Подполковник Л. Л. УТИН,
ведущий научный сотрудник
Научно-исследовательского института
Вооруженных Сил Республики Беларусь,
кандидат технических наук

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СВЯЗИ: ИСТОРИЧЕСКИЕ АСПЕКТЫ

В ходе анализа исторического пути развития системы связи было выявлено, что при разработке и внедрении новых средств доставки сообщений возникают дополнительные угрозы безопасности связи. При несвоевременном обнаружении или недооценке их потенциальной опасности создаются предпосылки для хищения, искажения или уничтожения передаваемых сообщений. В статье приведены результаты исследования антагонистического конфликта между разработчиками средств связи и специалистами в скрытом хищении информации, показаны допущенные ошибки при обеспечении безопасности связи и последствия, к которым они привели.

УДК 004.056

Под безопасностью связи понимают способность связи обеспечивать сохранение в тайне от противника содержания передаваемых сообщений и факт их передачи [1]. Исторически категория безопасности связи возникла, когда у людей появились интересы, которым может быть нанесен определенный ущерб путем воздействия на средства передачи информации. Например, факты использования содержания перехваченных писем для компрометации их авторов привели к появлению специалистов, способных составить послание таким образом, чтобы его смысл был доступен только тому, кто посвящен в тайну. Искусство тайнописи зародилось в 5 веке до н. э. Согласно «Истории» Геродота, именно это искусство спасло Грецию от порабощения царем Персии Ксерксом [2]. Из-за примитивности применяемых способов запутывания противника относительно содержания шифруемых текстов (спартанская скитала, шифр Цезаря, Полибианский квадрат и др.) временной отрезок до начала 19 века называют периодом наивной криптографии [3].

Практически одновременно с появлением тайнописи появились специалисты и по дешифровке шифров. История развития криптоанализа представляет собой многовековой поединок между создателями шифров и теми, кто их взламывает. Несмотря на то что многие шифры оставались неуязвимыми в течение столетий, криптоаналитики, как правило, находили в них слабые места. Например, арабский философ аль-Кинди обратил внимание, что изменения частоты появления букв в алфавите может быть использовано для дешифровки сообщений, использующих простые одноалфавитные шифры замены, и тем самым разрушил стойкость данных шифров [2]. Ч. Бэббидж взломал «неуязвимый» шифр Виженера.

XIX век ознаменовался огромным вкладом ученых и изобретателей в мировую науку и технику. С 1832 года в обеспечении безопасности связи начался новый этап, иногда называемый радиотелеграфным. В том году русский ученый П. Л. Шиллинг изобрел первый электромагнитный телеграфный аппарат [4], чем положил начало использованию искусственно создаваемых технических средств электросвязи для передачи сообщений. Основным достоинством телеграфной связи явилась возможность передачи сообщений на большие расстояния за небольшие промежутки времени.

В 1876 году американец А. Г. Белл создал первый телефонный аппарат. Это устройство очень быстро получило широкое признание во всем мире, так как позволило связываться на больших расстояниях без применения громоздких телеграфных аппаратов, обладало простотой и позволяло без посредников общаться любым пользователям [6]. Значительный вклад в развитие телефонной техники сделал русский изобретатель П. М. Голубицкий, который в 1885 году внес предложения о создании первой в мире телефонной станции с центральной батареей, что позволило осуществлять коммутацию множества абонентов.

В 1895 году русский ученый А. С. Попов на заседании Русского физико-химического общества демонстрирует первый в мире радиоприемник [5]. Оснащение армии телефонными, телеграфными аппаратами и радиосредствами позволило коренным образом изменить способы управления войсками, существенно облегчило работу командования. Вместе с тем применение технических средств связи способствовало появлению новых угроз безопасности связи (таблица 1).

