В. Барсуков

Интегральная защита информации

Технология XXI века

Сегодня в повседневной жизни мы сталкиваемся с различными видами безопасности: пожарной, охранной, химической, производственной, экологической, финансовой, личной. Однако такое их разделение весьма условно. Например, эффективная защита одного из самых ценных достояний человека — информации — возможна лишь в том случае, если безопасность от всех видов угроз будет гарантирована не только данным, но и устройствам их хранения и обработки, а также лицам, оперирующим этими данными. Вот почему сегодня все более широко используют понятие интегральной информационной безопасности.

Интегральный подход к обеспечению информационной безопасности предполагает в первую очередь выявление возможных угроз, включая каналы утечки информации. Реализация такого подхода требует объединения различных подсистем безопасности в единый комплекс, оснащенный общими техническими средствами, каналами связи, программным обеспечением и базами данных. Поэтому при выявлении технических каналов утечки информации рассматриваются основное оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные системы, оборудование электропитания, схемы заземления и т.п. Наряду с основными необходимо учитывать и вспомогательные технические средства и системы (ВТСС), например устройства открытой телефонной, факсимильной, громкоговорящей связи, радиофикации, часовые механизмы, электробытовые приборы и т.п. Анализ материалов отечественной и зарубежной печати позволил систематизировать возможные каналы утечки и несанкционированного доступа к информации (рис.). Рассмотрим подробнее их особенности (для наглядности цифрами в круглых скобках обозначаются каналы утечки в соответствии со схемой).

В зависимости от способов перехвата информации, физической природы возбуждения сигналов, а также среды их распространения можно выделить технические каналы утечки, каналы перехвата при передаче информации системами связи, утечки акустической и видовой информации, компьютерные методы съема информации. В свою очередь технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

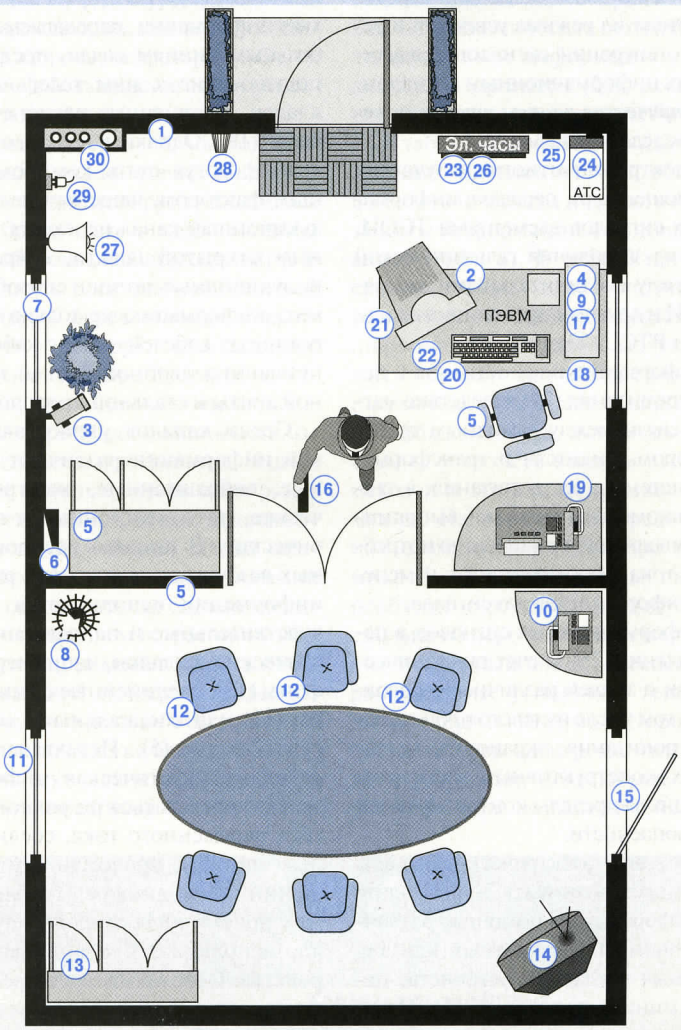

Схема возможных каналов утечки и несанкционированного доступа к информации в типовом одноэтажном офисе:

1) утечка за счет структурного звука в стенах и перекрытиях, 2) съем информации с ленты принтера, плохо стертых дискет и т.п., 3) съем информации с использованием видеозакладок, 4) программноаппаратные закладки в ПК, 5) радиозакладки в стенах и мебели, 6) съем информации по системе вентиляции, 7) лазерный съем акустической информации с окон, 8) производственные и технологические отходы, 9) компьютерные вирусы, логические бомбы и т.п., 10) съем информации за счет наводок и "навязывания", 11) дистанционный съем видеоинформации (оптика), 12) съем акустической информации с использованием диктофонов, 13) хищение носителей информации, 14) высокочастотный канал утечки в бытовой технике, 15) съем информации направленным микрофоном, 16) внутренние каналы утечки информации (через обслуживающий персонал), 17) несанкционированное копирование, 18) утечка за счет побочного излучения терминала, 19) съем информации за счет использования "телефонного уха", 20) съем информации с клавиатуры принтера по акустическому каналу, 21) съем информации с дисплея по электромагнитному каналу, 22) визуальный съем информации с дисплея и принтера, 23) наводки на линии коммуникаций и сторонние проводники, 24) утечка через линии связи, 25) утечка по цепям заземления, 26) утечка по сети электрочасов, 27) утечка по трансляционной сети и громкоговорящей связи, 28) утечка по охранно-пожарной сигнализации, 29) утечка по сети, 30) утечка по сети отопления, газо-и водоснабжения, электропитания

Электромагнитные каналы утечки формируются в результате побочного электромагнитного излучения:

— элементов ТСОИ (18,21), сигнал которых (ток, напряжение, частота и фаза) изменяется так же, как и информационный;

— ВЧ-генераторов ТСОИ и ВТСС (14), которое может непреднамеренно модулироваться электрическим сигналом, наведенным информационным;

— НЧ-усилителей технических средств передачи информации (ТСПИ) (27) в результате случайного преобразования отрицательной обратной связи в паразитную положительную, что может привести к самовозбуждению и переходу усилителя из режима усиления в режим автогенерации сигналов, модулированных информационным сигналом.

Электрические каналы утечки появляются вследствие наводки:

— электромагнитного излучения, возникающего при передаче информационных сигналов элементами ТСОИ, а также из-за наличия гальванической связи между соединительными линиями ТСОИ и другими проводниками или линиями ВТСС (23);

— информационных сигналов в цепи электропитания (29) вследствие магнитной связи между выходным трансформатором усилителя и трансформатором системы электропитания, а также неравномерной нагрузки выпрямителя, приводящей к изменению потребляемого тока в соответствии с изменениями информационного сигнала;

— информационных сигналов в цепи заземления (25) за счет гальванической связи с землей различных проводников (в том числе нулевого провода сети электропитания, экранов) и металлических конструктивных элементов, выходящих за пределы контролируемой зоны безопасности.

Кроме того, электрические каналы утечки могут возникать в результате съема информации с помощью различных автономных аппаратных или так называемых закладных устройств, например мини-передатчиков (5). Излучение этих устройств, устанавливаемых в ТСОИ, модулируется информационным сигналом и принимается специальными устройствами за пределами контролируемой зоны.

Возможно применение специального "ВЧ-облучения", электромагнитное поле которого взаимодействует с элементами ТСОИ и модулируется информационным сигналом. Это ***параметрический канал утечки***.

Особый интерес представляет ***перехват информации при передаче по каналам связи*** (24), поскольку в этом случае возможен свободный несанкционированный доступ к передаваемой информации. В зависимости от системы связи каналы перехвата информации можно разделить на ***электромагнитные, электрические и индукционные***. Каналы утечки первого типа образуются при перехвате сигналов передатчиков систем связи стандартными техническими средствами, широко используемыми для прослушивания телефонных разговоров по разнообразным радиоканалам (сотовым, радиорелейным, спутниковым) (24). Во втором случае перехват информации, передаваемой по кабельным линиям связи, предполагает подключение к ним телефонных закладок, оснащенных радиопередатчиками (19). Однако из-за того, что закладки могут стать компрометирующим фактором, чаще используют индукционный канал перехвата. По данным открытой печати, современные индукционные датчики способны снимать информацию не только с изолированных кабелей, но и с кабелей, защищенных двойной броней из стальной ленты и стальной проволоки.

