УДК 330.46

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

Лавникович Д.С., Корнилова А.М.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Тимофеев А.М. – канд.техн.наук, доцент, доцент кафедры ЗИ.

Аннотация. В данной статье рассматривается тема важности защиты информации от утечки её техническим каналам, описаны виды таких каналов, а также способы обезопасить свои данные физическими путями и криптографическими методами. Были сформированы основные замечания для каждого из методов.

Ключевые слова: технические каналы, криптографические методы, информация.

Введение. Двадцать первый век – это однозначно время для прорывов в информационном мире. Когда, если не сейчас, у людей есть абсолютно все возможности, чтобы совершать информационные открытия, создавать новые технологии. Но пропорционально перспективам, открывшимся людям, на них легла ответственность за обеспечение безопасности любой информации, хранящейся на устройствах и носителях.

Основная часть. Одна из самых главных проблем безопасности – утечка информации по техническим каналам, которые подразумевают под собой совокупность источника информации, линии связи (физической среды), по которой распространяется сигнал; шумов, препятствующих передаче, а также средств, которые перехватывают информацию. Источником сигнала может являться как голосовой аппарат человека, так и технические устройства. Сигнал, собственно являющийся материальным носителем информации, бывает разных видов: электрическим, электромагнитным, акустическим и др.

Все существующие технические каналы можно разделить на 4 группы: каналы, обрабатываемые техническими средствами, приема, обработки, хранения и передачи информации (ТСПИ); каналы утечки речевой информации, каналы утечки информации при ее передаче по каналам связи, канала утечки видовой информации. В свою очередь каждый из каналов подразделяется на несколько типов. Выделим основные характеристики каждого из каналов.

Каналы утечки информации, которые обрабатываются техническими средствами:

– электромагнитные каналы – каналы, возникающие за счет различных видов побочных электромагнитных излучений: излучений элементов ТСПИ, излучений на частотах работы высокочастотных генераторов;

– электрические каналы – каналы, образующиеся из-за наводок электромагнитных излучений ТСПИ на соединительные линии вспомогательных технических средств и систем (ВТСС) и посторонние проводники, выходящие за пределы контролируемой зоны; из-за просачивания информационных сигналов в линии электропитания и цепи заземления ТСПИ; использования закладных устройств;

– параметрические каналы. Перехват информации возможен путем "высокочастотного облучения" ТСПИ. При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля.

– вибрационные. У некоторых ТСПИ есть в составе печатающее устройство, для которого можно найти соответствие между распечатываемым символом и его акустическим образом.

Каналы утечки речевой информации:

Голосовой аппарат человека является первичным источником акустических колебаний. Различного рода преобразователи акустических и вибрационных колебаний являются

вторичными источниками.

– акустические каналы. В акустических каналах утечки информации средой распространения сигналов является воздух, и для перехвата используют высокочувствительные микрофоны и специальные направленные микрофоны;

– виброакустические каналы. Средой распространения сигналов являются ограждающие строительные конструкции помещений. Для перехвата в этом случае используются вибродатчики;

– акустоэлектрические каналы возникают за счет преобразований акустических сигналов в электрические;

– лазерные каналы образуются при облучении лазерным лучом вибрирующих под воздействием акустического речевого сигнала отражающих поверхностей помещений;

– параметрические каналы. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС.

Каналы утечки информации при ее передаче по каналам связи:

– электромагнитные каналы. Такие излучения могут перехватываться портативными средствами радиоразведки;

– электрические каналы подразумевают контактное подключение аппаратуры перехвата к кабельным линям связи.

– индукционные каналы. Используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются датчиками.

Технические каналы утечки видовой информации.

Видовая информация - информация, получаемая средствами перехвата в виде изображений объекта или документов.

– наблюдение за объектом;

– съемка объектов;

– съемка документов.

Инженерная защита информации подразумевает осуществлений мероприятий по защите информации от несанкционированного вмешательства, а также предугадывание вредоносных воздействий. К принципам проектирования защиты мы можем отнести:

– непрерывность защиты информации;

– иерархичность всех проблем по мере их степени важности;

– интеграция различных систем защиты информации;

По функциональному назначению вспомогательные средства бывают: инженерные средства, аппаратные, программные, криптографические [1].