Необходимость обеспечения безопасности связи особенно отчетливо проявилась в ходе Первой мировой войны. В это время противоборствующими сторонами широко использовалась постановка помех радиосвязи, радиоперехват сообщений и ввод ложной информации. Непринятие мер по шифрованию переданных сообщений способствовало вводу в систему управления и ложной информации. Так, в результате расследования причин гибели отдельных воинских частей 2-й армии в Восточно-Прусской операции было выявлено множество фактов перехвата противником радиограмм [5]. В итоге срочно разработали и довели до войск правила использования радиосвязи, в которых под страхом тяжелых наказаний запрещалось ведение открытых переговоров. В штаты штабов были введены офицеры-шифровальщики, а во все русские армии — специальные контрольно-слежечные радиостанции для радиоконтроля за соблюдением тре-

Таблица 1 — Основные угрозы безопасности связи при применении технических средств

Средства связи	Основные угрозы безопасности связи	Когда обнаружены, г.	Где подтверждено
Телеграфные	Наличие посредников между отправителем и получателем	1853	В английском журнале «Ежеквартальное обозрение» указано: «Наличие множества людей, знающих содержание сообщений, привело к появлению опасности, связанной с тем, что конкуренты могли подкупить телеграфиста и получить доступ к ведущейся переписке» [2].
Телефонные	Возможность подслушивания телефонных переговоров	1914	В статье капитана германского генерального штаба Р. Шмидта «Служба связи в германской армии во время войны» отмечено: «В августе 1914 года на Восточном фронте случайно удалось перехватить телеграммы русских радиостанций, посланные без соответствующих мер предосторожности. Русские депеши дали возможность принять решения, которые привели к успеху» [5].
	Подключение противника к телефонной сети для передачи дезинформации и ложных команд		
Радиосредства	Возможность перехвата сообщений	январь 1902	В докладе российского Морского технического комитета указывалось: «...телеграфирование без проводов обладает тем недостатком, что предаваемая телеграмма может быть уловлена на всякую иностранную станцию и, следовательно, прочтена, перебита и перепутана посторонними источниками электричества» [7].
	Искажение сообщения при воздействии непреднамеренных помех	17 марта 1903	В докладной записке А. С. Попова военному ведомству по вопросам организации радиосвязи между Одессой и Варной акцентировалось внимание на необходимости установки промежуточной радиостанции с целью повышения устойчивости связи и защиты ее от непреднамеренных помех [5].
	Искажение сообщения путем воздействия преднамеренными помехами	15 апреля 1904	В ходе Русско-японской войны российские моряки с броненосца «Победа», поставив преднамеренную помеху, нарушили радиосвязь японских кораблей — корректировщиков артиллерийского огня во время обстрела внутреннего рейда Порт-Артура японской эскадрой [7].

бований скрытого управления войсками при использовании средств радиосвязи.

Для определения местоположения неприятельских крупных штабов были сконструированы радиопеленгаторные станции, в основе работы которых использовался предложенный в 1906 году немецким ученым Шейлером принцип определения направлений пришедшей волны. Эти мероприятия привели к появлению нового вида разведки — радиоразведки [8].

Из-за обнаруженных фактов подключения противника к телефонным линиям, специальными директивами было запрещено при ведении телефонных переговоров передавать важные распоряжения и донесения, а также называть действительные наименования соединений и частей, места их дислокаций. К осени 1916 года на фронте начали работать прошедшие специальную подготовку «телефонные команды особого назначения». Их основными задачами являлись перехват телефонных переговоров противника, контроль мер специальной защиты телефонной сети связи и соблюдение абонентами при ведении переговоров требований скрытого управления войсками [5].

Возможность перехвата передаваемых сообщений резко обострила потребность в стойком шифровании. Однако, несмотря на то что криптографы противоборствующих сторон изобрели несколько новых шифров, они один за другим быстро раскрывались. Одна из лучших идей в шифровании данного периода принадлежит майору Дж. Моборну, руководителю криптографического исследовательского подразделения армии США. В 1918 году он ввел понятие «случайный ключ» и предложил использовать одноразовые шифрблокноты [3]. Его идея, несмотря на высокую стоимость реализации, используется и в настоящее время.

