Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ №5-6(60-61)/1998

Блокирование технических каналов утечки информации

Концептуальные вопросы оценки безопасности информационных технологий

Общие критерии оценки безопасности информационных технологий. Версия 2.0. Что нового?

Список лицензий и сертификатов, выданных ФАПСИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОФИЦИАЛЬНАЯ ХРОНИКА

Межведомственная комиссия по защите государственной тайны
Министерство общего и профессионального образования Российской Федерации
Головной совет по юридическим наукам Министерства общего профессионального образования Российской Федерации
Академия Федеральной службы безопасности Российской Федерации
Учебно-методическое объединение Администрации Санкт-Петербурга и Ленинградской области
Управление ФСБ России по Санкт-Петербургу и Ленинградской области
Санкт-Петербургский государственный университет

проводят 23–25 сентября 1998 года в Санкт-Петербурге научно-практическую конференцию

"ПЯТЬ ЛЕТ РОССИЙСКОМУ ЗАКОНУ "О ГОСУДАРСТВЕННОЙ ТАЙНЕ"

Тел.: (812) 2187-811 *E-mail: vus@grant.gc.spb.ru*

На конференции планируется рассмотреть вопросы, связанные со становлением правового режима защиты государственной и коммерческой тайн в Российской Федерации.

Предлагаемая программа конференции:

1. **Государственная и промышленная секретность, их роль и место в обеспечении национальной безопасности России.**
2. **Становление правового режима защиты государственной тайны в Российской Федерации – вопросы практической реализации положений действующего Закона Российской Федерации "О государственной тайне"**
3. **Вопросы развития и практики применения законодательства о коммерческой тайне.**

К участию в работе конференции приглашаются ученые и специалисты правоохранительных органов, практические работники служб и подразделений защиты информации предприятий, учреждений и организаций.

Заявки на участие в конференции принимаются только от организаций.

Планируется публикация материалов конференции. Тезисы докладов (объемом до 2-х страниц машинописного текста формата А-4 с приложением экспертного заключения о возможности публикации) направлять по адресу: ***199034, Санкт-Петербург, Университетская наб.7/9, Санкт-Петербургский государственный университет***, 1-й отдел не позднее 20 августа 1998 г .

Для участников конференции предусмотрен организационный взнос в размере 300 рублей.

Оргкомитет конференции

Сертификация линейки продуктов Bay Networks

14 апреля 1998 года Гостехкомиссия России завершила процесс сертификации линейки продуктов компании Bay Networks, присвоив им четвертый класс защищенности в соответствии с Руководящим документом по межсетевым экранам.

Напомним, что в январе 1998 года межсетевой экран "Застава-Джет" был сертифицирован по второму классу защищенности (см. Jet Info, 1998, 1). Теперь, после сертификации продуктов Bay Networks, появляется возможность построения из сертифицированных компонентов составных межсетевых экранов, обеспечивающих повышенный уровень информационной безопасности.

Копия сертификата приводится на стр. 3.

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU. 0001. 01БИ00

СЕРТИФИКАТ
№ 175

Выдан 14 апреля 1998 г.
Действителен до 14 апреля 2001 г.

Настоящий Сертификат удостоверяет, что единичные экземпляры **аппаратно-программных комплексов** на базе маршрутизаторов Bay Networks:

Advanced Remote Node (ARN) - заводской номер NEP0017306;
Access Stack Node 2 (ASN2) - заводской номер AF0002012;
BackBone Node (BN) - заводской номер BLA01816,

работающие под управлением программного обеспечения Site Manager Image: release /12.10/, MIB Ver. x 12.10 соответствуют техническим условиям № ДЖЕТ.МЭ.0001.98 ТУ, № ДЖЕТ.МЭ.0002.98 ТУ, № ДЖЕТ.МЭ.0003.98 ТУ соответственно, являются программно-техническими средствами защиты от несанкционированного доступа к информации и соответствуют требованиям Руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по **4 классу** защищенности при выполнении «Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам» и аттестации рабочих мест локальной вычислительной сети.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией Центра безопасности информации (аттестат аккредитации от 23.05.97 г. № СЗИ RU.117.Б08.025), протоколы испытаний от 12.04.98 г.

Заявитель – АОЗТ «Инфосистемы Джет»
Адрес - 103006, Москва, ул.Краснопролетарская, д.6
Тел. (095) 973-48-48

Инспекционный контроль соответствия аппаратно-программного комплекса требованиям нормативных документов Гостехкомиссии России и техническим условиям осуществляется испытательной лабораторией Центра безопасности информации.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ
ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ

Е.А.Беляев

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 14 апреля 1998 г.

Блокирование технических каналов утечки информаци

Вячеслав Барсуков,
кандидат технических наук

Содержание

1. ВВЕДЕНИЕ

Неблагоприятная криминогенная обстановка, недобросовестная конкуренция, активизация действий террористов заставляют общество повернуться лицом к проблеме обеспечения безопасности, одним из важнейших аспектов которой является информационная безопасность.

Основные надежды специалисты связывают с внедрением интегральных подходов и технологий. Мы уже излагали суть интегрального подхода к информационной безопасности (см. Jet Info, 1997, номер 1). Необходимым условием реализации интегрального подхода является **блокирование всех технических каналов утечки и несанкционированного доступа** к информации, поэтому для создания эффективных систем безопасности, в первую очередь, необходимо исследовать возможные каналы утечки и их характеристики.

2. ОСОБЕННОСТИ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

По результатам анализа материалов отечественной и зарубежной печати (см. [1-16]) на рис. 1 приведена обобщающая схема возможных каналов утечки и несанкционированного доступа к информации, обрабатываемой в типовом одноэтажном офисе.

Рассмотрим более подробно особенности каналов утечки и несанкционированного доступа к информации. Далее в тексте цифры в круглых скобках соответствуют обозначениям на рис. 1.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность компьютерного оборудования, включающую технические средства обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п. Следует учитывать также вспомогательные технические средства и системы (ВТСС), такие как оборудование открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрофикации, радиофикации, часофикации, электробытовые приборы и др.

Среди каналов утечки заметную роль играют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода, кабели, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции, проходящие через помещения, где установлены основные и вспомогательные технические средства.

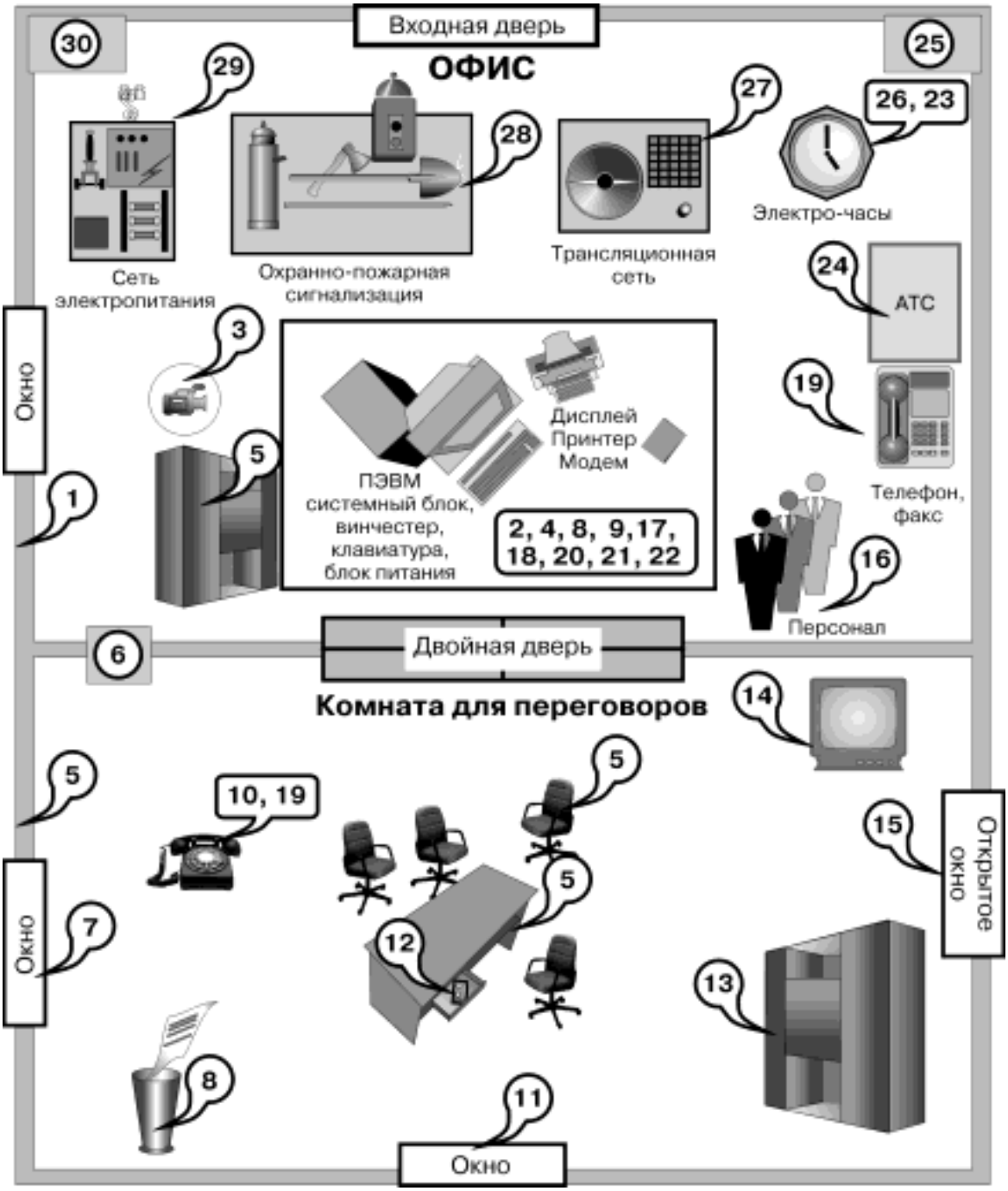
Рассмотрим сначала электромагнитные, электрические и параметрические технические каналы утечки информации.

