УДК 338.27:330.43

МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Титов В.А., Замараева О.А., Кузин Д.О.

ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова», Москва, e-mail: vtitov213@yandex.ru

Определена степень актуальности проблемы защиты информации в настоящее время. Представлены основные определения, связанные с инженерно-технической защитой. Описаны этапы обеспечения защиты информации, необходимые на предприятиях. Проведено распределение защищаемых объектов на соответствующие классы. Описаны возможные каналы утечки информации и представлена классификация технических каналов утечки информации. Установлены требования к объему и характеру комплекса мероприятий, направленных на защиту конфиденциальной информации от утечки по техническим каналам в процессе эксплуатации защищаемого объекта. Указаны основные должностные лица на предприятии, отвечающие за реализацию информационной безопасности. Рассмотрены виды технических средств приема, обработки, хранения и передачи информации. Описаны основные методы и способы защиты информации от утечки по техническим каналам – организационные, поисковые и технические. Представлены способы активной и пассивной защиты информации.

Ключевые слова: защита информации, средства, каналы утечки, классификация, информация

ACTIONS OF ORGANIZATION ENGINEERING AND TECHNICAL INFORMATION SECURITY

Titov V.A., Zamaraeva O.A., Kuzin D.O.

Plekhanov Russian University of Economics, Moscow, e-mail: vtitov213@yandex.ru

The degree of urgency of the problem of information security in the moment. The basic definitions related to engineering protection. Describes the steps to protect the information required in the workplace. Conducted distribution of protected objects to the appropriate classes. The possible channels of information leakage and classified technical information leakage. The requirements to the volume and nature of actions aimed at protecting confidential information from leaking via technical channels during operation of the protected object. Identifies the main officials of the company, responsible for the implementation of information security. The types of technical means for receiving, processing, storing and transmitting information. The main methods and ways to protect information leakage through technical channels – organizational, technical and search. The ways of active and passive protection information.

Keywords: information protection, funds, leak channels, the classification, information

В настоящее время информация занимает ключевое место. Информация – сведения о лицах, фактах, событиях, явлениях и процессах независимо от формы их представления. Владение информацией во все времена давало преимущества той стороне, которая располагала более точной и обширной информацией, тем более если это касалось информации о соперниках или конкурентах. «Кто владеет информацией, тот владеет миром» (Натан Ротшильд – британский банкир и политик).

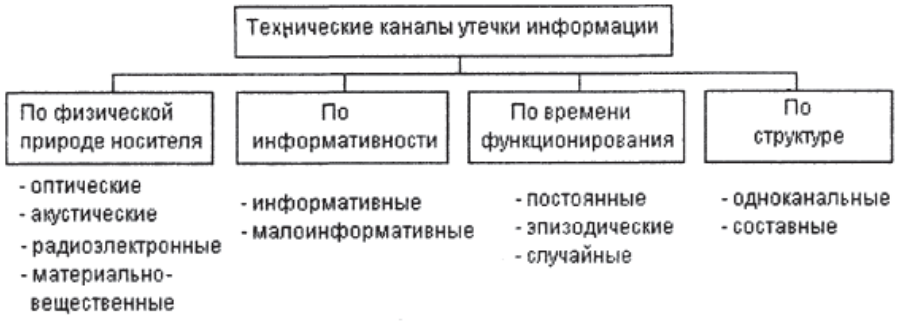
Проблема защиты информации существовала всегда, но в настоящее время из-за огромного скачка научно-технического прогресса она прибрела особую актуальность. Поэтому задача специалистов по защите информации заключается в овладении всем спектром приемов и методов защиты информации, способов моделирования и проектирования систем защиты информации. Одним из способов защиты информации является инженерно-техническая защита информации. Инженерно-техническая защита – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к конкуренту. Физический путь переноса информации от ее источника к несанкционированному получателю называется каналом утечки. Канал, в котором осуществляется несанкционированный перенос информации с использованием технических средств, называется техническим каналом утечки информации (ТКУИ). Классификация технических каналов утечки информации представлена на рисунке [1].

Для обеспечения высококачественной защиты информации от утечки по техническим каналам прежде всего необходим дифференцированный подход к защищаемой информации. Для этого их надо разделить на соответствующие категории и классы. При этом классификация объектов проводится в соответствии с задачами технической защиты информации. Здесь же устанавливаются требования к объему и характеру комплекса мероприятий, направленных на защиту конфиденциальной информации от

утечки по техническим каналам в процессе эксплуатации защищаемого объекта.