Таким образом, в ходе радиотелеграфного этапа по результатам выявленных недостатков, присущих техническим средствам электро- и радиосвязи, для обеспечения безопасности связи возникла необходимость не только защищать передаваемые сообщения от их дешифровки, но и решать новые задачи по защите линий связи от постановки помех, перехвата сообщений и приема ложной информации. Для решения задач безопасности связи в штаты всех армий вводятся подразделения радиоконтроля, контроля телефонных переговоров и офицеры-шифровальщики.

Благодаря достижениям, полученным в ходе развития электровакуумной техники, качественно изменились возможности средств связи, и с 1918 года начался очередной этап их развития — радиотехнический. Наиболее значимым событием для Красной Армии в ходе данного этапа явилось создание войск связи как самостоятельного специального рода войск (Приказ Революционного военного совета Республики № 1736/362 от 20 октября 1919 г.) [10]. Централизованное руководство связью способствовало выработке единых взглядов по вопросам организации и обеспечения связи, а также быстрейшему доведению накопленного опыта до всех частей связи.

Вместе с тем вопросы, касающиеся обеспечения безопасности связи, были решены не сразу. Только к 1929 году был разработан проект Полевого устава (ПУ-29), в котором конкретно были определены режимы работы радиосредств. В частности, радиосвязью разрешалось пользоваться только при полной невозможности использовать другие средства связи или при полном окружении противником. Оперативные приказы и донесения о принятых решениях в войсковых соединениях передавать с использованием радиосредств запрещалось [10]. Положения Полевого устава получили свое развитие в проектах Полевых уставов 1939 (ПУ-39) и 1941 (ПУ-41) годов. Необходимость внесения изменений в принятые документы была обусловлена выявленными недостатками организации связи в ходе Советско-финляндской войны (1939–1940 гг.). С целью защиты от радиоразведки противника в ПУ-41 было указано на целесообразность при-

менения паролей и позывных при использовании средств радиосвязи [10].

Однако в начале Великой Отечественной войны большинство командиров радиосредства, как правило, не применяли и не учитывали положения ПУ-41, касающиеся вопросов обеспечения безопасности связи. Одной из причин преимущественного использования проводной связи явилась «радиобоязнь», которой были подвержены многие командиры различных звеньев управления из-за наличия в немецко-фашистской армии средств пеленгования, позволяющих определять местоположение радиопередающих средств для последующего их поражения артиллерийским огнем или ударами авиации. Следует отметить, что возможности по радиоперехвату и пеленгованию советских радиосредств были высоко оценены А. Гитлером. В середине 1941 года он созвал особое совещание, результатом которого стало создание специальной зондеркоманды во главе с К. Гирингом. В данную команду вошли самые опытные работники абвера, гестапо и секретной службы. Сотни операторов круглосуточно прослушивали эфир, по улицам захваченных городов кружили автофургоны, оснащенные радиоприемными и пе[illegible]раторными станциями [11]. Достижению целей пеленгования способствовало и слабое знание офицерами Красной Армии оперативных кодов, а также передача срочных распоряжений и донесений по открытым радиоканалам.

Сложившееся положение дел в вопросах организации связи не могло не привлечь внимания руководства Советского Союза. Приказ Народного комиссара обороны от 23.07.1941 года «Об улучшении работы связи в Красной Армии» указывал: «...неудовлетворительное управление войсками в значительной мере явилось результатом плохой организации связи. Штабы соединений и объединений не ведут должной борьбы с нарушениями правил скрытого управления войсками, неправильно используют шифросвязь и запаздывают с доставкой оперативных документов в старшие и подчиненные штабы. Требую в кратчайшие сроки ликвидировать недооценку радиосвязи и обязываю командиров и офицеров штабов решительно бороться с нарушителями правил скрытого управления войсками, разгрузить шифрорганы от второстепенной переписки, повсеместно ввести таблицы позывных, сигналов и кодированные карты» [12].

