Гостехкомиссия России: точка зрения на техническую защиту информации

Интервью советника председателя Гостехкомиссии России Арнольда Петровича Каландина бюллетеню Jet Info

Советник председателя Гостехкомиссии России Арнольд Петрович Каландин

Расскажите, пожалуйста, об истории и нынешнем статусе Гостехкомиссии России.

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства. Проникая во все сферы деятельности государства, информация приобретает конкретные политические, материальные и стоимостные выражения. На этом фоне все более остроактуальный характер приобретает в последние десятилетия и, особенно в настоящее время, задача обеспечения информационной безопасности Российской Федерации, как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

Защита информации обеспечивается в любом государстве и в своем развитии проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств ее добывания, правового режима в государстве и реальных усилий его по обеспечению защиты информации.

Важным этапом становления и совершенствования такой системы в нашей стране явился период 70-80-х годов. С начала 70-х гг. в разведывательной деятельности ведущих стран мира началось широкомасштабное применение технических средств разведки. 80-е гг., ознаменовавшись бурным научно-техническим прогрессом, особенно в военной области, дали новые импульсы в дальнейшем наращивании возможностей технических средств иностранных разведок: до 70 процентов разведывательной информации добывалось в то время с помощью технических средств.

Сложившаяся обстановка потребовала совершенствования системы мер противоборства с иностранными разведками. Противодействие техническим разведкам стало задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны.

Для организации и координации работ в этой области решением руководства страны 18 декабря 1973 года была создана Государственная техническая комиссия СССР. Возглавил ее тогда Н.В. Огарков.

С созданием Гостехкомиссии начала формироваться система научного обеспечения комплексного противодействия иностранным техническим разведкам. В 1974 году были сформированы концептуальные, организационные, научно-методологические и нормативные основы противодействия иностранным техническим разведкам и развернута большая практическая работа. Появившиеся уже в последнее время свидетельства западных специалистов разведки показывают, что, в целом, в тот период под руководством Гостехкомиссии вся система защиты информации работала достаточно эффективно.

В 80-е годы задачи Гостехкомиссии значительно расширились. Была разработана цельная концепция по противодействию иностранной технической разведке. Совершенствовалась нормативная база, методы и средства контроля.

К началу 90-х годов произошли качественные изменения в военно-политической и научно-технической сферах, заставившие во многом пересмотреть государственную политику в области защиты информации в целом.

Во-первых — информационные технологии принципиально изменили объем и важность информации, циркулирующей в технических средствах ее передачи и обработки.

Во-вторых — в России отошла в прошлое фактическая государственная монополия на информационные ресурсы, в частности, получило конституционное закрепление право гражданина искать, получать и распространять информацию.

В-третьих — прежний административный механизм управления защитой информации стал и невозможен, и неэффективен, в то же время необходимость межведомственной координации в сфере защиты информации объективно возросла.

В-четвертых — завершилась острая военно-политическая конфронтация между СССР и странами НАТО, начавшееся контролируемое сокращение вооружений и развитие мер доверия в военной области потребовало обеспечить разумное сочетание мер открытости и мер по защите государственной тайны.

В-пятых — в связи с усиливающимся включением России в международное разделение труда, укреплением экономических, культурных, гуманитарных контактов с другими государствами многие режимно-ограничительные меры, облегчавшие защиту информации, например, система регионов, закрытых для посещения иностранными гражданами, стали не актуальными.

Наряду с традиционными приоритетами иностранных технических разведок в сферу их интереса в это время все в большей мере вовлекаются вопросы технологий, финансов, торговли, ресурсов, доступ к которым открывается в связи с конверсией, развитием международных интеграционных процессов, широким внедрением компьютерных технологий.

В этих условиях слепое следование оправдавшим себя в прошлом решениям непременно привело бы к ущербу государственных интересов России в военной, политической, экономической и других областях. Требовалось совершенствование сложившейся системы защиты информации, как в организационном плане, так и концептуальных, методологических подходов к защите информации от иностранной технической разведки и от ее утечки по техническим каналам.

Высшими органами государственной власти Российской Федерации был предпринят ряд принципиально важных шагов. В частности, Указом Президента Российской Федерации № 9 в январе 1992 года на базе Гостехкомиссии СССР был создан государственный орган более высокого статуса — Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России). Гостехкомиссия России, являясь органом государственного управления, была призвана проводить единую техническую политику и координацию работ в области защиты информации. Она создавалась с целью обеспечения национальной безопасности народов и территорий Российской Федерации в части приоритетов и защиты информации в области обороны, политики, экономики, науки, экологии, ресурсов и противодействия иностранным техническим разведкам.

Непосредственное подчинение Президенту Российской Федерации обеспечивало независимость Гостехкомиссии России от региональных, ведомственных и корпоративных влияний, гарантировало соответствие ее деятельности высшим государственным интересам.

Создание Гостехкомиссии России означало выход на новый качественный уровень развития не только самой Комиссии, но и всей Государственной системы защиты информации в Российской Федерации, сопровождаемый глубоким принципиальным реформированием государственных механизмов защиты информации в области обороны, политики, экономики, науки, экологии, ресурсов. Это, естественно, потребовало коренной реорганизации всей структуры Гостехкомиссии России, ее рабочего органа — центрального аппарата и проведения соответствующих организационных мероприятий в министерствах и ведомствах.

В соответствии с Указом Президента Российской Федерации от 19 февраля 1999 года № 212 Гостехкомиссия России получила статус федерального органа исполнительной власти, осуществляющего межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа

к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования и по противодействию техническим средствам разведки на территории Российской Федерации.

Гостехкомиссия России является организатором деятельности государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам. Гостехкомиссия России и региональные центры входят в состав государственных органов обеспечения безопасности Российской Федерации. Приказы, распоряжения и указания Гостехкомиссии России, изданные в пределах ее компетенции, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, предприятиями, учреждениями и организациями.

Гостехкомиссию России возглавляет председатель, назначаемый на должность и освобождаемый от должности Президентом Российской Федерации. Председатель Гостехкомиссии России в ходе осуществления межотраслевой координации деятельности по технической защите информации пользуется правами федерального министра. В 1977-1989 годах после Н. В. Огаркова, председателем Гостехкомиссии был В. М. Шабанов, в 1989-1998 годах — Ю. А. Яшин, в 1998-1999 годах — М. П. Колесников. С сентября 1999 года Председателем Гостехкомиссии России назначен генерал-полковник Сергей Иванович Григоров.

В новой обстановке значительно расширился круг решаемых Гостехкомиссией России задач. Деятельность в области защиты информации все более приобретает новый характер, соответствующий демократическим основам открытого общества. Большие изменения произошли в методологии защиты информации. Осуществляется переход от дорогостоящего скрытия заведомо завышенного объема данных к гарантированной защите принципиально важных «узловых точек».

С какими ведомствами взаимодействует Гостехкомиссия России и где проходит разграничительная линия между ними?

В нынешних условиях Гостехкомиссия России целенаправленно отказалась от жесткого директивного руководства, сосредоточив основные усилия на разработке и совершенствовании общей идеологии в сфере защиты информации, оказании помощи — технической, методической и консультативной, всем заинтересованным организациям и учреждениям. При этом Гостехкомиссия России активно взаимодействует в настоящее время со всеми органами государственной власти.

Жизнь подтверждает необходимость соблюдения в вопросах защиты информации принципа сочетания коллегиальности при принятии решений общегосударственного значения с персональной ответственностью за состояние дел по обеспечению защиты информации. Государственная техническая комиссия при Президенте Российской Федерации позволяет наиболее эффективно сочетать в своих решениях эти компоненты, учитывая общегосударственные, национальные интересы страны. С этой целью создана коллегия Гостехкомиссии России.

Членами коллегии Гостехкомиссии России по должности являются руководители федеральных органов исполнительной власти, государственных органов и организаций Российской Федерации. Перечень таких руководителей утверждает Президент Российской Федерации. Состав коллегии Гостехкомиссии России утверждается Правительством Российской Федерации.