Среди каналов утечки акустической информации различают воздушные, вибрационные, электроакустические, оптоэлектронные и параметрические. В широко распространенных ***воздушных каналах*** для перехвата информации используются высокочувствительные и направленные акустические закладки, например микрофоны (15), соединенные с диктофонами (12) или специальными мини-передатчиками (5). Перехваченная закладками акустическая информация может передаваться по радиоканалам, сети переменного тока, соединительным линиям, проложенным в помещении проводникам, трубам и т.п. Для приема информации, как правило, используются специальные устройства. Особый интерес представляют закладные устройства, устанавливаемые либо непосредственно в корпус телефонного аппарата, либо подключаемые к линии в телефонной розетке. Подобные приборы, в конструкцию которых входят микрофон и блок коммутации, часто называют "телефонным ухом" (19). При поступлении в линию кодированного сигнала вызова или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает к линии микрофон и обеспечивает передачу информации (обычно речевой) на неограниченное расстояние.

В вибрационных (или структурных) каналах среда распространения информации — конструктивные элементы зданий (стены, потолки, полы и др.), а также трубы водо- и теплоснабжения, канализации (1, 30). Для перехвата акустических сигналов в данном случае обычно применяют контактные, электронные (с усилителем) и радиостетоскопы.

Электроакустические каналы формируются в результате преобразования акустических сигналов в электрические путем "высокочастотного навязывания" или перехвата с помощью ВТСС. Канал утечки первого типа возникает в результате несанкционированного ввода сигнала ВЧ-генератора в линии, функционально связанные с элементами ВТСС, и модуляции его информационным сигналом. В этом случае для перехвата разговоров, ведущихся в помещении, чаще всего используют телефонный аппарат с выходом за пределы контролируемой зоны (10). Кроме того, некоторые ВТСС, например датчики систем противопожарной сигнализации (28), громкоговорители ретрансляционной сети (27) и т.п., могут и сами содержать электроакустические преобразователи. Перехватить акустические сигналы очень просто: подключив такие средства к соединительной линии телефонного аппарата с электромеханическим звонком, можно при не снятой с рычага трубке прослушивать разговоры, ведущиеся в помещении (так называемый "микрофонный эффект").

Облучая лазерным пучком вибрирующие в акустическом поле тонкие отражающие поверхности (стекла окон, зеркала, картины и т.п.), можно сформировать ***оптоэлектронный (лазерный) канал утечки*** акустической информации (7). Отраженное лазерное излучение, модулированное акустическим сигналом по амплитуде и фазе, демодулируется приемником, который и выделяет речевую информацию. Средства перехвата — локационные системы, работающие, как правило, в ИК-диапазоне и известные как "лазерные микрофоны". Дальность их действия — несколько сотен метров.

При воздействии акустического поля на элементы ВЧ-генераторов и изменении взаимного расположения элементов систем, проводов, дросселей и т.п. передаваемый сигнал модулируется информационным. В результате формируется ***параметрический канал утечки акустической инфор-***

мации. Модулированные ВЧ-сигналы перехватываются соответствующими средствами (14). Параметрический канал утечки создается и путем "ВЧ-облучения" помещения, где установлены полуактивные закладные устройства, параметры которых (добротность, частота и т.п.) изменяются в соответствии с изменениями акустического (речевого) сигнала.

По каналам утечки акустической информации могут перехватываться не только речевые сигналы. Известны случаи статистической обработки акустической информации принтера или клавиатуры с целью перехвата компьютерных текстовых данных (20). Такой способ позволяет снимать информацию и по системе централизованной вентиляции (6).

В последнее время большое внимание уделяется ***каналам утечки видовой информации***, по которым получают изображения объектов или копий документов. Для этих целей используют оптические приборы (бинокли, подзорные трубы, телескопы, монокуляры) (11), телекамеры, приборы ночного видения, тепловизоры и т.п. Для снятия копий документов применяют электронные и специальные закамуфлированные фотоаппараты, а для дистанционного съема видовой информации — видеозакладки (3). Наиболее распространены такие методы и средства защиты от утечки видовой информации, как ограничение доступа, техническая (системы фильтрации, шумоподавления) и криптографическая защита, снижение уровня паразитных излучений технических средств, охрана и оснащение средствами тревожной сигнализации.

