DOI: 10.25586/RNU.V9187.21.02.P.085 УДК 004.414.2:161.1

Э.И. Митряев, П.А. Филатов

АНАЛИЗ ФУНКЦИОНАЛЬНОЙ ВЗАИМОСВЯЗИ ПРИНЦИПОВ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ СЕТЕВЫХ КАНАЛОВ СВЯЗИ И ФИЗИЧЕСКОГО ОСЛАБЛЕНИЯ ИНФОРМАТИВНОГО СИГНАЛА В ТРАКТЕ ЕГО РАСПРОСТРАНЕНИЯ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Рассматривается задача защиты конфиденциальной информации от ее перехвата за счет индуцирования информативного сигнала на цепях электропитания основными техническими средствами связи. В качестве решения рассматриваемой задачи анализируются практически реализуемые методы и средства защиты информации от утечки по каналам ПЭМИН, основанным на уменьшении соотношения сигнал/шум в этих каналах до предела, при котором восстановление информации становится принципиально невозможным.
Ключевые слова: технические каналы утечки информации, защита информации, утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН), технические средства связи, технические средства компьютерных систем в защищенном исполнении.

E.I. Mitryaev, P.A. Filatov

ANALYSIS OF THE FUNCTIONAL INTERCONNECTION OF PRINCIPLES OF TECHNICAL IMPLEMENTATION OF NETWORK CHANNELS OF THE SBI AND THE PHYSICAL WEAKENING OF THE INFORMATIVE SIGNAL IN THE PATH OF ITS DISTRIBUTION WHEN DESIGNING INFORMATION SYSTEMS AND NETWORKS

The article discusses the task of protecting confidential information from its interception due to the induction of an informative signal on the power supply circuits by the main technical means of communication. As a solution of the problem under consideration, practically implemented methods and means of protecting information from leakage through side electromagnetic emissions and pressing channels based on a decrease in the signal-to-noise ratio in these channels to the limit at which information recovery becomes fundamentally impossible.
Keywords: technical channels leakage information, information protection, information leakage due to side electromagnetic emissions and pressing, technical means of communication, technical means of computer systems in a secure execution.

Вводные замечания

В современном мире своего рода популярность имеют средства экономической разведки, которые используются совместно со способами получения конфиденциальной информации лицами, не имеющими на это права.

На сегодняшний день информация рассматривается как ресурс, имеющий цену и значение для бизнеса. Информация рассматривается в современных условиях и как средство управления хозяйственной деятельностью организации.

Информационная безопасность

Митряев Эдуард Иванович
доктор технических наук, профессор, профессор кафедры телекоммуникационных систем и информационной безопасности Института информационных систем и компьютерных технологий Российского нового университета. Сфера научных интересов: проблемы кибербезопасности информационного общества, системный подход к управлению информацией. Автор 63 опубликованных научных работ.
E-mail: alger47@mail.ru

Филатов П.А.
студент Института информационных систем и компьютерных технологий Российского нового университета.

Для обработки и передачи информации в настоящее время широко используются компьютерные средства. В компьютерных системах информация существует в виде электронных процессов, которые являются физическими носителями информационных сообщений.

В силу физического представления информации в компьютерной среде потоками электронных частиц на процессы обработки и передачи информации в компьютерных системах действуют физические законы электромагнитных взаимодействий. В соответствии с законами физики электромагнитные поля неограниченно распространяются в материальном пространстве и, следовательно, информационные сообщения, преобразованные в данные электромагнитные волновые процессы, получают возможность распространяться в пространстве далеко за границы ее источника.

Предотвращение утечки информации

Практически каждая информационная система включает в себя набор элементов, узлов и проводников, набор источников сигналов и, конечно, набор технических каналов утечки конфиденциальной информации.

Таким образом, все технические каналы утечки информации в зависимости от реализации радиоэлектронных элементов и компонентов имеют определенное проявление. Физические процессы, которые происходят в технических средствах в процессе их эксплуатации, создают побочные излучения, которые так или иначе влияют на обрабатываемую пользователем информацию. Они имеют разную природу и рассматриваются как источники непреднамеренной передачи конфиденциальной информации из системы связи.

Говоря об электромагнитных каналах утечки информации, следует отметить, что в современных условиях насыщения техническими и электронными средствами крайне важно понимать опасность утечки через средства обработки информации конфиденциального характера. Кроме того, технические средства относятся к числу наиболее опасных и распространенных каналов утечки информации.