Для **электромагнитных каналов утечки** характерными являются побочные излучения:

- **электромагнитные излучения элементов ТСОИ** (носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала (18, 21));
- **электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС** (в результате воздействия информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство (14));
- **электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты** технических средств передачи информации (ТСПИ) (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом (27)).

Возможными причинами возникновения **электрических каналов утечки** могут быть:

- **наводки электромагнитных излучений ТСОИ** (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС (23));
- **просачивание информационных сигналов в цепи электропитания** (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала (29));
- **просачивание информационных сигналов в цепи заземления** (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируе-



1. Утечка за счет структурного звука в стенах и перекрытиях	11. Дистанционный съем видео информации (оптика)	20. Съем с клавиатуры и принтера по акустическому каналу
2. Съем информации с ленты принтера, плохо стертых дискет и т.п.	12. Съем акустической информации с использованием диктофонов	21. Съем с дисплея по электромагнитному каналу
3. Съем информации с использованием видеозакладок	13. Хищение носителей информации	22. Визуальный съем с дисплея и принтера
4. Программно-аппаратные закладки в ПЭВМ	14. Высокочастотный канал утечки в бытовой технике	23. Наводки на линии коммуникаций и сторонние проводники
5. Радио-закладки в стенах и мебели	15. Съем информации направленным микрофоном	24. Утечка через линии связи
6. Съем информации по системе вентиляции	16. Внутренние каналы утечки информации (через обслуживающий персонал)	25. Утечка по цепям заземления
7. Лазерный съем акустической информации с окон	17. Несанкционированное копирование	26. Утечка по сети электро-часов
8. Производственные и технологические отходы	18. Утечка за счет побочного излучения терминала	27. Утечка по трансляционной сети и громкоговорящей связи
9. Компьютерные вирусы, логические бомбы и т.п.	19. Съем информации за счет использования “телефонного уха”	28. Утечка по охранно-пожарной сигнализации
10. Съем информации за счет наводок и “навязывания”		29. Утечка по сети электропитания
		30. Утечка по сети отопления, газо- и водоснабжения

Рис. 1. Схема каналов утечки и несанкционированного доступа к информации в типовом одноэтажном офисе.

мой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п. (25));

- **съем информации с использованием закладных устройств** (последние представляют собой устанавливаемые в ТСОИ микропередатчики, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны (5)).

Параметрический канал утечки информации формируется путем высокочастотного облучения ТСОИ, при взаимодействии электромагнитного поля которого с элементами ТСОИ происходит переизлучение, промодулированное информационным сигналом (10).

Анализ возможных каналов утечки и несанкционированного доступа, приведенных на рис. 1, показывает, что существенную их часть составляют технические каналы утечки акустической информации. В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов, технические каналы утечки акустической информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

В **воздушных** технических каналах утечки информации средой распространения акустических сигналов является воздух и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны (15), которые соединяются с диктофонами (12) или специальными микропередатчиками (5). Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т.п. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с обычного телефонного аппарата. Для этого их устанавливают либо непосредственно в корпусе телефонного аппарата, либо подключают к телефонной линии в телефонной розетке. Подобные устройства, конструктивно объединяющие микрофон и специальный блок коммутации, часто называют "телефонным ухом" (19). При подаче в линию кодированного сигнала или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает микрофон к телефонной линии и осуществляет передачу акустической (обычно речевой) информации по линии практически на неограниченное расстояние.

В отличие от рассмотренных выше каналов, в **вибрационных** (или структурных) каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела (1,30). В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

Электроакустические каналы утечки информации обычно образуются за счет преобразования акустических сигналов в электрические по двум основным направлениям: путем "**высокочастотного навязывания**" и путем перехвата через вспомогательные технические средства и системы (ВТСС).

Технический канал утечки информации путем "высокочастотного навязывания" образуется при несанкционированном контактном введении токов высокой частоты от ВЧ-генератора в линии, имеющие функциональные связи с элементами ВТСС, на которых происходит модуляция ВЧ-сигнала информационным. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны (10). С другой стороны, ВТСС могут сами содержать электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации (28), громкоговорители ретрансляционной сети (27) и т.д. Используемый в них эффект обычно называют " **микрофонным эффектом**". Перехват акустических колебаний в этом случае осуществляется исключительно просто. Например, подключая рассмотренные средства к соединительным линиям телефонных аппаратов с электромеханическими звонками, можно при положенной трубке прослушивать разговоры, ведущиеся в помещениях, где установлены эти телефоны.

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т.п., создается **оптико-электронный** (лазерный) канал утечки акустической информации (7). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие, как правило, в ближнем инфракрасном диапазоне и известные как "лазерные микрофоны". Дальность перехвата составляет несколко сотен метров.

Параметрический канал утечки акустической информации образуется в результате воздействия акустического поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем, проводов, дросселей и т.п., что приводит к изменениям параметров сигнала, например, модуляции его информационным сигналом. Промодулированные высокочастотные коле-

бания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами (14). Параметрический канал утечки акустической информации может быть создан и путем высокочастотного облучения помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых (добротность, частота и т.п.) изменяются по закону изменения акустического (речевого) сигнала.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию (20), в том числе осуществлять съем информации по системе централизованной вентиляции (6).

Особый интерес представляет **перехват информации при ее передаче по каналам связи** (24). Как правило, в этом случае имеется свободный несанкционированный доступ к передаваемым сигналам. В зависимости от вида каналов связи, технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Этот **электромагнитный канал** перехвата информации широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи (24).

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. Этот канал наиболее часто используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называют телефонными закладками (19).

Вообще говоря, непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком, поэтому чаще используется **индукционный канал** перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики, по сообщениям открытой печати, способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

В последнее время пристальное внимание привлекают каналы утечки **графической информации**, реализуемые техническими средствами в виде изображений объектов или копий документов, получаемых путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе:

Радио-микрофоны (закладки)	Электронные “уши“	Средства перехвата телефонной связи	Средства скрытого наблюдения и поиска	Средства контроля компьютеров и сетей	Средства приема, записи, управления и др.
с автономным питанием	микрофоны с проводами	с непосредственным подключением	Оптические	пассивные средства контроля монитора	приемники для радиозакладок
с питанием от телефонной сети	электронные стетоскопы	с индукционным датчиком	фотографические	активные средства контроля монитора	устройства накопления и записи
с питанием от электросети	направленные микрофоны	с датчиками внутри телефонного аппарата	тепловизионные и ночного видения	пассивные средства контроля шины (магистрали)	средства переприема (ретрансляторы)
управляемые дистанционно	лазерные микрофоны	телефонной радиотрансляции	телевизионные	активные средства контроля шины (магистрали)	средства ускоренной передачи
с функцией включения по голосу	микрофоны с передачей по электросети	перехвата сотовой телефонной связи	определения местоположения	аппаратные закладки	устройства дистанционного управления
полуактивные	с использованием микрофона аппарата	перехвата пейджинговых сообщений	маркирования и целеуказания	программные закладки	источники питания
с накоплением и быстрой передачей	гидроакустические микрофоны	многоканального перехвата	видеозакладочные	компьютерные вирусы	вспомогательные и другие средства

Табл. 1. Основные технические средства коммерческой разведки.

оптика (бинокли, подзорные трубы, телескопы, монокуляры (11)), телекамеры, приборы ночного видения, тепловизоры и т.п. Для документирования результатов наблюдения проводится съемка объектов, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки (3).

Рассмотренные выше методы получения информации основаны на использовании внешних каналов утечки. Необходимо, однако, кратко остановиться и на внутренних каналах утечки информации, тем более, что обычно им не уделяют должного внимания. Внутренние каналы утечки (16) связаны, как правило, с администрацией и обслуживающим персоналом, с качеством организации режима работы . Из них, в первую очередь, следует отметить такие каналы, как хищение носителей информации (13), съем информации с ленты принтера и плохо стертых дискет (2), использование производственных и технологических отходов (8), визуальный съем информации с дисплея и принтера (22), несанкционированное копирование (17) и т.п.

Электронное средство контроля информации	Место установки	Дальность действия, м	Стоимость электронного средства контроля информации	1.Вероятность применения 2.Качество перехвата 3.Вероятность обнаружения	Методы защиты информации
Контроль телефона, факса, модема (телефонная линия в штатном режиме)					
Индуктивный или контактный датчик	Телефонная линия	Регистрирующая аппаратура рядом с датчиком	Низкая	1. Высокая 2. Хорошее 3. Не обнаруживается	Шифрование или маскирование (радиотехнических методов нет)
Контроль телефона (режим опущенной трубки)					
Контактный датчик	Телефонная линия	Регистрирующая аппаратура рядом с датчиком	Низкая	1. Низкая 2. Хорошее 3. Не обнаруживается	Установка фильтров на входе линии
Контроль радиотелефона, радиостанции					
Панорамный радиоприемник	Прием из эфира	В пределах дальности станции	Средняя	1. Высокая 2. Хорошее 3. Не обнаруживается	Шифрование (маскирование)
Контроль сотового телефона					
Устройство прослушивания сотовой сети	Прием из эфира	В пределах соты абонента	Высокая	1. Зависит от стандарта 2. Хорошее 3. Не обнаруживается	Шифрование (маскирование)
Контроль монитора персонального компьютера					
Широкополосная антенна с регистрирующим устройством	Прием из эфира	3...20 м (определяется качеством экранирования монитора)	Высокая	1. Низкая 2. Посредств. 3. Не обнаруживается	Пассивная защита (экранировка помещения)
Широкополосный контактный датчик	Питающая электросеть	0...50 м (определяется развязкой по сети питания)	Высокая	1. Низкая 2. Посредств. 3. Не обнаруживается	Установка сетевых фильтров
Контроль магистрали компьютерной сети					
Индуктивный или контактный датчик	Любое место на кабеле магистрали	Регистрирующая аппаратура рядом с датчиком	Высокая	1. Высокая 2. Хорошее 3. Радиотехн. методами не обнаруживается	Шифрование, оргмероприятия (радиотехнических методов нет)

Табл. 2. Сравнительные характеристики пассивных средств получения информации.

3. ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ СОВРЕМЕННЫХ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

К сожалению, в настоящее время имеется широкий выбор средств специальной техники, с помощью которых возможно попытаться получить несанкционированный доступ к информации. Для выбора возможных путей блокирования каналов утечки необходимо знать " противника в лицо". В табл. 1 представлены основные технические средства ведения коммерческой разведки.

Характеристики каналов утечки информации, представленные в табл. 2 и 3, достаточно понятны, весьма показательны и особых комментариев не требуют.

Электронное средство контроля информации	Место установки	Дальность действия, м	Стоимость электронного средства контроля информации	1. Вероятность применения 2. Качество перехвата 3. Вероятность обнаружения	Методы защиты информации
Контроль акустической информации					
Встроенный радиомикрофон	ПЭВМ, калькулятор телефон, телевизор, приемник	200...1000	Средняя	1. Высокая 2. Хорошее 3. Высокая	Активные и пассивные (экранировка помещения)
Радиомикрофон с передачей по телефонной сети	Телефонный аппарат, розетка	200...500	Низкая	1. Высокая 2. Хорошее 3. Высокая	Активные и пассивные (фильтры), выжигание
Радиомикрофон длительного действия с цифровой модуляцией, кодированием и дистанционным управлением	Элементы интерьера и строительных конструкций	200...1000	Высокая	1. Высокая 2. Средняя 3. Средняя	Активные и пассивные (экранировка помещения)
То же с записью информации в память и сбросом по команде	Элементы интерьера и строительных конструкций	200...1000	Высокая	1. Низкая 2. Хорошее 3. Средняя	Активные и пассивные (экранировка помещения)
Видеоконтроль помещений					
Миниатюрная камера с передачей изображения по сети питания	Различные электрическ. устройства	10...30	Высокая	1. Низкая 2. Посредств. 3. Высокая	Активные и пассивные (сетевые фильтры)
То же с передачей изображения по радиоканалу	Предметы интерьера	50...200	Высокая	1. Средняя 2. Низкая 3. Высокая	Активные и пассивные (экранировка помещений)
Контроль информации с сетевой магистрали					
Передатчик с контактным или индуктивным датчиком на кабеле магистрали	Кабель магистрали или сервер компьютерной сети	50...200	Высокая	1. Средняя 2. Хорошее 3. Средняя (для кабеля), высокая (для сервера)	Активные и пассивные, организационные мероприятия (контроль персонала)

Табл. 3. Сравнительные характеристики активных средств получения информации.

N п/п	Действие человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	Разговор в помещении или на улице	акустика	подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система	шумовые генераторы, поиск закладок, защитные фильтры, ограничение доступа
		виброакустика	стетоскоп, вибродатчик	
		гидроакустика	гидроакустический датчик	
		акустоэлектроника	радиотехнические спецприемники	
2	Разговор по проводному телефону	акустика	аналогично п.1	аналогично п.1
		электросигнал в линии	параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка	маскирование, скремблирование, шифрование
		наводки	радиотехнические спецустройства	спецтехника
3	Разговор по радиотелефону	акустика	аналогично п.1	аналогично п.1
		электромагнитные волны	радиоприемные устройства	аналогично п.2
4	Документ на бумажном носителе	Наличие	кража, визуально, копирование, фотографирование	ограничение доступа, спецтехника
5	Изготовление документа на бумажном носителе	наличие	аналогично п.4	аналогично п.4
		паразитные сигналы, наводки	специальные радио-технические устройства	экранирование
6	Почтовое отправление	Наличие	кража, прочтение	специальные методы защиты
7	Документ на небумажном носителе	Носитель	хищение, копирование, считывание	контроль доступа, физическая защита, криптозащита
8	Изготовление документа на небумажном носителе	изображение на дисплее	визуально, копирование фотографирование	контроль доступа, криптозащита
		паразитные сигналы, наводки	специальные радиотехнические устройства	
9	Передача документа по каналу связи	электрические и оптические сигналы	несанкционированное подключение, имитация зарегистрированного пользователя	криптозащита
10	Производственный процесс	отходы, излучения и т.п.	спецаппаратура различного назначения, оперативные мероприятия	оргтехмероприятия, физическая защита

Табл. 4. Основные методы и средства несанкционированного получения информации и возможная защита от них.

4.МЕТОДЫ И СРЕДСТВА БЛОКИРОВАНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Анализ представленных материалов показывает, что в настоящее время номенклатура технических средств коммерческой разведки весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной.

Решение подобной задачи возможно только с использованием профессиональных технических средств и с привлечением квалифицированных специалистов.

В табл. 4 сведены рассмотренные выше каналы утечки информации и возможные методы их блокирования.

Таким образом, основным направлением противодействия утечке информации является обеспечение **физической** (технические средства, линии связи, персонал) и **логической** (операционная система, прикладные программы и данные) **защиты** информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

5. ЗАКЛЮЧЕНИЕ

Бурное развитие современных технологий и технических средств способствует постоянному расширению спектра возможных каналов утечки информации, поэтому блокирование каналов утечки становится все более актуальной и сложной задачей.

На эффективность систем безопасности существенно влияют характеристики каналов утечки информации, поэтому создание систем эффективной защиты должно происходить с учетом особенностей реальных каналов. Этот вывод не является тривиальным, как может показаться на первый взгляд. Например, сам факт наличия излучения дисплея еще не говорит об утечке информации. Все определяется конкретным уровнем напряженности поля за пределами зоны безопасности и техническими возможностями противника, поэтому окончательный вывод об утечке информации может сделать только квалифицированный специалист, использующий специальные технические средства. С другой стороны, особенности реальных каналов утечки информации могут быть успешно использованы и противником для обеспечения несанкционированного доступа к информации, о чем необходимо постоянно помнить. Так, съем информации по акустическим каналам может быть осуществлен через стекла окон, строительные, сантехнические, вентиляционные, теплотехнические и газораспределительные конструкции, с использованием для передачи сигналов радио, радиотрансляционных, телефонных и компьютерных коммуникаций, антенных и телевизионных распределительных сетей, охранно-пожарной и тревожной сигнализации, сетей электропитания и электрочасов, громкоговорящей и диспетчерской связи, цепей заземления и т.п. Случайный пропуск хотя бы одного возможного канала утечки может свести к нулю все затраты и сделать систему защиты неэффективной.

6. Литература

1. Андрианов В.И., Бородин В.А., Соколов А.В. "Шпионские штучки" и устройства для защиты объектов и информации. Справочное пособие. — С-Пб.: Лань, 1996.
2. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. — М.: Гротек, 1997.
3. Барсуков В.С. , Дворянкин С.В., Шеремет И.А. Безопасность связи в каналах телекоммуникаций. — М.: Электронные знания, 1992.
4. Барсуков В.С., Водолазкий В.В. Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей. — М.: Электронные знания, 1993.
5. Барсуков В.С. Обеспечение информационной безопасности. — М.: Эко-Трендз, 1996.
6. Гавриш В.Ф. Практическое пособие по защите коммерческой тайны. — Симферополь: Таврида, 1994.
7. Гайкович В., Першин А. Безопасность электронных банковских систем. -М.: Единая Европа, 1994.
8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. — М.: Энергоатомиздат, 1994.
9. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах. — М.: Энергоатомиздат, 1996.
10. Лысов А.В., Остапенко А.Н. Промышленный шпионаж в России: методы и средства. — С-Пб.: Бум Техно, 1994.
11. Магауенов Р.Г. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации. — М.: Мир безопасности, 1997.
12. Медведовский И., Семьянов П., Платонов В. Атака через ИНТЕРНЕТ. — С-Пб.: Мир и семья, 1997.
13. Мироничев С.Ю. Коммерческая разведка или промышленный шпионаж в России и методы борьбы с ним. — М.: Дружок, 1995.
14. Оружие шпионажа. Каталог — справочник. — М.: Империал, 1994.
15. Хорев А.А. Технические средства и способы промышленного шпионажа. — М.: Дальснаб, 1997.
16. Ярочкин В.И. Безопасность информационных систем. — М.: Ось-89, 1996.

Концептуальные вопросы оценки безопасности информационных технологий

Александр Трубачев
Центр безопасности информации

Содержание

1. Введение

Одной из наиболее серьезных проблем, затрудняющих применение современных информационных технологий (ИТ), является обеспечение их информационной безопасности. Особенно важна безопасность так называемых критических приложений, к числу которых относятся системы государственного и военного управления, объекты атомной энергетики, ракетно-космическая техника, а также финансовая сфера, нарушение нормального функционирования которых может привести к тяжелым последствиям для окружающей среды, экономики и безопасности государства.

Обеспечение безопасности информационных технологий представляет собой комплексную проблему, которая включает правовое регулирование применения ИТ, совершенствование технологий их разработки, развитие системы сертификации, обеспечение соответствующих организационно-технических условий эксплуатации. Основополагающим аспектом решения проблемы безопасности ИТ является выработка системы требований, критериев и показателей оценки уровня безопасности ИТ.

Состояние дел в области нормативного регулирования, методического и инструментального обеспечения оценки и сертификации безопасности ИТ в России, по общему признанию (см., например, [5]), не соответствует современному уровню развития ИТ, масштабам и разнообразию информационных угроз, требованиям законодательных и нормативных актов. Нормативные документы, применяемые различными ведомствами в рамках их полномочий, касаются отдельных аспектов обеспечения информационной безопасности. При этом отсутствует комплексность решения проблемы при разработке, внедрении и эксплуатации информационных систем (ИС).

