$$E = \frac{R_{old} - R_{new}}{R_{old}};$$

В результате работы алгоритма мы получим:
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам после задания контрмер;
- эффективность контрмеры;
- эффективность комплекса контрмер.

Список использованных источников:

1. Бармен Скотт. Разработка правил информационной безопасности. − М.: Вильямс, 2002. − 208с.

2. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. − 544 с.

3. Петренко С. А. Управление информационными рисками. − М.: Компания АйТи; ДМК Пресс, 2004. − 384с.

СИСТЕМА ЗАЩИТЫ ПОМЕЩЕНИЯ ФИРМЫ (КАБИНЕТ ДИРЕКТОРА) ОТ УТЕЧКИ ИНФОРМАЦИИ

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

Высоцкий В.Н.

Алефиренко В.М. – канд. техн. наук, доцент

В работе были рассмотрены и проанализированы каналы утечки информации из кабинета директора, методы и технические устройства её съема, способы и технические средства защиты информации. В результате была разработана система защиты помещения фирмы (кабинета директора) от утечки информации.

Проблема безопасности информации всегда волновала общество. Сегодня она заключается в том, что от качества мер защиты напрямую зависит экономическая безопасность организации.

В качестве объекта защиты был выбран кабинет директора филиала ОАО «АСБ Беларусбанк» на улице Сурганова. Кабинет директора расположен на третьем (последнем) этаже. Вход в него организован через приемную. Защищаемое помещение также граничит с коридором и кабинетом первого заместителя директора. Этажом ниже расположен кабинет отдела инвестиций и корпоративного финансирования. План защищаемого помещения представлен на рисунке 1.

Рисунок 1 – План защищаемого помещения

Помещение рассматривалось с учетом: характеристик ограждающих конструкций (стен, пола, потолка, двери, окон), предметов мебели и интерьера (столы, кресла, шкаф, сейф, доска-экран, картина, комнатные растения), радиоэлектронных средств и электрических приборов (компьютер, телефоны, видеодвойка, вентилятор, настольная лампа, настенные часы), средств коммуникаций (электропроводка, телефонные линии, кабель локальной вычислительной сети, шлейф пожарной сигнализации). В результате исследования были определены каналы утечки информации, перечень угроз и уязвимости объекта. Самые актуальные угрозы приведены ниже.

Наиболее вероятен съем речевой и/или видовой информации при применении миниатюрных фотоаппаратов, видеокамер, диктофонов, закладных аудио записывающих устройств. Их преимущество определяется небольшими размерами, широкими возможностями для маскировки, невысокой стоимостью, возможностью

передавать информацию по радиоканалу, сложностью определения злоумышленника (для закладных устройств).

Также злоумышленник может получать информацию следующими способами:

— наблюдение из окна противоположного здания текста и изображений на плакатах, экранах, укрепленных на стенах кабинета;

— подслушивание разговора в кабинете через приоткрытую дверь в приемную руководителя;

— наблюдение через окно противоположного здания за участниками совещания;

— наблюдение через приоткрытую дверь за участниками совещания;

— перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора;

— перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, пожарной сигнализации, электропитания и заземления;

— подслушивание речевой информации акустических сигналов, распространяющихся по воздуховодам и трубам отопления;

— скрытое проникновение к источникам информации, хранящихся в ящиках стола, в компьютере, в сейфе.

Внедрение системы защиты информации позволяет предотвратить или снизить величину ущерба, наносимого владельцу системы, вследствие реализации угроз безопасности информации. При её создании необходимо защищать информацию во всех фазах существования и от любых несанкционированных действий.

Выбор конкретных технических средств защиты информации осуществлялся комплексным методом определения уровня качества изделия. Для определения комплексных показателей качества необходимо было выполнить следующее: провести преобразование параметров, выраженных несколькими числовыми значениями в параметры, выраженные одним числовым значением; провести нормирование значений параметров; назначить параметрам коэффициенты значимости; провести нормирование значений коэффициентов значимости; провести расчет комплексных показателей качества; провести анализ и оценку полученных результатов. Далее производились расчеты (количества виброизлучателей, электромагнитной совместимости технических устройств, потребляемой мощности) для правильной расстановки выбранных технических изделий в защищаемом помещении.

В результате была разработана система защиты кабинета директора, которая позволяет предотвратить утечку информации или снизить величину ущерба, вследствие реализации угроз безопасности информации.

Список использованных источников:

1.Торокин, А. А. Инженерно-техническая защита информации : учеб. пособие / А. А. Торокин. — М. : Гелиос АРВ, 2005. — 960с.

2.Бузов, Г.А. Защита информации от утечки по техническим каналам : Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. — М. : Горячая линия — Телеком, 2005. — 416 с.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ КОМПАНИИ ПО РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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

Белич А. А.

Дусь А.В. – ассистент

Вопросы информационной безопасности занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация.

Для успешной работы многих компаний, особенно занимающихся разработкой программного обеспечения, чрезвычайно важно поддерживать безопасность и целостность своей компьютерной сети. Это обязывает многие компании к организации индивидуальной системы защиты информации локальной вычислительной сети.

Система защиты информации ЛВС включает в себя совокупность различных средств и методов, направленных на предотвращение утечки информации по различным каналам.

Стандартная система защиты ЛВС производится по следующим направлениям:

Аппаратные средства защиты информации

Рассматриваются различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др.