Вот перечень руководящих работников федеральных органов исполнительной власти, государственных органов и организаций Российской Федерации, которые входят в состав коллегии по должности:

- Первый заместитель Министра Российской Федерации по атомной энергии;
- Первый заместитель Министра внутренних дел Российской Федерации;
- Первый заместитель Министра Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;
- Заместитель Министра иностранных дел Российской Федерации;
- Первый заместитель Министра науки и технологий Российской Федерации;
- Заместитель Министра экономики Российской Федерации;
- Заместитель Министра юстиции Российской Федерации;
- Заместитель Госкомэкологии России;
- Первый заместитель Министра Российской Федерации по связи и информатизации;
- Первый заместитель директора ФСБ России;
- Заместитель руководителя ФСО России;
- Заместитель директора СВР России;
- Первый заместитель генерального директора ФАПСИ;
- Начальник вооружения Вооруженных Сил Российской Федерации;
- Начальник Главного оперативного управления Генерального штаба Вооруженных Сил Российской Федерации — первый заместитель начальника Генерального штаба Вооруженных Сил Российской Федерации;
- Первый заместитель начальника ГУСПа;
- Заместитель Председателя Банка России;
- Вице-президент Российской академии наук.

Члены коллегии Гостехкомиссии России обладают равными правами при обсуждении рассматри-

ваемых на ее заседании вопросов, а ее решения принимаются большинством голосов присутствующих на заседании и при необходимости оформляются приказом Гостехкомиссии России, подписываемым ее председателем.

Принимаемые решения не являются прерогативой какого-либо одного ведомства, в них учитываются, прежде всего, интересы государства, общества и личности. Этим полностью исключается монополия в принятии решений по важнейшим вопросам обеспечения национальной безопасности. В случае несогласия с принятым решением члены коллегии Гостехкомиссии России вправе высказать свое мнение, которое председатель докладывает Президенту Российской Федерации. Члены коллегии также могут сообщить свое мнение Президенту Российской Федерации.

В случае необходимости для участия в заседаниях коллегии Гостехкомиссии России могут приглашаться представители федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, руководители предприятий, учреждений и организаций.

Особое место занимает международное сотрудничество в области технической защиты информации. Это одно из основных направлений деятельности Гостехкомиссии России. Здесь на повестке дня — координация национальных законодательств в сфере защиты информации на базе уже принятого «Рекомендательного законодательного акта о принципах правового регулирования информационных отношений в государствах — участниках Межпарламентской ассамблеи».

Идея сотрудничества России со странами СНГ в области защиты информации нашла свое воплощение в заключенных межправительственных соглашениях с республиками Казахстан, Украина и Белоруссия. Руководство Гостехкомиссии России и ее представители участвуют в международных симпозиумах и конференциях, принимают непосредственное участие в подготовке межправительственных соглашений в области защиты информации со странами как «ближнего» так и «дальнего» зарубежья.

В 1998 году был принят закон о лицензировании отдельных видов деятельности. Изменил ли он положение Гостехкомиссии России?

Пунктом 3 статьи 19 Федерального закона «О лицензировании отдельных видов деятельности» определено, что установленный данным Федеральным законом порядок лицензирования отдельных видов деятельности не распространяется на порядок лицензирования конкретных видов деятельности, лицензирование которых установлено иными, ранее вступившими в силу, федеральными законами.

Принимая во внимание, что лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны проводится в соответствии с Законом Российской Федерации «О государственной тайне», Законом Российской Федерации «Об информации, информатизации и защите информации», вступившими в силу раньше, и постановлением Правительства Российской Федерации 1995 г. № 333, порядок лицензирования в целом не изменился.

Федеральный Закон «О лицензировании отдельных видов деятельности» устанавливает общий порядок проведения лицензирования в Российской Федерации. В настоящее время приводятся в соответствие с данным законом соответствующие положения о лицензировании.

Введение в 1994 году в действие механизма Государственного лицензирования явилось прогрессивным шагом и способствовало улучшению положения дел в области защиты информации в сложных экономических условиях. Практика пятилетней работы по лицензированию этой деятельности показывает, что Гостехкомиссией России был найден эффективный механизм управления деятельностью предприятий в условиях их разгосударствления.

Можно ли оценить, какую долю от общего объема работ по сертификации, проводимой Гостехкомиссией России, составляют программные средства защиты информации?

За период с августа 1993 года по настоящее время в Системе сертификации Гостехкомиссии России прошли сертификационные испытания и имеют Сертификат соответствия более 270 средств защиты информации. В том числе по типам:

- технические средства защиты информации — 22%;
- защищенные технические средства обработки информации — 16%;
- технические средства контроля эффективности мер защиты — 5%;
- средства защиты от несанкционированного доступа к информации — 47%;
- защищенные программные средства обработки информации — 7%;
- программные средства контроля защищенности информации — 3%.

Таким образом, видно, что программные средства защиты информации от несанкционированного доступа в настоящее время превалируют на рынке услуг по защите информации и составляют более 50%.

Техническая защита информации развивается быстрыми темпами. Что делается в Гостехкомиссии России, чтобы обеспечить соответствие современному уровню?

Следует отметить, что Гостехкомиссия России, понимая настоятельную необходимость повы-

шения технической защиты информации министерств, ведомств и организаций, проводит целенаправленную техническую политику по организации сертификации современных средств защиты информации, программных средств, выполненных в защищенном исполнении, в том числе зарубежного производства.

Кроме того, развитие системы сертификации сдерживает отсутствие ряда нормативных документов, регламентирующих сертификационные испытания средств защиты информации. Прежде всего, это относится к сертификационным испытаниям общесистемного и прикладного программного обеспечения, особенно операционных систем и систем управления базами данных, сертификации цифровых АТС.

Понимая насущную необходимость разработки таких документов, Гостехкомиссия России постоянно работает над этим вопросом. Под ее руководством разработаны и разрабатываются Руководящие документы, определяющие требования, предъявляемые к новым средствам защиты информации.

Сухие цифры статистики говорят следующее.

На начало 1996 года имелись 5 Руководящих и 4 нормативных документа.

В 1996 году организована разработка и принят Руководящий документ.

В 1997 году организована разработка и приняты 2 Руководящих и 1 нормативный документ. При этом принятие Руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», позволило не только упорядочить требования по защите информации, предъявляемые к межсетевым экранам, но и сопоставлять защитные свойства сертифицированных изделий этого вида. Область применения таких экранов довольно широка — от защиты информации в ЛВС, до защиты информации отдельных рабочих мест. Следует отметить, что в настоящее время на рынке сертифицированной продукции появились сертифицированные межсетевые экраны высокого класса защищенности («Застава», «AltaVista Firewall 97» — 3 класс защищенности, «Застава-Джет» — 2 класс защищенности), обеспечивающие надежную защиту информационных ресурсов от несанкционированного доступа извне.

На наш взгляд, следовало бы особо отметить появление Руководящего документа «Защита информации. Специальные защитные знаки. Классификация и общие требования», устанавливающего классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки.

В 1998 году организована разработка 7 проектов Руководящих документов. Это достаточно объемные документы, поэтому работа над ними еще продолжается.

В 1999 году уже принят Руководящий документ — «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей».

В этом же году также организована разработка нормативного документа «Специальные требования и рекомендации по защите конфиденциальной информации», алгоритма фиксации (контроля) исходного состояния программного обеспечения средств вычислительной техники и автоматизированных систем при проведении сертификационных испытаний и программной реализации этого алгоритма для их последующей аттестации, проектов типовых профилей защиты автоматизированных систем критических приложений на основе проекта международного стандарта «Общие критерии безопасности информационных технологий».

В дополнение к имеющейся нормативно методической базе в настоящее время разрабатываются 7 типовых методик и методических рекомендаций:

- «Сертификационные испытания межсетевых экранов на соответствие требованиям Руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- «Требования к сертификационным испытаниям сетевых помехоподавляющих фильтров и методические рекомендации по проведению испытаний»;
- «Сертификационные испытания активных средств защиты информации от утечки по каналу побочных электромагнитных излучений»;
- «Сертификационные испытания систем телевизионного наблюдения по требованиям безопасности информации»;
- «Типовые программы и методики сертификационных испытаний программных и программно-аппаратных средств защиты от несанкционированного доступа к информации»;
- «Специальные исследования технических средств обработки информации на побочные электромагнитные излучения и наводки»;
- «Требования по оформлению материалов сертификационных испытаний».

Еще один вопрос на близкую тему. Информационные технологии развиваются быстро. Есть ли в Гостехкомиссии система повышения квалификации персонала испытательных лабораторий, органов по сертификации и аттестации? Нужна ли такая система?