В результате анализа причин сложившейся обстановки в вопросах организации связи был выявлен ряд недостатков [12], в том числе касающихся вопросов обеспечения безопасности связи (таблица 2).

Следует отметить, что выявленные недостатки были устранены только к осени 1942 года. С этой целью были введены трехзначные позывные, разработаны запасные радиоданные, используемые при фактах дискредитации основных таблиц, сокращены сроки их действия, наложены временные ограничения при использовании радиосвязи, установлены регулярные сроки смены позывных, проведена работа по дезинформации противника. Повышению скрытности способствовало и значительное улучшение организации шифровальной службы в штабах, использование для переговоров кодировочных таблиц, а также присвоение представителям Ставки и командующим фронтами других фамилий, которые периодически менялись. Для своевременного вскрытия и пресечения нарушений установленных правил ведения переговоров по радио и проводным средствам была организована служба контроля и разработано Положение о радиоконтроле и организации службы контроля.

Проведенные организационные мероприятия способствовали повышению радиодисциплины, улучшению качества подготовки и работы радистов, соблюдению правил скрытого управления войсками офицерами штабов при ведении ими оперативных переговоров. Г. К. Жуков по достоинству оценил качественные изменения, произошедшие в вопросах организации связи. В частности, он отмечал: «Советские Вооруженные Силы научились сохранять в глубокой тайне свои намерения, производить в широких масштабах дезинформацию и вводить противника в заблуждение. Скрытая перегруппировка и сосредоточение войск позволяли осуществлять внезапные удары по врагу» [13].

Изменения коснулись и используемой техники связи. Так, 30 марта 1942 года на радиолиниях Генерального штаба впервые была установлена радиосвязь с использованием аппаратуры буквопечатания «Алмаз». К декабрю 1942 года была разработана радиоустановка «Комета», являющаяся прототипом радиорелейных станций. С 1944 года в войска связи стала поступать аппаратура «Карбид» и «Бекан», используемая для развертывания помехозащищенных радиолиний. Также были разработаны первые ультракороткоход-

Таблица 2 — Основные недостатки в обеспечении безопасности связи, выявленные в ходе первого периода Великой Отечественной войны

Перечень выявленных недостатков
1. Отсутствие ограничений на длительность радиопередач
2. Отсутствие планов радиомаскировки
3. Игнорирование вопросов создания ложных радиосетей
4. Отсутствие регулярной смены радиоданных
5. Отсутствие службы радиоконтроля линий связи
6. Сосредоточение на небольших участках местности большого количества радиосредств, создающих взаимные помехи
7. Самовольное использование частот различными ведомствами и спецслужбами
8. Отсутствие строго закрепленных участков диапазона частот для наиболее важных радиосетей
9. Использование радиостанций большой мощности, если возможно использовать менее мощные средства связи
10. Низкая помехозащищенность приемников от воздействия преднамеренных радиопомех
11. Злоупотребление передачей радиограмм открытым текстом

новые радиостанции «А-7А», «А-7Б» [13].

Приобретенный в ходе Великой Отечественной войны опыт оперативной и войсковой радиомаскировки, дезинформации противника, разработанные организационные мероприятия, направленные на повышение защищенности радиоприемных средств от воздействия маскирующих радиоэлектронных помех, актуальны и в настоящее время.

