Приведенные выше шкалы, помогают провести оценку рисков хоть и весьма приближенно, зато без высоких затрат времени и средств.

Выводы: применительно к понятию информационного риска рассмотрены основные способы количественной оценки риска в относительном выражении.

Поскольку количественные показатели могут использоваться не всегда. То представляется целесообразным рассмотреть в дальнейшем качественную оценку рисков.

Список литературы

1. Кочевская И.А. Общие методы количественной оценки информационных рисков в абсолютном выражении.

2. Широчин В.П., Мухин В.Е., Крамар Д.И. Анализ рисков в задачах мониторинга безопасности компьютерных систем и сетей // «Захист інформації» № 1 (14) 2003р.

3. Машина Н.І. Економічний ризик і методи його вимірювання: Навчальний посібник. _ Київ: Центр навчальної літератури, 2003. – 188с.

4. Браіловський М.М., ЛазарєвГ.П., Дорошко В.О.Захист інформації у банківській діяльності. – К.: ТОВ «ПоліграфКолналтінг», 204. – 216 с.

УДК 000.684

С.Р. Коженевский, Г.Т.Солдатенко

ПАССИВНЫЕ МЕТОДЫ БОРЬБЫ С УТЕЧКОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ

Проблема обеспечения информационной безопасности в Украине, как и на всех странах мира, не утрачивает своей актуальности, поскольку она непосредственно связана с национальной безопасностью страны.

В конце пришлого и начале этого столетия начала происходить существенная переоценка ценностей цивилизации. К сожалению, в сфере информационных ресурсов, приобретающей первостепенное значение в научно-техническом, социально-экономическом и политическом развитии мирового общества уделяется, на наш взгляд, недостаточно внимания. Развитие рыночных отношений в нашей стране обострило проблему безопасности информации, при этом одновременно стали стремительно развиваться два процесса.

- **первый** – по защите информационных ресурсов;
- **второй** – по добыванию информации или причинению ей ущерба, вплоть до трагических ситуаций.

Информационная безопасность страны базируется на правовой и нормативных базах. В Украине это отражено в ст..17 Конституции Украины «Про інформацію» о 02.10.1992г., «Про державну таємницю» от 21.09.1999 г.и в других документах согласно перечня нормативных актов Украины по вопросам технической защиты информации от 23.04.2001 г.

Тенденции развития современного мира характеризуется созданием единого глобального информационного пространства на планете, а следовательно, проблема информационной безопасности становится проблемой коллективной, а не отдельно взятой страны. Изучение юридических проблем, связанных с расследованием компьютерных преступлений, привело, например, к разработке «Проекта Европейской Конвенции о киберпреступности» [1], в США – к пересмотру «Национальной информационной стратегии, как основе внешней и внутренней политики США в XXI веке» [2], а в России помимо Федеральных законов «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене принята «Доктрина информационной безопасности РФ».

ней политики США в XXI веке» [2], а в России помимо Федеральных законов «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене принята «Доктрина информационной безопасности РФ».

В начале 70-х годов прошлого столетия в СССР государственная задача по обеспечению безопасности информации была сформулирована в концепции противодействия иностранным техническим разведкам. Было введено понятие – **канал утечки информации.** Основное внимание уделялось следующим каналам утечки информации.

- прямое хищение носителей информации (в том числе копирование информации, находящейся на носителях);
- несанкционированное подключение к аппаратуре и линиям передачи данных или незаконное использование зарегистрированных терминалов пользователей;
- несанкционированный доступ (НДС) к информации за счет специального приспособления математического и программного обеспечения;
- перехват электромагнитного излучения (ЭМИ) с информационными сигналами при обработке информации.

