ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ «ЭЛЕКТРОННОЙ РОССИИ»

Материалы Четвертой межрегиональной научно-практической конференции

2 – 5 июня 2005 г.

г. Ханты-Мансийск

указывают цифру 0,999 (или 99,9%), которую современные АОЛС могут обеспечить на дистанциях в 1–1,5 км.

Следует отметить, что никакое кабельное соединение не обеспечит 100% доступности, а затраты на восстановление поврежденного кабеля достаточно обременительны и по финансовым и по временным составляющим.

Начиная с 2004 года в наиболее энерговооруженных системах используются запатентованные технологии Hybrid Emission и Super Avalanche.

1. Hybrid Emission:

В качестве источников излучения одновременно на разных длинах волн используются некогерентный светодиод с широким спектром излучения, большим углом расходимости и с равномерным распределением энергии в апертуре, и когерентный лазерный диод с существенно меньшей угловой расходимостью. В системах БОКС НПК «Катарсис» это позволяет достигать соотношения энергий в излучаемых лучистых потоках до 3000 раз. При этом оба излучателя используют одну оптическую систему.

Такое сочетание источников обеспечивает:

- одновременную трансляцию излучений в разных окнах прозрачности;
- полную устойчивость системы к воздействиям в условиях сильного ветра и естественных сезонных подвижек зданий (когда есть ветер – нет туманов);
- устойчивость к сцинтилляциям в атмосфере, за счет широкой спектральной характеристики светодиодного источника;
- возможность использования высокоплотного (за счет малых размеров и малой угловой расходимости) излучения лазера именно в сложных погодных условиях (прежде всего в условиях тумана – когда нет ветра и есть естественное рассеяние лазерного излучения).

2. Super Avalanche:

В приемнике используется 2 лавинных фотодиода. Поскольку системы БОКС могут использоваться в очень широком температурном диапазоне (-50 … +50), а зависимость чувствительности лавинных фотодиодов от температуры представляет сложную функцию – специальная компоновка схемы АРУ в приемниках систем БОКС позволяет достигать предельных значений чувствительности во всем температурном диапазоне с одновременным исключением засветки.

Для удобства определения поведения систем БОКС в реальных условиях нашей компанией разработано семейство номограмм, позволяющих определить пороги отказа связи по метеорологическим причинам на различных рекомендованных рабочих дистанциях. Все параметры, рассчитанные теоретически, подтверждены многочисленными инсталляциями. На сегодняшний день отправлено заказчикам около 1500 систем. Оборудование БОКС работает в транспортных сетях всех общероссийских операторов сотовой связи. Подписаны соглашения со многими операторами фиксированной связи. География распространения: от Калининграда до Анадыря и от Дудинки до Владикавказа.

Конопкин Н.И.
технический директор Управления защиты информации
ООО «ПРАЙМ ГРУП», г. Москва

Сертификация и аттестация объектов информатизации по требованиям безопасности информации

Государственным органом, всесторонне регламентирующим деятельность предприятий и организаций по защите информации от технических разведок и от ее утечки по техническим каналам, является Федеральная служба по техническому и экспортному контролю (ФСТЭК России) – правопреемник Государственной технической комиссии при Президенте Российской Федерации.

Впервые о создании ФСТЭК России было объявлено в указе Президента РФ «О системе и структуре федеральных органов исполнительной власти» № 314 от 9 марта 2004 г., которым было начато реформирование органов исполнительной власти России. Но история организации началась гораздо раньше.

