УДК 004.056 ББК У9(2), 0

КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

© 2004 Д. С. Мащенко

Центр спецсвязи ФСО России

Рассматриваются вопросы организации безопасности конфиденциальной информации, циркулирующей в электронном виде.

Анализируются проблемы, возникающие при обработке систем информационно-экономической безопасности, и предлагаются пути их решения.

Что такое информационно-экономическая безопасность? В первую очередь, это одна из составляющих экономической безопасности, под которой принято понимать то состояние экономики и институтов власти, при котором обеспечиваются гарантированная защита национальных интересов, социальная направленность политики, достаточный оборонный потенциал даже при неблагоприятных условиях развития внутренних и внешних процессов.

В то же время информационно-экономическая безопасность является составляющей информационной безопасности, которая в разных контекстах может иметь различный смысл. Мы остановимся на одном. Доктрина информационной безопасности Российской Федерации термин «информационная безопасность» определяет как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Таким образом, под информационно-экономической безопасностью, наверное, надо понимать защищенность экономических интересов в информационной сфере. Интересов в экономике очень много, и все рассматривать у нас нет возможности. Мне по роду своей деятельности ближе аспект безопасности информации, циркулирующей в экономической сфере. Вещи эти несколько различны, так как понятия информационной безопасности и безопасности информации путать ни в коем случае нельзя. К сожалению, закон арифметики, по которому от перестановки слагаемых сумма не изменяется, в данной области приводит к печальным результатам.

Я буду говорить именно о безопасности информации.

С точки зрения построения информационных взаимосвязей в экономике, мы получаем полнодоступную схему, в которую включены органы государственной власти, производственные структуры и, соответственно, потребители. Очевидно, что информация в этих потоках носит различный характер как по своему содержанию, так и по способам ее обработки и хранения.

Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.95 г. определил, что по категории доступа информация может быть:

- открытая;
- ограниченного доступа.

В свою очередь, информация ограниченного доступа подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Именно эту информацию с точки зрения организации информационно-экономической безопасности я рассмотрю.

Приступая к организации безопасности, любому на практике придется столкнуться с достаточно большим объемом вопросов, которые необходимо решить. Любая система защиты должна непременно отвечать требованиям современного законодательства, быть надежной в эксплуатации и эффективной в отношении объекта защиты. Немаловажен и вопрос стоимости такой системы – она не должна превышать стоимости объекта защиты, иначе мы получим систему, суще-

ствующую ради самой себя.

Существующее законодательство в области защиты информации далеко от идеала. Если в области защиты государственной тайны мы имеем более или менее стройную систему законодательных и нормативных документов, то в вопросах о защиты конфиденциальной информации такая система отсутствует.

В настоящей статье рассматриваются вопросы организации безопасности конфиденциальной информации. Хочу сразу обратить внимание на то, что информация, не только защищаемая, а вообще информация различается не только по своему типу, но и по видам носителей, на которых она находится. Соответственно и подходы к защите различны. Способы защиты информации на бумажном носителе в корне отличаются от защиты информации, обрабатываемой в электронном виде. Что-то можно защитить, применяя только организационные меры, а где-то нужны еще и технические мероприятия. Опять же сделаю оговорку, рассматривая информационно-экономическую безопасность, я буду делать упор именно на защиту информации, циркулирующей в электронном виде, как наименее защищенную сейчас.

Итак, что мы имеем в области законодательства? Во-первых, мы не имеем самого главного – закона «О конфиденциальной информации» как основополагающего документа. Закон «Об информации, информатизации и защите информации» понимает под конфиденциальной информацией документированную информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Существует еще и Указ Президента № 188 от 6 марта 1997 г., который определил перечень сведений конфиденциального характера. К этой информации относятся:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Не в моей компетенции обсуждать указанные законодательные акты, но мне кажется, что понятие конфиденциальной информации несколько шире. В любом случае закон «О конфиденциальной информации» необходим уже в самое ближайшее время. Если мы говорим о законах в области защиты информации, то перечислим некоторые из них:

1. Закон РФ от 21 июля 1993 года № 5485-1 «О государственной тайне».

2. Закон РФ от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».

3. Закон РФ от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене».

4. Закон РФ от 10 января 2002 года № 1-ФЗ « Об электронной цифровой подписи».

Существует и еще целый ряд других законов, перечислять которые нет особого смысла. Тем более, что в принципе важно не количество законов, а понимание требований, которые необходимо выполнять на практике.