Существующие угрозы потери информации можно классифицировать следующим образом. Первая группа – это так называемые tempes – атаки, или утечка по побочным ЭМИ. Первая подобная атака была впервые продемонстрирована еще в конце 60-х годов прошлого века. Тогда голландский инженер перехватывал с помощью обычного телевизора изображение на мониторе компьютера. Это наиболее понятная и очевидная угроза то есть и более опасные, хотя и, менее показательные. Для осуществления атаки подобным способом необходимо внедрение программы-вируса на отдельно стоящий компьютер, даже не подключенный к Интернету или локальной сети. Этот вирус передает информацию наружу, используя радиоканал, но в отличие от жучка- передатчика ПЭМИН-вирус для передачи информации использует технические средства и их излучения, которые уже присутствуют в компьютере. Данные излучения в широком спектре – от нескольких килогерц до нескольких гигагерц. С помощью модулирования одной или несколько частот в этом диапазоне можно передавать информацию, которая хранится на жестком диске. При это могут не пользоваться этой информацией, не вызывать ее на экран монитора ПЭМИН-вирус находит нужные данные на диске и передает ее злоумышленнику.

Принимать такую информацию можно на простые устройства – узкополосные приемники и делать это на большом расстоянии. Такой способ проведения атаки не позволяет обнаружить факт ее проведения ни визуальным путем, ни средствами анализа радиоэфира, ни средствами нелинейной локации. Вторая проблема в этой области – работа компьютера в локальной сети. Требования по паразитным излучениям предъявляются сегодня не только к одиночным ПК, но и к активному сетевому оборудованию ЛВС. На сегодняшний день в стране нет единого понимания того, как строить защищенные сети. Поэтому !!! проводятся научно-исследовательские, конструкторские работы, делаются стенды, проводятся семинары со специалистами для того, чтобы разработать определенные методики, требования к построению ЛВС.

Крупные корпоративные сети составляют сети с разными политиками безопасности, которые соответствуют разной степени секретности циркулирующей информации. Сети одного уровня защищенности объединяют в зоны. В подобных корпоративных сетях требуется организовать безопасный способ обмена информацией между разными зонами. Как правило, корпоративные сети также имеют выход в сеть Интернет. Здесь существуют две проблемы. Во-первых, воздействие Интернета на корпоративную сеть. Сюда относится целенаправленное, умышленное или неумышленное воздействие на корпоративную сеть. Для защиты корпоративной сети, как правило, применяется разделение сетей с помощью межсетевых экра-

нов (firewall), которые представляют собой компьютеры (обычный или специализированный) и ПО, настроенное определенным образом. Проблема этого подхода – потенциальная надежность системы. Так как это программа, то чем лучше она работает по разделению сетей, тем она сложнее. А чем она сложнее, тем больше вероятность, что она имеет достаточно много «дыр». Это подтверждают популярные ОС, на протяжении всего жизненного цикла которых обнаруживаются уязвимости. То же касается межсетевых экранов. Эта проблема привела к тому, что в государственных структурах применяется политика использования двух физически разделенных сетей – корпоративной и открытой, которая подключается к Интернету. По сути, это приводит к использованию двух компьютеров на одном рабочем месте. Этот способ регламентирован специальным постановлением Кабинета Министров Украины, и пока ничего лучшего не придумали. Но и в этой системе все равно есть ряд недостатков, о которых мы неоднократно говорили.

Для предотвращения утечки информации необходимы специальные мероприятия и средства. С целью выявления потенциальных каналов утечки информации были созданы межотраслевые комиссии и проведено обследование категорированных объектов – от кабинетов членов правительства до выделенных помещений в организациях, предприятиях и заводах. Соответствующим Министерствам было поручено закрытие каналов утечки информации и разработка средств защиты информации в средствах вычислительной техники (ВТ), оргтехники и т.д. С этого момента началось широкомасштабное развитие методов, способов и средств защиты информации с целью предотвращения ее утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) и за счет НДС.

Наибольшее внимание было уделено:

- программным средствам;
- программно-аппаратным средствам;
- пассивному методу – экранированию и фильтрации;
- активному методу – зашумлению.