С окончанием Второй мировой войны начался невидимый и нигде не афишируемый процесс, который в Советском Союзе называли радиоэлектронной борьбой, а на Западе – радиоэлектронной войной. Иностранные разведки все более и более интересовали новейшие радиоэлектронные средства вероятного противника. Создавались новые системы связи, навигации, радиолокации, управления оружием. И тут же по другую сторону воображаемой «линии фронта» создавались средства постановки помех этим системам. В ответ разрабатывались новые, все более и более помехоустойчивые системы и все более и более изощренные способы их радиоэлектронного подавления, для чего обеим сторонам было жизненно необходимо иметь сведения о новейших разработках противника, технических характеристиках разрабатываемых радиоэлектронных средств (РЭС). Иностранные разведки, и в первую очередь США, начали применять на территории СССР технические средства разведки, скрытно устанавливаемые в дипломатических автомобилях и переносимые в ручной клади. В зданиях и на крышах посольств и консульств в Москве и других городах СССР разворачивались целые разведывательные комплексы. По некото-

рым оценкам, количество информации, добываемой с помощью технических средств, превосходило количество информации, добываемой с помощью агентурной разведки, а ее достоверность была выше в десятки раз.

В оборонной промышленности и в Вооруженных силах СССР принимались энергичные, но разрозненные меры по снижению эффективности иностранных технических разведок (ИТР). Воздействовать на самые опасные – стационарные – средства разведки возможности не было ввиду экстерриториальности посольств, на территориях которых они располагались. Отдельные режимные меры были не всегда эффективны, а различные пространственные, временные и другие ограничения на работу РЭС не всегда были тщательно обоснованы, проработаны и постоянно нарушались ввиду невежества подавляющего большинства эксплуатирующего персонала. Возникла настоятельная необходимость создания единого органа, направляющего и контролирующего всю деятельность по противодействию иностранным техническим разведкам (ПД ИТР). И 18 декабря 1973 года специальным постановлением Совета Министров СССР была создана Государственная комиссия СССР по противодействию иностранным техническим разведкам – Государственная техническая комиссия СССР (Гостехкомиссия СССР).

Под этим наименованием организация просуществовала 18 лет, в течение которых в стране была создана мощная, стройная система противодействия техническим разведкам. Но августовский путч 1991 года и последовавший за этим распад СССР поставили будущее Гостехкомиссии России под удар. В сентябре 1991 года был вынужден уйти в отставку генерал армии Ю.А. Яшин – заместитель министра обороны, бывший в ту пору председателем Гостехкомиссии СССР. Важнейший орган обеспечения безопасности государства едва не был низведен до второразрядного управления Министерства обороны. И только своевременное обращение Ю.А. Яшина к Президенту России и свойственная Б.Н. Ельцину решительность привели к появлению Указа Президента Российской Федерации от 5 января 1992 г. № 9.

Значение данного Указа переоценить невозможно. Он состоял всего из нескольких пунктов и умещался на одной странице, но в нем было главное, в чем нуждалась в тот момент страна: решение о создании на базе Гостехкомиссии СССР Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России), а также указание на обязательность исполнения всех нормативных и руководящих документов бывшей Гостехкомиссии СССР на всей территории России всеми предприятиями и организациями независимо от их организационно-правовой формы и формы собственности.

В дальнейшем Указом Президента Российской Федерации от 19 февраля 1999 г. № 212 было утверждено Положение о Гостехкомиссии

России как о федеральном органе исполнительной власти, осуществляющем межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну.

В соответствии с Указами Президента Российской Федерации от 9 марта 2004 г. № 314 и от 20 мая 2004 г. № 649 Государственная техническая комиссия при Президенте Российской Федерации преобразована в Федеральную службу по техническому и экспортному контролю с передачей ей функций по экспортному контролю Министерства экономического развития и торговли Российской Федерации.

В соответствии с Положением о ФСТЭК России, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, Федеральная служба по техническому и экспортному контролю является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

– обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;

– противодействия техническим разведкам на территории Российской Федерации;

– обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

– осуществления экспортного контроля.

ФСТЭК России в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, приказами и директивами министра обороны Российской Федерации в части, касающейся ФСТЭК России, а также другими нормативными правовыми актами Российской Федерации, касающимися деятельности ФСТЭК России.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными ор-

ганами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

Об уникальности статуса ФСТЭК России говорит то, что только этот орган из всех органов исполнительной власти России, не являющихся федеральными министерствами, согласно Положению, обладает правом законодательной инициативы.

