техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). ***2.*** *Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ -ПЕМВН-95).* ***3.*** *А А Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Принципы построения. // Компьютеры + программы – 1998. – № 3.* ***4.*** *А. А Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Защита от физического разрушения. // Компьютеры + программы. – 1998. – № 4.* ***5.*** *А. А. Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Защита от утечки информации по техническим каналам. // Корпоративные системы. – 1999. – № 2.* ***6.*** *А. А. Саурин, А. Л. Шихутский. Безопасные структурированные кабельные системы. Особенности реализации. // Корпоративные системы. – 1999. – № 3.* ***7.*** *Е. А. Зайцев. Резонанс экранированных систем. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., – 2002. – Вип. 5. – С. 207–210.* ***8.*** *http://www.mitsubishi-cable.co.jp/product/hikari/leakycl.html.* ***9.*** *ISO/IEC 1180. Second Edition. Information technology – Generic cabling for customer premises.* ***10.*** *А. Савчук. Проблемы технической защиты информации и электромагнитной совместимости для структурированных кабельных систем. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., – 2002. – Вип. 5. – С. 58–63.* ***11.*** *http://www.andrew.com.*

УДК 621.391.883

К ВОПРОСУ О ЗАЩИТЕ АБОНЕНТСКИХ ТЕЛЕФОННЫХ ЛИНИЙ УСТРОЙСТВАМИ КОМПЛЕКСНОЙ ЗАЩИТЫ

Владимир Луценко, Александр Архипов, Валерий Худяков*, Сергей Дедусенко**
НТУУ "КПИ", Физико-технический институт
**НИИ Электромеханических приборов, г. Киев*
***ЧП фирма "Бумекс", г. Киев*

Аннотация: **Рассматриваются вопросы технической защиты информационных потоков в абонентских телефонных линиях общего пользования. Сформулированы направления развития этих вопросов и проведен обзор существующих средств защиты телефонных аппаратов и линий. Определен круг наиболее дефицитных технических средств, проблемы, стоящие перед разработчиками и пользователями таких средств и возможные пути их решения.**

Summary: **The problems of technical protection of information flows in lines TLF of abonents of the general use. The directions are formulated, in which one it is necessary to develop activities for protection of the information against unauthorised users, the analysis of available and substantially created the hardware of protection. The circle of the most deficient means, systems in area of technical information protection, and possible paths of their creation as soon as possible is determined.**

Ключевые слова: **Защита информационных потоков, безопасность переговоров, активные и пассивные методы защиты.**

I Введение

Актуальность вопроса защиты телефонных линий и оконечных аппаратов телефонной связи в сетях общего пользования повышается из года в год. Важность вопроса не уменьшается по причине возрастания объемов оснащения различных структур импортной техникой, не прошедшей сертификации по технической защите информации (ТЗИ). И если процесс оснащения государственных структур в какой-то мере поставлен под контроль Департамента специальных телекоммуникационных систем и защиты информации (ДСТСЗИ) Службы безопасности Украины, то в остальных случаях этот процесс практически бесконтролен. Одной из причин такого положения дел является отсутствие целостной программы создания системы безопасности в рамках национальной системы ТЗИ. Кроме того, актуальность вопроса возрастает и в связи с интенсивным насыщением страны все более развитыми средствами связи, использующими "гибридные" каналы, аналоговые и цифровые, проводные и радиоканальные в единой системе связи. Это происходит на фоне неизбежных глобальных информационных процессов, характеризующихся повышенным вниманием к уязвимости информационных ресурсов и связных каналов коммерческих и государственных структур, страны в целом, что приводит к заметному возрастанию ущерба владельцев информационных ресурсов в результате объективной возможности утечки конфиденциальной информации.

II Постановка задачи

Ключевым условием быстрейшего создания комплекса технических средств (ТС) и его реализации в рамках защиты информационных потоков, циркулирующих по проводным линиям связи, является систематизация существующих и пользующихся спросом ТС. Это должно явиться основой для определения направлений, в которых необходимо развивать работы по защите информации от утечки по каналам связи проводного типа и определению круга наиболее дефицитных ТС, систем, методик и норм в области ТЗИ, а также определение возможных путей их создания и использования в ближайшее время.