На достоинствах и недостатках прежней концепции противодействия иностранным технически разведкам не стоит останавливаться, так как это достаточно освещено в различных источниках. Между прочим, следует отметить, что активный метод (зашумление) разрабатывался интенсивнее и быстрее внедрялся, так как не требовал серьезных финансовых затрат при постановке на производство. Такое положение сохранялось до конца 90-х годов. Процесс, так называемой, переходной экономики сгенерировал создание структур негосударственной собственности, занимающихся проблемами безопасности информации, в которые пришли опытные специалисты из госпредприятий. Доступнее стали и высокие технологии, и публикации по проблеме защиты информации. Эти факторы стимулировали ускоренное развитие целого ряда методов , способов и средств защиты информации, так как негосударственные структуры более мобильны в достижении цели.

В общем случае под **защитой информации** понимают совокупность технических средств, организационных мероприятий и правовых норм для предупреждения причинения ущерба интересам собственника информации. При этом средства защиты информации направлены на осуществление следующих целей:

- предупреждение уничтожения или искажения информации;
- исключение несанкционированного доступа к информации;
- предупреждение несанкционированной модификации информации;
- снижение уровней ЭМИ и т.д.

Перечень сведений, разглашение которых может причинить вред интересам собственника информационных ресурсов, это;

1. В сфере основной деятельности:
   - сведения 0 научно-производственных возможностях;
   - сведения о планах развития предприятия и методах управления;
   - объемы покупок и продаж.
2. В сфере финансов:
   - банковские счета и операции:
   - международные расчеты с инофирмами
   - источники и размеры кредитов.
3. В сфере партнерских отношений:
   - списки контрагентов и сведения об их финансовом состоянии;
   - сведения о подготовке переговоров, включая тактику их ведения.

Перечисленные виды информации хранятся, обрабатываются в средствах ВТ и передаются по линиям связи абонентов. Поэтому, если не приняты необходимые и достаточные меры по предотвращению утечки информации по каналам, образованным средствам ВТ, то ни о какой защите информации не может идти речи – т.е. несанкционированный доступ к информационным потокам предприятия «имеет место быть».

В настоящее время в концепции технической защиты информации появились дополнительные требования по:

- аутентификации, достоверности и целостности информации;
- биологической защите оператора;
- противодействию электромагнитному терроризму и т.д.

Расширение спектра требований, которые необходимо учитывать при изготовлении ПК в специсполнении, вызвало изменения в концепции защиты информации. Например, при применении активного метода защиты необходимо понимать суть его негативного воздействия при решении задачи обеспечения биологической защиты оператора.

Электромагнитное излучение (ЭМИ_ имеет следующие факторы воздействия на организм человека:

- биологический;
- специфический (биохимическое изменение);
- тепловой (локальный нагрев тканей).

Такие воздействия приводят к профзаболеваниям: по статистике наиболее компьютеризованной страны – США – темпы роста компьютеризации населения соответствуют темпам роста профзаболеваний [4]. В настоящее время ряд европейских стран, Россия и 25 штатов США разработали документы, регламентирующие правила пользования ПК. Наиболее известны шведские стандарты MPRII и TCO, а также российские СанПиН 2.2.2.542-96 и ГОСТ 50948-96. В этих документах содержаться рекомендации по защите от вредных факторов. Это применение различных классов фильтров, например, «полная защита» или «максимальная защита. Эти фильтры изготовлены из стекла [5], сильно легированного атомами тяжелых металлов. На стороне, обращенной к пользователю нанесено полиэфирное и 5-слойное диэлектрическое покрытие, а на противоположной стороне вакуумным напылением нанесен слой металлического серебра.

При этом достигается ослабление:

- магнитной и электрической составляющих поля – на 40 дБ;
- электростатического поля – на 40 дБ;
- ультрафиолетового излучения – полностью;
- рентгеновского излучения в 250 раз;
- блики отсутствуют полностью, повышение контрастности – в 10 раз.

