Тюмень, 2004. ***9.*** *Потий А., Леншин А. Методика формирования вербальных оценок защищенности ИТС на основе требований нормативных документов //«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 10, К., 2005. С. 8 – 18.* ***10.*** *Потий А., Леншин А. Методика определения мыслей экспертов относительно зрелости безопасности информации с применением математического аппарата субъективной логики //«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 9, К., 2004. С. 38 – 47.* ***11.*** *Гладыш С. В. Использование теории нечетких множеств при экспертной оценке и многокритериальной оптимизации систем защиты информации// Материалы IX Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», Харьков, 2005 г.* ***12.*** *GAO/AIMD-12.19.6. Federal Information Systems Control Audit Mnual. 1999.* ***13.*** *NIST SP 800-53. Marianne Swanson. Security Metrics Guide for Information Technology Systems. 2003.* ***14.*** *NIST SP 800-26. Marianne Swanson. Security Self-Assessment Guide for Information Technology Systems.* ***15.*** *ISO/IEC 21827:2002 – Systems Security Engineering – Capability Maturity Model.* ***16.*** *ISO/IEC 17799:2000E – Information Technology – Practice for Information Security Management.* ***17.*** *Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985.* ***18.*** *Information Tecnhology Security Evaluation Criteria, v. 1. 2. - Office for Official publications of the European Communities, 1991.* ***19.*** *Canadian Tusted Computer Product Evaluation Criteria, v. 3. 0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.* ***20.*** *Federal Criteria for Information Technology security. - NIST, NSA, US Government, 1993.* ***21.*** *ISO/IEC 15408-1:2000 - Information technology - Security techniques - Evaluation criteria for IT security.* ***22.*** *CEM-97/017. Common Evaluation Methodology for Information Technology Security - Part 1.* ***23.*** *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в КС від НСД.* ***24.*** *НД ТЗІ 3.7-002-99. ТЗІ на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).* ***25.*** *Положення про державну експертизу в галузі ТЗІ (приказ ДСТСЗІ СБ України від 29. 12. 99 № 62).* ***26.*** *Воробиенко П., Нечипорук О., Щербина Ю. Проблемы нормативно-правового обеспечения оценки защищенности автоматизированных систем//«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 9, К., 2004. – с. 17 – 20.* ***27.*** *С. М. Доценко, А. А. Зайчиков, В. Н. Малыш. Повышение объективности исходных данных как альтернатива методу нечеткой логики при оценке риска информационной безопасности//«Защита информации. Конфидент» № 5 '2004 г., С-Пб., 2004.*

УДК 004.049.2

ПРАКТИКА ПРИМЕНЕНИЯ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Михаил Дивизинюк, Владимир Шахайда

Севастопольский национальный университет ядерной энергетики и промышленности

Анотація: **Дана оцінка сучасних вимог стосовно ТЗІ, доведени недолікі та шляхи їх усунення.**

Summary: **The estimation of modern requirements concerning a technical privacy is given, existing problems and ways of their decision are resulted.**

Ключевые слова: **Техническая защита информации, поисковые средства, ТЗИ, закладные устройства.**

Введение

Говоря об информационной безопасности, в настоящее время чаще всего имеют в виду компьютерную безопасность. Действительно, информация, находящаяся на электронных носителях, играет все большую роль в жизни современного общества. Уязвимость такой информации обусловлена целым рядом факторов: огромные объемы, большое количество пользователей, возможность анонимного доступа к информации, простота переноса информации. Все это создает возможность проведения "информационных диверсий", делает задачу обеспечения защиты информации, размещенной в компьютерной среде, гораздо более сложной проблемой, чем, скажем, сохранение тайны традиционной почтовой переписки. Тем не менее, понятие ТЗИ подразумевает защиту всех видов информации.

I Применяемые в настоящее время средства ТЗИ

В настоящее время при лицензировании помещений для получения разрешения на обработку документов с ограниченной формой доступа, оговорен ряд мероприятий организационно-технического характера, направленных на ограничение доступа посторонних лиц в помещения. Также оговорен

перечень технических средств подавления излучений и зашумления помещений.

С технической точки зрения рекомендован ряд мероприятий, таких как:

- защита входных дверей от пролома;
- установка пожарно-охранной сигнализации;
- установка тревожных кнопок;
- заземление оборудования;
- установка сетевых фильтров;
- установка средств радиозашумления помещений типа «Волна – 4»;
- установка систем аудиозашемления помещений;
- установка фильтров на телефонные линии связи;
- удаление из помещений всех незадействованных линий связи;
- проведение исследований всего электронного оборудования, находящегося в помещении, на наличие побочных излучений.

В настоящее время средства съема информации с каналов связи и оборудование вычислительных комплексов шагнули далеко вперед по сравнению со средствами ТЗИ. Рекомендуемые и требуемые для лицензирования помещений средства ТЗИ разработаны в лучшем случае в 80-х годах прошлого столетия и не позволяют подавить излучения от новых компьютеров, работающих на частотах свыше 1 ГГц.