Отдельно следует остановиться на результатах противоборства между криптоаналитиками и шифровальщиками в годы Второй мировой войны, сконцентрированного вокруг шифровальной машины «Энигма», изобретенной в 1918 году немецкими изобретателями А. Шербиусом и Р. Риттером [2]. Раскрыть шифр данной машины накануне Второй мировой войны безуспешно пытались лучшие криптоаналитики из США, Франции и Великобритании. Считалось, что связь в немецкой армии была защищена системой, которая не имела аналогов. Однако, как учат уроки истории, излишняя самоуверенность приводит к неисправимым ошибкам. Первый шаг к взлому «Энигмы» был сделан в результате предательства немца Х. Шмидта, который позволил французским агентам сфотографировать инструкции по пользованию «Энигмой» [2].

Однако наличие точной копии шифровальной машины при неизвестных начальных установках (ключа) не позволяло дешифровывать сообщения. Из-за неудачных попыток отыскать ключ французы передали полякам материалы по «Энигме» как «не представляющие особой ценности». К удивлению французов, польский математик М. Реевский уже к 1934 году разработал каталог ключей, использование которого позволяло читать секретные сообщения немцев. Скрытая передача копий «Энигмы» и рабочих чертежей устройства механического дешифрования ключей британской разведке позволила последней на протяжении всей войны узнавать о намерениях немецкого верховного командования. Несмотря на то что немецкие инженеры постоянно совершенствовали «Энигму», достижения поляков показали, что ее шифр не может считаться совершенным. Успехам британских криптоаналитиков способствовала и атмосфера жесточайшей секретности о взломе шифров «Энигмы». До последнего дня немецкое командование объясняло свои потери невезением либо шпионажем среди офицеров, но самоуверенно считало, что взлом «Энигмы» невозможен и невероятен [2]. Немецкие криптографы были уверены, что сложные шифры механических шифровальных машин представляют собой одну из самых надежных и стойких форм шифрования.

Очередной этап развития вопросов безопасности связи начат 15 февраля 1946 года, когда профессором Пенсильванского университета Д. У. Мочли была осуществлена демонстрация первой электронной вычислительной машины (ЭВМ) [14]. Несмотря на то что первые ЭВМ были очень дорогими и громоздкими, криптоаналитики, оценив возможности ЭВМ по быстродействию, приняли ее на вооружение для подбора шифрключей. С другой стороны, применение компьютера для шифрования позволяло создавать виртуальные шифровальные машины огромной сложности, учитывающие достоинства механических шифраторов, но дающие исключительно стойкие шифры за малый промежуток времени.

С появлением компьютеров возникают новые задачи, которые первоначально были связаны только с защитой от несанкционированного доступа к информации, а также от несанкционированного воздействия на информацию (преднамеренное или непреднамеренное изменение или уничтожение информации и ее носителей). Задачи обеспечения безопасности информации решались в основном путем ограничения физического доступа к ЭВМ и помещениям, в которых они располагались.

Благодаря научным открытиям и технологическим достижениям 60-х годов двадцатого века были минимизированы габаритные размеры и стоимость компьютеров. Начался этап компьютеризации. В ходе данного этапа ЭВМ стали широкого внедряться во все сферы жизнедеятельности общества. В 1965 году компания Rand Corporation, Массачусетский технологический институт и Калифорнийский университет в Лос-Анжелесе разработали первый сетевой протокол, обеспечивающий связь между несколькими компьютерами в сети [15]. Следует отметить, что в данном протоколе был впервые реализован адаптированный к обрывам соединительной линии выбор маршрута доставки информации.

Средства связи и методы криптографии продолжали интенсивно развиваться. Была создана засекречивающая аппаратура связи временной и гарантированной стойкости, станции тропосферной и спутниковой связи, разработаны блочные шифры и асимметричные криптосистемы.

В 1970 году компанией Bell Telephone Laboratories, являющейся частью корпорации AT&T, была разработана первая аналоговая система сотовой связи, которая за непродолжительный промежуток времени приобрела популярность у большого количества пользователей [16]. Проблемы безопасности, возникающие при применении такой связи должностными лицами, рассмотрены в [17].

В 1981 году американский программист Р. Скрента написал один из первых компьютерных вирусов и показал уязвимость используемого программного обеспечения локальных сетей и возможность скрытого хищения и модификации информации пользователей [9].