Весьма динамично сейчас развиваются ***компьютерные методы съема информации***. Хотя здесь также применяются разнообразные закладные устройства, несанкционированный доступ, как правило, получают с помощью специальных программных средств (компьютерных вирусов, логических бомб, "троянских коней", программных закладок и т.п.) (9). Особенно много неприятностей в последнее время доставляют компьютерные вирусы, которых сегодня известно свыше трех тысяч. Поэтому весьма актуальна информация о возможных последствиях их вторжения и методах защиты. К счастью, большую группу реальных вирусов составляют "безобидные", не нарушающие режим работы компьютера. Как правило, их авторы — школьники старших классов, студенты и те, кто стремится повысить свою квалификацию в области программирования. Среди вирусов, нарушающих режим функционирования компьютера, есть неопасные (не повреждающие файловую структуру), опасные (повреждающие эту структуру) и очень опасные (повреждающие аппаратуру и влияющие на здоровье оператора) (табл. 1). Эти вирусы в большенстве своем конструируются профессионалами.

Как видно из табл. 1, наибольший вред с точки зрения утечки информации наносят криптовирусы, способные пробить брешь даже в таком мощном средстве обороны, как криптозащита. В момент ввода электронной подписи криптовирусы перехватывают секретные ключи и копируют их в заданное место. Более того, при проверке электронной подписи они могут вызвать команду подтверждения подлинности заведомо неправильной подписи. И даже при вводе в систему лишь один раз, в момент генерации ключей, криптовирус приводит к созданию слабых ключей. Например, при формировании ключа на основе датчика случайных чисел с использованием встроенного таймера криптовирус может вызвать изменение показаний таймера с последующим возвратом в исходное состояние. В результате ключи легко вскрыть. Сегодня практически единственная защита от таких криптовирусов — загрузка информации с чистой дискеты и использование "чистого" (фирменного) программного продукта.

Все рассмотренные выше каналы утечки информации по сути являются внешними по отношению к источнику. Однако нельзя забывать и о так называемых внутренних каналах, которым обычно не придается должного значения, что нередко приводит к потере информации. Такие каналы утечки (16), как правило, связаны с администрацией и обслуживающим персоналом. В первую очередь это хищение носителей информации (13), съем информации с ленты принтера и плохо стертых дискет (2), с производственных и технологических отходов (8), визуальный съем информации с экрана дисплея и принтера (22), несанкционированное копирование (17).

В табл. 2 на основе анализа рассмотренных каналов утечки обобщены возможные методы и средства съема и защиты информации в типовых ситуациях (табл. 2). В табл. 3 приведены сравнительные характеристики современных электронных средств съема информации, которые могут послужить основой при выборе оптимальных методов и средств ее защиты.

Эффективность активных и пассивных устройств защиты зависит от методов и средств получения информации. Например, для предотвращения съема информации при помощи микрофона с автономным питанием необходимо осуществить одну или несколько из перечисленных мер: провести визуальный поиск, обеспечить экранирование, установить генераторы шума и радиопомех, селекторы сигналов, детекторы электромагнитного поля и излучения, нелинейные локаторы, устройства воздействия на микро-

Таблица 1

Классификация компьютерных вирусов, потенциально опасных с точки зрения несанкционированного доступа к информации

Класс вируса	Вид	Характер воздействия
Не повреждающие файловую структуру	Размножающиеся в ОЗУ	Имитация неисправности процессора, памяти, НМД, НГМД, принтера, портов RS-232, дисплея, клавиатуры
	Раздражающие оператора	Формирование на терминале текстовых и графических сообщений
		Синтез речи, формирование мелодии и звуковых спецэффектов
	Сетевые	Переключение режимов настройки клавиатуры, дисплея, принтера, портов RS-232
Повреждающие файловую структуру	Повреждающие пользовательские программы и данные	Разрушение исходных текстов программ, выполняемых программ, библиотек компиляторов, искажение баз данных, текстовых документов, графических изображений и электронных таблиц
	Разрушающие системную информацию (в том числе криптовирусы)	Разрушение логической системы диска, искажение структуры заполнения носителя, форматирование носителей, повреждение файлов ОС
Действующие на аппаратуру и оператора	Выводящие из строя аппаратуру	Выжигание люминофора, повреждение микросхем, магнитных дисков, принтера
	Действующие на оператора	Воздействие на психику и т.п.

