ния информационного сигнала от АТС к ЦТ и от ЦТ к АТС, не оказывая влияния на работу ЦТ и АТС.

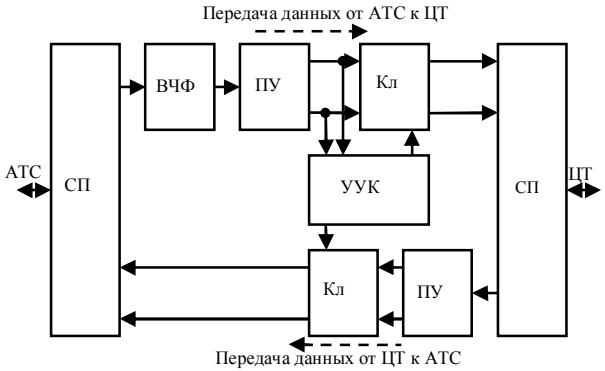

Рис. 1. Структурная схема устройства пассивной технической защиты цифровых телефонных аппаратов

В канал входят ПУ и Кл. ПУ отделяет положительное напряжение от отрицательного (рис. 2 б, в, г). Кл предназначен для переключения каналов и управляется УУК, которое синхронизируется от сигнала АТС.

Если сигнала АТС нет, то открыт канал от АТС к ЦТ, а второй канал закрыт. Это связано с тем, что передачу данных первой начинает АТС, а затем отвечает ЦТ. СП формирует из двух сигналов ПУ (рис. 2 в, г) выходной сигнал с тремя уровнями (рис. 2 д).

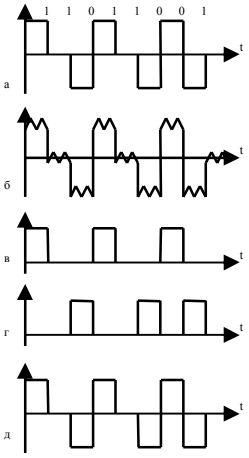

Рис. 2. Цифровой сигнал:
а – без помех (сверху – соответствующий сигналу бинарный код);
б – с помехой (вход ПУ);
в – и *г* – с помехой на выходе ПУ;
д – с помехой на выходе устройства защиты

На рис. 3 представлен внешний вид устройства пассивной технической защиты цифровых телефонных аппаратов.

Рис. 3. Внешний вид устройства пассивной технической защиты цифровых телефонных аппаратов

Опытная партия устройств защиты изготовлена в Гомельском филиале Научно-исследовательского института технической защиты информации и проходит сертификацию. Устройство защиты предназначено для работы с цифровыми телефонами Panasonic (KX-DT321RU и др.) и АТС KX-TDE600, KX-TDA100, 200 и др., в состав которых входит плата для работы с двухпроводными цифровыми телефонами KX-TDA0172. Устройство защиты изготавливается и для работы с цифровыми телефонами Samsung (DS-5021D и др.) и АТС iDCS 500 и др., в состав которых входит модуль расширения для работы с двухпроводными цифровыми телефонами 8DLI, 16DLI.

УДК 004.42

Е.М. Клачкевич, Р.В. Кислинский

СОВРЕМЕННЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Информация сегодня – важный ресурс, потеря которого чревата неприятными последствиями. Утрата конфиденциальных данных компании несет в себе угрозы финансовых потерь, поскольку полученной информацией могут воспользоваться конкуренты или злоумышленники. Для предотвращения столь нежелательных ситуаций все фирмы, учреждения используют методы защиты информации.

Безопасность информационных систем (ИС) как учебную дисциплину изучают программисты и специалисты в области построения ИС. Однако знать виды информационных угроз и технологии защиты должны все, кто работает с секретными данными.

Основным видом информационных угроз, для защиты от которых на каждом предприятии разрабатывается целая технология, является

несанкционированный доступ злоумышленников к данным. Злоумышленники планируют заранее преступные действия, которые могут осуществлять путем прямого доступа к устройствам или путем удаленной атаки с использованием специально разработанных для кражи информации программ.

Кроме действий хакеров, фирмы нередко сталкиваются с ситуациями потери информации по причине нарушения работы программно-технических средств. В данном случае секретные материалы не попадают в руки злоумышленников, однако утрачиваются и не подлежат восстановлению либо восстанавливаются слишком долго. Сбои в компьютерных системах могут возникать по следующим причинам: потеря информации вследствие повреждения носителей – жестких дисков, ошибки в работе программных средств, нарушения в работе аппаратных средств из-за повреждения или износа.

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется семь основных методов (способов) защиты: препятствие, маскировка, механизмы шифрования, регламентация, управление доступом, принуждение, побуждение. Все перечисленные методы нацелены на построение эффективной технологии защиты информации, благодаря которой исключаются потери по причине халатности персонала и успешно отражаются разные виды угроз.