При выборе метода, обеспечивающего комплексное предотвращение утечки информации, необходимо учитывать следующие требования:

- гарантированное обеспечение степени защиты информации;
- биологическую защиту оператора;
- защиту от электромагнитного терроризма;
- технологическую пригодность к серийному производству;
- приемлемые экономические показатели;
- сохранение дизайна устройств ПК.

В наибольшей степени удовлетворяет этим требованиям **только пассивный метод защиты** информации. В общем плане – это локализация источников побочных ЭМИ, т.е. экранирование и фильтрация токонесущих цепей.

Для полного устранения излучений от ПК, линий которые выходят за пределы контролируемой зоны. Необходимо не только подавить их, но и ограничить или уменьшить сферу действия электрического опля. Эта задача решается путем применения опрашивания, которое подразделяется на [3] :

- электростатическое;
- магнитостатическое;
- электромагнитное.

Электростатическое и магнитостатическое экранирование основывается на замыкании экраном, обладающим в первом случае высокой электропроводностью, а во втором - магнитопроводностью, соответственно, электрического и магнитного полей. На высокой частоте применяется исключительно электромагнитное экранирование. Действие электромагнитного экрана основывается на том, что высокочастотное электромагнитное поле ослабляется им же созданным полем обратного направления.

Очень важно также и заземление – как ПК так и самого экрана. В первую очередь необходимо, чтобы заземление не выходило за пределы помещения, где находится ПК.

Очень важным фактором является применение сетевых фильтров. Сетевые фильтры обеспечивают защищенность ПЕ не только от внешних помех, но и от различного рода сигналов, генерируемых устройствами, которые могут служить источником утечки информации. При этом сетевые фильтры выполняют две очень важные защитные функции в целях питания ПК:

- защита ПК об внешних импульсных помех;
- защита от наводок, создаваемых самим ПК.

Следует заметить, что в последние нескольких лет заметно оживление на рынке ПК с защитой информации. Но все производители, независимо от формы собственности, действуют по одной технологии, которая была отработана в 70-80-х годах прошлого столетия на предприятиях СССР. Эта технология обеспечивала хорошие результаты, поскольку базировалась на ПК отечественного производства. Полное и безвозвратное исчезновение отечественного производителя ПК и ориентация на постановку ПК зарубежных производителей потребовало новых подходов в решении задач проблемы защиты информации.

Комплектующие для сбора ПК на Украине поставляются из-за рубежа. С периодичностью 3-6 месяцев происходит изменение их конструкторских решений, технических характеристик, форм, габаритов и конфигураций. Следовательно, технология, ориентированная на защиту каждой новой модели ПК, требует высочайшей маневренности производства.

Возможен вариант изготовления из металла набора универсальных корпусных изделий и размещения в них комплектующих ПК, а также периферийных устройств зарубежного производства. Недостатком этого подхода является то, что он приемлем только для полигонного или катастрофоустойчивого исполнения.

Другой вариант – это выбор комплектующих из большого количества однотипных изделий по признаку минимального излучения информативных сигналов. С точки зрения организации серийного производства это заманчивый вариант. Ведь на предприятиях, в которых внедрена система управления качеством (согласно ISO 9001) осуществляется входной контроль комплектующих. Вполне резонно осуществлять входной контроль и по уровням излучений. Однако, сложность осуществления контроля излучений комплектующих, невозможность учета взаимного влияния всех элементов компьютера и быстрое старение комплектующих, делают этот вариант практически неосуществимым.

Вариант защиты информации методом зашумления, т.е. радиомаскировки, имеет недостатков намного больше, чем достоинств. Например, является демаскирующим признаком категорированного объекта, ухудшают экологию на рабочем месте и главное – что, при определенных условиях, не обеспечивает гарантированную защиту информации.