Понятия «сертификация» и «аттестация» в системе руководящих и нормативно-методических документов ФСТЭК России сформулированы и охарактеризованы достаточно чётко:

1. Сертификация – деятельность по подтверждению соответствия средств защиты информации требованиям по безопасности информации.

2. Аттестация – комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по безопасности информации.

Тем не менее отдельные руководители и некоторые сотрудники, отвечающие в организациях за техническую защиту информации, порой путают эти понятия или отождествляют их, что приводит к неточностям и ошибкам в организационно-распорядительной документации организаций. Чтобы избежать недоразумений, предлагаем запомнить и использовать несколько простых правил.

Правило первое. Целью всех процессов, включающих в себя элементы сертификации и аттестации, является обеспечение необходимого уровня защищенности информации в конкретном объекте информатизации (защищенном помещении, персональном компьютере, локальной вычислительной сети), то есть создание объекта, на который может быть выдан аттестат соответствия – документ, посредством которого подтверждается наличие на объекте необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов по защите информации.

Итак, во главе угла – объект и аттестат на объект.

Правило второе. Если по результатам предварительных испытаний делается вывод о необходимости применения технических средств защиты, следует выбирать сертифицированные средства защиты. О сертификатах на свою продукцию заботятся ее производители. Специалисты, принимающие решения о выборе того или иного средства защиты, должны позаботиться лишь о том, чтобы оно имело действующий сертификат.

Итак, сертификат – документ, относящийся не к объекту в целом, но лишь к одному из средств его защиты.

Правило третье. Категорически запрещается проводить закрытые мероприятия с обсуждением конфиденциальной информации в помеще-

ниях или обрабатывать конфиденциальную информацию на компьютерах, на которые не выданы аттестаты.

Правило четвертое. Аттестат соответствия требованиям по безопасности информации может быть выдан даже в том случае, если нет ни одного сертификата, но только тогда, когда по результатам аттестационных испытаний применение сертифицированных средств защиты не является обязательным. Необходимо помнить, что правом выдачи аттестата соответствия обладают только организации, аккредитованные при ФСТЭК России в качестве органов по аттестации в системе сертификации РОСС RU.0001.01БИ00.

Правило пятое. Одного аттестата на помещение достаточно не всегда. Если речь идет о защищенном помещении, в котором разрешается проведение мероприятий с обсуждением конфиденциальной информации и отсутствуют технические средства ее передачи, обработки и хранения, это помещение рассматривается как автономный защищаемый объект информатизации, и на него выдается один аттестат. Если же в этом помещении, например, дополнительно установлен компьютер, на котором обрабатывается конфиденциальная информация, на этот компьютер выдается отдельный пакет аттестационных документов, включающий аттестат.

Здесь есть один небольшой нюанс: надо помнить, что, во-первых, компьютер может быть аттестован только в привязке к конкретному помещению, и только система «компьютер+помещение» имеет право называться «объектом аттестации». Во вторых, в рассматриваемом случае мы должны говорить о сочетании двух взаимодействующих между собой защищенных объектов информатизации: защищенном помещении и объекте вычислительной техники, – и эта особенность должна быть отражена в обоих комплектах аттестационных документов.

Бывают и более сложные случаи. Как определить количество аттестуемых объектов, если в одном помещении находятся несколько автономных ПЭВМ, на которых разрешается обработка конфиденциальной информации, не имеющих между собой физических линий связи?

Еще не так давно теория и практика давали разные толкования этого вопроса. Но сейчас и требования ФСТЭК России, и опыт деятельности органов по аттестации и организаций, эксплуатирующих защищенные объекты информатизации, диктуют нам необходимость рассматривать такую систему как несколько автономных объектов вычислительной техники, размещенных в одном помещении, и на каждый из этих объектов должен оформляться свой собственный пакет аттестационных документов.