Рекомендуемое и применяемое в настоящее время средство радиозашумления помещений типа «Волна» по своим ТТХ вообще не отвечает требованиям ТЗИ.

Объясняется это тем, что по паспорту потребляемая мощность изделия 20 Вт; при этом он обеспечивает зашумление в диапазоне от 100 кГц до 1ГГц. Учитывая то, что антенны изделия размещены в 3-х проекциях, мощность излучения в одной проекции в переводе на 1 МГц ориентировочно составляет 6 МВт/1МГц.

Это без учета КПД всего устройства. Вопрос о согласовании излучающих антенн вообще не оговорен в руководстве по эксплуатации. А это означает, что коэффициент бегущей волны (КБВ) может принимать значение от 0 до 1 в зависимости от излучаемой частоты. На некоторых частотах излучение может вообще отсутствовать.

II Поисковые средства

В перечень аппаратуры, необходимой для обследования помещений на наличие закладочных устройств, входят:

- средства, для обеспечения эффективности визуального обзора элементов интерьера и труднодоступных мест;
- приборы для проверки проходящих коммуникаций;
- аппаратура для выявления закладных устройств, излучающих радиоволны: детектор-локатор излучений, частотомеры, панорамные приемники, поисковые системы;
- металлоискатели;
- приборы нелинейной радиолокации;
- переносные рентгеновские комплексы;
- тепловизоры;
- аппаратура для проведения акустических и вибро-акустических измерений;
- приборы для исследований побочных электромагнитных излучений.

При этом рекомендуется объединять проведения поисковых мероприятий еще и с контролем радиационной обстановки в помещениях. Для этого применяется дозиметр или индикатор радиоактивного излучения.

Все перечисленные средства поиска источников электромагнитного излучения и радиоконтроля помещений не могут локализовать новые типы закладных устройств, использующих шумоподобный спектр сигнала, пакетную передачу информации, имеющих дистанционное управление.

Для примера рассмотрим характеристики одного из устройств передачи аудиоинформации:

способ кодирования – адаптивная дельта-модуляция;

маскировка сигнала – преобразование информации в псевдослучайный цифровой поток с индивидуальным кодированием.

В результате работоспособность изделия невозможно определить даже спектральным коррелятором типа «OSCOR».

При этом изделие имеет следующие характеристики:

- дистанционное управление;

- выходная мощность до 100 мВт;
- девиация частоты 100 КГц;
- габаритный размер 30*80*3 мм.

Для сравнения мощность излучения устройства «Волна» в том же участке частотного диапазона составляет 0.6 $*10^{-3}$ Вт, что в 165 раз меньше мощности излучения закладного устройства. При этом мы не делаем ссылку на КПД устройства, о чем говорилось выше. Из всего вышесказанного следует, что изделие «Волна» не оказывает никакого противодействия съему информации.

III Средства активного обнаружения

Приведенный список измерительной и поисковой техники рассчитан на поиск закладных устройств, работающих на частотах до 1 ГГц с модуляцией АМ, FM, WFM. Учитывая особенности работы радиопередающих устройств, использующих шумоподобный спектр излучения, данного оборудования уже недостаточно. Однако применение новых типов оборудования сопряжено с несколькими проблемами:

- разработка методик поиска новых типов закладных устройств;
- разработка и приобретение нового оборудования для поиска и противодействия новым закладным устройствам;
- согласование методик поиска и инструкций в различных ведомствах и управлениях.

На решение указанных вопросов необходимо несколько месяцев научных исследований и целевое выделение финансовых средств на разработку методик, приобретение техники в масштабах всей страны.

У нападающей стороны всегда выигрышная ситуация, потому что для нападения не требуется никаких инструкций и согласований, при этом наносится точечное нападение на одну определенную организацию. Выигрыш, как во времени, так и в финансовых средствах, вложенных в это мероприятие.

Единственным из предлагаемых к использованию прибором, способным решить вопрос поиска закладных устройств, является нелинейный детектор – локатор.

Принцип работы этого устройства заключается в облучении предметов электромагнитным излучением большой мощности качающейся частоты. Данный метод позволяет обнаружить даже выключенные электронные устройства – путем получения модулированного эхо сигнала от полупроводниковых переходов. Данный метод имеет 100% гарантию обнаружения средств съема информации в помещениях. Однако обладает одним недостатком, исключающим возможность его применения. Наличие излучения высокой плотности может вывести из строя все изделия полупроводниковой техники не только в проверяемом помещении, но и далеко за его пределами, не говоря уже о воздействии на организм сотрудника, работающего с прибором.

Десятилетний опыт применения средств съема информации показал, что во время проведения оперативных мероприятий с применением даже примитивных устройств съема информации не было ни одного случая обнаружения установленных средств передачи информации. Наличие средств ТЗИ также ни разу не препятствовало проведению мероприятий.

Анализируя вышесказанное, можно отметить основные причины, которые :способствуют съему информации:

- отсутствие эффективных средств ТЗИ;
- отсутствие эффективной поисковой техники;
- отсутствие специалистов, владеющих методами поиска средств нападения;
- назначение на должности, ответственные за ТЗИ, сотрудников, не имеющих элементарных знаний физики процесса;
- халатное отношение сотрудников к соблюдению правил обращения с документами ограниченной формы допуска;
- формальное проведение работ по лицензированию помещений;
- отсутствие контроля со стороны руководства за соблюдением правил обращения с конфиденциальными документами.