Новая техника связи привела к тому, что ведущие иностранные государства вынуждены были увеличить расходы на разработку средств перехвата информации и постановки помех. Например, во Вьетнаме американская авиация впервые применила забрасываемые передатчики помех. Выброшенные с самолета при ударе о землю они автоматически включались и создавали помехи радио и радиолокационным станциям [7]. В 1982 году в ходе израильско-ливанского конфликта израильскими вооруженными силами впервые комплексно применялась радиотехническая, радиолокационная, фотографическая и телевизионная разведка, осуществляемая как с наземных стационарных центров, так и с использованием средств, размещенных на самолетах и беспилотных летательных аппаратах (Мастиф, Скаут, AQM-34 и др.). При этом разведывательные данные существенно дополнялись сведениями, перехваченными с подземных кабельных линий связи. Заблаговременная установка специальной записывающей аппаратуры и передатчиков позволяла своевременно узнавать об изменении планов противоборствующей стороны [7].

Из-за применения при передаче информации стойких алгоритмов шифрования получили развитие методы перехвата информации через побочные излучения и наводки (ПЭМИН) радиоэлектронных средств. Часто их применение

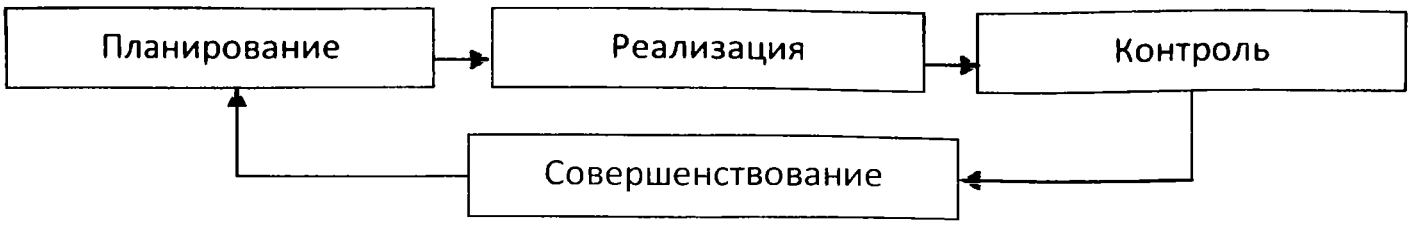

Рисунок — Процессная модель управления Деминга

было единственным способом получения хотя бы части информации до того, как она будет зашифрована. Первые сообщения о возможности перехвата информации с использованием ПЭМИН принадлежит голландскому инженеру В. Эку, опубликовавшему в 1985 году статью «Электромагнитное излучение видеодисплейных модулей: риск перехвата» [18].

Для обеспечения конфиденциальности, целостности и доступности информационных ресурсов были разработаны организационные и технические меры. Исследования, проведенные в области защиты информации, показывают, что наибольшая эффективность в противодействии злоумышленникам обеспечивается путем создания в организациях объединенной системы обеспечения безопасности связи и защиты информации, при условии наличия в ней подсистемы мониторинга угроз и оценки эффективности мер, принятых по их нейтрализации. Для описания процессов управления системой обеспечения безопасности связи и защиты информации целесообразно использовать процессную модель управления Деминга, представленную на рисунке.

Как видно из рисунка, использование процессного подхода позволяет связать в замкнутый цикл мероприятия по планированию мер защиты, их реализации на практике, проверке эффективности нейтрализации угроз безопасности связи, корректировке спланированных мероприятий. В совокупности модель позволяет непрерывно совершенствовать подходы к обеспечению безопасности связи при поддержании неразрывной связи между циклами и учитывать ранее накопленный положительный опыт.