III К вопросу защиты информации от утечки по телефонным каналам

В связи с развитием и внедрением различных методов передачи данных, в том числе цифровых и криптозащищенных, совершенствованием научно-технических принципов построения нового поколения ТС и систем связи [1] и модернизации оборудования специальных систем военной связи, становится актуальной задача защиты указанных систем от возможной утечки информации как за счет побочных электромагнитных излучений и наводок (ПЭМИН), так и за счет перехвата сообщений, передаваемых по проводным линиям связи. Для радиоканальных устройств связи вопрос защиты информации решается только путем шифрования информации методами криптографии. Для проводных каналов связи скремблирование не является единственным путем “закрытия” конфиденциальной информации. Не менее остро стоит вопрос о защите проводных линий от несанкционированного доступа к ним с целью перехвата передаваемых сообщений. Речевые сообщения, передаваемые по телефонным каналам тональной частоты, наименее защищены от перехвата несанкционированным пользователем.

Кратко рассмотрим наиболее известные способы защиты, устройства и системы защиты оконечных устройств и линий аналоговой телефонной связи. При защите используют активные способы, пассивные способы, средства контроля несанкционированного подключения к линии. Все эти способы в конечном счете направлены на компенсацию тех или иных недостатков оконечных устройств телефонной связи, присущих практически всем телефонным аппаратам (ТА), позволяющим специалистам по промышленному шпионажу применить “беззаходовые” методы информационного перехвата. К недостаткам ТА относятся: наличие в аппаратах с электронным номеронабирателем “естественного” канала утечки информации в виде паразитного высокочастотного излучения в широкой полосе частот с модуляцией звуковым сигналом; конструктивные особенности ТА, приводящие к воздействию звукового сигнала на элементы конструкции и электронные элементы (прежде всего звонково-вызывные цепи и выходные коммутаторы ТА) и за счет акустоэлектрических преобразований, вызывающих появление информативных сигналов в линии связи; отсутствие мер защиты от методов энергетической накачки в виде “высокочастотного навязывания”, при котором проникающий в ТА сигнал несущей частоты формируется принудительно извне и может модулироваться информативным звуковым сигналом при положенной трубке, в результате чего появляется дополнительный канал утечки информации и в линии, и в радиоэфире.

Одним из средств защиты информации от утечки абонентскими телефонными линиями вследствие акустоэлектрических преобразований в ТА являются устройства защиты телефонных линий (УЗТЛ) “Рикас-1” и “Рикас-2” (ГНПП “Рикас”, г. Киев, ТУ У 16400411.001-95 и ТУ У 16400411.002-95) [2]. Устройства обеспечивают указанную защиту в режиме “ожидания вызова” с величиной подавления не менее 65 дБ. Прибор “Рикас-3” позволяет осуществить подавление сигналов утечки на уровне не менее 120 дБ по двум линиям. Устройство “Рикас-8Т” осуществляет тот же вид защиты и подавление сигналов ВЧ-навязывания и ПЭМИН в диапазоне частот 150-1000 кГц на уровне 80 дБ. Аналогично работает “Рикас-10”, а “Рикас-9” осуществляет зашумление телефонной линии цифровых АТС 28 и 48В. Приборы “Рикас-4” и “Рикас-16” являются средствами защиты телефонных линий от несанкционированного подключения и в этом смысле являются средствами контроля несанкционированного подключения. Киевское ОАО “Укрспецтехника” предлагает также весьма перспективную серию приборов “Базальт” для защиты от утечки информации различным каналами. В частности, для закрытия канала утечки речевой информации в телефонной линии применяется устройство“Базальт-3”, предназначенное для защиты посредством фильтрации и нелинейной коммутации возможных акустоэлектрических преобразований, которое дополнительно формирует в линии сигнал псевдослучайной помехи с эффективным напряжением на уровне 0,1 В в диапазоне частот 0.15-5.0 кГц. Такие устройства, как “Барьер-3”, предлагаемый Киевским ООО “Квирин”, устройства “Щит”, SEL SP17/D, предлагаемые Запорожским ООО “Защита LUX”, московское устройство контроля телефонных линий КТЛ-400 и устройство комплексной защиты телефонных переговоров “ПРОКРУСТ-2000” обеспечивают те или иные защитные функции в различных комбинациях или раздельно, но по сути не привносят ничего нового в уже описанные возможности устройств защиты.