Требования перед применяемой или планируемой к применению системой защиты информации таковы:

- деятельность по защите информации может осуществляться только при наличии соответствующих лицензий;

- технические средства, применяемые для защиты информации, должны быть сертифицированы;

- должны проводиться аттестационные мероприятия в отношении объектов информатизации.

Подход к защите информации техническими средствами может быть двояким: можно реализовать систему защиты информации как с помощью криптографических, так и некриптографических средств, или тех и других одновременно. Однако в любом случае необходимы лицензии. Ситуация с применением средств некриптографической защиты осталась прежней – лицензирование в этой области осталось в компетенции Гостехкомиссии России. Изменилась ситуация в области применения криптографии. До недавнего времени вопросами в этой области занималось федеральное агентство правительственной связи и информации, однако после его упразднения функции по лицензированию переданы федеральной службе безопасности. Правопреемником ФАПСИ, как известно, стала Служба специальной связи при федеральной службе охраны, в компетенции которой осталось применение электронно-цифровой подписи в интересах органов государственной власти.

Применение именно сертифицированных средств защиты информации сегодня обязательно только для органов государственной власти. Для коммерческих структур это требование не носит обязательного характера, рекомендуется только выполнять его. Однако негосударственные структуры постоянно взаимодействуют с госорганами, что обязательно приведет к необходимости использования таких же сертифицированных средств. Кроме этого, уже давно назрела необходимость использования электронно-цифровой подписи (ЭЦП). Известно, что электронный документ, защищенный ЭЦП, будет иметь юридическую силу только в случае применения сертифицированного средства. В статье 5 Закона об ЭЦП говорится, что «…при создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи…».

Сегодня многие коммерческие фирмы боятся сертифицированных средств защиты информации именно потому, что они сертифицированы, а значит, по их мнению, как это не парадоксально звучит – не надежны. Но я уверен, что продукция, сделанная неизвестно где и неизвестно кем, гораздо менее надежна, а чаще всего попросту опасна. Похожая ситуация сложилась сегодня с доверием или недоверием к разработкам отечественных производителей. Нередко приходится слышать, что все сделанное в России плохо, а вот зарубежные продукты выше всяких похвал. Но не надо забывать, и западные компании не скрывают этого, что на территорию России поставляются ослабленные версии систем защиты. К примеру, в стандарте GSM во всем мире используется алгоритм шифрования А5, и только в России используется ослабленная версия этого алгоритма А5/2. Какие цели здесь преследуются, я думаю, очевидно. В то же время наше государство заставляет производителей средств защиты информации идти в ногу со временем. Например, принят новый ГОСТ по электронно-цифровой подписи – Р-34.01. Причиной его появления послужил тот факт, что во Франции после долгих усилий со стороны заинтересованных лиц информация, защищенная с помощью ЭЦП по старому ГОСТу, была вскрыта. И естественно, что всех разработчиков средств ЭЦП государство обязало изменить свою продукцию в соответствии с новым стандартом.

Ну и, наконец, аттестование. Приведу только один документ Гостехкомиссии РФ, который появился совершенно недавно, а именно в прошлом году: «Основные и специальные требования по защите конфиденциальной информации» и известный как СТР-К.

Требования, которые этот руководящий документ ставит перед организованной системой защиты, достаточно жесткие.

Он устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти,

органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций независимо от их организационно-правовой формы и формы собственности, должностных лиц и граждан Российской Федерации, взявших на себя обязательства либо обязанных по статусу исполнять требования правовых документов Российской Федерации по защите информации.

Сегодня эти требования относятся ко всем, за исключением защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (например, информации, составляющей коммерческую, банковскую тайну и т. д.), для которых данный документ носит рекомендательный характер.

Комплекс работ по аттестации довольно большой и включает в себя и организационные мероприятия, и целый ряд аппаратных проверок. Своими силами решить этот вопрос может только очень крупное предприятие, обладающее сильной службой противодействия техническим разведкам, которая должна быть оснащена современными техническими средствами и обученными специалистами. В противном случае необходимо привлекать специализированные аттестационные центры.