В настоящее время сложилась насущная необходимость выработки общей политики в области оценки и сертификации безопасности информационных технологий и построения на ее основе системы нормативных документов в ранге государственных стандартов. Госстандарты позволят создать нормативную основу деятельности органов сертификации независимо от их ведомственной принадлежности.

В настоящей статье рассматриваются основы подхода к формированию нормативно-методической базы оценки и сертификации ИТ. Уточняются основные понятия, предлагаются направления совершенствования нормативной базы, методического обеспечения и инструментальных средств проведения сертификационных испытаний.

2. Понятийные основы

Отправной точкой при разработке нормативно-методического обеспечения оценки и сертификации безопасности ИТ должно являться однозначное установление терминологии в этой предметной области.

В существующих нормативных документах и у различных специалистов, в том числе за рубежом, существует различное понимание того, что включать в основополагающее понятие "безопасность ИТ". Наиболее часто, как, например, в Европейских критериях [1], безопасность ИТ определяется как комбинация конфиденциальности, целостности и доступности, где под ними понимается соответственно:

- предотвращение несанкционированного раскрытия информации;
- предотвращение несанкционированной модификации информации;
- предотвращение несанкционированного отказа в получении информации.

Данные аспекты достаточно полно характеризуют безопасность ИТ, только если считать это понятие тождественным понятию "защита информации". Такой подход принят в Руководящих документах Гостехкомиссии России [2], определяющих безопасность информации как состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Более современная точка зрения отражена в проекте международного стандарта "Общие критерии оценки безопасности информационных технологий" [3], где определяется, что "нарушение безопасности обычно включает, но не ограничено, раскрытием ресурса неразрешенным получателям (потеря конфиденциальности), повреждением ресурса через неразрешенную модификацию (потеря целостности) или неразрешенным лишением доступа к ресурсу (потеря доступности)". При этом процессы распространения и модификации информационных ресурсов должны строго управляться.

На наш взгляд, безопасность ИТ - это гораздо более широкое и глубокое понятие, чем защита информации. Угрозу представляет не только возможность несанкционированного доступа к ресурсам информационных систем, но и возможность через информационные технологии нанесения неприемлемого ущерба тем, в интересах кого

они применяются. Эти две грани можно определить, соответственно, как внутреннюю и внешнюю безопасность ИТ.

С учетом изложенного, под безопасностью ИТ предлагается понимать их способность обеспечивать защиту информационных ресурсов от действия внешних и внутренних, случайных и преднамеренных угроз, а также выполнять предписанные им функции без нанесения неприемлемого ущерба потребителям информации.

Следует обратить внимание на используемый здесь термин "неприемлемый ущерб". Он является принципиальным, разделяя угрозы, связанные с ухудшением качества функционирования ИТ и нарушением их безопасности.

Следующей исходной позицией является определение того, что же понимать под оценкой безопасности ИТ. Оценка безопасности ИТ производится с целью проверки соответствия достигнутого уровня безопасности заданному в ТЗ на разработку ИТ, а также соответствия требованиям стандартов и нормативных документов в отношении ИТ данного класса.

При проведении оценки безопасности используются требования ТЗ, проектные материалы, программно-методический аппарат проведения оценок и принятые критерии. Взаимосвязь элементов оценки безопасности иллюстрирует рис. 1.

В отношении оценки безопасности ИТ важным дискуссионным вопросом является использование количественных показателей.

В настоящее время общеупотребительным подходом к построению критериев оценки безопасности ИТ является использование совокупности определенным образом упорядоченных качественных требований к функциональным механизмам обеспечения безопасности, их эффективности и гарантированности реализации. Результирующая оценка уровня безопасности ИТ также имеет качественное выражение. Такой подход положен в основу всех реально действующих нормативных документов по оценке безопасности. Пока ни в одном из нормативных документов по оценке безопасности количественные показатели не применяются, хотя в некоторых допускается их использование.

Получение количественных характеристик безопасности было бы, несомненно, весьма полезным, особенно для сравнения различных проектов обеспечения безопасности, анализа влияния угроз и отдельных механизмов на общий уровень безопасности, учета изменения безопасности в процессе жизненного цикла ИТ. Однако для того, чтобы количественный показатель корректно использовать, он должен иметь объективную интерпретацию, однозначную зависимость от отдельных аспектов безопасности.

Специфика информационных технологий как объекта оценки определяется присутствием в них в качестве определяющей компоненты программного обеспечения. Ввиду большой функциональной, структурной и логической сложности программного обеспечения на практике невозможно в полном объеме оценить его поведение во всем возможном диапазоне его применения.

Предметная область безопасности обладает той особенностью, что при ее оценке приходится применять как объективные, так и субъективные критерии. Оцениваемые характеристики безопасности ИТ могут иметь как детерминированную, так и случайную природу. Некоторые исследуемые элементы ИТ, как, например, преднамеренные закладки, имеют уникальное пред-

Рис. 1. Оценка безопасности объекта ИТ.

ставление и скрытый характер, что также затрудняет проведение оценок безопасности ИТ.

В силу указанных обстоятельств получение интегральных количественных оценок безопасности ИТ является проблематичным. В упоминавшихся уже "Общих критериях" говорится, что "точные и универсальные оценки безопасности ИТ невозможны". Это, однако, не исключает использования отдельных частных количественных показателей там, где это целесообразно. В частности, эти показатели могут использоваться для оценки уровня механизмов криптографической и парольной защиты, контрольного суммирования и др.

В качестве общих требований к нормативно-методической базе оценки безопасности ИТ можно выделить следующие:

- универсальность, способность обеспечивать оценку безопасности любых видов ИТ и отдельных их компонентов;
- гибкость, способность формирования требований и получения оценок безопасности ИТ, максимально учитывающих особенности их применения;
- конструктивность, способность объективным образом оценивать уровень безопасности ИТ и влиять на процесс ее обеспечения;
- преемственность, способность интерпретировать результаты оценок, полученных в других системах оценки безопасности ИТ;
- расширяемость, способность наращивания системы критериев и показателей без нарушения их общего построения.

Рассмотрение существующих систем нормативных документов в области сертификации ИТ показывает, что в своей основе они в значительной мере этим требованиям не удовлетворяют. Необходимо их совершенствование.

3. Направления совершенствования нормативно-методического обеспечения

Основными направлениями развития нормативно-методического обеспечения оценки и сертификации безопасности ИТ являются:

- нормативная база;
- методическое обеспечение;
- инструментальные средства.

3.1 Нормативная база

В настоящее время в России действует ряд систем сертификации безопасности ИТ: Гостехкомиссии России, ФАПСИ, Минобороны, ФСБ. Нормативная база оценки безопасности ИТ в этих системах сертификации формально является различной, хотя на практике наблюдается взаимное использование отдельных нормативных документов. Например, широко применяются руководящие документы Гостехкомиссии России по защите автоматизированных систем и средств вычислительной техники от несанкционированного доступа.

Наличие нескольких систем сертификации обусловлено рядом объективных обстоятельств: особенностями предметной области, режимными соображениями и др. В целом оно не препятствует развитию в области сертификации ИТ, чего нельзя сказать о различии их нормативных баз, поскольку:

- различие требований к механизмам обеспечения безопасности ИТ затрудняет разработку унифицированных проектных решений и приводит к созданию специализированных средств для различных областей применения, что сопровождается их удорожанием;
- возникает необходимость в разработке различного методического и инструментального обеспечения оценки безопасности ИТ, что также сопровождается значительными дополнительными затратами;
- значительно усложняется и удорожается подготовка специалистов в области безопасности ИТ;
- осложняется процесс взаимного признания сертификатов, полученных в разных системах;
- качество нормативных документов является недостаточным в силу невозможности в каждой системе сертификации выделить необходимые ресурсы на их разработку.

Указанные проблемы могут быть преодолены путем создания единой для всех систем сертификации нормативной базы оценки безопасности ИТ в ранге государственных стандартов. Использование государственных стандартов для сертификации напрямую определяется также Законом Российской Федерации "О государственной тайне", в статье 28 которого говорится: "Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации".

Совершенствование нормативной базы оценки безопасности ИТ может идти по трем направлениям:

- принять в качестве базовой одну из существующих в России систем и дополнить ее необходимыми документами;
- принять в качестве базовой наиболее прогрессивную международную систему оценки безопасности и осуществить ее адаптацию с учетом особенностей российских условий;
- разработать принципиально новую систему оценки безопасности ИТ.

Существует, конечно, и четвертый путь - продолжение самостоятельного развития нормативной базы в каждой системе сертификации, но движение по этому пути, по меньшей мере, неразумно.

Первый путь является наиболее дешевым и быстро реализуемым, однако действующие нормативные документы систем сертификации уже не отвечают требованиям сегодняшнего дня. Дальнейшее совершенствование нормативной базы сертификации путем разработки новых документов по отдельным областям приложения ИТ без коренной переделки основы ее построения в конечном итоге приведет в тупик.

Третий путь представляется самым бесперспективным. Прежде всего потому, что пока еще никем в России не предложено достаточно ясной, полной и детально проработанной концепции построения перспективной системы оценки безопасности ИТ. Отдельные проработки в этом направлении показывают, что недостатков в них пока больше, чем достоинств, в своей основе они не удовлетворяют указанным выше требованиям и даже концептуальная их доработка может потребовать очень много времени. Следует также отметить, что в этом случае мы изолируем себя от наиболее развитых стран, идущих по пути применения "Общих критериев оценки безопасности ИТ", лишимся возможности использовать их методический и инструментальный аппарат, а также использовать их сертифицированные продукты и продвигать свои на их рынок.

На наш взгляд, наиболее приемлемым является построение системы российских государственных стандартов по оценке безопасности ИТ на основе самого совершенного на настоящий момент документа в этой области - "Общих критериев" (ОК) [6].

Анализ ОК свидетельствует, что этот документ в полной мере удовлетворяет всем указанным выше требованиям.

Рассмотрим наиболее важные положительные качества ОК.

1. Охват всего спектра информационных технологий и возможность учета особенностей каждой конкретной системы при задании требований по безопасности.