К классу защиты А относятся объекты, на которых осуществляется полное скрытие информационных сигналов, возникающих при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте).



Классификация технических каналов утечки информации

К классу защиты Б относятся объекты, на которых осуществляется скрытие параметров информационных сигналов, возникающих при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте) [1].

В зависимости от природы источника конфиденциальной информации каналы утечки имеют следующую классификацию [2]:

– электромагнитные каналы утечки информации в радиочастотном диапазоне электромагнитных волн, в которых техническим разведывательным (демаскирующим) признаком объектов защиты являются электромагнитные излучения, параметры которых качественно или количественно характеризуют конкретный объект защиты;

– электромагнитные каналы утечки информации в инфракрасном диапазоне электромагнитных волн, в которых техническим демаскирующим признаком объекта защиты являются собственные излучения объектов в этом диапазоне;

– акустический канал утечки информации. Используется для получения информации в акустической речевой и сигнальной разведках;

– гидроакустические каналы утечки информации. Используется при получении информации о передаче звукоинформационной связи, разведке шумовых полей и гидроакустических сигналов;

– сейсмические каналы утечки информации, позволяющие за счет обнаружения и анализа деформационных и сдвиговых полей в земной поверхности определять координаты и силу различных взрывов, а также перехват ведущихся на небольшой дальности переговоров;

– магнитометрические каналы утечки информации, обеспечивающие получение информации об объектах за счет обнаружения локальных изменений магнитного поля Земли под воздействием объекта;

– химические каналы утечки информации, позволяющие получать информацию об объекте путем контактного или дистанционного анализа изменений химического состава окружающей объект среды [2].

Процесс обеспечения защиты информации можно разделить на несколько этапов.

Первый этап (анализ объекта защиты) заключается в определении, что нужно защищать.

Анализ проводится по следующим направлениям:

• определяется информация, которая нуждается в защите в первую очередь;

• выделяются наиболее важные элементы (критические) защищаемой информации;

• определяется срок жизни критической информации (время, необходимое конкуренту для реализации добытой информации);

• определяются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;

• классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения, управления и т.д.).

Второй этап сводится к выявлению угроз:

• определяется – кого может заинтересовать защищаемая информация;

• оцениваются методы, используемые конкурентами для получения этой информации;

• оцениваются вероятные каналы утечки информации;

• разрабатывается система мероприятий по пресечению действий конкурента.

Третий – анализируется эффективность принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т. д.).

Четвертый – определение необходимых мер защиты. На основании проведенных первых трех этапов аналитических исследований определяются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

Пятый – руководителями фирмы (организации) рассматриваются представленные предложения по всем необходимым мерам безопасности, и производится расчет их стоимости и эффективности.

Шестой – реализация дополнительных мер безопасности с учетом установленных приоритетов.

Седьмой – осуществление контроля и доведение реализуемых мер безопасности до сведения персонала фирмы.

В рамках организации процесс защиты информации проходит, в той или иной мере, через вышеприведенные этапы.

Под системой безопасности предприятия в настоящее время понимается организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз [3].

Система безопасности фирмы состоит из следующих основных элементов (должностные лица и органы):

- Руководитель фирмы, курирующий вопросы безопасности информации.
- Совет по безопасности фирмы.
- Служба безопасности фирмы.
- Подразделения фирмы, участвующие в обеспечении безопасности фирмы.

Руководство безопасностью возлагается, как правило, на руководителя фирмы и его заместителя по общим вопросам (1-го заместителя), которым непосредственно подчиняется служба безопасности.

Для организации защиты информации на предприятии необходимо сформировать Совет по безопасности. Он представляет собой коллегиальный орган при руководителе фирмы, состав которого назначается им из числа квалифицированных и ответственных по вопросам информационной безопасности должностных лиц. Совет по безопасности разрабатывает для руководителя предложения по основным вопросам обеспечения защиты информации, в том числе:

- направления деятельности фирмы по обеспечению безопасности;
- совершенствование системы безопасности;
- взаимодействия с органами власти, заказчиками, партнерами, конкурентами и потребителями продукции и др. [4].

Наряду с техническими средствами приема, обработки, хранения и передачи информации (ТСПИ) в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС).

В организациях работа по инженерно-технической защите информации, как правило, состоит из двух этапов:

– построение или модернизация системы защиты;

– поддержание защиты информации на требуемом уровне.

Формирование системы защиты информации проводится во вновь создаваемых организациях, в остальных осуществляется модернизация существующей системы.