С развитием глобальных информационно-коммуникационных сетей начался процесс информатизации общества. Данный этап характеризуется массовым внедрением цифровых средств связи и их интеграцией в единое телекоммуникационное пространство. В настоящее время информационный ресурс стал важным ресурсом государства, а обеспечение его безопасности — важнейшей обязательной составляющей национальной безопасности. В Вооруженных Силах Республики Беларусь также принимаются все необходимые меры для обеспечения безопасности связи и безопасности информации. Например, была создана автоматизированная система администрирования и мониторинга цифровой системы связи (ЦСС) Вооруженных Сил, позволяющая осуществлять сбор, обобщение, хранение и отображение информации о состоянии узлов, линий связи и используемой цифровой аппаратуре. Опытная эксплуатация данной системы подтвердила ее способность в масштабе времени, близком к реальному, оптимизировать решения по большинству кризисных ситуаций и доводить их до подчиненных пунктов управления связью.

Вместе с тем применение в ЭВМ, используемых для управления сетью связи, а также в создаваемой цифровой технике иностранных комплектующих создает предпосылки к внедрению в ЦСС аппаратных и программных закладных элементов, которые могут после их активизации выдавать точные координаты расположения элементов ЦСС, осуществлять скрытое хищение и модификацию информации, циркулирующей в ЦСС, навязывать определенные режимы работы, ухудшать скорость обмена информацией, блокировать передачу информации на отдельных направлениях связи [19].

Положение усугубляется тем, что многие офицеры, не задумываясь о последствиях, оставляют свои личные данные, номера паспортов, прописку, телефоны в различных интернет-сообществах. Вместе с тем невинные «ностальгические мотивы» участников этих сообществ позволяют использовать представленную информацию для сбора сведений о важнейших объектах инфраструктуры страны. Фотографии и видеоролики, выложенные в Интернете, часто содержат подробную и исчерпывающую информацию о роде войск, характере вооружений, особенностях службы и позволяют специалистам определять географические координаты военных объектов с учетом временной динамики. Кроме того, размещенные данные позволяют просто выйти на связь с действующими военнослужащими, а при необходимости и получить от них нужную информацию.

Принимая во внимание, что для создания и совершенствования интернет-сообщества «Одноклассники» задействованы лучшие программисты с зарплатами около 90 тыс. российских рублей [20], можно предположить, что это теневой проект, созданный по заказу спецслужб ведущих иностранных государств.

Таким образом, опыт войн и вооруженных конфликтов учит, что развитие средств связи и средств перехвата информации находится в непрекращающемся антагонистическом конфликте. Разработка и внедрение более совершенных средств передачи, приема, хранения и обработки сообщений способствует появлению новых угроз безопасности связи, которые используются для скрытого хищения информации. Несвоевременное выявление негативных факторов, сопровождающих новые технологии, непринятие эффективных мер по их нейтрализации (уменьшению последствий применения), самоуверенность отдельных должностных лиц в надежности используемых средств обеспечения безопасности связи, недооценка возможностей средств разведки армий иностранных государств отрицательно сказывались на исходах сражений, приводили к гибели десятков тысяч людей. В то же время элементарное соблюдение основных мероприятий по обеспечению безопасности связи существенно затрудняет работу разведывательных служб иностранных государств. Учет положительного исторического опыта, накопленного при решении вопросов обеспечения безопасности

связи, позволяет более правильно и целеустремленно совершенствовать существующие и разрабатывать перспективные средства связи. При этом создание автоматизированной системы обеспечения безопасности связи остается одним из перспективных направлении развития системы связи, которое позволит своевременно и непрерывно обнаруживать новые угрозы, а также принимать меры по их нейтрализации.

ЛИТЕРАТУРА

1. Связь военная. Термины и определения: ГОСТ В 23609-86. Введ. 01.01.88. — 8 с.

2. *Сингх, С.* Книга кодов: тайная история кодов и их «взлома»/С. Сингх; пер. с англ. А. Галыгина. — М.: АСТ: Астрель, 2007. — 447 с.