Под препятствием подразумевается способ физической защиты информационных систем, который не позволяет злоумышленникам попасть на охраняемую территорию.

Маскировка как способ защиты информации предусматривает преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Механизмы шифрования – криптографическое закрытие информации. Этот метод защиты все шире применяется как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Управление доступом регулирует использование всех ресурсов ИС и информационных технологий и противостоит несанкционированному доступу к информации на всех возможных путях. Управление доступом включает следующие функции защиты:

идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

разрешение и создание условий работы в пределах установленного регламента;

регистрацию (протоколирование) обращений к защищаемым ресурсам;

реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т. п.) при попытках несанкционированных действий.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение как метод защиты обязывает пользователей и персонал ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений используются следующие средства: физические, программные и аппаратные, организационные, законодательные, психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основными и наиболее старыми средствами физического препятствия являются прочные двери, надежные замки, решетки на окнах. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства защиты используются для охраны данных как на бумажных, так и на электронных носителях.

Программные и аппаратные средства – незаменимый компонент обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства – программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко

выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства защиты – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации. В Республике Беларусь в этом направлении активно ведется работа, результатом которой является Закон Республики Беларусь «Об информации, информатизации и защите информации».

Психологические средства защиты – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

Таким образом, мы можем сделать вывод, что защита информации является актуальной проблемой, особенно для силовых структур, так как попавшая «не в те руки» информация (даже не военного характера) может нести угрозу. Именно по этой причине было разработано много способов и средств защиты информации.

В заключение хотелось бы вспомнить выражение «Кто владеет информацией – владеет миром», так как в последнее десятилетие информация стала одним из самых ценных ресурсов.

УДК 681.3.05

А.Н. Коваленко

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ РАДИОЛУЧЕВЫХ СРЕДСТВ ОБНАРУЖЕНИЯ

Радиолучевыми средствами обнаружения (РЛСО) называют двухпозиционные датчики, в которых передатчик и приемник конструктивно размещены в различных устройствах с целью получения информации о нахождении в электромагнитном поле этих устройств перемещающегося объекта обнаружения.

Физический принцип функционирования радиолучевых средств обнаружения основан на преобразовании в сигнал тревоги изменений параметров электромагнитного поля на входе приемного устройства при появлении нарушителя в зоне обнаружения.

Передающее устройство (ПРД) генерирует электромагнитное поле сверхвысокой частоты и в виде радиоволн излучает его в сторону приемного устройства (ПРМ). Излучение производится в виде радиоимпульсов, имеющих постоянную амплитуду и частоту следования. Таким образом, в пространстве между передающим и приемным устройствами РЛСО создается зона обнаружения. Приемное устройство принимает радиоимпульсы, поступающие от передающего устройства, и осуществляет их обработку. До появления нарушителя в зоне обнаружения амплитуда принимаемых радиоволн практически постоянна. Сигнал тревоги РЛСО не подает.

Когда в зону обнаружения входит нарушитель, то в антенну ПРМ поступают дополнительные, отраженные от нарушителя радиоволны (рис. 1). В приемной антенне отраженные и прямые радиоволны либо складываются, либо вычитаются – все зависит от разности хода прямых и отраженных волн. Если разность хода радиоволн равна нечетному числу полуволн, то результирующая амплитуда радиоимпульса максимально уменьшается. Можно доказать, что в зоне обнаружения существуют области пространства, в которых появление нарушителя приводит к увеличению результирующей амплитуды. С ними соседствуют области, в которых нарушитель уменьшает результативную амплитуду. При идеально проводящей поверхности почвы и при отсутствии предметов на местности эти области имели бы форму чередующихся полуколец, как показано на рис. 1. В реальных условиях эта картина оказывается искаженной, но общая закономерность сохраняется.

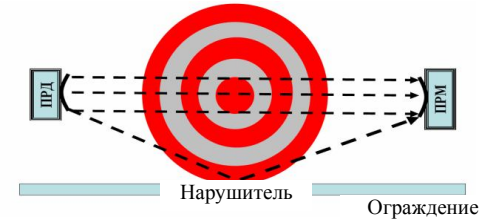

Рис. 1. Ход радиолучей между передающим и приемным устройством

Из приведенных рассуждений очевидно, что на пути нарушителя у границы зоны обнаружения может оказаться любая из указанных областей. Следовательно, амплитуда результирующих радиоимпульсов в приемной антенне с появлением нарушителя в зоне обнаружения может либо увеличиваться, либо уменьшаться. Изменения амплитуды радиоимпульсов в приемной антенне и является первичным электрическим сигналом о входе нарушителя в зону обнаружения.

Опыт эксплуатации радиолучевых средств обнаружения показывает, что для них характерна некоторая неустойчивость работы, которая проявляется в пропуске нарушителя без выдачи сигнала «Тревога» на отдельных участках зоны обнаружения.