Рассмотрим подробнее способы защиты информации для каждого из каналов.

Для защиты речевой информации используются пассивные и активные методы и средства.

Пассивные методы защиты речевой информации направлены на:

– ослабление акустических (речевых) сигналов на границе контролируемой зоны;

– ослабление информационных электрических сигналов в соединительных линиях ВТСС;

– исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства;

– обнаружение несанкционированных подключений к телефонным линиям связи.

Активные методы защиты акустической информации направлены на:

– создание маскирующих электромагнитных помех в соединительных линиях ВТСС;

– электромагнитное подавление диктофонов в режиме записи;

– ультразвуковое подавление диктофонов в режиме записи;

– создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом, в целях уменьшения отношения сигнал/шум до

величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

В основе активных методов защиты акустической информации лежит использование различного типа генераторов помех, а также применение других специальных технических средств [2].

Видовую информацию можно защищать, располагая объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения); уменьшая отражательные свойства объекта защиты; используя средства преграждения или значительного ослабления отраженного света: ширмы, экраны, и другие преграждающие среды, преграды; осуществлять маскировку объектов защиты.

Методы защиты информации в канале связи можно разделить на две группы:

–ограничивающие физический доступ к линии и аппаратуре связи:

–преобразующие сигналы в линии к форме, исключающей для злоумышленника восприятие или искажение содержания передачи.

Методы защиты каналов, обрабатываемых техническими средствами, также включают Пассивные методы защиты информации, включающие применение разделительных трансформаторов и помехоподавляющих фильтров; экранирование; заземление всех устройств, как необходимое условие эффективной защиты информации;

Активные методы защиты информации направлены на создание маскирующих пространственных электромагнитных помех; создание маскирующих электромагнитных помех в посторонних проводниках, соединительных линиях, цепях электропитания и заземления. К активным методам защиты относятся пространственное и линейное зашумление [3].

Криптографические методы защиты информации основаны на использовании криптографических систем, или шифров. Можно выделить два криптографических метода защиты информации: шифрование и цифровая подпись. Под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритм криптографического преобразования. Основной характеристикой шифра является криптостойкость.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. В качестве ключа в шифрующих таблицах используется: размер таблицы, слово или фраза, задающие перестановку, особенности структуры таблицы.

Шифрование заменой (подстановкой) подразумевает то, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста.

Шифрование гаммирования означает, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра.

Гамма шифра – это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы [4].

При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является электронная цифровая подпись.

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания.

Каждая подпись содержит следующую информацию: дату подписи, срок окончания действия ключа данной подписи, информацию о лице, подписавшем файл, идентификатор подписавшего, собственную цифровую подпись [5].

Заключение. Исходя из всей информации, можно сделать выводы о том, что на сегодняшний момент существует, как и обильное количество новых технологий для передачи информации, так и несанкционированных способов добраться до неё. Соответственно, для того чтобы обезопасить себя и свои данные, следует изучить как можно больше потенциальных угроз, самой главной из которых является утечка информации по техническим каналам, и способов обойти эти угрозы: как физические, так и криптографические.

Список литературы:

1. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. – 2-е изд. – М.: Радио и связь, 2001. – 376 с;

2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – М.: Горячая линия-Телеком, 2020. – 586 с.

3.Торокин, А.А. Инженерно-техническая защита информации / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

4.Технические средства и методы защиты информа-ции: Учебник для вузов/ Зайцев А.П., Шелупанов А.А., МещеряковР.В. и др.;

5. Ворона В.А., Костенко В.О. Способы и средства полу-чения акустической речевой информации. -М.: Вестник ВНИИНМАШ – Техническое регулирование и стандарти-зация, № 1 (14), с. 130-151. 2013.

UDC 330.46

INFORMATION SECURITY OF INFORMATION AND COMPUTER SYSTEMS

Lavnikovich D.S., Kornilova A.M.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Timofeev A.M. - PhD, assistant professor, associate professor of the department of IS.

Annotation. This article discusses the topic of the importance of protecting information from leakage to its technical channels, describes the types of such channels, as well as ways to secure your data by physical means and cryptographic methods. The main remarks for each of the methods were formed.

Keywords. technical channels, cryptographic methods, information.