Это означает, что на пять отдельных компьютеров, стоящих в одном помещении, должны быть оформлены:

– пять комплектов протоколов и предписаний по результатам лабораторных (стендовых) специальных исследований;

– пять комплектов протоколов и предписаний по результатам контроля защищенности объектов вычислительной техники;
– пять актов о категорировании:
– пять актов классификации;
– пять технических паспортов;
– пять заключений о результатах аттестационных испытаний;
– пять аттестатов соответствия требованиям по безопасности информации.

Такой подход, с одной стороны, позволяет органу по аттестации – упростить процедуру аттестации (особенно – в случае переаттестации части из аттестованных ранее объектов), контролирующим органам – проведение экспертизы представляемой документации и контроля защищенности, а организации, эксплуатирующей аттестованные объекты, – упорядочить их учет, облегчить выполнение требований предписаний на эксплуатацию объектов и избежать излишних затрат на проведение повторной аттестации и избавит от крупных проблем в случае выхода из строя какого-либо отдельного элемента из состава средств вычислительной техники или средств защиты аттестованных объектов.

Конопкин Н.И.
технический директор Управления защиты информации
ООО «ПРАЙМ ГРУП», г. Москва

Решения ООО «ПРАЙМ ГРУП» в области защиты информации

Любая организация обладает огромным объемом информации, которая – по определению – интересует тех, кому как раз иметь эту информацию не следовало бы. О чем идет речь, понятно каждому: уголовные преступные организации интересует финансовое состояние организаций и частных лиц и его надежность, спекулянтов недвижимостью – персональные данные владельцев недвижимости и ситуация на рынке жилья, иностранные разведывательные структуры – состояние экономического и оборонного потенциала страны и конкретного региона, производственные и финансовые возможности того или иного участника рынка и т.п.

Здесь не ставится задача перечислять все информационные ресурсы, которые по тем или иным причинам требуют защиты. Частные организации их определяют самостоятельно исходя из собственных интересов (коммерческая тайна). Нас эта проблема интересует прежде всего применительно к государственному информационному ресурсу, требования по защите которого определены в соответствующих документах, составляющих основу нормативно-правовой базы в области защиты информации. Кроме того, наша страна, как и весь мир, сейчас вплотную приблизилась и стоит перед фактом необходимости защиты персональных данных.

Необходимо четко уяснить, что в эксплуатируемых в большинстве организаций системах и объектах информатизации и связи в ряде случаев присутствует как минимум служебная информация или персональные данные, а в отдельных случаях – информация, составляющая государственную тайну. Организации обязаны принимать меры по защите государственного информационного ресурса от несанкционированного распространения и утечки по любым каналам (а непринятие таких мер карается не только гражданским законодательством – крупными штрафами, но иногда – уголовным законодательством). При надлежащем внимании к этой проблеме и при достаточно скромном финансировании, используя возможности организаций, предлагающих свои услуги в области защиты информации и имеющих необходимый пакет лицензий, любая организация может быть гарантированно защищена от всяческих проблем и неприятностей, связанных с утечкой конфиденциальной информации.

Примеров неожиданной и неприятной утечки информации перед нами предостаточно. «Отличились» не только крупные частные компании, такие, как «Мобильные телесистемы», «Московская городская телефонная сеть» и ряд других, но и такие уважаемые государственные структуры, как Росимущество, ГИБДД МВД России, Московская лицензионная палата, Земельный комитет г. Москвы и др. Очевидно, что невнимание к защите информации приводит к непоправимым последствиям. И, напротив, своевременное предотвращение возможных угроз безопасности информации сводит проблему ее защиты до уровня назойливого, неизбежного, но неопасного спутника в нашем продвижении по пути научно-технического прогресса.