ОК предназначены для оценки безопасности как систем информационных технологий, разрабатываемых для автоматизации в конкретной области применения, так и отдельных продуктов ИТ, которые имеют универсальное предназначение. ОК применимы к оценке безопасности как аппаратных средств, так и программного обеспечения ИТ. Исключение составляют:

- административные меры обеспечения безопасности ИТ;
- оценка технических аспектов обеспечения безопасности типа побочного электромагнитного излучения;
- специфические свойства криптографических методов и алгоритмов защиты информации. (Общие требования к применению криптографических средств входят в состав функциональных требований ОК.)

В ОК отсутствует жесткая шкала классификации ИТ по уровню безопасности. Вместо этого предусмотрено использование сформированных по определенным правилам типовых наборов требований по различным видам ИТ, уровням защиты информации и другим классификационным признакам. Перечень типовых наборов требований не регламентируется ОК. Они формируются по результатам прохождения определенной процедуры согласования и апробации, предусмотренной в ОК.

С целью оптимального сочетания как предопределенного набора требований, так и требований, учитывающих особенности конкретной области применения ИТ, в ОК используются два ключевых понятия: профиль защиты и задание по безопасности.

Профиль защиты представляет собой функционально полный, прошедший апробацию, стандартизованный набор требований, предназначенный для многократного использования.

Задание по безопасности — это полная комбинация требований, являющихся необходимыми для создания и оценки информационной безопасности конкретной системы или продукта ИТ.

2. Учет специфики подхода к безопасности ИТ со стороны заказчиков (потребителей), разработчиков и лиц, осуществляющих оценку и сертификацию безопасности ИТ (оценщиков).

Для заказчиков ОК предоставляют возможности по грамотному, обоснованному заданию требований к безопасности ИТ. ОК могут также использоваться заказчиками для сравнительного анализа различных систем и продуктов ИТ.

Разработчикам ИТ ОК предоставляют развитую систему структурированных требований для выбора механизмов обеспечения безопасности при проектировании и разработке ИТ. Общие критерии содержат также требования к процессу разработки ИТ в целях обеспечения необходимого уровня гарантии реализации заданных функций безопасности.

Для специалистов по оценке безопасности ИТ ОК предоставляют систему критериев для формирования заключений об уровне безопасности ИТ и определяют виды, объем и глубину испытаний ИТ по требованиям безопасности.

3. Широкий спектр, детальность и структурированность требований к механизмам безопасности, мерам и средствам обеспечения их реализации.

ОК содержат две категории требований: функциональные требования и требования гарантированности.

Функциональные требования описывают те функции, которые должны быть реализованы в ИТ для обеспечения их безопасности. Требования гарантированности определяют меры и средства, которые должны быть использованы в процессе создания ИТ для получения необходимой уверенности в правильности реализации механизмов безопасности и в их эффективности.

Все требования ОК структурированы по классам, семействам, компонентам и элементам с определением зависимостей одних компонентов от других. Определены допустимые действия над компонентами, которые могут применяться для конкретизации задаваемых требований безопасности.

4. Охват всего процесса создания ИТ, начиная от формирования целей и требований обеспечения безопасности и кончая поставкой и наладкой ИТ на конкретном объекте.

Важной отличительной чертой ОК является полнота охвата требованиями всего жизненного цикла ИТ. В соответствии с ОК, на начальном этапе разработки ИТ должна быть определена модель жизненного цикла ИТ, в которой необходимо представить все меры и средства, применяемые разработчиком для достижения требуемого уровня безопасности ИТ. Меры и средства обеспечения гарантированности безопасности охватывают следующие аспекты:

- среда и средства разработки;
- состав, полнота и адекватность проектных материалов;
- конфигурационное управление;
- документация;
- тестирование;
- оценка уязвимости;
- поставка и наладка.

5. Возможность формирования наборов требований по уровням безопасности ИТ, сопоставимых с другими системами оценки.

В ОК указывается, что они разработаны с учетом совместимости с существующими критериями, чтобы сохранить преемственность оценок безопасности. Преемственность достигается за счет возможности формирования профилей защиты, соответствующих наборам требований, определяющих уровни безопасности ИТ в других системах критериев.

6. Комплексность подхода к обеспечению безопасности ИТ.

В соответствии с ОК, безопасность должна обеспечиваться на всех уровнях представления ИТ, от наиболее абстрактного на этапе формирования замысла создания информационной системы до ее применения в конкретных условиях. Предусмотрены следующие уровни рассмотрения безопасности ИТ:

- безопасность окружающей среды - законы, нормативные документы, организационные меры, физическое окружение, определяющие условия применения ИТ, а также существующие и возможные угрозы безопасности ИТ;
- цели безопасности - намерения, определяющие направленность мер по противодействию выявленным угрозам и обеспечению безопасности ИТ;
- требования безопасности - полученный в результате анализа целей безопасности набор технических требований для механизмов безопасности и гарантированности их реализации, обеспечивающий достижение сформулированных целей;
- спецификации безопасности - проектное представление механизмов безопасности, реализация которых гарантирует выполнение требований безопасности;
- разработка - реализация механизмов безопасности в соответствии со спецификациями.

ОК содержат требования по полноте, корректности и последовательности представления безопасности ИТ на различных уровнях и доказательству взаимосогласованности различных уровней представления ИТ.

7. Комплексность оценки безопасности ИТ.

В соответствии с ОК, оценка безопасности должна проводиться в процессе разработки ИТ на наиболее важных этапах. Предусмотрены следующие стадии оценки:

- оценка профиля защиты;
- оценка задания по безопасности;
- оценка реализованных механизмов безопасности.

Оценка профиля защиты производится с целью установления того, что сформированный профиль является полным, последовательным, технически правильным и пригодным для использования в качестве типового для определенного класса ИТ. Использование оцененных, апробированных и стандартизованных профилей защиты дает возможность заказчикам ИТ избежать крупных ошибок при задании требований к разрабатываемым системам и изделиям и исключить дополнительные затраты на обоснование требований.

Оценка задания по безопасности проводится с целью установления того, что задание соответствует требованиям профиля защиты и содержит полный, последовательный и технически правильный набор требований, необходимых для обеспечения безопасности конкретного объекта. Задание по безопасности подлежит согласованию между заказчиками, разработчиками и оценщиками и является в дальнейшем основным документом, в соответствии с которым оценивается безопасность разрабатываемой ИС.

Цель оценки реализованных механизмов обеспечения безопасности ИТ заключается в установлении того, что механизмы безопасности обеспечивают выполнение всех требований, содержащихся в задании по безопасности.

8. Расширяемость требований к безопасности ИТ.

"Общие критерии" представляют собой наиболее полный на настоящее время набор критериев в области безопасности ИТ, который удовлетворяет потребностям основных категорий и групп пользователей ИТ. Это является основанием для принятия ОК в качестве международного стандарта.

Требования ОК являются базовыми для формирования стандартизованных профилей защиты. При необходимости на этапе составления задания по безопасности они могут быть дополнены не входящими в ОК специфическими требованиями. Однако при этом заключение о безопасности ИТ не будет обладать той степенью универсальности и сопоставимости оценок, как полученное только на основаняии требований из ОК.

3.2 Методическое обеспечение

Нормативные документы по оценке безопасности ИТ не содержат методик контроля выполнения заданных в них требований. Вместе с тем в ОК содержатся положения о порядке проведения испытаний и их методическом обеспечении.

Методическое обеспечение должно охватывать все аспекты проверки выполнения требований, предъявляемых к безопасности ИТ.

Важнейшим и наиболее объемным видом испытаний при оценке безопасности ИТ является функциональное тестирование, предназначенное для проверки работоспособности механизмов безопасности и их соответствия предъявленным к ИТ функциональным требованиям. Для проведения тестирования должна быть подготовлена необходимая программно-методическая документация. В ее состав входят: программа тестирования, методика тестирования и контрольные результаты.

В программе тестирования для каждой функции безопасности, определенной в функциональных требованиях, должны быть заданы цель тестирования, объем и порядок его проведения. Методика проведения тестирования должна содержать описание условий и процедур проведения испытаний, состав тестов и порядок обработки результатов тестирования.

Выделяются два аспекта, которые определяют качество и гарантированность проведения тестирования: достаточность и глубина.

Достаточность характеризует полноту охвата тестированием функций безопасности и объем проводимого тестирования. При анализе достаточности должно быть продемонстрировано соответствие между параметрами функций безопасности и результатами тестирования, подтверждающее проверку выполнения заданных требований.

Глубина характеризует уровень детальности проводимого тестирования. Она определяет вероятность выявления ошибок в реализованных механизмах обеспечения безопасности ИТ. Кроме того, от глубины тестирования зависит возможность обнаружения в ИТ закладных элементов.

Важным аспектом испытаний средств безопасности ИТ, на который не всегда в должной мере обращается внимание, является оценка уязвимости средств безопасности (СБ).

Оценка уязвимости СБ ИТ производится с целью проверки способности реализованных механизмов безопасности противостоять информационным воздействиям, являющимся результатом неправильной конфигурации, неправильной эксплуатации, либо попыткам взлома.

Задачами, решаемыми при оценке уязвимости СБ ИТ, являются:

- анализ уязвимостей СБ ИТ;
- оценка мощности функций безопасности;
- оценка возможностей неправильного применения;
- анализ тайных каналов.

Анализ уязвимостей СБ ИТ предназначен для выявления возможных недостатков, которые могли бы быть использованы злоумышленниками для проникновения в среду ИТ, доступа к защищаемым ресурсам, а также для нарушения нормального режима функционирования ИТ. Анализ уязвимостей должен проводиться как путем аналитического исследования проектных материалов, так и путем натурного моделирования с использования имитаторов угроз безопасности. В зависимости от заданного уровня гарантированности предполагается различная степень знакомства злоумышленника с проектными материалами, а также различный уровень его подготовленности и оснащенности.