Вопросы защиты информации требуют наличия в государственных и других структурах, являющихся владельцами или пользователями информа-

ции ограниченного распространения, высокопрофессиональных специальных служб, укомплектованных компетентными специалистами в области защиты информации.

В настоящее время подготовка специалистов по защите информации стала одним из важнейших направлений деятельности Гостехкомиссии России. Во исполнение решения Гостехкомиссии России от 20 марта 1990 года создана стройная, хорошо продуманная, нашедшая большую поддержку в министерствах и ведомствах, система подготовки и переподготовки кадров по проблеме комплексной защиты информации. Работа этой системы проводится при методическом руководстве Гостехкомиссии России.

В учебных заведениях, входящих в систему подготовки кадров в области защиты информации и противодействия техническим разведкам за последние 5 лет прошли первичную подготовку, переподготовку и усовершенствовали свои знания около 4500 человек.

В настоящее время ведущими среди учебных заведений, осуществляющих подготовку и переподготовку кадров в области защиты информации, являются МИФИ, РГГУ, Военный институт радиоэлектроники, Межотраслевой специальный учебный центр при Минатоме России.

Важной задачей в этом плане является для нас перспектива подготовки специалистов в области защиты информации для стран СНГ. Так, в настоящее время ведется проработка данного вопроса специалистами Гостехкомиссии России и Республики Казахстан, соответствующие запросы поступали и от других стран СНГ.

Необходимо также упомянуть систему конференций, регулярных семинаров и сборов с представителями испытательных лабораторий и органов по сертификации. На этих семинарах идет активный обмен опытом, изучение новых руководящих документов, поднимаются и обсуждаются серьезные проблемные вопросы. Решения таких семинаров, как правило, ложатся в основу перспективных планов развития системы сертификации Гостехкомиссии России. За последние годы проведены 3 конференции, 8 семинаров и 4 сбора. Среди них наиболее важными можно назвать такие как международная конференция «Безопасность информации», международный конгресс «Телекоммуникации в аспекте национальной безопасности, перспективы развития информационно-телекоммуникационной инфраструктуры», региональная конференция по вопросам сертификации и защиты информации, традиционные семинары с руководителями испытательных лабораторий. Кроме того регулярно проводятся семинары с руководителями подразделений защиты информации министерств и ведомств и региональные семинары по вопросам защиты информации.

Хотелось бы, чтобы Гостехкомиссия не только выдвигала требования, но и помогала организациям обеспечивать техническую защиту информации. Есть ли наработки в этом направлении?

За время существования системы сертификации средств защиты информации Гостехкомиссией России осуществлено методическое руководство разработкой более 30 средств защиты от несанкционированного доступа к информации, в том числе:

- Программный комплекс защиты информации от НСД «Страж»;
- Система защиты локальной вычислительной сети «SECRET NET»;
- Программное средство защиты информации от НСД «СНЕГ» в АС;
- Программно-аппаратный комплекс «Аккорд»;
- Программно-аппаратный комплекс защиты информации от НСД в ЛВС Novel Netware (v.3.11), Windows for Workgroups (v.3.11);
- Программный продукт SKIP для регулирования доступа на интерфейсе локальная/глобальная сеть для Windows 3.11 и Windows 95;
- Система управления базами данных «ЛИНТЕР»;
- Операционная система МС ВС;
- Интегрированная система охранной сигнализации и контроля доступа «AS-101»;
- Базовый программно-технический комплекс «Холст»;
- Вычислительный комплекс «ЮНИНТ»;
- Межсетевой экран «Застава»;
- Программное средство защиты информации от вторжения компьютерных вирусов «AVP Евгения Касперского» и другие.

Гостехкомиссия России оказывает практическую помощь в организации защиты информации на объектах. Так, специалисты Гостехкомиссии России совместно с Банком России приняли участие в разработке нормативно-правовых основ, организационной структуры и предложений по организации системы защиты государственной тайны в коммерческих банках Российской федерации, подготовили со специалистами фирмы «ЛАНИТ» для использования в кредитно-финансовых учреждениях концепции обеспечения безопасности информации. Большая работа была проведена по разработке ведомственных норм и типовых требований по обеспечению технической защиты информации при проектировании и строительстве объектов Центрального Банка Российской Федерации автоматизированной информационной системы Пенсионного фонда Российской Федерации

Как Вы относитесь к идее организации центра реагирования на нарушения технической защиты информации? Какова могла бы быть роль Гостехкомиссии в таком центре?

Вопрос довольно сложный. Дать однозначный ответ на него трудно. С одной стороны существует международная практика таких центров. Есть такие

центры и в России, правда созданные на общественных началах. Гостехкомиссии России также поступали предложения принять участие в таких проектах, в частности, от Российского научно-исследовательского института общественных сетей (РосНИИРОС).

Вместе с тем, Гостехкомиссия России пока очень настороженно относится к их созданию. Объясняется это тем, что кроме положительного эффекта такие центры могут принести и отрицательные явления, явившись своего рода «школой» для новых хакеров. Информация о нарушениях систем безопасности должна содержать конкретные условия объекта и способов преодоления систем защиты. В противном случае простая констатация факта нарушения пользы не принесет, а может только повредить имиджу и деловой репутации той или иной информационной системы. Факты нарушений систем безопасности, безусловно, должны подвергаться детальному анализу с целью выявления ошибок систем зашиты и поиска путей их устранения. Но, по нашему мнению, вопросами сбора и анализа информации о технических нарушениях защиты должны заниматься государственные органы, а сама информация о таких нарушениях не должна быть слишком общедоступной. По сути дела, такая информация формирует модель угроз нападения на конкретные информационные сети.

Другое дело разработанные на основе обобщенных и проанализированных сведений о нарушениях рекомендации по защите информации, безусловно, должны быть известны собственникам информационных систем.

Некоторые сертификаты, выданные Гостехкомиссией России, вызывают вопросы. В одних случаях отсутствовали исходные тексты, в других сертификация выполнялась в слишком короткие сроки, иногда оценивались продукты, содержащие криптографические компоненты. Можете ли Вы это прокомментировать?

Во-первых, сразу о криптографических элементах систем защиты информации. Гостехкомиссия России в 1995 году в Госстандарте России зарегистрирована система сертификации средств защиты по требованиям безопасности информации № РОСС RU 0001.01БИ00. В ней предусматривается сертификация программных, программно-аппаратных и аппаратных средств защиты информации. Перечень средств, подлежащих сертификации в данной системе, введен в действие в январе 1996 года. Средства криптографической защиты информации в этот перечень не входят.

При проведении сертификационных испытаний проверяется соответствие средств защиты информации требованиям ГОСТ 29339-92 «Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники»; ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники»; ГОСТ Р 50752-95 «Средства вычислительной техники. Защита от несанкционированного доступа (НСД) к информации», вышеперечисленных Руководящих документов Гостехкомиссии России и ряда других документов.

Причем, при присвоении соответствующего класса защищенности, наличие элементов криптографии в средствах защиты принимается во внимание лишь в том случае, если имеется соответствующий сертификат системы сертификации средств криптографической защиты информации (СКЗИ) № РОСС RU 0001.03001. В противном случае элементы криптографической защиты рассматриваются как дополнительные средства защиты и не учитываются при определении класса защищенности. Существуют средства разграничения доступа и защиты от НСД, которые не используют криптографические преобразования. Однако они успешно выполняют свои функции и широко применяются в государственных, банковских и коммерческих структурах.

Сертификат Гостехкомиссии России подтверждает соответствие средства защиты информации нормативным документам и гарантирует выполнение всех оговоренных в присвоенном классе защищенности функций (с предусмотренными в сертификате ограничениями организационного характера).

Теперь о сроках проведения сертификационных испытаний. Действительно эти сроки колеблются в достаточно широких пределах. Это объясняется и уровнем подготовки специалистов испытательных лабораторий, и наличием в этих лабораториях автоматизированных систем анализа, и языком написания программ, и сложностью этих программ. Кроме того, при проведении испытаний по определенным классам защиты достаточно оценить и провести тестирование только ядра безопасности, что также может значительно сократить объемы и сроки тестирования. Надо также учитывать и тот факт, что еще до момента проведения сертификационных испытаний, испытательными лабораториями проводится этап предварительного анализа и ознакомления с предлагаемым продуктом, который может длиться довольно большое время, но не входит в период сертификационных испытаний. Поэтому говорить о коротких сроках проведения сертификационных испытаний того или иного программного продукта без учета конкретной технологии сертификации, по меньшей мере, не корректно.