Таким образом, появилась необходимость в разработке нового подхода, который обеспечивал бы функции, обрабатываемой на ПК, любого состава, структуры построения, назначения, геометрических форм и размеров, при сохранении всех эксплуатационных характеристик, дизайна и был бы свободен от вышеуказанных недостатков.

Новый подход к решению задач защиты информации базируется на пассивном методе (экранирование и фильтрация), но в отличие от прежних универсальных вариантов его применения, мы предлагаем индивидуальный подход к закрытию каналов утечки информации. В основу индивидуального подхода положен анализ устройств и комплектующих ПК с целью определения общих конструкторских и схемотехнических решений исполнения, определения параметров побочных излучений. На основании анализа этих данных осуществляются мероприятия по защите.

В общем случае ПК состоит из:

-системного блока;

- монитора;
- клавиатуры;
- манипулятора (мышь);
- принтера;
- акустической системы.

Анализ конструктивного исполнения устройств ПК позволил определить их обобщенные признаки подобия в зависимости от функционального назначения.

1. Системный блок. Большое многообразие корпусов вертикального и горизонтального исполнения.

ОПП: каркас, кожух, передняя панель, органы управления и индикации, блок питания и ввод – вывод коммуникаций.

2.Монитор. Различные геометрические формы из пластмассы, три типа экранов (ЭЛТ): плоский, цилиндрический и с двумя радиусами кривизны в различных плоскостях.

ОПП: пластмассовые корпусные детали, ввод коммуникаций, органы управления и сигнализации.

3.Клавиатура. Незначительные различия в геометрии корпусов из пластмассы (у некоторых типов поддон из металла).

ОПП: пластмассовые корпусные детали, ввод коммуникаций и органы сигнализации.

4.Манипулятор (мышь). Незначительные различия в геометрии корпусных деталей из пластмассы.

ОПП: пластмассовые корпусные детали, ввод коммуникаций.

5. Принтер (лазерный, струйный). Корпуса различной геометрии из пластмассы управления и различные разъемные соединения.

ОПП: пластмассовые корпусные детали, ввод коммуникаций, органы управления и сигнализации.

6. Акустические системы. Большое многообразие геометрических форм корпусов из пластмассы и дерева;

ОПП: ввод-вывод коммуникаций, органы управления и сигнализации, а для отдельных групп - пластмассовые корпусные детали.

Таким образом, Обобщенные признаки подобия образуют **три основные группы,** присущие базовому составу ПК, с которым приходится работать при решении задач защиты информации, такие как:

- Корпусные детали из пластмассы;
- Ввод-вывод коммуникаций;
- Органы управления и сигнализации.

При этом учитываются и **общесистемные проблемные вопросы,** как то:

- Разводка и организация электропитания и шин заземления;
- Согласование сопротивлений источников и нагрузок;
- Блокирование взаимного ЭМИ устройств ПК;
- Исключение влияния электростатического поля;
- Эргономика рабочего места и т.д.

Понимание обобщенных признаков подобия и влияния на характер излучения отличный конкретных конфигураций компьютера позволил разработать типовые конструкторско-технологические решения, реализация которых направлена на предотвращение утечки информации за счет расширения функций конструктивов устройств ПК. Набор типовых конструкторско-технологических решений варьируется в зависимости от состава устройств ПК, но для базовой модели ПК с учетом обобщенных признаков подобия он содержит решения по:

- Металлизации внутренних поверхностей деталей из пластмассы;
- Экранированию проводных коммуникаций;
- Согласованию сопротивлений источников и нагрузок;
- Экранированию стекол для монитора и изготовлению заготовок различных форм из стекла;
- Фильтрации сетевого электропитания и его защите от перенапряжений;
- Нейтрализации влияния электростатического поля;
- Расположению общесистемных проводных связей;
- Точечной локализации ЭМИ;
- Исключению ЭМИ органами управления и сигнализации;
- Радиогерметизирующим уплотнителям из различных материалов;
- Исключению взаимного влияния ЭМИ устройств ПК.