В силу того, что механизмы безопасности обладают ограниченными возможностями по противодействию угрозам, существует определенная вероятность нарушения защиты, даже если механизмы безопасности не могут быть обойдены или блокированы. Для оценки этой вероятности должны быть проведены аналитические или статистические исследования.

Нарушение безопасности СБ ИТ может произойти по причине его неправильной конфигурации, настройки или некорректного применения вследствие неточности или противоречивости эксплуатационной документации. С учетом этого, при оценке уязвимости эксплуатационные документы должны быть проанализированы на предмет пол-

ноты и непротиворечивости инструкций, отсутствия возможности их неоднозначного толкования.

Анализ тайных каналов направлен на выявление существования и оценку потенциальной возможности использования непредусмотренных каналов проникновения в среду ИТ и передачи информации. Задача выявления тайных каналов в методическом плане является весьма сложной и трудно поддается формализации.

В настоящее время общепринятой практикой является разработка программ и методик испытаний для каждого сертифицируемого изделия и согласование их с разработчиком ИТ, органом сертификации и испытательной лабораторией. Таким образом, даже для однотипных изделий, сертифицируемых разными лабораториями, программы и методики испытаний могут быть совершенно различными. Вместе с тем, для обеспечения доказательности и сопоставимости результатов оценок, процедура их проведения должна быть проверяемой и обеспечивать повторяемость результатов.

В целях унификации методического обеспечения сертификации представляется целесообразным иметь типовые методики испытаний по базовым механизмам безопасности, мерам гарантированности и однородным группам изделий ИТ. Использование типовых методик способно положительным образом повлиять на повышение качества сертификационных испытаний.

Необходимость наличия типовых методик испытаний будет возрастать по мере увеличения числа однородных продуктов для типовых механизмов безопасности. Только наличие типовых методик испытаний по единым критериям способно обеспечить возможность сопоставления различных продуктов.

Разработка типовых методик может быть выполнена по заказу федеральных органов сертификации наиболее подготовленными в конкретных областях испытательными лабораториями. После апробации при оценке безопасности конкретных образцов ИТ они могли бы быть приняты как нормативные документы в соответствующих системах сертификации.

3.3 Инструментальные средства

Качество и сроки выполнения работ по сертификации в значительной мере зависят от используемых инструментальных средств. Наибольшее применение инструментальные средства находят в следующих направлениях:

- генерация тестов;
- имитация угроз;
- анализ текстов программ.

Генераторы тестов можно разделить на две большие группы:

- генераторы стохастических тестов;
- генераторы целенаправленных тестов.

Методы применения генераторов тестов достаточно хорошо отработаны и широко используются при проведении испытаний функциональных возможностей ИС [4, 7, 8]. Генераторы стохастических тестов эффективно применяются, прежде всего, при исследовании качества и надежности функционирования ИС.

В приложении к анализу безопасности ИТ более предпочтительными являются генераторы целенаправленных тестов. Помимо испытаний функциональных механизмов безопасности, областью применения генераторов тестов является также анализ текстов программ для выявления недекларированных возможностей и закладных элементов.

Генераторы тестов, предназначенные для испытаний безопасности ИТ, должны обладать следующими функциональными возможностями:

- формирование заданных структур и последовательностей входных данных, определяемых особенностями реализации механизмов безопасности;
- обеспечение заданной степени покрытия области входных данных и элементов структуры исследуемых программ;
- выявление критичных условий функционирования механизмов безопасности и маршрутов реализации программного кода;
- формирование тестов по условиям реализации предыдущих этапов тестирования.

Имитаторы угроз предназначены для натурного моделирования воздействия на ИТ типовых угроз. Посредством имитаторов угроз проверяются механизмы защиты от программных вирусов, средства экранирования от проникновения из внешних вычислительных сетей и т.д.

Наиболее сложной областью применения инструментальных средств является исследование недекларированных возможностей ИТ, поиск закладных элементов и анализ уязвимых мест в программном обеспечении. В большинстве испытательных лабораторий выполнение указанных работ осуществляется путем "ручного" анализа исходных текстов программ. Ввиду большой сложности современного программного обеспечения, на проведение таких работ затрачивается большое время, исчисляемое месяцами, и требуется привлечение значительного числа высококвалифицированных специалистов, что определяет очень высокую стоимость выполнения указанных работ и практическую невозможность их повторения.

Для автоматизации исследования исходных текстов программ применяются статические и динамические анализаторы. Статические анализаторы предназначены для оценки корректности структуры построения программ, выявления участков программного кода, к которым отсутствует обращение, установления точек входа и вы-

хода из программ, не предусмотренных спецификациями, проверки полноты описания и использования программных переменных, поиска специальных программных конструкций, которые могут быть идентифицированы как программные закладки.

Динамические анализаторы используются для трассировки выполнения программ, выявления критических путей, оценки полноты покрытия возможных ветвей программ при функциональном тестировании.

Создание анализаторов исходных текстов программ представляет собой сложную задачу. В настоящее время в России только ограниченный круг испытательных лабораторий применяет в своей практике инструментальные средства анализа программного обеспечения. В этом плане следует отметить серию средств, разработанных "Центром безопасности информации". Опыт применения анализаторов программ показал их исключительно высокую эффективность. Время проведения анализа программ сокращается практически на порядок, результаты анализа исчерпывающе документируются, что обеспечивает их контроль и, при необходимости, повторение.

В настоящее время развивается еще одна область применения инструментальных средств — использование информационных и экспертных систем для формирования требований к безопасности ИТ и оценки уровня их выполнения. Применение таких средств позволит значительно повысить степень обоснованности задания требований, их адекватность реальным условиям применения ИТ, даст возможность осуществлять выбор механизмов безопасности, наиболее полно удовлетворяющих заданным требованиям.

4. Заключение

Анализ состояния дел в области сертификации безопасности информационных технологий показывает, что имеется существенное отставание в уровне развития нормативного, методического и инструментального обеспечения оценки безопасности от тех потребностей, которые продиктованы масштабами развития и внедрения ИТ в системы критических приложений. Требуется выработка общей политики по оценке и сертификации безопасности ИТ и формирование на ее основе комплекса нормативных документов в ранге государственных стандартов.

Систему российских государственных стандартов представляется рациональным разрабатывать на основе наиболее совершенного на настоящий момент документа в этой области — "Общих критериев оценки безопасности информационных технологий", который планируется к принятию в качестве международного стандарта. "Общие критерии" в полной мере удовлетворяют всем современным требованиям и обладают огромным потенциалом развития и адаптации к различным условиям применения. Они позволяют сформировать совокупности критериев оценки, аналогичные принятым в настоящее время в действующих системах сертификации средств защиты информации в России, и тем самым обеспечить безболезненный переход на новую нормативную базу.

Качество проведения сертификации ИТ может быть повышено путем внедрения типовых методик испытаний по базовым механизмам обеспечения безопасности, мерам гарантированности и однородным группам изделий ИТ, а также применения соответствующего инструментария.

Выработка общей концепции совершенствования сертификации информационных технологий и разработка на ее основе комплекса нормативных документов, методического и инструментального обеспечения потребует скоординированных усилий действующих в России систем сертификации средств зашиты информации. Это может быть сделано в рамках государственной программы по созданию безопасных информационных технологий.

5. Литература

1. Information Technology Security Evaluation Criteria(ITSEC). Harmonised Criteria of France — Germany — the Netherlands — the United Kingdom. — Department of Trade and Industry, London, 1991.
2. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. — Москва, 1992.
3. Common Criteria for Information Technology Security Evaluation. Version 1.0, 96.01.31.
4. Липаев В.В. Программно-технологическая безопасность информационных систем. — Jet Info, 1997 № 6,7.
5. Бетелин В., Галатенко В. Информационная безопасность в России: опыт составления карты. — Jet Info, 1998 № 1.
6. Кобзарь М.Т., Калайда И.А. Общие критерии оценки безопасности информационных технологий и перспективы их использования. — Jet Info, 1998 № 1.
7. Липаев В.В. Отладка сложных программ. — М.: Энергоатомиздат, 1993.
8. Howden W.E. Functional program testing and analysis. — N.Y.: McGraw Hill,1987.

ОБЩИЕ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

Версия 2.0. Что нового?

Марк Кобзарь, Михаил Долинин
Центр безопасности информации

Рабочая группа 3 подкомиссии 27 Международной организации по стандартизации (ИСО) завершила разработку версии 2.0 "Общих критериев оценки безопасности информационных технологий" [1].

Во второй версии Общих критериев сохранены основные концептуальные положения версии 1.0 [2]. Изменения коснулись структуры всего документа, некоторых классов, семейств и компонентов требований безопасности.

В версии 2.0 Общих критериев остались только три части:

часть 1 — "ПРЕДСТАВЛЕНИЕ И ОБЩАЯ МОДЕЛЬ";

часть 2 — "ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ";

часть 3 — "ТРЕБОВАНИЯ ГАРАНТИРОВАННОСТИ".

Часть 4 "ПРЕДОПРЕЛЕННЫЕ ПРОФИЛИ ЗАЩИТЫ" вынесена за пределы проекта стандарта, что логично, учитывая постоянное пополнение каталога Профилей защиты.

В разделе "ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ" (часть 2) появились два новых класса: FCS ("КРИПТОГРАФИЧЕСКАЯ ПОДДЕРЖКА") и FMT ("УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ").

Класс FCS был анонсирован еще в версии 1.0. Он включает два семейства: FCS_CKM ("Управление криптографическими ключами") и FCS_COP ("Криптографические операции").

Класс FMT явился результатом перегруппировки требований, связанных с управлением безопасностью объекта оценки. В него вошли семейства: FMT_MOF ("Управление функциями безопасности объекта оценки"), FMT_MSA ("Управление признаками безопасности"), FMT_MTD ("Управление данными функций безопасности"), FMT_REV ("Аннулирование"), FMT_SAE ("Истечение признака безопасности") и FMT_SMR ("Функции управления безопасностью").

