За все

время войны 8-е управление Генштаба разослало нижестоящим подразделениям и войскам почти 3,3 миллиона комплектов шифров.

2.4.3. Этапы развития системы защиты информации в настоящее время.

За истекшее после возникновения необходимости в обеспечении защиты информации время существенно изменилось как представление о ее сущности, так и методологические подходы к решению. Указанные изменения происходили постепенно и непрерывно, поэтому всякая периодизация этого процесса в значительной мере будет носить искусственный характер. Тем не менее, весь период активных работ по рассматриваемой проблеме в зависимости от подходов к ее решению довольно четко делится на три этапа.

Начальный этап защиты (60-е — начало 70-х гг.) характеризовался тем, что под защитой информации понималось предупреждение несанкционированного ее получения лицами, не имеющими на то полномочий. Для этого использовались формальные, функционирующие без участия человека средства. Наиболее распространенными в автоматизированных системах обработки данных (АСОД) в тот период были проверки по паролю прав на доступ к электронно-вычислительной технике (ЭВТ) и разграничение доступа к массивам данных. Эти механизмы обеспечивали определенный уровень защиты, однако проблему в целом не решали, поскольку для опытных злоумышленников не составляло большого труда найти пути их преодоления. Для объектов обработки конфиденциальной информации задачи по ее защите решались в основном с помощью установления так называемого режима секретности, определяющего строгий пропускной режим и жесткие правила ведения секретного документооборота.

Этап развития (70-е — начало 80-х гг.) отличается интенсивными поисками, разработкой и реализацией способов и средств защиты и определяется следующими характеристиками: постепенным осознанием необходимости комплексирования целей защиты. Первым итогом на этом пути стало совместное решение задач обеспечения целостности информации и предупреждения несанкционированного ее получения; расширением арсенала используемых средств защиты, причем как по их количеству, так и по их разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов, которое проявлялось в следующем:

1. Постепенное осознание необходимости комплексирования целей защиты. Первым итогом на этом пути стало совместное решение задач обеспечения целостности информации и предупреждения несанкционированного ее получения.

2. Расширение арсенала используемых средств защиты, причем как по их количеству, так и по их разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов. Широко стала практиковаться защита информации путем криптографического ее преобразования.

3. Все более целенаправленное объединение всех применяемых средств защиты в функциональные самостоятельные системы.

Например, только для решения режимных задач, имеющих право пользования конфиденциальной информацией, разрабатывались следующие *методы и средства идентификации лиц:*

- традиционные пароли, но по усложненным процедурам;
- голос человека, обладающий индивидуальными характеристиками;
- отпечатки пальцев;
- геометрия руки, причем доказано, что по длине четырех пальцев руки человека можно опознать его с высокой степенью надежности;
- рисунок сетчатки глаза;

– личная подпись человека, причем идентифицируемыми характеристиками служит графика написания букв, динамика подписи и давление пишущего инструмента;

– фотография человека.

Широко стала практиковаться защита информации путем криптографического ее преобразования; целенаправленным объединением всех применяемых средств защиты в функциональные самостоятельные системы.

Однако механическое нарастание количества средств защиты и принимаемых мер привело в конечном итоге к проблеме эффективности системы защиты информации, учитывающей соотношение затраченных на создание этой системы средств, к вероятным потерям защищаемой информации. Для проведения такой оценки необходимо применять основные положения теории оценки сложных систем. Кроме того, к концу второго периода математически было доказано, что обеспечить полную безопасность информации в системах ее обработки невозможно. Максимально приблизиться к этому уровню можно, лишь используя системный подход к решению проблемы. Другими словами, успешное решение проблемы комплексной защиты информации требует не только научно обоснованных концепций комплексной защиты, но и хорошего инструментария в виде методов и средств решения соответствующих задач. Разработка же такого инструментария, в свою очередь, может осуществляться только на основе достаточно развитых научно-методологических основ защиты информации.

Таким образом, характерной особенностью *третьего, современного этапа (середина 80-х гг. – настоящее время)* являются попытки аналитико-синтетической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты и формирования на этой основе научно-методологического базиса системы защиты информации. Основной задачей третьего этапа является перевод процесса защиты информации на строго научную основу, а также разработка целостной теории защиты информации. К настоящему времени уже разработаны основы теории

защиты информации. Формирование этих основ может быть принято за начало третьего этапа в развитии защиты информации.

Принципиально важным является то, что российские специалисты и ученые на данном этапе внесли существенный вклад в развитие основ теории защиты информации, чему способствовал бурный рост интереса к этой проблеме в высшей школе.

Контрольные вопросы

1. Каким образом передавались сообщения в Древней Руси, и как осуществлялась их защита?
2. С какой целью была учреждена ямская гоньба?
3. Кто из правителей лично проводил криптоанализ некоторых русских шифров для оценки их стойкости?
4. Кто входил в штат «чёрных кабинетов»?
5. Назовите основную причину, по которой в конце XIX – начале XX вв. Россия активно использовала возможности подкупа иностранцев, имевших доступ к шифрам, кодам, шифрованной переписке?
6. Назовите основные направления по созданию и совершенствованию системы по защите военной тайны в начале XX века.
7. Было ли у России преимущество в Первой мировой войне в отношении криптографии? Почему?
8. Когда и с какой целью было создано было создано «Совинформбюро»?
9. Назовите основные этапы развития защиты информации в послевоенное время.
10. Охарактеризуйте третий этап развития защиты информации.