На основании анализа конструктивных особенностей конкретного ПК и возможностей, отработанных конструкторско-технологических решений разрабатываются технические требования по защите информации в конкретном составе ПК. Практика выполненных опытно-конструкторских работ по изготовлению ПК с защитой информации показал, что реализация таких конструкторско-технологических решений удовлетворяет техническим требованиям и нормативной документации по предотвращении утечки информации.

В заключении необходимо отметить, что желание обеспечить высокоэффективную систему безопасности информации вполне оправдано, но это требует значительных финансовых затрат. Вместе с тем, чрезмерные затраты на защиту не всегда адекватны гарантированной степени надежности защиты. Чтобы избежать «саморазорения» от чрезмерных затрат на обеспечение безопасности информации, следует придерживаться принципа необходимой

достаточности, т.е. – стоимость защиты не должна превышать риска ущерба от негативного воздействия на информационные ресурсы.

Список литературы

1. Волеводз А.Г. Проект Европейской Конвенции о киберпреступности, «Конфидент» №5, №6, 2001 г.

2. Гриняев С.Н. Национальная информационная стратегия как основа внешней и внетренней политики США в XXI веке, «Конфидент» №5, №6, 2001 г.

3. Чекатков А.А., Хорошко В.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.

4. Бурлаков Г.Н. «Безопасность работы на компьютере» М.:»Финансы и статистика» 1998. – 286 с.

5. Домарев В.В. «безопасность информационных технологий. Системный подход», ТИД «ДС», 2004. – 688с.

УДК 654.924

І.Н.Прудиус, Р.В. Проць, В.Г.Сторож

ЗАСІБ ОХОРОНИ ПЕРИМЕТРУ НА ВИПРОМІНЮЮЧИХ КАБЕЛЯХ

Вступ

Вирішення ряду питань забезпечення охорони периметрів важливих об'єктів, до яких відносяться окремі будівлі, склади, військові об'єкти, автостоянки і т.п. вимагає застосування засобів охорони, які базуються на різних принципах роботи і тільки при їх комплексному використанні забезпечують необхідну надійність охорони.

В останні роки інтенсивно розробляються і впроваджуються технічні засоби охорони (ТЗО), в яких роль чутливих елементів виконують випромінюючі кабелі (ВК), тобто коаксіальні кабелі з прорідженою або спеціальною перфорованою екрануючою оболонкою [1,2]. В одному з кабелів – передавальному, збуджуються високочастотні коливання, а в другому – приймальному, розміщеному паралельно на невеликій віддалі від передавального, вимірюється напруга, наведена в ньому електромагнітним полем передавального кабелю. При перетині таких ліній порушником змінюється електромагнітний зв'язок між лініями, що приводить до зміни величини наведеної напруги, яка реєструється приймачем.

Порівняно з існуючими засобами охорони периметрів, ТЗО ВК мають наступні переваги:

- забезпечення рубежу охорони довільної конфігурації, що дозволяє використовувати їх на місцевості без попередньої інженерної підготовки, а також існування можливості зміни напряму лінії охорони без застосування додаткового обладнання;
- збільшення довжини ділянки охорони при невеликих апаратурних затратах;
- забезпечення скритності ТЗО (наприклад, при прокладанні випромінючих кабелів в грунті);
- можливість прокладання ВК на довільних перешкодах, таких як загорожі, будівлі, опори і т.д.

Незважаючи на вказані переваги, багаторічні дослідження ТЗО ВК [3-5], а також дослідження проведені авторами [6-7], показали, що використання таких систем має певні обмеження:

- системи охорони мають зони пониженої чутливості до перетину периметра порушником, положення яких залежить від розподілу електромагнітного поля вздовж кабелів. Нерівномірність чутливості вздовж ВК може досягати 20 дБ і більше;