УДК 681.3.06

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

В.К. Железняк, О.В. Чурко, О.Ю. Кондрахин
УО «Полоцкий государственный университет», Новополоцк, Беларусь

Научно-технический прогресс в современных условиях основывается на использовании большого объема информации, накопленной в обществе за предыдущий период, а также добываемой последними исследованиями и изысканиями. Стратегия перехода на более высокие ступени развития немыслима без получения и использования больших массивов информации.

Таким образом, характеристика современного состояния зашиты информации информационных систем определяется достижением научно-технического прогресса, позволяющего характеризовать развитие общества как науко- и информационноемкое.

Процессы и явления, связанные с генерацией, передачей информации, обусловливают побочные явления: поля рассеивания различной физической природы, их взаимное преобразование и вторичное рассеивание. Физические процессы и явления в сложном информационном пространстве обусловливают взаимодействие переносчиков сигналов и информационных полей, вследствие чего информация излучается в преобразованной форме.

Актуальным является обнаружение ведущихся научных разработок о новых технических системах, технологиях, применяемых в лабораториях или на стадии испытания систем до того, как они найдут применение на практике. Полученная информация на ранних стадиях позволяет принять меры для опережения таких разработок или снижения эффекта от применения их результатов.

Разведывательные программы предусматривают выявление на самых ранних стадиях концептуального проектирования новых технологических, тактических параметров проектируемых систем с помощью разноплановых технических средств разведки.

Приближение технических средств разведки к разведывательным объектам и наращивание технических возможностей для ведения непрерывного наблюдения позволяет наилучшим образом обеспечивать высокую верность извлечения информации при тех же предельных возможностях технических средств разведки.

Защита информации от утечки по техническим каналам в условиях быстро меняющейся разведобстановки и бурного роста технических и организационных возможностей перехвата информации обусловила необходимость повышения требований к показателям качества защиты информа-

ции, поиску, обнаружению, сбору, обработке и представлению количественных и качественных сведений в реальном масштабе времени.

Защита информации как составная часть безопасности информации является многогранной. Она затрагивает аспекты вещественных, энергетических, информационных систем, их взаимодействие с внешней средой либо в виде физических полей различной природы, либо с помощью преобразования энергии, вещества, информации.

Управление защитой информации базируется на сформулированной научной основе научно-методических требований (НМТ) [2]. Научно-методические требования учитывают важнейшие аспекты, основным из которых является возможность исключения каналов утечки информации (КУИ). Элементы НМТ – это нормативные параметры, их предельное значение, дифференциация по видам сигналов, а также методики оценки параметров в условия фоновых (нормированных) помех.

Из многообразия систем различной физической природы выделим класс систем обработки семантической информации, включающий:

– первичную речевую информацию;

– речевую информацию, преобразованную в цифровую форму или аналоговую форму;

– речевой сигнал, прошедший через аппаратуру магнитной записи-воспроизведения, радиоканал;

– видеоинформацию, преобразованную в видеосигнал либо в телевизионный сигнал;

– сигналы передачи данных ЭВМ (знаковая информация).

Меры по защите информации (ЗИ) основаны:

– на локализации излучения полей рассеивания сигналов с целью ослабления взаимодействия с системами их обнаружения и перехвата;

– на разрушении КУИ с обеспечением скрытности функционирования информационных систем;

– на формировании информационных параметров сигналов маскирующими помехами, максимально затрудняющих перехват и обработку информации;

– на оценке обстановки и условий использования информационной системы и ее взаимодействия с другими системами;