Этот перечень является небольшой частью приборного парка с аналогичными функциями, предлагаемого

на украинском рынке. Если учесть огромное разнообразие совершенно аналогичных по функциональным возможностям так называемых "устройств защиты телефонных линий", не имеющих утвержденных ТУ, сертификатов или экспертных заключений на соответствие требованиям ТЗИ, т. е. любительских поделок по необычайно низким ценам, а также импортных аппаратов, совершенно не адаптированных к нашим телефонным сетям даже на предмет согласования с импедансом телефонных линий, то невольно возникает вопрос: не является ли такое разнообразие результатом главенства торгово-коммерческих интересов производителей и торгующих организаций в ущерб реальному качеству или даже функциональному соответствию имеющихся приборов. При этом и профессиональные разработчики, и производители могут оказаться в условиях, при которых их экономические интересы вынуждают их остановиться в своем развитии в направлении совершенствования ТС. В частности, данные ТС обладают недостатками, присущими всем измерительным, поисковым и другим комплексам и отдельным функциональным приборам ТЗИ. Рассмотрим некоторые из них. Как известно, метрологическая аттестация измерительных приборов и систем, а также характеристики аппаратуры ТЗИ, такие, как величина подавления проникающих опасных сигналов различными фильтрующими устройствами и др. определяются относительно тестирующих сигналов синусоидальной формы с измеренной амплитудой. В то же время при зондировании реальными импульсными сигналами, например при атаке на ТА по телефонной линии, необходимо учитывать распределение спектральной плотности в полосе частот, определяемой Фурье разложением формы зондирующего импульса, а не амплитудой посылки. То есть необходимо оценивать качество работы аппаратуры ТЗИ с учетом возможности атаки шумоподобными сигналами при использовании вероятным противником активных методов информационной атаки.

Определенные трудности возникают при формировании, сопровождении и управлении комплексной системы защиты информации. Динамичное изменение технологий систем связи, используемых в этой сфере основных технических средств определяет как одно из важнейших концептуальных требований к системе защиты ее адаптируемость, т. е. целенаправленное приспособление к изменяющимся условиям среды, в которой функционируют системы защиты. На практике это означает возможность обеспечения текущей модернизации компонентов системы защиты, в частности, замену либо наращивание комплекса соответствующих ТС. К сожалению, в реальной ситуации имеет место плохая совместимость элементов и ТС систем зашиты, поставляемых от различных производителей, из-за существенных различий в требованиях к проектированию и технологиям изготовления ТС. Это существенно осложняет организацию и проведение проверок правильности функционирования системы защиты информации в целом, а также приводит к тому, что аппаратно-программное обеспечение определенных технологий защиты оказывается привязанным к конкретной организации-производителю, что иногда влечет неоправданно высокие экономические затраты на сопровождение и развитие систем защиты.

IV Выводы

Для эффективной защиты объектов информационной деятельности (ОИД) и линий связи необходимо использовать только такую приборную базу, которая позволяет обслужить объект защиты комплексно, с наращиванием, при необходимости, функциональных возможностей средств защиты, например за счет блочно-модульного принципа формирования устройства комплексной защиты с согласованными между отдельными приборами характеристиками, полученными на единой методической и нормативной основе. Например, оценку эффективности фильтрации опасных сигналов в телефонных линиях необходимо проводить в диапазоне частот, значительно превышающем звуковой (речевой диапазон), а саму фильтрацию производить только после принятия мер к преобразованию всех форм сигналов к близким к тестирующим при аттестации ТС, например, за счет дросселирования. Однако это требует совершенствования имеющихся методик и пересмотра норм. С учетом отставания нормативной базы, а также методик контроля и измерений реального уровня защищенности ОИД, видимо, можно полагать, что реальные функции защиты ТА и линий телефонной связи имеют только такие ТС, которые разрабатывались в рамках комплексных систем защиты. Причем на выделенном ОИД может существовать комплексное ТС защиты только одного типа, а совмещение на одном объекте устройств разных производителей из разных серийных групп приводит к неоднозначности определения уровня закрытия объекта или отдельного оконечного устройства.