Таблица 2

Основные методы и средства получения и защиты информации

Типовая ситуация	Канал утечки информации	Методы и средства получения информации	Методы и средства защиты
Разговор в помещении и на улице	Акустический	Подслушивание: диктофон, микрофон, полуактивная система	Шумовые генераторы, поиск закладных устройств, защитные фильтры, ограничение доступа
	Виброакустический	Стетоскоп, вибродатчик	
	Гидроакустический	Гидроакустический датчик	
	Акустоэлектронный	Специальные радиоприемники	
Разговор по телефону	Акустический	Подслушивание (диктофон, микрофон полуактивная система)	Те же
проводному	Сигнал в линии	Параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка	Маскирование, скремблирование, шифрование, спецтехника
	Наводки	Специальные радиотехнические устройства	Спецтехника
радиотелефону	ВЧ-сигнал	Радиоприемники	Маскирование, скремблирование, шифрование, спецтехника
Документ на бумажном носителе	Непосредственно документ	Кража, прочтение, копирование, фотографирование	Ограничение доступа, спецтехника
изготовление	Продавливание ленты или бумаги	Кража, прочтение	Огртехмероприятия
	Акустический шум принтера	Аппаратура акустического контроля	Устройства шумоподавления
	Паразитные сигналы, наводки	Специальные радиотехнические устройства	Экранирование
почтовое отправление	Непосредственно документ	Кража, прочтение	Специальные методы
Документ на небумажном носителе	Носитель	Хищение, копирование, считывание	Контроль доступа, физическая защита, криптозащита
изготовление	Изображение на дисплее	Визуальный, копирование, фотографирование	Контроль доступа, криптозащита, поиск закладок, экранирование
	Паразитные сигналы, наводки	Специальные радиотехнические устройства	
	Электрический сигнал	Аппаратные закладки	
	Программный продукт	Программные закладки	
передача документа по каналам связи	Электрические и оптические сигналы	Несанкционированное подключение, имитация зарегистрированного пользователя	Криптозащита
Производственный процесс	Отходы, излучение и т.п.	Спецаппаратура различного назначения	Оргтехмероприятия, физическая защита
Работа с удаленными базами данных	Сигналы, наводки	Программные и аппаратные закладки, несанкционированный доступ, компьютерные вирусы	Криптозащита, специальное программное обеспечение, оргтехмероприятия, антивирусная защита

Таблица 3

Характеристики современных электронных средств съема информации

Устройство перехвата информации	Место установки	Дальность действия, м	Стоимость	Вероятность применения
Контроль акустической информации				
Радиомикрофон с передачей по телефону	Телефонный аппарат, розетка	200—500	Низкая	Высокая
Радиомикрофон с передачей по сети питания	Устройства с сетевым питанием, розетки, удлинители	До силового трансформатора	Низкая	Высокая
Автономный радиомикрофон однократного действия	Любое место в помещении	50—200	Средняя	Высокая
Встроенный радиомикрофон	Калькулятор, телефон, приемник, телевизор, ПК	200—1000	Средняя	Высокая
Радиомикрофон длительного действия с аналоговой модуляцией и дистанционным управлением	Строительные конструкции, элементы интерьера	200—1000	Выше средней	Высокая
Радиомикрофон с цифровой передачей и кодированием	Строительные конструкции, элементы интерьера	200—1000	Высокая	Средняя
Радиомикрофон с цифровой передачей и кодированием и записью и сбросом информации в случае необходимости	Строительные конструкции, элементы интерьера	200—1000	Очень высокая	Низкая
Видеоконтроль помещений				
Миниатюрная камера с передачей изображения по сети питания	Различные электрические приборы	10—30	Высокая	Низкая
Миниатюрная камера с передачей изображения по радиоканалу	Предметы интерьера	50—200	Высокая	Средняя
Контроль информации на мониторе ПК				
Передатчик с модуляцией видеосигналом монитора	Монитор ПК	50—200	Высокая	Средняя
Контроль информации внутренней шины ПК или сетевого сервера				
Передатчик с модуляцией информацией, передаваемой по шине	Материнская плата ПК или сервера	50—200	Очень высокая	Низкая
Контроль информации сетевой магистрали				
Передатчик с датчиком на кабеле магистрали	Кабель магистрали или сервер	50—200	Очень высокая	Средняя

Примечание. Качество перехвата всех электронных средств, за исключением миниатюрной камеры с передачей изображения по сети питания, хорошее. Труднее всего обнаружить радиомагнитофоны с цифровой передачей и кодированием, особенно устройства с записью и сбросом информации в случае необходимости.