И, наконец, об исходных текстах. Проведение сертификации для программных средств защиты информации достаточно высокого класса защиты, а также по требованиям некоторых руководящих документов, например, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», требует обязательного анализа исходных кодов программного продукта. Этот факт фиксируется в программе и методике про-

ведения сертификационных испытаний и неукоснительно соблюдается испытательными лабораториями. Однако в некоторых случаях, о которых говорилось ранее, достаточно фрагментарного изучения исходных кодов ядра безопасности системы защиты. Результаты такого анализа фиксируются в протоколах испытаний и только при наличии таких протоколов, принимается решение о выдаче сертификата. Во всех необходимых случаях такой анализ проводился.

В то же время нежелание некоторых зарубежных разработчиков программных средств предоставить на сертификационные испытания исходные тексты программного обеспечения, а также ряд ограничений на поставку исходных текстов со стороны законодательства США существенно затрудняют сертификацию, а часто делают ее невозможной. Сказанное, в первую очередь, относится к общесистемным программным средствам и цифровым АТС, сложность программного обеспечения которых не позволяет сделать заключения о его безопасности в результате испытаний по методу «черного ящика».

А что делать, если сам сертификат все-таки вызывает сомнения или при эксплуатации средств защиты в них обнаружены «дыры»?

В настоящее время Гостехкомиссией России в связи с участившимися случаями подделки сертификатов, принято решение о введении специальных защитных знаков для защиты сертификатов Гостехкомиссии России и выпускаемой продукции от подделки. Начиная с Сертификата № 230, все сертификаты снабжены таким знаком, а продукция маркируется аналогичным знаком.

Для этих целей используются специальные защитные знаки, предназначенные для подтверждения подлинности сертификатов не ниже 6 класса защиты согласно Руководящего документа «Защита информации. Специальные защитные знаки. Классификация и общие требования», которые прошли сертификационные испытания. Разработана и утверждена «Инструкция о порядке маркирования сертификатов, их копий, единичных экземпляров, ограниченных партий и серийно выпускаемых средств защиты информации, прошедших испытания в Системе сертификации средств защиты информации по требованиям безопасности».

Такие защитные знаки позволяют визуально определить любому пользователю подлинность сертификата. В сомнительных случаях подлинность сертификата может быть подтверждена инструментально, с применением специальных контрольных приборов. Для этого необходимо обратиться непосредственно в Гостехкомиссию России.

Кроме того, в Гостехкомиссии России хранятся все экземпляры подлинных сертификатов. Поэтому со всеми вопросами можно так же обращаться в Гостехкомиссию России.

Если же возникают вопросы относительно выполнения средствами защиты своих заявленных функций или другие претензии к работе испытательных лабораторий, органов по сертификации и производителей средств защиты, то для этих целей вместе с созданием системы сертификации, был создан и Апелляционный совет, возглавляемый заместителем Председателя Гостехкомиссии России. В своей деятельности Совет руководствуется Положением о сертификации средств защиты информации по требованиям безопасности информации и законодательством Российской Федерации по вопросам сертификации продукции и услуг.

Апелляционный совет рассматривает претензии на основании надлежащим образом оформленного заявления, в котором указывается суть вопроса. Заявление подписывается предъявителем претензий. В исключительных случаях основанием для рассмотрения на Апелляционном совете вопросов деятельности испытательных лабораторий и органов по сертификации могут служить сообщения в средствах массовой информации либо обращения в органы государственной власти, связанные с такой деятельностью. Решение о рассмотрении таких вопросов принимается руководителем федерального органа по сертификации.

В состав Апелляционного совета с правом решающего голоса входят по должности руководители органов по сертификации. Дополнительно в его состав с правом решающего голоса могут включаются руководители испытательных лабораторий, области аккредитации которых соответствует рассматриваемым вопросам.

Рассматриваются претензии по несоответствию специальных свойств сертифицированной продукции требованиям руководящих документов, на соответствие которым эта продукция проходила сертификацию и условиям выданных сертификатов. Претензии о несоответствии специальных свойств сертифицированной продукции, выходящие за рамки сертификационных испытаний, проведенных в соответствии с требованиями руководящих документов, не принимаются. Претензии рассматриваются при наличии оформленных установленным порядком в соответствии с Арбитражным процессуальным кодексом Российской Федерации письменных доказательств несоответствия сертифицированной продукции требованиям нормативных документов и условиям выданных сертификатов. Устные заявления претензий не допускаются.

Претензии рассматриваются на заседании Апелляционного совета в ходе дискуссии на основе состязательности и равноправия сторон. Обязанность доказательства претензий лежит на стороне, предъявившей их. По окончании заседания оформляется Постановление Апелляционного совета по рассматриваемому вопросу, в котором отражается обоснованность и доказательность предъявленных претензий, решение Апелляционного совета и определяются меры по устранению претензий.

Если не секрет, какие наиболее интересные сертификационные работы ведет в настоящее время Гостехкомиссия России?

Все работы по сертификации средств защиты информации очень интересны. В частности, Гостехкомиссией России начаты сертификационные испытания средств защиты от несанкционированного доступа и подделки документов, основанные на оптико-химических технологиях.

Активно ведутся переговоры с крупнейшими иностранными производителями программных продуктов по сертификации их средств. К числу таких фирм относятся Microsoft, Novell, Oracle. В текущем году планируется сертификация операционной системы Windows-NT, системы управления базами данных Oracle, сетевой операционной системы Novell Intraware.

Как организована процедура аттестации объектов?

Аттестация объектов информатизации является заключительной стадией перед выдачей разрешения на обработку на нем информации ограниченного доступа.

Система аттестации объектов информатизации устанавливает основные принципы, организационную структуру, порядок проведения аттестации, а также порядок контроля и надзора за эксплуатацией аттестованных объектов информатизации. Она разработана в соответствии с законами Российской Федерации «О сертификации продукции и услуг» и «О государственной тайне», «Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», «Положением о сертификации средств защиты информации по требованиям безопасности информации», «Системой сертификации ГОСТ Р».

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является Гостехкомиссия России.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем конфиденциальности и на период времени, установленными в «Аттестате соответствия».

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Аттестация проводится органом по аттестации в установленном порядке в соответствии со схемой, выбираемой на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

В ходе этого процесса компетентные специалисты убеждаются, что системы защиты информации, установленные на конкретном объекте, соответствуют условиям их эксплуатации, организационные ограничения на объекте выполнены, система защиты информации настроена и установлена с соблюдением правил и работоспособна.

Аттестация проводится специально уполномоченными органами — Органами по аттестации объектов информатизации. Органы по аттестации аккредитуются Гостехкомиссией России. Правила ак-

кредитации определяются действующим в системе «Положением об аккредитации органов по аттестации объектов информатизации по требованиям безопасности информации». Каждый такой орган имеет лицензию Гостехкомиссии России на право выполнения работ в области защиты информации и Аттестат аккредитации с уникальным регистрационным номером. Виды работ, которые он может выполнять указываются в области аккредитации, являющейся приложением к Аттестату аккредитации. В своей деятельности органы по аттестации руководствуются нормативно-методическими документами Гостехкомиссии России. Сам аттестат соответствия утверждается руководителем органа по аттестации объектов информатизации, который и несет юридическую и финансовую ответственность за качество проведенных работ. Кроме того, органы по аттестации несут ответственность за обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

К выполнению конкретных видов работ при аттестации объектов информатизации органами по аттестации могут привлекаться организации, имеющие лицензию Гостехкомиссии России на право выполнение работ в области защиты информации по п. 2 перечня работ (контроль защищенности информации ограниченного доступа, аттестация средств и систем на соответствие требованиям по защите), но не имеющие Аттестата аккредитации. В этом случае ответственность за качество выполнения работ несет привлекающий орган по аттестации и организация, непосредственно выполняющая работы.

Специализированные штатные подразделения, предназначенные для защиты конфиденциальной информации предприятий и организаций, которые не оказывают услуги сторонним организациям и, соответственно не имеют лицензии Гостехкомиссии России, могут также быть аккредитованы как органы по аттестации объектов информатизации. Однако их полномочия распространяются только на объекты этого предприятия, а ответственность в этом случае в равной степени несут руководитель предприятия и руководитель этого подразделения. Для таких подразделений, осуществляющих защиту государственной тайны, наличие соответствующих лицензий обязательно.