IV Программное обеспечение

В настоящее время ряд подразделений силовых структур для обработки полученной информации взяли на вооружение программное обеспечение, разработанное коммерческими структурами. В связи с отсутствием государственных программ создания подобных программных продуктов, другого выхода просто не существует. Однако использование программного продукта, даже тестированного в стенах СБУ и других научных учреждениях, не дает гарантии отсутствия в них специально оставленных шлюзов, с помощью которых разработчик может войти в программу с целью снятия информации. Анализ

использования подобных продуктов говорит о следующем: коммерческие структуры умышленно, с целью получения дополнительных доходов. оставляют в программах временные заглушки, с помощью которых периодически выводят программы из строя. Например, использование финансовой программы «Парус» требует ежеквартального вмешательства программиста-разработчика, в результате чего коммерческая структура получает доступ ко всем счетам предприятия и спискам сотрудников. В других случаях коммерческие фирмы поставляют обновленные версии программ, установка которых также требует присутствия программистов. Одновременно при зависании программы автоматически формируется файл отчета, в котором может содержаться любая информация, распознать которую может только разработчик программы.

В целом, анализируя нынешнюю ситуацию, можно с уверенностью сказать, что уровень средств ТЗИ и уровень специалистов, занимающихся на практике этими вопросами, не отвечают требованиям настоящего времени.

Что можно противопоставить в сложившейся ситуации?

Применение новых разработок в области ТЗИ

Постоянно действующая система пеленгации позволяет отслеживать появление, перемещение, и график работы излучающих устройств в помещениях. В комплексе с системой видеонаблюдения она позволяет выявить лиц, приносящих эти изделия в помещения с целью их установки, замены источников питания, снятия информации.

Учитывая то, что съем информации может происходить и без использования источников электромагнитного излучения – путем применения изделий, использующих проводные линии связи, или просто записывающих устройств таких, как проводные микрофоны, цифровые диктофоны – необходима разработка систем, подавляющих микрофон – как единственный элемент, без которого невозможно создать устройства, работающие с аудио-сигналом.

Работа с персоналом

Учитывая то, что использование средств съема информации с каналов связи требует применения дорогостоящей техники, использование которой требует определенных навыков установки, обслуживания и съема самой информации, заинтересованными структурами с целью получения необходимой информации все чаще производится привлечение высококвалифицированных сотрудников, работающих на предприятиях. Действительно, учитывая мизерные зарплаты персонала, достаточно потратить сумму в 100, а то и в 1000 раз меньшую, чем при организации снятия информации и получить информацию с первых рук, причем 100% качества.

Чтобы мы не говорили, но в любой даже особо режимной организации постоянно происходит нарушение инструкций по работе с документами ограниченного доступа. Причин, которые этому способствуют, несколько, начиная с отсутствия навыков у сотрудников, бесконтрольности со стороны руководителей и заканчивая полным непониманием со стороны персонала необходимости выполнения определенных инструкций.

Для противодействия использованию сотрудников в сборе информации, необходимо проведение ряда организационных мероприятий:

- строгий отбор при приеме на работу;
- проведение тестирования на профессиональную пригодность, привлечение службы безопасности для проверки достоверности автобиографических данных и отзывов с предыдущего места работы;
- создание служб безопасности, в функции которых должны входить: создание условий для работы с документами ограниченного доступа, контроль за персоналом, физическая защита помещений, технический контроль за электромагнитными излучениями в помещениях;
- выделение и обучение одного из руководителей организации, в функциональные обязанности которого должен входить контроль за деятельностью самой службы безопасности. Основные задачи: проведение мероприятий по проверке деятельности СБ с целью недопущения халатного отношения сотрудников СБ к своим обязанностям.

Заключение

Исходя из выше изложенного, можно наметить несколько способов решения проблем, возникших в области ТЗИ:

1. отказаться от работы, направленной только на применение технических средств, в пользу применения организационно–технических методов, направленных одновременно и на техническую защиту

информации, и на работу с персоналом, работающим с документами ограниченной формы доступа;

2. разработку постоянно действующей системы пеленгации, позволяющей отслеживать появление, перемещение и график работы излучающих устройств;

3. разработка систем подавления микрофонов;

4. создания государственной структуры по лицензированию программного обеспечения, предназначенного для обработки конфиденциальной информации; разрешение на его использование должно даваться только поле тестирования и экспертной оценки исходного кода программного продукта;

5. создание программы подготовки специалистов в области ТЗИ, владеющих одновременно как аппаратно-техническими, так и административными методами защиты информации;

6. проведение с руководителями организаций и предприятий, имеющих в обороте документацию с ограниченным допуском, ознакомительных занятий по вопросам организации документооборота и ТЗИ;

7. обеспечить проведение объективной аттестации сотрудников, занимающихся вопросами ТЗИ.