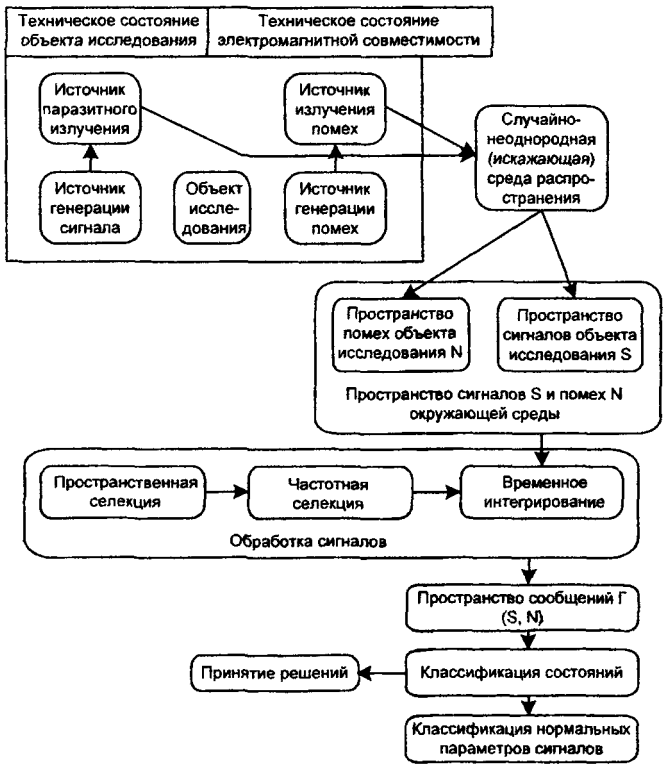
– на оценке ограничивающих факторов, существенных связей между источником информации и средством обнаружения и перехвата;

– на оценке, контроле параметров, определяющих степень ЗИ (аппаратурными, программными методами).

Защите информации предшествует аналитическое и инструментальное выявление каналов утечки информации.

Каналы утечки акустической информации

Важным средством извлечения информации является акустическая разведка (АР), представленная на рисунке в виде функциональной схемы акустической информационной системы.



Функциональная схема акустической информационно системы

Акустическая разведка включает комплекс мероприятий, методов и специальных технических средств, обеспечивающих извлечение данных (развединформации) посредством перехвата (приема, переизлучения и приема) возбужденных объектом АР упругих волн в газовой (воздушной), жидкой и твердой средах. Акустическая разведка извлекает и анализирует акустические речевые сигналы (первичные), акустические широкополосные, акустические структурные (кодовые), акустические тональные (узкополосные) сигналы.

Акустические речевые сигналы (АРС) генерируются органами человека, воспринимаются его органами чувств, а также воспроизводящей и регистрирующей технической системой, относятся к биологическим сигналам и являются первичными. В речевых сигналах заключена содержательная и структурная информация (лингвистическая или синтаксическая). Согласно первому подходу производятся измерения характеристик (существенных), свойств (признаков), формируемых в вектор признаков. При структурном подходе сигнал описывается как композиция своих составляющих.

Учитывая специфику распространения акустических колебаний, представим *классификацию каналов утечки*:

– воздушный (разделяется на атмосферный и искусственный газовый; среда обитания водолазов, космонавтов, в которой изменяется спектральная плотность речевого сигнала и предельная бинауральная чувствительность уха в зависимости от изменения давления);

– вибрационный (структурный), обусловленный распространением механических колебаний в твердой среде (работа телеграфных, буквопечатающих аппаратов);

– виброакустический, обусловленный преобразованием речевого сигнала в механические колебания твердой среды и механических – в акустические колебания обратным преобразованием;

– микросейсмический, обусловленный преобразованием акустических речевых колебаний воздушной среды в микроколебания земной поверхности;

– электроакустический, обусловленный прямым преобразованием акустических речевых колебаний воздушной среды в электрические сигналы (микрофонный эффект) и обратным преобразованием;

– опто-электронно-акустический, обусловленный процессом когерентного облучения точечным источником монохроматического облучения объекта, модуляцией зеркального или диффузного отражения волны от объекта разведки, модулированной по закону колеблющейся поверхности объекта разведки.

Для речевых сигналов критерием степени защищенности принято считать заданное значение разборчивости. Факторами, необходимыми для анализа защищенности акустических речевых сигналов, следует считать неравномерность спектральной плотности речевого сигнала, предельную биноуральную чувствительность уха, затухание в типовых элементах ограждающих конструкций, спектральная плотность фонового акустического шума, реверберационные помехи, резонансные явления в помещениях (замкнутых пространствах). Оценка защищенности речевого сигнала на одной измерительной частоте по энергетическому критерию (отношение сигнал/шум (ОСШ)) не учитывает ряд факторов, существенно влияющих на разборчивость речи.

Кроме перечисленных, к таким факторам относятся: линейные, нелинейные искажения входного сигнала, точность передачи речевого сигнала через систему звукопередачи, возможность его предыскажений.