Существенно изменились структура и содержание классов FAU ("АУДИТ БЕЗОПАСНОСТИ"), FDP ("ЗАЩИТА ДАННЫХ ПОЛЬЗОВАТЕЛЯ") и FIA ("ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ").

В классе FAU исключено шесть семейств: FAU_MGT ("Управление аудитом безопасности"), FAU_POP ("Обработка сохраняемых данных аудита безопасности"), FAU_PRO ("Защита трассы контроля безопасности"),FAU_PRP ("Обработка данных аудита безопасности до хранения") — их требования сгруппированы в близких по назначению других модернизированных семействах этого же класса; FAU_PAD ("Обнаружение аномалии по базовому образцу"), FAU_PIT ("Средства идентификации проникновения") — их требования сгруппированы в модернизированном и дополненном еще двумя компонентами семействе FAU_SAA ("Анализ аудита безопасности").

В классе FDP исключены три семейства: FDP_ACI ("Инициализация признаков объекта"), FDP_SAM ("Модификация признаков безопасности"), FDP_SAQ ("Запрос признака безопасности") — их требования сгруппированы в новом классе FMT, а также добавлено новое семейство FDP_DAV ("Аутентификация данных"). Это семейство, состоящее из двух компонентов: FDP_DAU.1 ("Базисная аутентификация данных") и FDP_DAU.2 ("аутентификация данных с идентификацией гаранта"), требует обеспечения гарантий проверки правильности специфицированного модуля данных, которые впоследствии могут быть использованы для проверки того, что, например, информация не была изменена или подделана. Это — своего рода нотаризация данных, но, в отличие от нотаризации при обмене данными в сетевых конфигурациях (класс FCO), применяемая для "статических" данных.

В классе FIA исключены семейства: FIA_ADA ("Администрация данных аутентификации пользователей"), FIA_ADP ("Защита данных аутентификации пользователей") и FIA_ATA ("Администрирование признака пользователя") — их основные требования сгруппированы в соответствующих семействах нового класса FMT.

Незначительные изменения претерпели остальные классы функциональных требований.

В разделе "ТРЕБОВАНИЯ ГАРАНТИРОВАННОСТИ" (часть 3) в классе ADV ("РАЗРАБОТКА") выделены в отдельное семейство ADV_SPM ("Модель политики безопасности") требования к модели политики безопасности объекта оценки.

В классе ATE ("ТЕСТИРОВАНИЕ") в семействе ATE_FUN ("Функциональное тестирование") появился дополнительный компонент ATE_FUN.2 ("Упорядоченное функциональное тестирование"), используемый в уровнях гарантии оценки УГО-6 и УГО-7 и требующий включения в тестовую документацию анализа последовательности процедур тестирования, входивших ранее в компонент ATE_COV.3.

В классе AVA ("АНАЛИЗ УЯЗВИМОСТЕЙ") в семействе AVA_MSU ("Неправильное применение") добавлен третий компонент, предусматривающий дополнительное выполнение Оценщиком независимого тестирования (типа атаки) для подтверждения идентификации в тестовой документации всех возможных опасных состояний. В семействе AVA_SOF ("Сила функций безопасности объекта оценки") исключено описание ранжирования силы функции на "базовую", "среднюю" и "высокую" и введено требование оценки соответствия силы функции безопасности, заданной в Задании по безопасности или Профиле защиты.

В свою очередь, требования к Профилю защиты (класс APE) и Заданию по безопасности (класс ASE) теперь предусматривают необходимость включения в функциональные требования минимального уровня силы для функций безопасности, реализуемых механизмами случайной выборки или перестановки (например, паролирование или хэш-функции). Уровень определяется как "базовый", "средний" или "высокий" в зависимости от целей безопасности объекта оценки. Для некоторых целей безопасности возможно применение специфических метрик силы функции. Если в требованиях гарантированности используется уровень гарантии оценки УГО-1, который не включает компонента семейства AVA_SOF, сила функций безопасности в функциональных требованиях не задается.

В классе AGD ("ДОКУМЕНТЫ РУКОВОДСТВА") в семействе AGD_ADM требования к Руководству администратора представлены в более общем виде.

Версия 2.0 "Общих критериев оценки безопасности информационных технологий" представлена в ИСО в качестве проекта международного стандарта. Официальный документ ИСО планируется к выпуску весной 1999 года.

ЛИТЕРАТУРА

1. Common Criteria for Information Technology Security Evaluation (CCEB). Version 2.0. 98.05.22.
2. М.Кобзарь, И.Калайда. Общие критерии оценки безопасности информационных технологий и перспективы их использования. Информационный бюллетень — Jet Info, 1998, 1.

Список сертификатов

на шифровальные средства, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну

(на 01.04.1998)

1	**СФ/124-0004 от 10.04.96 до 09.04.99**	"Верба"
2	СФ/114-0005 от 10.04.96 до 09.04.99	"Верба-О"
3	СФ/124-0012 от 10.04.96 до 09.04.99	"АПДС"
4	СФ/124-0013 от 10.04.96 до 09.04.99	"АПДС-В"
5	СФ/124-0014 от 10.04.96 до 09.04.99	"АПДС-С"
6	СФ/124-0061 от 08.05.96 до 07.05.99	"Анкрипт" ("Электроника МК-85С")
7	СФ/114-0063 от 27.05.96 до 26.05.99	"АРМ АБ-О"
8	СФ/124-0064 от 27.05.96 до 26.05.99	"АРМ АБ-С"
9	СФ/124-0065 от 27.05.96 до 26.05.99	"Защищенный почтамт-С"
10	СФ/124-0066 от 27.05.96 до 26.05.99	"Криптографический Сервер"
11	СФ/100-0100 от 30.07.96 до 29.07.99	"СТА-1000М"
12	СФ/120-0164 от 31.12.96 до 31.12.99	SCR-M1.2
13	СФ/124-0172 от 02.04.97 до 31.12.00	"АРМ АБ"
14	СФ/114-0173 от 10.04.97 до 09.04.00	"Верба-OU"
15	СФ/114-0174 от 10.04.97 до 09.04.00	"Верба-OW"
16	СФ/114-0175 от 10.04.97 до 09.04.00	"Верба-U"
17	СФ/114-0176 от 10.04.97 до 09.04.00	"Верба-W"
18	СФ/110-0177 от 10.04.97 до 09.04.00	"Верба-OM"
19	СФ/111-0178 от 10.04.97 до 09.04.00	"Верба-OS"
20	СФ/124-0179 от 10.04.97 до 09.04.00	"УКДС"
21	СФ/124-0180 от 10.04.97 до 09.04.00	"УКДС-В"
22	СФ/124-0181 от 10.04.97 до 09.04.00	"УКДС-С"
23	СФ/124-0182 от 10.04.97 до 09.04.00	"Титан"
24	СФ/124-0183 от 10.04.97 до 09.04.00	"ЦУКС"
25	СФ/114-0184 от 10.04.97 до 09.04.00	"ЯНТАРЬ"
26	СФ/124-0185 от 10.04.97 до 09.04.00	"ШИП"
27	СФ/124-0186 от 10.04.97 до 09.04.00	"ЦУКС ШИП"
28	СФ/124-0187 от 27.05.97 до 26.05.00	"ЯНТАРЬ АСБР"
29	СФ/120-0215 от 30.12.97 до 31.12.00	"SCR-M1.2 MINI"

Список лицензий и аттестатов аккредитации,

выданных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации

на 01.04.1998 г.

Сертификационные испытания	№№ лицензий
Научно-исследовательский институт автоматики РГНПО "Автоматика"	ЛФ/01-129
Государственное унитарное предприятие научно-технический центр "Атлас" (Испытательный сертификационный центр)	ЛФ/01-148
Научно-производственное объединение "Импульс"	ЛФ/01-68

Научно-исследовательская лаборатория №13 Центрального конструкторского бюро Научно-производственного предприятия "Сигнал"	ЛФ/01-71
Государственное унитарное предприятие научно-технический центр "Атлас" (Пензенский филиал)	ЛФ/02-151
Закрытое акционерное общество "Московское отделение Пензенского научно-исследовательского электротехнического института"	ЛФ/07-192

Подготовка и переподготовка кадров	№№ лицензий
Военная академия Ракетных войск стратегического назначения	ЛФ/02-104
Рязанская государственная радиотехническая академия	ЛФ/02-105
Санкт-Петербургский государственный технический университет	ЛФ/02-106
Межотраслевой специальный учебный центр при Министерстве Российской Федерации по атомной энергии	ЛФ/02-128
Военный институт правительственной связи	ЛФ/02-158
Московский государственный инженерно-физический институт (технический университет)	ЛФ/02-20
Краснодарское высшее военное училище имени генерала армии С.М.Штеменко	ЛФ/02-42
Академия Федеральной службы безопасности Российской Федерации	ЛФ/02-5
Российский государственный гуманитарный университет	ЛФ/02-66
Московский государственный институт радиотехники, электроники и автоматики (технический университет)	ЛФ/02-72
Московский государственный институт электроники и математики (технический университет)	ЛФ/02-98
Негосударственное образовательное учреждение "Учебный центр банковских технологий МГТУ-Промстройбанк"	ЛФ/08-157
Некоммерческое образовательное учреждение "Научно-технический Центр Ассоциации Российских Банков"	ЛФ/17-76

Аккредитованные ФАПСИ аттестационные центры

Аттестационный центр	№№ аттестатов аккредитации
Государственное унитарное предприятие "Научно-технический центр "Атлас"	АТФ/001-06.001
Государственное унитарное предприятие "Научно-технический центр "Атлас" (Пензенский филиал)	АТФ/001-07.001
Управление правительственной связи и информации в Северо-Кавказском регионе	АТФ/052-08.001
Управление правительственной связи и информации в Северо-Западном регионе	АТФ/052-09.001
Центр правительственной связи в Краснодарском крае	АТФ/052-10.001
Центр правительственной связи в Самарской области	АТФ/052-11.001
Центр правительственной связи в Свердловской области	АТФ/052-12.001
Закрытое акционерное общество "Московское отделение ПНИЭИ"	АТФ/057-04.002 АТФ/117-04.005
Ассоциация Документальной Электросвязи	АТФ/057-05.002