Как Гостехкомиссия контролирует выполнение требований действующего законодательства и собственных решений? Были ли случаи отзыва лицензий, сертификатов или свидетельств об аттестации?

В силу предоставленных Президентом Российской федерации полномочий, Гостехкомиссии России осуществляет в пределах своей компетенции контроль за состоянием работ по технической защите информации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях, а также организует проведение радиоконтроля за соблюдением установленного порядка передачи служебных сообщений должностными лицами предприятий, учреждений и организаций, выполняющими работы, связанные со сведениями, составляющими государственную или служебную тайну, при использовании открытых каналов радио- и радиорелейных, тропосферных и спутниковых линий связи.

Указом Президента Российской Федерации 1999 года № 212 определено, что Гостехкомиссия России имеет право не только осуществлять контроль за соблюдением федерального законодательства о технической защите информации и требований руководящих и нормативно-методических документов Гостехкомиссии России, но и контролировать с применением технических средств эффективность защиты государственных и промышленных объектов, информационных систем, средств и систем связи и управления органов государственной власти.

По результатам контроля, в случае выявления нарушений норм и требований, касающихся технической защиты информации, Гостехкомиссия России имеет право выдавать предписания на приостановление работ на объектах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций. Кроме того, на заседаниях коллегии Гостехкомиссии России могут быть заслушаны должностные лица, ответственные за организацию технической защиты информации. Для этого в составе Гостехкомиссии России имеются специальные региональные подразделения.

Контроль и надзор за полнотой и качеством работ, проводимых предприятиями и организациями, имеющими лицензию Гостехкомиссии России на право оказания услуг по защите информации, осуществляется Центральным аппаратом Гостехкомиссии России и лицензионными центрами, проводившими экспертизу в ходе плановых проверок состояния защиты информации у потребителей, воспользовавшихся услугами лицензиатов или по их рекламациям. Лицензиаты ежегодно представляют отчет о выполненных работах.

Механизм отзыва лицензий и сертификатов, выданных Гостехкомиссией России предусматривается соответствующими положениями. Отзыв лицензии возможен по решению судебного органа на основании представления Гостехкомиссии России. Решение об отзыве сертификата может быть принято Председателем Гостехкомиссии России. Для этого должны быть достаточно веские и обоснованные причины.

За все время случаев отзыва лицензий или сертификатов не отмечалось, хотя приостановка действия лицензий и сертификатов до устранения отмеченных нарушений имела место.

Доверенные центры как звено системы обеспечения безопасности корпоративных информационных ресурсов

Виктор Горбатов
Ольга Полянская
Московский государственный
инженерно-физический институт
(технический университет)

1. Введение

К важнейшим задачам поддержания безопасности относятся идентификация пользователей, соблюдение конфиденциальности сообщений, управление доступом к секретным документам. Устанавливая контакт, стороны, обменивающиеся электронными сообщениями или документами, должны быть полностью уверены в «личности» партнера и твердо знать, что их документы — тайна для третьих лиц. Сегодня уже существуют индустриальные решения этих задач, центральная роль в них принадлежит криптографии.

После того как шифрование с открытыми ключами приобрело популярность, стала вырисовываться потребность в цифровых сертификатах. Сертификат и соответствующий ему секретный ключ позволяют идентифицировать их владельца. Универсальное применение сертификатов обеспечивает стандарт Международного Телекоммуникационного Союза X.509, который является базовым и поддерживается целым рядом протоколов безопасности.

Стандарт X.509 задает формат цифрового сертификата. Основными атрибутами сертификата являются имя и идентификатор субъекта, информация об открытом ключе субъекта, имя, идентификатор и цифровая подпись уполномоченного по выдаче сертификатов, серийный номер, версия и срок действия сертификата, информация об алгоритме подписи и др. Важно, что цифровой сертификат включает в себя цифровую подпись на основе секретного ключа доверенного центра (Certificate Authority, CA). В настоящее время не существует общепризнанного русского аналога термина, который берет начало в области шифрования с открытыми ключами, — Certificate Authority. Это понятие получило множество совершенно разных названий: служба сертификации, уполномоченный по выпуску сертификатов, распорядитель сертификатов, орган выдачи сертификатов, доверенный центр, центр сертификации, сертификатор и т.д. Подлинность сертификата можно проверить с помощью открытого ключа CA.

Однако одного наличия сертификата недостаточно. Защищенный обмен сообщениями, надежная идентификация и электронная коммерция невозможны без инфраструктуры с открытыми ключами (Public Key Infrastucture, PKI). PKI служит не только для создания цифровых сертификатов, но и для хранения огромного количества сертификатов и ключей, обеспечения резервирования и восстановления ключей, взаимной сертификации, ведения списков аннулированных сертификатов и автоматического обновления ключей и сертификатов после истечения срока их действия. Продукты и услуги, входящие в инфраструктуру с открытыми ключами, предлагаются на рынке целым рядом компаний. Большинство компаний, начинающих использовать технологию PKI, из двух путей выбирают один: они либо создают собственный орган выдачи сертификатов, либо предоставляют это сделать другим компаниям, специализирующимся на услугах PKI, например, VeriSign и Digital Signature Trust. Как правило, создание собственного доверенного центра предполагает выработку и обнародование правил организации сертификации, установку серверов управления сертификатами и серверов каталогов.

В последнее время в развитых странах банки, университеты, правительственные учреждения начали выдавать сотрудникам цифровые сертификаты, которые позволяют отдельным лицам шифровать сообщения электронной почты и электронные документы, а также снабжать их цифровой подписью. По прогнозам специалистов, цифровые сертификаты как способ электронной идентификации получат распространение в корпоративных сетях в течение ближайших двух лет. Со временем создание и распространение цифровых сертификатов должно стать одним из самых важных процессов защиты корпоративных информационных ресурсов, организации безопасного электронного документооборота и защищенного обмена сообщениями.

2. Основные понятия технологии цифровых сертификатов

2.1. Терминология

1. **Сертификат.** Цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Он содержит определенную, цифровым образом подписанную информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название доверенного центра и т.д.

2. **Выпуск сертификата** — генерация сертификата и уведомление пользователя, зафиксированного в нем, о подробном содержании этого сертификата.

3. **Аннулирование сертификата** — это признание сертификата недействительным в пе-

риод его действия в случаях компрометации секретного ключа или изменения атрибутов сертификата с момента его выпуска (например, при изменении имени пользователя).

4. **Список аннулированных сертификатов (CAC)** — список недействительных сертификатов, в большинстве случаев генерируется доверенным центром.

5. **Подписчик (абонент) сертификата** — лицо, которое получает сертификат, выпущенный доверенным центром.

6. **Приостановление сертификата** — временное аннулирование сертификата в период его действия.

7. **Пользователь сертификата** — лицо, которое использует сертификат, например, подписчик сертификата или доверенная сторона.

8. **Сертификация** — это процесс генерации сертификатов для физических и юридических лиц, оборудования и т.д.

9. **Доверенный центр (ДЦ)** — доверенное лицо (физическое или юридическое), которое выпускает, публикует, аннулирует сертификаты, приостанавливает их действие.

10. **Правила организации сертификации** — документ, который устанавливает процедуры сертификации в соответствии с политикой конкретного ДЦ. Правила организации сертификации раскрываются всем лицам, внешним по отношению к ДЦ, в том числе пользователям.

11. **Взаимная (перекрестная) сертификация** — двусторонний процесс сертификации двух доверенных центров.

12. **Регистрационный центр (РЦ)** — лицо (физическое или юридическое), которое с санкции ДЦ выполняет функции аутентификации в процессе выпуска или аннулирования сертификата. Регистрационный центр не выпускает сертификаты и не ведет списки аннулированных сертификатов.

13. **Доверяющая сторона** — лицо, которое получает сертификат и полагается на него при совершении сделок или обмене сообщениями. Доверяющей стороной может быть не только подписчик.

14. **Архив** — система хранения сертификатов и списков аннулированных сертификатов.

15. **Иерархия доверия** — система проверки цифровых сертификатов. Каждый сертификат связан с сертификатом подписи того субъекта, который снабдил его цифровой подписью. Так, сертификат абонента связан с сертификатом ДЦ низшего уровня, который, в свою очередь, связан с сертификатом ДЦ более высокого уровня и так далее до ДЦ высшего уровня. Следуя по цепочке доверия до известной доверенной стороны, можно убедиться в действительности сертификата.