Компания «ПРАЙМ ГРУП», основанная в 1999 г., предлагает организациям и предприятиям различных форм собственности комплексные решения по проектированию и внедрению объектов и систем информатизации и связи, в том числе – в защищенном исполнении. Деятельность «ПРАЙМ ГРУП» по технической защите конфиденциальной информации осуществляется Управлением защиты информации Департамента системных решений на основе следующих лицензий:
– Федеральной службы по техническому и экспортному контролю на деятельность по технической защите информации;
– Федеральной службы по техническому и экспортному контролю на осуществление разработки и производства средств защиты информации;
– Аттестата аккредитации органа по аттестации в системе сертификации средств защиты информации ФСТЭК России;

– Министерства обороны Российской Федерации на деятельность в области создания средств защиты информации;

– Аттестата аккредитации испытательной лаборатории в системе сертификации средств защиты информации Министерства обороны;

– Управления ФСБ России по г. Москве и Московской области на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.

Работы выполняются по следующим направлениям:

1. Проектирование информационных и телекоммуникационных систем в защищенном исполнении.

ООО «ПРАЙМ ГРУП» проводит любые работы по разработке, проектированию, внедрению, испытаниям и техническому сопровождению систем защиты информации в информационных и телекоммуникационных системах, созданием которых занимается наша компания. Это – одна из составных частей того комплексного подхода, который предлагает компания, поскольку, и это понятно, своевременное внедрение систем информационной безопасности в создаваемые информационные системы намного проще и дешевле, чем их внедрение в уже готовые функционирующие системы.

2. Создание защищенных объектов информатизации.

ООО «ПРАЙМ ГРУП» обеспечивает создание защищенных объектов – от нулевого цикла до сдачи «под ключ». Такими объектами могут быть средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы связи и передачи данных), технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), предназначенные для обработки конфиденциальной информации, технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается, а также помещения, предназначенные для ведения конфиденциальных переговоров.

3. Испытания защищаемых объектов информатизации с использованием современных сертифицированных средств программно-аппаратного контроля.

ООО «ПРАЙМ ГРУП» проводит испытания защищенных объектов любой сложности и конфигурации на соответствие требованиям и рекомендациям ФСТЭК России по защите конфиденциальной информации от утечки по техническим каналам и от несанкционированного доступа к ней – от небольших кабинетов до больших актовых залов, от автономных автоматизированных рабочих мест на базе персональных ЭВМ до глобальных автоматизированных систем.

4. Оказание услуг по подбору, поставке, настройке и установке аппаратных и программных средств защиты информации.

В соответствии с требованиями заказчика и разработанной политикой безопасности, специалисты ООО «ПРАЙМ ГРУП» готовы подобрать, установить, поставить, настроить технические средства защиты информации, оказать любую помощь в разработке, создании и вводе в строй подсистем информационной безопасности (ПИБ) эксплуатируемых и создаваемых защищаемых объектов, техническое сопровождение ПИБ в течение гарантийного срока эксплуатации, а также постгарантийное обслуживание.

5. Консалтинг в области информационной безопасности.

При необходимости специалисты ООО «ПРАЙМ ГРУП» помогут разработать весь комплекс нормативно-методической документации, которая должна быть или которую рекомендуется иметь на объекте, проконсультировать сотрудников организации-заказчика по теоретическим и практическим аспектам технической защиты информации, провести обучение специалистов по правилам эксплуатации систем и средств защиты информации.

Актуальность задач обеспечения информационной безопасности как государственных, так и коммерческих организаций, защиты государственных и коммерческих информационных ресурсов возрастает прямо пропорционально растущей информатизации общества. Быть на острие научно-технического прогресса, обеспечить защиту интересов государства в сфере информационной безопасности – общая задача органов государственной власти и управления, правоохранительных структур, государственных предприятий, органов и организаций, осуществляющих деятельность в области защиты информации.