Лицензиаты ФАПСИ по иным видам деятельности	№№ лицензий
Акционерный Восточно-Сибирский транспортно-коммерческий банк	ЛФ/06-188
Акционерное общество закрытого типа "Инфотел"	ЛФ/17-118
Акционерное общество закрытого типа "Калугаприборсвязь"	ЛФ/17-63

Акционерное общество закрытого типа "Межбанковский финансовый дом"	ЛФ/06-80
Акционерное общество закрытого типа "ЭЛТЕХ"	ЛФ/17-87
Акционерное общество открытого типа "Гипросвязь-Самара"	ЛФ/17-62
Акционерное общество открытого типа "Информационные телекоммуникационные технологии"	ЛФ/17-155
Акционерное общество открытого типа "Ленполиграфмаш"	ЛФ/17-67
Акционерное общество открытого типа "Релком"	ЛФ/17-120
Акционерное общество открытого типа "Телеком"	ЛФ/17-94
Акционерный коммерческий банк "Держава"	ЛФ/06-100
Акционерное общество закрытого типа НПП "Антей"	ЛФ/17-29
Банк "Аресбанк"	ЛФ/06-30
Банк "Банк Городского развития"	ЛФ/06-34
Банк "Гранит"	ЛФ/06-38
Банк "Зенит"	ЛФ/06-78
Банк "Империал"	ЛФ/06-77
Банк "Лакар"	ЛФ/06-36
Банк "Меритбанк"	ЛФ/06-31
Банк "Российский акционерный инвестиционно-коммерческий промышленно-строительный банк"	ЛФ/06-79
Банк "Русский банкирский дом"	ЛФ/06-40
Банк "Сервис-Резерв"	ЛФ/06-41
Банк "Федеральный банк развития"	ЛФ/06-37
Банк "Фидес-Банк"	ЛФ/06-27
Банк "Филин"	ЛФ/06-32
Банк "Экспресс-кредит"	ЛФ/06-33
Банк "Элика"	ЛФ/06-35
Банк "Интеркредит"	ЛФ/06-39
Башкирское ПО "Прогресс"	ЛФ/11-75
Государственное научно-производственное объединение "Альтаир"	ЛФ/13-114
Государственное предприятие "Казанский научно-исследовательский институт радиоэлектроники"	ЛФ/11-163
Государственное предприятие "Калужский электромеханический завод"	ЛФ/12-61
Государственное предприятие "Конструкторское бюро полупроводникового машиностроения" КБПМ	ЛФ/13-18
Государственное предприятие "Пензенский научно-исследовательский электротехнический институт"	ЛФ/11-50 ЛФ/11-200
Государственное предприятие "ПО Сибирские приборы и системы"	ЛФ/12-140
Государственное предприятие "РФЯЦ-ВНИИЭФ"	ЛФ/11-243
Государственное предприятие "Специальное научно-производственное объединение "Элерон"	ЛФ/13-108
Государственное предприятие "Уфимский завод микроэлектроники "Магнетрон"	ЛФ/11-74
Государственное предприятие "Центр автоматизированного оперативно-технического управления связью"Государственного комитета Российской Федерации по связи и информатизации	ЛФ/12-173
Государственное предприятие "Электромеханический завод "Авангард"	ЛФ/12-204
Государственное предприятие завод "Алмаз"	ЛФ/12-57

Государственное предприятие завод "Калугаприбор"	ЛФ/12-56
Государственное унитарное предприятие "Научно-технический центр информационных региональных систем" - дочернее предприятие НИИ автоматической аппаратуры им. академика В.С.Семенихина	ЛФ/11-193
Государственное унитарное предприятие научно-технический центр "Атлас"	ЛФ/11-149
Государственное унитарное предприятие научно-технический центр "Атлас" (Пензенский филиал)	ЛФ/11-150
Государственное унитарное предприятие научно-технический центр "Атлас"	ЛФ/13-116
Государственное унитарное предприятие по телекоммуникациям и информатике "Салют"	ЛФ/13-49
Государственный космический научно-производственный центр им. М.В.Хруничева	ЛФ/11-161
Документальные системы - МФД	ЛФ/17-136
Закрытое акционерное обществе "Центр финансовых технологий"	ЛФ/17-190
Закрытое акционерное общество" Авиателеком"	ЛФ/17-43 ЛФ/17-44
Закрытое акционерное общество "SCAN"	ЛФ/17-198
Закрытое акционерное общество "АЛТ-М"	ЛФ/17-88
Закрытое акционерное общество"Анкорт"	ЛФ/17-51
Закрытое акционерное общество "Банковские системы и технологии"	ЛФ/17-73
Закрытое акционерное общество "Депозитарно-Клиринговая Компания"	ЛФ/17-111
Закрытое акционерное общество "Информационные системы Джет"	ЛФ/17-197
Закрытое акционерное общество"КомФАКС"	ЛФ/17-47
Закрытое акционерное общество "ЛАНИТ"	ЛФ/17-175
Закрытое акционерное общество "Московская межбанковская валютная биржа"	ЛФ/17-110
Закрытое акционерное общество "Московская телекоммуникационная корпорация"	ЛФ/17-121
Закрытое акционерное общество "Моспроминформ"	ЛФ/17-172 ЛФ/17-154
Закрытое акционерное общество "Научно-техническая фирма "Криптон"	ЛФ/17-124
Закрытое акционерное общество "Нижегородский научно-производственный центр современных технологий "Берег-Волна"	ЛФ/17-203
Закрытое акционерное общество "Производственная организация вычислительной техники и средств автоматизации"	ЛФ/07-210
Закрытое акционерное общество "Распределенная общего пользования сеть передачи данных с коммутацией пакетов" (ЗАО РОСПАК)	ЛФ/17-147
Закрытое акционерное общество "Регистратор-Связь"	ЛФ/17-201
Закрытое акционерное общество "Санкт-Петербургский региональный центр защиты информации"	ЛФ/17-162
Закрытое акционерное общество "Синус-Ф"	ЛФ/17-53
Закрытое акционерное общество "Транспорная Клиринговая Палата"	ЛФ/17-93
Закрытое акционерное общество "Центр разработок информационных технологий "Аргонавт"	ЛФ/17-143
Закрытое акционерное общество "Московское отделение Пензенского научно-исследовательского электротехнического института"	ЛФ/17-191 ЛФ/07-192 ЛФ/17-119
Закрытое акционерное общество Тольяттинский региональный центр "Деловая сеть"	ЛФ/17-152 ЛФ/17-153
Коммерческий акционерный банк "Банк Сосьете Женераль Восток"	ЛФ/06-137
Коммерческий банк "Еврофинанс"	ЛФ/06-99
Концерн "Системпром"	ЛФ/14-48

Московский региональный аналитический центр	ЛФ/15-174 ЛФ/05-187
Московский филиал "Мак-Банк"	ЛФ/06-45
Научно-исследовательский институт "Квант"	ЛФ/13-113
Научно-исследовательский институт автоматики (НИИА)	ЛФ/11-55 ЛФ/11-26
Научно-исследовательский институт микроэлектронной аппаратуры "Прогресс"	ЛФ/11-59
Научно-исследовательское предприятие "Аргус", филиал Пензенского НИИ	ЛФ/11-24 ЛФ/12-60
Научно-производственное государственное предприятие "Гамма"	ЛФ/13-101
Нерюнгринский коммерческий банк "НЕРЮНГРИБАНК"	ЛФ/06-138
НПП "Сигнал"	ЛФ/11-70
Общество с ограниченной ответственностью "ТехИнформКонсалтинг"	ЛФ/17-207
Общество с ограниченной ответственностью Фирма "АНКАД"	ЛФ/17-144
Объединение юридических лиц "Депозитарно-расчетный союз"	ЛФ/17-109
Открытое акционерное общество "Банк энергетического машиностроения"	ЛФ/06-195
Открытое акционерное общество "Владимирское конструкторское бюро радиосвязи"	ЛФ/17-142
Открытое акционерное общество "Гипросвязь"	ЛФ/17-156
Открытое акционерное общество "Ижевский мотозавод "Аксион"	ЛФ/17-139
Открытое акционерное общество "Инфотекс"	ЛФ/17-69
Открытое акционерное общество "КБ Импульс"	ЛФ/17-160
Открытое акционерное общество "Научно-производственное предприятие "Звукотехника"	ЛФ/17-141 ЛФ/17-196
Открытое акционерное общество "НИИ Кром"	ЛФ/17-241
Открытое акционерное общество "Объединенный Экспортно-Импортный Банк" ("ОНЭКСИМ БАНК")	ЛФ/06-189
Открытое акционерное общество "Оптима"	ЛФ/17-107
Открытое акционерное общество "Промышленно-строительный банк"	ЛФ/06-171
Открытое акционерное общество "Псковский завод автоматических телефонных станций"	ЛФ/17-242
Открытое акционерное общество "Центральный Московский Депозитарий"	ЛФ/17-70 ЛФ/17-205
Пензенское ПО "Электроприбор"	ЛФ/12-25
Пензенское ПО электронно-вычислительной техники	ЛФ/12-23
Российский Банк Реконструкции и Развития	ЛФ/06-92
Товарищество с ограниченной ответственностью "Инженерный центр "Анкей"	ЛФ/17-65
Товарищество с ограниченной ответственностью "Маском"	ЛФ/17-89
Товарищество с ограниченной ответственностью "Стар"	ЛФ/17-64
Товарищество с ограниченной ответственностью"Витязь-ЛТД"	ЛФ/17-244
Товарищество с ограниченной ответственностью "Пензенское Научно-исследовательское предприятие "Сталл"	ЛФ/17-46
ЦНИИАтоминформ	ЛФ/17-112

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*

Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su

Подписной индекс по каталогу Роспечати **32555**