Таблица 4

Соотношение методов и средств защиты и добывания информации

Методы и средства добывания: / защиты:	Спец. режимы работы	Детекторы металла	Поиск визуальный	Экранирование помещений	Экранир. кабелей, техники	Генераторы шума	Виброгенераторы	Генераторы радиопомех	Воздействие на микрофон	Детекторы поля	Селекторы сигналов	Локаторы	Стирание записи	Детекторы излучения	Контроль параметров ТЛ	Тестирование ТЛ	Нарушение режима ТСДИ	Уничтожение ТСДИ	Прослушивание ТЛ	Фильтрация сигналов	Техническое закрытие	Криптозащита	Антивирусы
Радиомикрофон (автономное питание)			◆	◆		◆		◆	◆	◆	◆	◆		◆									
Радиомикрофон (питание от телефона)			◆	◆		◆		◆	◆	◆	◆	◆		◆	◆	◆	◆	◆					
Радиомикрофон (питание от сети)			◆	◆		◆		◆	◆	◆	◆	◆		◆									
Микрофон (передача от электросети)			◆			◆			◆			◆											
Направленный микрофон	◆		◆			◆																	
Радиостетоскоп						◆	◆	◆	◆	◆	◆	◆											
Специальный эндоскоп	◆		◆																				
Лазерные средства	◆					◆	◆																
Миниатюрные магнитофоны	◆	◆				◆			◆			◆	◆	◆									
Проводные линии объекта						◆													◆	◆			
Микрофон с передачей по телефонной линии			◆			◆		◆				◆			◆	◆	◆	◆	◆	◆			
Контроль телефонной линии															◆	◆	◆	◆			◆	◆	
Контроль телекса и факса															◆	◆	◆	◆			◆	◆	
Бесконтактный контроль ТЛ					◆											◆					◆	◆	
Визуальный контроль (ТВ, ИК)	◆												◆	◆									
Приемники излучений		◆	◆		◆			◆				◆	◆								◆		
Хищение письма, ленты, дискеты	◆																						
Копирование информации	◆	◆											◆									◆	
Программные закладки, вирусы	◆																					◆	◆

Примечание. В таблице использованы следующие сокращения: ТСДИ – технические средства добывания информации; ТЛ – телефонная линия; ТВ – телевизионный; ИК – инфракрасный

фон (табл. 4). Методы и средства защиты выбираются в зависимости от реальных возможностей и обстоятельств, а также с учетом важности информации. Но наиболее эффективны интегральные системы, позволяющие преобразовывать исходные данные в цифровой вид и обрабатывать их программно-аппаратными методами. Возможности таких систем значительно расширились с использованием в них ПК, к которым могут быть подключены различные устройства связи и терминалы на базе печатных плат. Такая многофункциональная система способна не только заменить множество отдельных технических средств связи и обработки информации, но и выполнять ряд новых функций.

Примером такой системы служит разработанная в России система индекс. Она предназначена для передачи речевой, графической, буквенно-цифровой и другой информации по обычным и коммерческим каналам связи. Интегральная безопасность обеспечивается как физической, так и логической (в том числе и криптографической) защитой. Система индекс, выполненная на базе ПК модели PC IBM, обеспечивает интегральный подход к защите информации, единый порядок регистрации и хранения всех видов данных, дистанционное (глобальное) управление с использованием устройств тонального набора (табл. 5).

Таблица 5

Функциональные возможности системы ИНДЕКС

Обработка речевых данных	Шифратор	Модем	Факсимильное устройство	Контроль доступа
Запись и хранение речевых сообщений	Гарантированная защита всех видов информации	Скорость передачи: 300—2400 бод	Скорость передачи до 9600 бод	Прием сигналов от внешних датчиков
Регистрация телефонных вызовов, автоответчик	Конфиденциальность и достоверность данных	Коррекция ошибок по протоколу MNR-5 и выше	Криптозащита в соответствии с ГОСТ28147-89	Автонабор записанных в память номеров
Распознавание кодов и команд	Разграничение прав доступа	Кодирование	Сжатие передаваемой информации	Автодозвон
Автодозвон и передача речевых сообщений	Распределение ключей по схеме “открытого ключа”	Цифровая подпись	—	Передача речевого сообщения о характере нарушения

Появление на российском рынке не только интегральных электронных устройств (датчиков, видеокамер, терминалов и т.п.), но и интегральных радиосетей позволяет надеяться, что это перспективное и очень важное направление получит в нашей стране дальнейшее развитие.

