УДК 355.23:004.056.55

ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ В ПОДГОТОВКЕ ВОЕННЫХ СПЕЦИАЛЬНОСТЕЙ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

МАРГЕЛЬ А.Б., САЙКО Р.И.

Белорусский государственный университет информатики и радиоэлектроники

Аннотация. Рассмотрена проблема подготовки специальности по криптографической защите информации, особенности работы с криптографической информацией. Также рассматриваются особенности подготовки специалистов военных учебных заведений в сфере криптографической защиты информации и особенности их процесса обучения.

Ключевые слова: защита информации, информационная безопасность, криптография, подготовка специалистов, педагогика, образование, военное образование.

За последние 10–15 лет информационные технологии существенно расширили и усилили свой плацдарм во всех сферах нашей жизнедеятельности. Это обстоятельство – безусловный положительный фактор, влияющий на инновационный характер развития реального сектора экономики, здравоохранения, сферы услуг, досуга и, конечно же, образования. Однако наряду с этим указанный тренд со все большей очевидностью обнажает остроту проблем, негативных последствий информатизации. В наибольшей степени эти проблемы связаны с возможностями несанкционированного доступа к информационным ресурсам, объектам инфраструктуры, принадлежащим другим физическим лицам, субъектам хозяйствования, банковской сферы, другим государствам. Это напрямую связано с необходимостью обеспечения не только информационной, но и государственной безопасности. Указанные причины возлагают на систему военного образования ответственность в части не только информатизации самой сферы образования, но и подготовки специалистов, способных эффективно решать указанные проблемы.

Одним из способов защиты информации является использование криптографических методов. Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст. Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию. Военный специалист в области криптографии должен быть подготовлен к решению следующих типов задач:

− участие в построении и анализе защищенных систем и сетей передачи информации;

− сопровождение разработки и исследования программно-аппаратных средств криптозащиты информации в телекоммуникационных системах;

− разработка и анализ новых алгоритмов криптозащиты передаваемой информации;

− разработка и программирование типовых криптосхем;

− проведение сравнительного анализа программно-аппаратных средств криптозащиты информации по показателям информационной безопасности;

− проведение контрольных проверок работоспособности и эффективности применяемых криптографических средств защиты информации;

− разработка предложений по совершенствованию и повышению эффективности принимаемых математических методов и алгоритмов криптозащиты и реализующих их технических средств;

− эксплуатация специальных технических и программно-аппаратных средств защищенных телекоммуникационных систем;

− сопоставительный анализ данных исследований и испытаний, изучение возможных источников и каналов утечки информации;

− оценка технических возможностей сетей передачи информации общего и специального назначения;

− выполнение оперативных заданий, связанных с обеспечением контроля технических средств и механизмов системы защиты информации;

− проведение аттестации программ и алгоритмов криптозащиты на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.[1]

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность. Программная реализация более практична, допускает известную гибкость в использовании. Независимо от способа реализации для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

− стойкость шифра противостоять криптоанализу должна быть такой, чтобы вскрытие его могло быть осуществлено только решением задачи полного перебора ключей и должно либо выходить за пределы возможностей современных компьютеров (с учетом возможности организации сетевых вычислений) или требовать создания использования дорогих вычислительных систем;

− криптостойкость обеспечивается не секретностью алгоритма, а секретностью ключа (разделяет криптосистемы общего использования (алгоритм доступен потенциальному нарушителю) и ограниченного использования (алгоритм держится в секрете));

− зашифрованное сообщение должно поддаваться чтению только при наличии ключа; − шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных;

− незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста;

− структурные элементы алгоритма шифрования должны быть неизменными;

− шифртекст не должен существенно превосходить по объему исходную информацию; дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

− ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

− не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

− любой ключ из множества возможных должен обеспечивать равную криптостойкость (обеспечение линейного (однородного) пространства ключей);

− время шифрования не должно быть большим;

− стоимость шифрования должна быть согласована со стоимостью закрываемой информации.[2]

Потребности в криптографических исследованиях в современном компьютеризированном мире неуклонно возрастают. Этот процесс выглядит вполне естественным, так как криптография предоставляет пользователю современных автоматизированных систем надежный инструментарий в области защиты информации. В то же время именно стремительное развитие информационных технологий поставило перед криптографией ряд новых задач, которые перед прежним криптографическим сообществом не стояли. Современная криптография в современном мире — это создание самых передовых защищенных информационных технологий для автоматизированных систем различного назначения: операционных систем, специального и прикладного программного обеспечения. Это и создание защищенных распределенных вычислительных сред и многое другое. И современная криптография может предоставить разработчикам и пользователям необходимый инструментарий в этих областях, в основном состоящий из моделей и методов математической криптографии.

Специалисты в области криптографической защиты информации должны овладеть основными математическими методами теории чисел, теорией групп, колец и полей, конечных полей для их последующего использования в защите информации как от помех, так и от несанкционированного доступа, в цифровой обработке сигналов и изображений, в помехоустойчивом кодировании.[3]

Список использованных источников:

1. Криптографические методы защиты информации: учебное пособие для академического бакалавриата / С. В. Запечников [и др.] // Издательство Юрайт – 2019. – С. 19–21.

2. Криптографическая защита информации : учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та – 2019. – С. 10–12.

3. Асмыкович И.К. Преподавание современных разделов математики в техническом университете с использованием информационных технологий / И.К. Асмыкович // Проблемы повышения эффективности образовательного процесса на базе информационных технологий: материалы XI Межд. науч.- практ. конф. на ВФ в УО «Белорус. гос. ун-т информатики и радиоэлектроники» (Минск, 27 апреля 2018 г.). – Минск: БГУИР, 2018. – с. 68-71.