3. *Левин, М.* Криптография: Руководство пользователя/ М. Левин — М.: Познавательная книга, 2001. — 320 с.

4. Эпоха практического внедрения электрических систем связи в повседневную жизнь [Электронный ресурс]. — Режим доступа: http://www.sernam.ru. — Дата доступа: 28.01.2013.

5. История военной связи: в 3 т./А. И. Белов [и др.]; под общ. ред. А. И. Белова. — М.: Военное издательство, 1983–1990. — Т. 1: Становление и развитие военной связи в России — 1983. — 384 с.

6. *Соколов, А. В.* Альтернатива сотовой связи: транкинговые системы/А. В. Соколов, В. И. Андрианов. — СПб.: БХВ–Петербург; Арлит, 2002. — 448 с.

7. *Перунов, Ю. М.* Радиоэлектронная борьба: Исторический аспект/Ю. М. Перунов, М. Д. Любин//Военная мысль. — 2012. — № 12. — С. 58–72.

8. История развития пеленгационной техники [Электронный ресурс]. — Режим доступа: http://ddB.ru/arhives/1014. — Дата доступа: 28.01.2013.

9. История развития информационной безопасности [Электронный ресурс]. — Режим доступа: http://goodbasis.com/istoriya/infobezopasnost.htm. — Дата доступа: 12.02.2013.

10. История военной связи: в 3 т./А. И. Белов [и др.]; под общ. ред. А. И. Белова. — М.: Военное издательство, 1983–1990. — Т. 2: Военная связь в годы гражданской войны и строительства социализма в СССР. — 1984. — 368 с.

11. *Бабиевский, В. В.* Вторая мировая: Агентурная радиосвязь/В. В. Бабиевский [и др.] — [Электронный ресурс]. — Режим доступа: http://www.agentura.ru. — Дата доступа: 05.02.2013.

12. История военной связи: в 3 т./А. И. Белов [и др.]; под общ. ред. А. И. Белова. — М.: Военное издательство, 1983–1990. — Т. 3. Кн. 1: Военная связь в первом периоде Великой Отечественной войны 1941–1942. — 1989. — 320 с.

13. История военной связи: в 3 т./А. И. Белов [и др.]; под общ. ред. А. И. Белова. — М.: Военное издательство, 1983–1990. — Т. 3. Кн. 2: Военная связь во втором и третьем периодах Великой Отечественной войны 1942–1945. — 1990. — 392 с.

14. История развития ЭВМ [Электронный ресурс]. — Режим доступа: http://ru.wikibooks.org. — Дата доступа: 13.03.2013.

15. Локальные сети: История возникновения вычислительных сетей [Электронный ресурс]. — Режим доступа: http://www.lessons_tva.info. — Дата доступа: 15.03.2013.

16. *Хелд, Г.* Технологии передачи данных/Г. Хелл. — 7-е изд. — СПб.: Питер, К.: Издательская группа BHV, 2003. — 720 с.

17. *Утин, Л. Л.* Негативные стороны применения мобильной связи должностными лицами Вооруженных Сил/Л. Л. Утин//Наука и военная безопасность. — 2009 — № 4. — С. 2–5.

18. Зашита компьютерной информации от утечки по каналам побочных электромагнитных излучений и наводок [Электронный ресурс]. — Режим доступа: http://www.support17.com. — Дата доступа: 15.03.2013.

19. *Утин, Л. Л.* Анализ возможных способов активизации компьютерных закладок/Л. Л. Утин, Е. Л. Остромухов// Управление защитой информации. — 2003. — Т. 7. — № 4. — С. 423–427.

20. Одноклассники.ru вскрыли структуру базирования Вооруженных сил Российской Федерации [Электронный ресурс]. — Режим доступа: http://rnd.cnews.ru/armu/news. — Дата доступа: 03.04.2013.

Статья поступила в редколлегию 08.04.2013.