Можно отметить, что созданный к настоящему времени арсенал мер и средств блокирования каналов утечки за счет побочных излучений и наводок характеризуется конкрет-

ностью и полнотой. Их внедрение во многих случаях связано с необоснованно большим уровнем возможностей программно-аппаратных методов и средств встроенных в систему защиты информации и нередко сопрягается со сверхизбыточными экономическими расходами.

Рассмотренные в статье материалы могут быть практически использованы применительно к задаче защиты информации от утечек вследствие наводок во всевозможные протяженные токопроводящие системы. К цепям, имеющим выход за пределы контролируемой зоны, в которые могут проникнуть опасные сигналы через паразитные связи любых видов, относятся, прежде всего, цепи электропитания.

Поэтому предотвращение утечки информации по этим цепям является одной из задач инженерно-технической защиты информации.

Механизмы утечки и защиты информации

Каналы утечки информации вследствие наводок в сеть электропитания технических средств связи (ТСС) образуются за счет паразитных связей (в общем случае разного характера) между информационными цепями рассматриваемых ТСС и электронными цепями силовых кабелей, именно подводящих электричество к ТСС.

Информативные сигналы благодаря паразитным связям попадают в силовые кабели и вслед за этим распространяются по ним дальше по разным составляющим сетей электроснабжения. В силу физических процессов электромагнитной индукции возникающих в силовых кабелях при протекании по ним электронных потоков, информативные сигналы имеют все шансы быть перехваченными злоумышленниками в пространстве за пределами контролируемой зоны с помощью специальных технических средств и систем. По принятым таким образом сигналам можно восстановить переносимую отмеченными сигналами информацию.

Рассмотрим группу каналов утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН), в частности утечки конфиденциальной информации по электрическим сетям.

Дело в том, что все современные системы связи и обработки данных строятся на базе электронных устройств, при работе которых возникает электромагнитное излучение. Часть этого излучения информативна по происхождению. Это излучение распространяется подобно радиосигналу вещательных станций за пределы помещения (здания). Кроме того, в качестве среды распространения могут выступать любые токопроводящие элементы здания (сеть 220 В, линии сигнализации, телефонные линии, трубы отопления и др.). При этом за пределами контролируемой зоны эти сигналы становятся доступными для перехвата с использованием специальной радиоприемной аппаратуры [1].

В основе практически реализуемых методов и средств защиты информации от утечки по каналам ПЭМИН лежит уменьшение соотношения сигнал/шум в этих каналах до предела, при котором восстановление информации становится принципиально невозможным.

Возможными методами решения этой задачи могут быть следующие.

1. Снижение уровня излучений сигналов в аппаратных средствах компьютерной системы (КС).

2. Увеличение мощности помех в соответствующих этим сигналам частотных диапазонах.

Для применения первого метода – снижение уровня излучений сигналов в аппаратных средствах КС – необходим выбор системно-технических и конструкторских решений при создании технических средств КС в защищенном исполнении, а также рациональный выбор места размещения этих средств относительно мест возможного перехвата ПЭМИН (для соблюдения условия максимального затухания информационного сигнала) [4].

Требования к средствам вычислительной техники в защищенном исполнении определяются в специальных ГОСТах.

Реализация второго метода – увеличение мощности помех в соответствующих этим сигналам частотных диапазонах – возможна путем применения активных средств защиты в виде генераторов сигналоподобных помех или шума [3].

Перспективные методы и средства защиты информации

Отметим перспективные методы и средства защиты информации в КС от утечки по каналам ПЭМИН:

- выбор элементной базы технических средств КС с возможно более малым уровнем информационных сигналов;
- замена в информационных каналах КС электрических цепей волоконно-оптическими линиями;
- локальное экранирование узлов технических средств, являющихся первичными источниками информационных сигналов;
- включение в состав информационных каналов КС устройств предварительного шифрования обрабатываемой информации.

Основными принципами, на которых строится использование наиболее распространенных мер защиты информации от утечки за счет наводок в сеть электропитания ТСС информатизации, являются:

- физическое устранение отдельных трактов распространения информативных сигналов;
- маскирование информативного сигнала специально создаваемым шумовым сигналом;
- ослабление информативного сигнала в тракте его распространения.

Меры защиты, основанные на первом принципе, реализуются путем ликвидации потребителей электроэнергии, находящихся за границей контролируемой зоны, снабжающихся от той же трансформаторной подстанции, от которой получают энергию защищаемые технические средства связи (ТСС) информатизации, и др. [2].