Определенный оптимизм вселяет то, что отечественные производители и разработчики несколько активизировались в создании новых комплексных средств защиты информации, в том числе и в области телефонной связи, и разрабатывают в настоящее время ТС ТЗИ с учетом изменяющихся условий и реальных потребностей пользователей. Примером может служить новая разработка ЧП фирмы "Бумекс" (г. Киев) комплексной системы защиты информации абонентов телефонной сети "Скеля", в настоящее время находящейся на этапе согласования ТУ с целью сертификации. Комплекс состоит из шести функциональных приборов, позволяющих создать гибкую систему защиты с необходимым для каждого конкретного случая

уровнем защищенности ТА и телефонной линии абонентской сети. В состав комплекса входит прибор "Скеля-1", который подключается к абонентским линиям АТС последовательно с оконечным устройством абонента. Количество одновременно контролируемых линий – две. Прибор обеспечивает контроль линий от несанкционированного параллельного подключения любого устройства в режиме "ожидание вызова" с внутренним сопротивлением до 150 кОм и в режиме "разговорный" – не более 5,1 кОм. Прибор имеет функцию контроля линий от обрыва в режиме "ожидание", обеспечивает подачу сигнала шума в обе контролируемые линии с заданным энтропийным коэффициентом качества шума 0,8 и амплитудой не менее 1,5 В в диапазоне частот 0,1-10 кГц, обеспечивает 120 дБ подавления сигналов ВЧ-навязывания в диапазоне частот 0,18-250 кГц. Прибор имеет автоматически включаемое резервное питание и обеспечивает связь с абонентом при отсутствии питания 220 В и выключенном резервном питании (например, при разряде аккумулятора). Прибор работает с концевыми устройствами абонентских линий всех типов (телефоны, факсы, модемы и др.), работающими с аналоговыми сигналами. В комплекс входит отдельный генератор шума "Скеля-2" (с характеристиками, соответствующими генератору шума прибора "Скеля-1"), отдельный прибор для защиты факсов "Скеля-3" (обеспечивает безопасность факса для режима "спикерфон" и исключающий применение кода доступа к факсу), индикатор ВЧ-навязывания "Скеля-4" (определяет наличие опасных сигналов в диапазоне до 50 МГц), определитель емкостной характеристики линии "Скеля-5" и определитель индуктивного несанкционированного подключения к линии "Скеля-6". По мнению авторов разработки – это минимальный набор функций, необходимый для реальной защиты ТА.

*Литература: **1**. В. А. Худяков. "Особенности применения мер технической защиты информации в специальных телекоммуникационных системах". Тез. докл. на "Научно-технической конференции по безопасности информации", г. Киев, КВИУС, 2001. **2**. Перелік засобів забезпечення технічного захисту інформації. Засоби загального призначення. Бизнес и безопасность. № 2, 2001, с. 41.*

УДК 654.1 (045)

ВИКОРИСТАННЯ ПРИНЦИПУ ФІЗИЧНОГО ВІДОКРЕМЛЕННЯ КАНАЛІВ КЕРУВАННЯ В КОРПОРАТИВНИХ IP-МЕРЕЖАХ

Юрій Кочергін
Національний авіаційний університет

Анотація: **З позицій технічного захисту інформації обгрунтована доцільність фізичного відокремлення каналів керування від каналів транспорту даних користувачів при побудові корпоративних комп'ютерних мереж.**
Summary: **From positions of technical protection of the information the expediency of use is proved physical branch of channels of management from channels of transport of the given users at construction of corporate computer networks.**
Ключові слова: **Інформація, система керування, інформаційна безпека.**

I Вступ

Наразі в корпоративних комп'ютерних мережах, що функціонують на основі стеку телекомунікаційних протоколів TCP/IP, технологічна інформація та інформація користувачів, як правило, транспортується одними і тими ж шляхами через спільні канали зв'язку. Іншими словами, маємо ситуацію, коли протокольні блоки даних (Protocol Data Unit – PDU) з даними користувачів і PDU, що містять пакети з керуючою інформацією, циркулюють в спільному фізичному середовищі, несанкціонований доступ до якого в багатьох випадках не є проблемою для зловмисників навіть з невеликими ресурсними можливостями. Зокрема, якщо в підсистемі керування корпоративною мережею для технічного забезпечення експлуатаційних задач використовується найбільш розповсюджена сьогодні схема "агент – менеджер" відповідно до специфікацій протоколу керування SNMP (Simple Network Management Protocol), то PDU з керуючою інформацією за допомогою міжмережного екрану (Firewall) відносно легко можуть бути відфільтровані зловмисником і використані з метою реалізації загроз в підсистемі керування. Тому традиційні методи спільного використання середовищ розповсюдження сигналів для транспорту як інформації користувачів, так і різного роду технологічної інформації не в змозі забезпечити необхідну ступінь захищеності інформаційних ресурсів в більшості корпоративних застосувань.

Основний шлях підвищення захищеності інформації в каналах її транспортування, що практикується сьогодні, – це використання механізмів криптографічного перетворення інформації. Однак застосування