2.2. Инфраструктура с открытыми ключами

Инфраструктура с открытыми ключами (PKI) — это комплексная система, обеспечивающая все необходимые сервисы для использования технологии с открытыми ключами. Цель PKI состоит в управлении ключами и сертификатами, посредством которого корпорация может поддерживать надежную сетевую среду. PKI позволяет использовать сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, функционирующих в среде с открытыми ключами.

Эффективная PKI должна включать следующие элементы:

- доверенный центр;
- архив сертификатов;
- систему аннулирования сертификатов;
- систему создания резервных копий и восстановления ключей;
- систему поддержки невозможности отказа от цифровых подписей;
- систему автоматической корректировки пар ключей и сертификатов;
- систему управления «историей» ключей;
- систему поддержки взаимной сертификации;
- клиентское программное обеспечение, взаимодействующее со всеми этими подсистемами безопасным, согласованным и надежным способом.

2.3. Сервисы PKI

2.3.1. Сервисы управления сертификатами

Сервисы управления сертификатами — это сервисы, образующие ядро инфраструктуры с открытыми ключами. К ним относятся:

(1) Выпуск сертификата.

Сертификаты выпускаются для пользователей (физических и юридических лиц), для доверенных центров, находящихся на более низких уровнях иерархии доверия, а также для других доверенных центров в случае взаимной сертификации.

(2) Аннулирование сертификата.

Если пользователь теряет свой секретный ключ, если ключ похищается или компрометируется, или есть вероятность наступления таких событий, действие сертификата должно быть прекращено. После получения подтверждения

запроса пользователя об аннулировании сертификата ДЦ уведомляет об аннулировании все заинтересованные стороны, используя список аннулированных сертификатов (CAC). Аналогично аннулированию осуществляется приостановление действия сертификата. Оно заключается в однократной отмене сертификата на определенный период времени в течение срока его действия. После этого действие сертификата возобновляется автоматически или же сертификат аннулируется. Приостановление действия сертификата осуществляется в тех ситуациях, когда невозможно установить подлинность лица, обращающегося с запросом об аннулировании.

(3) Публикация сертификата.

Выпущенный однократно сертификат включается в каталог (в соответствии со спецификациями стандарта X.500 или иными требованиями), чтобы третьи стороны могли иметь к нему доступ. В одних случаях каталог контролируется доверенным центром, в других — третьей стороной.

Доступ к каталогу может быть ограничен. Если необходимо соблюдение прав приватности абонентов, применяются профилактические меры для защиты от лиц, не имеющих полномочий доступа.

(4) Хранение сертификата в архиве.

Выпускаемые сертификаты и списки аннулированных сертификатов хранятся в архиве длительное время. Это делается потому, что заверенный цифровой подписью документ продолжает свое существование и по истечении срока действия сертификата, следовательно, сертификаты с истекшим сроком действия должны быть по-прежнему доступны.

(5) Выработка политики ДЦ.

Для реализации операций сертификации формируется политика операционной работы ДЦ, работы с персоналом и оборудованием и политика выпуска сертификатов на основе критериев контроля за созданием сертификатов для пользователей и других доверенных центров.

2.3.2. Вспомогательные сервисы

В инфраструктуре с открытыми ключами могут поддерживаться также различные дополнительные сервисы.

(1) Регистрация.

Регистрационные сервисы обеспечивают регистрацию и контроль индивидуальной информации, а также аутентификацию, необходимую для выпуска или аннулирования сертификатов (от имени доверенного центра). Фактический выпуск сертификатов осуществляется ДЦ.

(2) Хранение информации в архиве.

Сервисы хранения информации в архиве предназначены для долговременного хранения и управления цифровыми документами и другой информацией. Сервисы обеспечивают создание резервных копий и восстановление информации в случае уничтожения или старения среды хранения.

(3) Нотариальная аутентификация.

Нотариальная аутентификация включает аутентификацию отправителя сообщения, подтверждение целостности и юридической силы цифровых документов.

(4) Создание резервных копий и восстановление ключей.

ДЦ должен иметь возможность восстановить зашифрованную информацию в случае потери пользователями их ключей шифрования. Это означает, что доверенному центру, к которому относится пользователь, необходима система создания резервных копий и восстановления этих ключей. Этот процесс известен как коммерческое создание резервных копий и восстановление ключей, и он отличается от принудительного депонирования ключей третьей стороной (обычно правоохранительными органами), которая получает доступ к ключам для расшифровки необходимой информации. Коммерческие сервисы восстановления ключей обеспечивают заблаговременное засекречивание копии ключа на случай утери ключа пользователем, его ухода с работы, забывания пароля, необходимого для доступа к ключу, и восстановление ключа в ответ на запрос пользователя или его работодателя. В одних случаях ключ является секретным ключом из алгоритма с открытыми ключами, в других — это распределяемый ключ.

(5) Каталог.

Сервисы каталога осуществляют всестороннее управление и обеспечение информацией, имеющей отношение к пользователю (атрибутами). К атрибутам относится не только сертификат, но и номер телефона, адрес электронной почты абонента и т.д.

(6) Поддержка невозможности отказа от цифровых подписей

При бумажной технологии подписи лиц законно связывают их с документами, что не позволяет в дальнейшем отказаться от подписания документа. При электронных технологиях обычная подпись заменяется цифровой. Самое главное требование для невозможности отказа от цифровой подписи состоит в том, что ключ, используемый для выработки цифровых подписей — ключ подписи, должен генерироваться и безопасно храниться все время исключительно под контролем пользователя. Когда пользователи забывают свои пароли или теряют свои ключи подписи, на резервирование или восста-

новление предыдущей пары ключей подписи не накладывается никаких технических ограничений (в отличие от аналогичной ситуации с парами ключей шифрования сообщений). В таких случаях допускается генерация и дальнейшее использование пользователями новых пар ключей подписи.

Параллельное функционирование систем резервного копирования и восстановления ключей и системы поддержки невозможности отказа от цифровых подписей вызывает определенные проблемы. При резервном копировании и восстановлении ключей должны создаваться копии секретных ключей пользователя. Чтобы обеспечить невозможность отказа от цифровой подписи, не должны создаваться резервные копии секретных ключей пользователя, используемых для выработки цифровой подписи. Для соблюдения этих требований в инфраструктуре с открытыми ключами должны поддерживаться две пары ключей для каждого пользователя. В любой момент времени пользователь должен иметь одну пару ключей для шифрования и дешифрования, а другую пару — для выработки или проверки цифровой подписи.

(7) Корректировка ключей и управление историями ключей

В ближайшем будущем пользователи будут иметь огромное количество пар ключей, которые должны будут поддерживаться как криптографические ключи, даже если никогда не будут использоваться. Ключи шифрования должны со временем обновляться и должна поддерживаться история всех ключей, использованных ранее. (Например, у пользователей появится необходимость расшифровать информацию мно-