Обоснованием второй части являются результаты анализа частотных характеристик затухания и других параметров участков и элементов трактов распространения информативных сигналов по сетям электропитания ТСС информатизации [3].

Меры защиты, в основу которых положен третий принцип, следующие.

1. При проведении работ по защите информации от утечки за счет наводок в сети электропитания ТСС информационных объектов необходимо иметь в виду, что с расширением диапазона частот информативных сигналов возможности по перехвату этих сигналов в целом снижаются из-за увеличения затухания трактов их распространения.

Увеличение ослабления информативных сигналов, источником которых являются ТСС информатизации, наведенных в сети их электропитания, может достигаться увеличением собственных затуханий отдельных элементов таких трактов и рассогласованием волновых сопротивлений этих элементов в диапазонах частот наведенных информативных сигналов (при сохранении их согласования на частоте 50 Гц).

2. В целях увеличения ослабления уровней информативных сигналов в сетях электропитания ТСС и информатизации рекомендуется применять двухмашинные агрегаты (двигатели-генераторы), разделительные трансформаторы, помехоподавляющие фильтры, источники бесперебойного питания [3].

3. Для электроснабжения ТСС и информатизации лучше использовать цепи электроснабжения, элементами которых являются силовые трехфазные трансформаторы как можно меньшей мощности. Также рекомендуется применять двигатели-генераторы или разделительные трансформаторы минимально возможной мощности.

4. Выбирать (в случае наличия альтернативных вариантов) в качестве цепей электропитания ТСС информатизации цепи, имеющие на участке «ТСС информатизация – граница контролируемой зоны» максимально возможное число элементов (силовых кабелей, трансформаторных подстанций и др.). Также следует использовать в составе этих цепей силовые кабели, имеющие максимально возможную длину в пределах контролируемой зоны.

Выводы

Таким образом, возможности перехвата информативных сигналов и восстановление по ним информации, переносчиком которой они являются, во многом зависят от величины этих сигналов в каналах связи и точке их приема, а также от уровней и маскирующих свойств шумов, на фоне которых он осуществляется.

В связи с этим параметры трактов, характеризующие степень ослабления информативных сигналов, играют первостепенную роль при проведении работ по защите информации от утечки по техническим каналам.

Таким образом, следует со всей ответственностью относиться к такому серьезному вопросу, как обеспечение защиты информации, из-за разглашения и попадания которой к конкурентам ущерб для организации может быть очень значительным.

Учет функциональной взаимосвязи принципов физического устранения отдельных трактов распространения информативных сигналов и принципов ослабления информативного сигнала в тракте его распространения при технической реализации проектов информационных систем и сетей должен повысить эффективность их защиты от несанкционированного доступа, нарушения целостности и структурированности данных.

Литература

1. *Бузов Г.А.* Защита информации ограниченного доступа от утечки по техническим каналам. М.: Горячая линия – Телеком, 2016. 678 с.
2. *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. 615 с.
3. *Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В.* Информационная безопасность открытых систем. В 2 т. Т. 1. Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая линия – Телеком, 2006. 536 с.
4. *Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г.* Защита информации в телекоммуникационных системах. М.: МК-Пресс, 2015. 288 с.

References

1. Buzov G.A. (2016) *Zashchita informatsii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam* [Protection of Restricted Information From Leakage Through Technical Channels]. Moscow, Publishing House Hot Line – Telecom. 678 p. (in Russian).
2. Galitskij A.V., Ryabko S.D., Shan'gin V.F. (2016) *Zashchita informatsii v seti – analiz tekhnologij i sintez reshenij* [Protection of Information in the Network – Analysis of Technologies and Synthesis of Solutions]. Moscow, DMK Press Publishing. 615 p. (in Russian).
3. Zapechnikov S.V., Miloslavskaya N.G., Tolstoj A.I., Ushakov D.V. (2006) *Informatsionnaya bezopasnost' otkrytykh sistem. V 2 t. T. 1. Ugrozy, uyazvimosti, ataki i podkhody k zashchite* [Information Security of Open Systems. In 2 Vols. Vol. 1. Threats, Vulnerabilities, Attacks and Approaches to Defense]. Moscow, Publishing House Hot Line – Telecom. 536 p. (in Russian).
4. Konakhovich G.F., Klimchuk V.P., Pauk S.M., Potapov V.G. (2015) *Zashchita informatsii v telekommunikatsionnykh sistemakh* [Information Protection in Telecommunication Systems]. Moscow, MK-Press Publishing. 288 p. (in Russian).