Белый дом запрещает использование подслушивающих систем для сотовых телефонов

Дайджест

Палата представителей Конгресса США 414 голосами против одного проголосовала за запрещение подслушивания переговоров, ведущихся с помощью сотовых телефонов. Поправка об обеспечении безопасности беспроводных систем связи к Закону о связи от 1934 г. "запрещает модификацию любого электронного коммуникационного устройства, оборудования или системы, в результате которой это устройство может попасть в разряд подслушивающих". Новый закон также запрещает выдачу лицензий на использование любого сканирующего приемника, который можно оборудовать устройствами, декодирующими зашифрованные радиосообщения. Подобные действия можно будет производить только по решению суда. Пересмотрено и само определение "сканирующего приемника", чтобы предотвратить продажу устройств, которые можно незаконно использовать для перехвата радиопереговоров.

Newsbytes

ВЧ ИС для бумажных бирок

Новости

Фирма SCS – разработчик ВЧ-схем устройств идентификации – заключила производственное и технологическое соглашение с изготовителем разумных карт Hitachi Maxell, согласно которому схемы SCS, работающие с шупоподобным сигналом будут встроены в сверхтонкие (толщиной 24 мкм) карты. Поскольку процесс фирмы Maxell совместим со стандартной технологией печати методом литографии, ВЧ-схемы идентификации можно будет объединить с наклейками багажа и этикетками со штриховым кодом. SCS выпускает свои схемы на частоту 2,4 ГГц в небольших монтируемых на поверхность корпусах. На фирме Maxell пластины с КМОП-схемами устройств идентификации с помощью специального запатентованного метода полировки крепятся на гибкой подложке. На подложке также монтируются антенна длиной 50 см для приема сигнала в нелицензируемой полосе 2,4 ГГц и схемы для реализации протокола идентификации. Фирма Maxell как единственный изготовитель сверхтонких разумных карт имеет право их продажи по всему миру. SCS остается единственным дистрибьютором всей системы модели i2, включая устройства считывания карт. Система пригодна для многократного считывания и мультиплексирования сигналов. Она уже использовалась для отслеживания контейнеров британской фирмой Sainsbury, занимающейся хранением и складированием бакалейных товаров. Весьма перспективна система и для считывания багажных бирок в аэропортах.

htpp://techweb.cmp.com/eet/news/98

Конференции и семинары в области систем и средств безопасности

Дайджест

◇ В рамках форума "Технологии безопасности" компания "Гротек" организовала семинар "Технические средства безопасности", на котором присутствовало более 200 представителей правоохранительных органов, Таможенного комитета, Госкомсвязи, служб безопасности ведущих российских банков, а также предприятий, производящих средства и системы безопасности. Большое внимание на семинаре было уделено интегрированным системам безопасности. Какие функции по безопасности и обеспечению жизнедеятельности объекта должны быть включены в систему, на базе какой аппаратуры строить комплекс, как интегрировать уже установленное оборудование в новую систему, как оценить ее эффективность – эти вопросы стали предметом оживленной дискуссии. Активно обсуждался и вопрос о выборе фирмы, которая будет оснащать объект системой безопасности, и проведении конкурсов-тендеров с этой целью.

◇ Системы и средства обеспечения пожарной безопасности стали темой обсуждения на Международной научно-практической конференции, организованной Московским институтом пожарной безопасности МВД РФ. Один из главных вопросов, вынесенных на обсуждение участников конференции, – защита высокорисковых объектов с угрозой массового поражения при возникновении пожаров и сопровождающих их взрывов, объектов ядерной энергетики и химически опасных предприятий. Многие участники конференции говорили о быстром устаревании противопожарного оборудования и о необходимости его модернизации. Большой интерес вызвали сообщения о развитии систем газового пожаротушения, использовании компьютерных систем в пожарной охране и др.

◇ "Безопасность офисов и предприятий: системы контроля и управления доступом" – такова тема бизнес-семинара, организованного НИЦ "Охрана" ВНИИПО МВД РФ, ассоциацией охранных структур "Лига охраны", Промрадтехбанком и МЦНТИ. Цель этого мероприятия – обмен информацией и опытом, разработка рекомендаций для государственных и коммерческих организаций по построению, производству и эксплуатации систем контроля доступа и управления доступом. В рамках семинара была организована экспозиция новых образцов изделий в этой области.

По материалам журнала "Системы безопасности", март-апрель 1998 г.