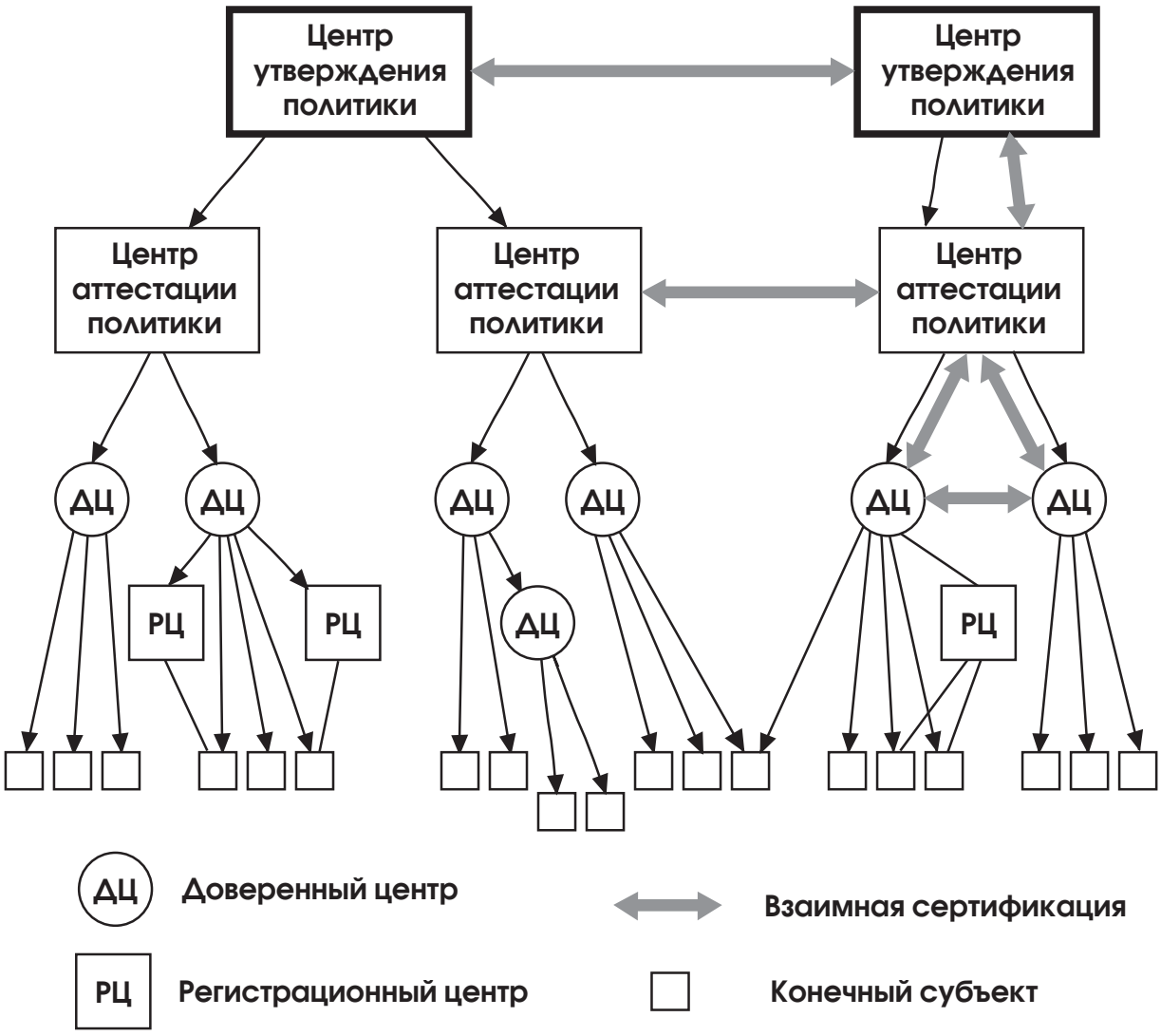

Рис.1. Архитектура сертификации.

голетней давности и проверять цифровую подпись на контракте многие годы в дальнейшем).

Процесс корректировки пар ключей должен быть «прозрачен» для пользователя. Это означает, что пользователи не должны понимать, что осуществляется обновление ключей, и никогда не должны получать отказ сервиса из-за недействительности своих ключей. Для удовлетворения этого требования пары ключей пользователя должны автоматически обновляться до истечения срока их действия. При обновлении пары ключей подписи предыдущий ключ подписи безопасно уничтожается. Тем самым предотвращается получение несанкционированного доступа к ключу подписи и устраняется необходимость хранения предыдущих ключей подписи.

(8) Другие сервисы

В ряде случаев необходимы и другие сервисы, например, сервисы генерации пар ключей и записи их на смарт-карты, если ключи хранятся на смарт-картах.

3. Архитектура сертификации

3.1. Структура и субъекты

Сертификация в инфраструктуре с открытыми ключами строится по двум основным типам архитектуры (см. рис. 1): иерархической (сверху вниз) и взаимной сертификации (разделенное доверие). В иерархической модели в сертификации участвуют следующие субъекты.

(1) Центры утверждения политики

Центр утверждения политики устанавливает стандарты для подчиненных ему центров сертификации политики, одобряет их политику и выпускает для них сертификаты.

Центр утверждения политики выпускает сертификаты (корневые сертификаты), имеющие цифровую подпись, с его собственным секретным ключом, соответствующим его собственному открытому ключу. В основном, срок действия этих сертификатов дольше срока действия сертификатов, выпускаемых центрами сертификации политики и доверенными центрами.

Выпуск корневых сертификатов и сертификатов для центров сертификации политики, как правило, выполняется независимо.

(2) Центры аттестации политики

Центр аттестации политики устанавливает политику для подчиненных ему доверенных центров и контролирует ее соблюдение при их работе.

Центр аттестации политики выпускает сертификаты для подчиненных ему ДЦ, а не для конечных пользователей. Выпуск корневых сертификатов и сертификатов для доверенных центров, как правило, выполняется независимо.

Центры аттестации политики способствуют широкому распространению сертификатов среди доверенных центров, снижая влияние компрометации ключей любого ДЦ или других непредвиденных обстоятельств. Благодаря тому, что срок действия сертификата центра аттестации политики превышает срок действия сертификата ДЦ, срок действия последнего может плавно удлиняться.

(3) Доверенные центры (ДЦ)

ДЦ подчиняется политике, устанавливаемой его центром аттестации политики, и выпускает сертификаты для подчиненных ему доверенных центров, конечных субъектов и регистрационных центров.

В некоторых случаях ДЦ устанавливает свою собственную политику в соответствии с политикой своего центра аттестации политики, а иногда ДЦ просто следует политике своего центра аттестации политики. В последнем случае ДЦ называют эмиссионным центром, для того чтобы отличать от того, что обычно называют доверенным центром.

(4) Регистрационные центры (РЦ)

Регистрационные центры регистрируют процедуры своих доверенных центров, а также конечных субъектов, расположенных по удаленным адресам, но не выпускают сертификаты. При регистрации РЦ проверяет подлинность данных о субъектах, следуя процедурам, согласующимся с политикой его ДЦ. РЦ может состоять из локальных регистрационных центров и организационных регистрационных центров.

(5) Конечные субъекты

Конечный субъект — это физическое или юридическое лицо, сервер или другой субъект, использующий сертификат.

В модели взаимной сертификации доверие распределяется между доверенными центрами, которые известны друг другу (иногда это называется «паутиной доверия»). В узком смысле взаимная сертификация — это взаимный выпуск сертификатов доверенными центрами друг для друга. Взаимная сертификация распространяет отношения доверенных третьих сторон на разные ДЦ. Например, большая, разветвленная организация может нуждаться в многочисленных доверенных центрах в различных географических регионах. Взаимная сертификация позволяет различным доверенным центрам устанавливать и поддерживать надежные электронные связи.

Версия	Элемент	Описание
v1	version	Версия (0 означает v1, 2 означает v3)
	serialNumber	Серийный номер сертификата
	signature.algorithmIdentifier algorithm parameters	Тип алгоритма подписи
	issuer	Уникальное название центра, выпускающего сертификат*4
	Validity NotBefore notAfter	Период действия Дата и время начала действия Дата и время конца действия
	subject	Уникальное имя субъекта
	SubjectPublicKeyInfo Algorithm subjectPubkicKey	Информация об открытом ключе субъекта Криптографический алгоритм Ключ (строка битов)
v2	issuerUniqueID	Уникальный идентификатор центра, выпускающего сертификат
	subjectUniqueID	Уникальный идентификатор субъекта
v3	AuthorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber	Идентификатор ключа, используемого для подтверждения подписи ДЦ Идентификатор ключа Общее название ДЦ Серийный номер сертификата ДЦ
	subjectKeyIdentifier	Идентификатор, используемый тогда, когда субъект имеет более одного ключа (например, во время возобновления сертификата)
	keyUsage	Применение ключа (строки битов) 1. Цифровая подпись 2. Невозможность отказа получателя/отправителя сообщения от факта его передачи/приема и содержания 3. Шифрование ключа 4. Шифрование информации 5. Соглашение о ключе 6. Подписание сертификата 7. Подписание CAC
	privateKeyUsagePeriod	Период действия секретного ключа ДЦ для подписи. Стандартно он короче периода действия соответствующего открытого ключа
	CertificatePolicies policyIdentifier PolicyQualifiers	Политика ДЦ (комбинация следующего) Идентификатор политики (как для ISO/IEC 9834-1) Критерии сертификации
	PolicyMappings IssuerDomainPolicy SubjectDomainPolicy	Используется только для сертификата ДЦ. Оговаривает, что политика эмитента и политика сертификации субъекта одинаковы.
	SupportedAlgorithms AlgorithmIdentifier IntendedUsage intendedCertificatePolicies	Определяют атрибуты каталога. Используются, чтобы сделать атрибуты известными заранее в случаях, когда партнер по связи использует данные каталога
	SubjectAltName OtherName rfc822Name dNSName x400Address directoryName ediPartyName uniformResourceIdentifier iPAddress registeredID	Альтернативное имя субъекта. Свободный выбор имени. Произвольное имя Адрес электронной почты Имя домена Адрес отправителя/получателя Имя каталога EDI-имя Унифицированный указатель ресурсов WWW URL IP-адрес Зарегистриров.ID объекта
	issuerAltName	Альтернативное имя ДЦ
	subjectDirectoryAttributes	Необязательные атрибуты субъекта, например, почтовый адрес, номер телефона и т.п.
	BasicConstraints cA pathLenConstraint	Отличает ключ ДЦ от ключей конечных пользователей (используется только для сертификата ДЦ) Для ключа ДЦ cA истинно. Ограничение длины пути