Важным фактором, определяющим разборчивость речи, является ограничение полосы речевого сигнала. Воздействие мультипликативных помех в виде паразитных АМ и ЧМ снижает разборчивость. Разработана корреляциооная теория разборчивости речи, учитывающая факторы, влияющие на погрешность оценки разборчивости речи [1, 2, 3].

Задачи контроля каналов утечки информации в реальном масштабе времени

Утечка информации исключается автоматизированным контролем.

Процесс получения информации о состоянии КУИ в темпе ее поступления (в реальном масштабе времени – РМВ) включает:

- формирование сигналов измерительной информации, их разрешение (обнаружение), выделение слабых сигналов из шума за счет различий сигналов измерительной информации и шума, измерение их параметров (характеристик) с минимально допустимыми погрешностями при наличии мешающих сигналов, наводок, шумов;

- оптимальное обнаружение сигнала со случайной фазой с помощью согласованного приемника. Источник информации определяют на основании описания параметров, являющихся исходными в оценке степени защищенности информации. При этом важно обеспечить воспроизводимость результатов измерений, отражающих количественное описание параметров. Выполнение измерений в различных условиях воздействия внешних факторов уменьшает быстродействие. С помощью информационно-измерительной системы (ИИС) осуществляют автоматизированную обработку информации об излучаемом объекте, выдают данные в виде совокупности чисел, отражающих состояние данного объекта;

- анализ данных в РМВ, т.е. процесс преобразования данных, направленный на получение описания этих данных через их свойства или составные части и их отношение с целью извлечения полезной информации в темпе ее поступления;

- обработка данных РМВ, т.е. вычислительный процесс, направленный на извлечение из них информации для ее последующего воспроизведения в темпе поступления. Функциональное назначение определяет структурную организацию ИИС. Общими в структурной организации ИИС являются первичные измерительные преобразователи с устройствами согласования, предварительный анализ и обработка информации с управлением от микропроцессора.

Функции автоматизированной ИИС (АИИС) включают:

– программное управление системой;

– автоматизированный сбор данных от первичных измерительных преобразователей (ПИП);

– автоматизированное управление;

– генерирование измерительных сигналов с заданными параметрами;

– предварительная обработка смеси сигнала с шумом в квазиреальном масштабе времени с целью выделения слабых сигналов;

– автоматизированное отображение генерализуемой информации, ее документирование.

Автоматизированная информационно-измерительная система незаменима при рассредоточении объектов измерения, одновременном измерении многих параметров, длительных измерениях, измерениях по сложной программе; реализована для речевого сигнала.

Селекцию сигналов, получаемых от физических полей различной природы, осуществляет ПИП.

Значение АИИС заключается в том, что впервые она реализована для оценки сигналов, поступающих в смеси с шумом при ОСШ меньше единицы. Представление результатов измерений получается во много раз быстрее по сравнению с неавтоматизированным методом измерения. Чувствительность ПИП, методы обработки позволяют оценить нормированные значения параметров в заданной точке приема.

Выводы

Защиту информации оценивают, контролируют в условиях сложной помеховой обстановки, так как нормируемые параметры меньше уровня непреднамеренных (фоновых) либо маскирующих (организованных) помех. Результаты измерений должны отвечать требованиям помехозащищенности (способность надежного выполнения заданных функций в условиях воздействия непреднамеренных и организованных помех), а также требованиям достоверности (верности) степени соответствия нижнего порогового уровня защищенности, оцениваемого по параметрам сигналов при ОСШ меньше единицы.

ЛИТЕРАТУРА

1. Железняк, В.К. Корреляционная теория разборчивости речи / В.К. Железняк, А.А. Колесников, В.Ф. Комарович // Вопросы радиоэлектроники. – 1995. – С. 3 – 7.
2. Общесистемные вопросы защиты информации: коллект. моногр / под ред. Е.М. Сухова.– М.: Радиотехника, 2003. – Кн. 1. – 296 с. (Сер. Защита информации; ред. Е.М. Сухов).
3. Хореев, А.А. Оценка эффективности методов защиты речевой информации / А.А. Хореев, В.К. Железняк, Ю.К. Макаров // Общесистемные вопросы защиты информации; под ред. Е.М. Сухова. – М.: Радиотехника, 2003. – С. 221 – 231.