В зависимости от целей, порядка проведения мероприятий по обеспечению безопасности информации и применяемого оборудования методы и способы защиты от утечки информации по техническим каналам можно разделить на организационные, поисковые и технические.

Организационные способы защиты

Эти меры осуществляются без применения специальной техники и предполагают следующее:

– установление контролируемой зоны вокруг объекта;

– введение частотных, энергетических, временных и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации;

– отключение на период проведения закрытых совещаний вспомогательных технических средств и систем (ВТСС), обладающих качествами электроакустических преобразователей (телефон, факс и т.п.), от соединительных линий;

– применение только сертифицированных ТСПИ и ВТСС;

– привлечение к строительству и реконструкции выделенных (защищенных) помещений, монтажу аппаратуры ТСПИ, а также к работам по защите информации исключительно организаций, лицензированных соответствующими службами на деятельность в данной области;

– категорирование и аттестация объектов информатизации и выделенных помещений на соответствие требованиям обеспечения защиты информации при проведении работ со сведениями различной степени секретности;

– режимное ограничение доступа на объекты размещения ТСПИ и в выделенные помещения.

Поисковые мероприятия

Портативные подслушивающие (закладные) устройства выявляют в ходе специальных обследований и проверок. Обследование объектов размещения ТСПИ и выделенных помещений выполняется без применения техники путем визуального осмотра. В ходе специальной проверки, выполняемой с применением пассивных (приемных) и активных поисковых средств, осуществляется:

– контроль радиоспектра и побочных электромагнитных излучений ТСПИ;

– выявление с помощью индикаторов электромагнитного поля, интерсепторов, частотомеров, сканеров или программно-аппаратных комплексов негласно установленных подслушивающих приборов;

– специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок.

Техническая защита

Подобные мероприятия проводятся с применением как пассивных, так и активных защитных приемов и средств. К пассивным техническим способам защиты относят:

– установку систем ограничения и контроля доступа на объектах размещения ТСПИ и в выделенных помещениях;

– экранирование ТСПИ и соединительных линий средств;

– заземление ТСПИ и экранов соединительных линий приборов;

– звукоизоляция выделенных помещений;

– встраивание в ВТСС, обладающие «микрофонным» эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров;

– ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ;

– монтаж в цепях электропитания ТСПИ, а также в электросетях выделенных помещений помехоподавляющих фильтров.

Активное воздействие на каналы утечки осуществляют путем реализации [5]:

– пространственного зашумления, создаваемого генераторами электромагнитного шума;

– прицельных помех, генерируемых на рабочих частотах радиоканалов подслушивающих устройств специальными передатчиками;

– акустических и вибрационных помех, генерируемых приборами виброакустической защиты;

– подавления диктофонов устройствами направленного высокочастотного радиоизлучения;

– зашумления электросетей, посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зоны;

– режимов теплового разрушения электронных устройств [5].

В результате использования средств для проведения мероприятий по обеспечению инженерно-технической защиты информации организация существенно уменьшит вероятность реализации угроз, что несомненно способствует сохранению материального и интеллектуального капитала предприятия.

Список литературы

1. Хорев А.А. Организация защиты информации от утечки по техническим каналам // Специальная Техника. – 2006. – № 3.

2. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. – М.: НОУ ШО Баярд, 2004.

3. Аверченков В.И., Рытов М.Ю. Служба защиты информации: организация и управление: учебное пособие для вузов [электронный ресурс] – М.: ФЛИНТА, 2011.

4. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Гелиус, 2005.

5. Бузов Г.А. Защита от утечки информации по техническим каналам. М.: Горячая линия, 2005.

References

1. Horev A.A. Organization of Information leakage through technical channels. M.: Magazine «Special Technique», no. 3, 2006.

2. Halyapin D.B. Information Security. You overhear? Defend. M.: NOU SHO Bayard, 2004.

3. Averchenkov V.I., Rytov M.Y. Service information protection organization and management: a manual for high schools [electronic resource] M.: FLINTA, 2011.

4. Torokin A.A. Basics of technical protection of information. M: Gelius, 2005.

5. Buzov G.A Protection against leakage of information through technical channels. M. Hotline Telecom, 2005.

Рецензенты:

Китова О.В., д.э.н., профессор, заведующая кафедрой информатики, ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова» Министерства образования и науки РФ, г. Москва;

Петров Л.Ф., д.т.н., профессор кафедры математических методов в экономике, ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова» Министерства образования и науки РФ, г. Москва.

Работа поступила в редакцию 18.03.2014.