Табл. 1. Формат сертификата X.509.

v3	NameConstraints PermittedSubtrees Base minimum maximum excludedSubtree	Используется только при сертификации ДЦ Определяет сертификацию домена по имени по отношению к ДЦ более низкого уровня в пределах пути, устанавливаемого параметром BasicConstraints ДЦ более низкого уровня и домен его поддерева Имя ДЦ более низкого уровня Верхний предел домена Нижний предел домена ДЦ более низкого уровня, исключенный из домена
	PolicyConstraints PolicySet InhibitPolicyMapping	Ограничения политики (используется только для requireExplicitPolicy ДЦ)
	cRLDistributionPoints distributionPoint reasons keyCompromise cACompromise affiliationChanged superseded cessationOfOperation certificateHold cRLIssuer	Пункты распределения CAC Имя центра распределения. Abbreviates cRLIssuer. Вид списка, распределяемого данным пунктом 1. Скомпрометированный ключ конечного пользователя 2. Скомпрометированный ключ ДЦ 3. Измененная информация в сертификате (не повреждение) 4. Приостановленный ключ 5. Завершение использования 6. Приостановление использования Имя центра-эмитента CAC

Табл. 1. Формат сертификата X.509 (окончание).

В случае двусторонней взаимной сертификации два доверенных центра безопасно обмениваются своими открытыми ключами, и каждый ДЦ подписывает открытый ключ другого в сертификате, известном как взаимный сертификат.

В среде взаимной сертификации доверие поддерживается при помощи клиентского прикладного программного обеспечения, проверяющего подпись ДЦ на сертификатах. Эту операцию часто называют «движением по цепочке доверия». Цепочкой считается последовательность проверок взаимных сертификатов, которые выполняются от ключа ДЦ проверяющего пользователя к ключу ДЦ, необходимому для проверки сертификата другого пользователя. При движении по цепочке каждый взаимный сертификат проверяется на предмет действительности, так как взаимные сертификаты, как и сертификаты пользователей, могут аннулироваться.

В иерархии, описанной выше, существуют различные комбинации: взаимная сертификация может выполняться между центрами утверждения политики, между центрами аттестации политики, между доверенными центрами или между доверенными центрами и центрами аттестации политики. Однако во всех случаях должна гарантироваться согласованность политики между теми двумя центрами, о которых идет речь.

3.2. Сертификаты

Подпись ДЦ на сертификате гарантирует, что любые изменения содержания могут быть легко обнаружены. В силу своей безопасности сертификаты могут распространяться открыто, и пользователи, получающие открытый ключ из сертификата, могут быть уверены в его подлинности. То есть пользователи могут считать, что ключ принадлежит субъекту, названному уникальным именем, и что этот ключ может безопасно использоваться тем способом, для которого он был сертифицирован.

Наиболее распространен формат сертификата, установленный Международным Телекоммуникационным Союзом (ITU Rec. X.509 | ISO/IEC 9594-8). Сертификат содержит элементы данных, определенные в приведенной выше таблице 1, сопровождаемые цифровой подписью.

Цифровая подпись для всех элементов вырабатывается при помощи ключа «authority key identifier». Элементы, включенные в версию 1, являются обязательными; элементы, включенные в последующие версии — необязательные. Имя субъекта сначала было обязательным элементом и должно было быть уникальным. Начиная с версии v3, оно стало необязательным. В формат уникального имени включается такая информация, как название страны, региона и данного имени, которые объединяются так, чтобы образовать уникальный идентификатор. Использование одинаковых идентификаторов запрещено.

3.3. Архивы сертификатов и распределение сертификатов

Термин «архив» относится к сервису, осуществляющему распределение сертификатов. ДЦ действует как доверенная третья сторона,

выпускающая сертификаты для пользователей. Сертификаты должны распределяться так, чтобы они могли быть использованы приложениями. Фактически действующим стандартом доступа к этим архивам является упрощенный протокол доступа к каталогу LDAP (Lightweight Directory Access Protocol). Он наиболее адекватен в качестве стандарта для сохранения и извлечения сертификатов после их генерации. Поддерживается большинством серверных операционных систем и баз данных и достаточно открыт для того, чтобы его могли поддерживать практически любые инфраструктуры с открытыми ключами.

4. Заключение

Большинство компаний, желающих использовать технологию цифровых сертификатов, выбирают один из двух возможных путей: либо создают свой доверенный центр, либо обращаются к помощи компаний, специализирующихся на услугах PKI.

В организационном плане создание доверенного центра требует выработки его политики и правил организации сертификации с учетом требуемого уровня надежности самого центра и выпускаемых им цифровых сертификатов. Для реализации операций сертификации формируется политика операционной работы ДЦ, работы с персоналом и оборудованием и политика управления сертификатами.

Правильная организация процесса выпуска и обслуживания цифровых сертификатов, точное следование нормам практики сертификации являются основой безопасного и надежного функционирования доверенных центров, ключевых элементов системы обеспечения безопасности корпоративных информационных ресурсов.

5. Литература

1. Open Group Guide. Architecture for Public-Key Infrastructure (APKI). http://www.opengroup.org/onlinepubs/009219899/toc.htm
2. Certification Authority Guidelines. 1997—1998. Electronic Commerce Promotion Council of Japan (ECOM). http://www.ecom.or.jp
3. European Trusted Services (ETS) — results of 1995 TTPS projects. A.Nilson. Marinade Limited. April 1997
4. Legal and Regulatory Issues for the European Trusted Services Infrastructure — ETS. ISTEV. June 1997
5. ISO/IEC 9594-8: 1995| ITU-T Recommendation X. 509 (1993E), Information Technology — Open Systems Interconnection — The Directory: Authentication Framework, 1993.11 [Information: http://www.itu.ch/itudoc/itu-t/rec/x/ x500up/x509_27505.html]
6. ISO/IEC JT1/SC27 WD 14516-1, Guidelines for the use and management of Trusted Third Party services — Part 1: General Overview, 1995.11
7. ISO/IEC JT1/SC27 WD 14516-2, Guidelines for the use and management of Trusted Third Party services — Part 2: Technical aspects, 1996.6.21
8. Utah Digital Signature Act (1996) http://www.gvnfo.state.ut.us/ccjj/digsig/dsut-act.htm
9. German Draft Digital Signature Law (SigG), English translation by Christopher Kuner 1996 http://ourworld.compuserve.com/homepages/ckuner/digsig.htm
10. B.O'Higgins. What is the Difference Between a Public-Key Infrastructure and a Certification Authority? http://www.ema.org/html/pubs/mmv4n2/pki.htm
11. Л.Бруно. Certificate Authorities: Кому Вы доверяете? — Data Communications (Russian edition). 1998, №3
12. А.Карве. Инфраструктура с открытыми ключами. LAN/ Журнал сетевых решений, 1997, №8
13. Э.Месмер. Сертификаты достойны вашего внимания. Computerworld Россия, 1998, №21
14. У.Вонг. Обслуживание цифровых сертификатов. LAN/ Журнал сетевых решений, 1998, №7-8
15. А.Карве. Защищенный обмен сообщениями. LAN/ Журнал сетевых решений, 1998, №12
16. А.Карве. PKI — инфраструктура защиты следующего поколения. LAN/Журнал сетевых решений, 1999, №7