Следующий этап организации безопасности – эксплуатация защищенной системы. Естественно, что в идеале нам бы хотелось иметь абсолютную защиту от любого типа злоумышленников, надежно работающую в любых условиях, легко модернизируемую под возникающие задачи и простую в обслуживании и управлении. В реальности все выглядит несколько не так. Для того, чтобы хоть немного достичь желаемого результата, необходимо прежде всего продумать и спланировать всю систему защиты. Дело это кропотливое и очень трудоемкое. К сожалению, этим важнейшим моментом зачастую попросту пренебрегают. В результате получаются настолько громоздкие системы, что они не только не обеспечивают безопасности, но и в большинстве случаев просто не работают. Планирование, как один из важнейших этапов организации информационно-экономической безопасности, отвечающий за будущую эффективность всей системы защиты информации, можно разбить на несколько подэтапов:

1. Четкое определение функций и понимание предназначения будущей системы безопасности.

2. Оценка реально существующих угроз как внутреннего, так и внешнего характера.

3. Анализ существующих и предлагаемых продуктов защиты информации и оценка полноты выполняемых ими функций защиты.

4. Определение порядка эксплуатации будущей защищенной системы, то есть ввод ее в эксплуатацию, техническое обслуживание, порядок модернизации в дальнейшем и т.д.

Дальше, в принципе, можно приступать непосредственно к построению системы защиты.

И снова возникает немаловажная проблема: какими силами осуществлять строительство? Крупное и богатое предприятие, которое серьезно заинтересовано в своей информационной безопасности, может себе позволить обучить специалистов, закупить оборудование, получить необходимую лицензию и работать по внедрению системы безопасности. Путь очень неплохой, даже можно сказать оптимальный, но дорогой. Очень немногие предприятия могут позволить себе идти по этому пути. Выход для остальных предприятий – привлечение специализированных организаций, которые профессионально занимаются именно построением систем защиты. Путь тоже недешевый, однако по сравнению с первым, стоимость все-таки ниже. С другой стороны, в первом случае мы получаем более безопасный вариант, чем во втором, так как при построении системы безопасности с помощью сторонней организации неизбежно, что какая-то часть конфиденциальной информации становится известной людям со стороны. Единственное, что можно сказать: надо более тщательно выбирать партнеров и всегда обращать внимание на наличие у них лицензий и сертификатов. Никогда не будет лишним обратиться в компетентные органы для проверки подлиннос-

ти этих документов. Все это вроде бы очевидно, однако мне приходилось сталкиваться с тем, что люди доверяются в таких серьезных вопросах даже каким-то ксерокопиям лицензий, причем выданных совершенно другой организации и в другом городе.

Сталкиваясь с организацией информационной, информационно-экономической безопасности, нельзя забывать о так называемом «человеческом факторе». Известно, что именно благодаря ему чаще всего случается нарушение безопасности. Здесь можно говорить и о некомпетенции специалистов, обеспечивающих безопасность, и о «злоумышленниках», и о простой халатности. Уделять этому вопросу всестороннее внимание следует на всех этапах организации безопасности.

В процессе эксплуатации системы защиты придется столкнуться с проблемой ее организации. Облегчить эту задачу в известной степени помогут два документа, которые были разработаны Гостехкомиссией РФ и ФАПСИ:

1. Специальные требования и рекомендации по защите конфиденциальной информации – СТР-К.

2. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты, информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, объявленная приказом ФАПСИ № 152 от 13.06.2001 г.

Вы можете задать вопрос, почему несмотря на то, что ФАПСИ упразднено, я продолжаю ссылаться на документы этого учреждения. Все документы и требования, изданные под редакцией федерального агентства, по-прежнему имеют юридическую силу. Это касается и лицензий, которые были выданы кому-либо. Все они действительны до окончания срока их действия.

Эффективность информационно-экономической безопасности зависит от всех участников этого процесса, от простых исполнителей до руководителей самого высокого ранга, от всех без исключения звеньев экономики страны. Не зря сейчас говорится о создании «электронного государства», поднимается вопрос о создании «интеллектуальных домов, районов» и т.д. К этому надо стремиться, но вопросов и проблем в этой области еще очень и очень много. Их решение, если мы хотим жить в надежном и развитом государстве, зависит в первую очередь от нас с вами.

CONCEPTUAL ISSUES OF ENSURING INFORMATION AND ECONOMICS SECURITY

© 2004 D. S. Mashchenko

Communication Centre of Federal Security Service of Russia

The paper deals with the issues of ensuring the security of confidential information circulating in the electronic form.

Problems arising when processing systems of information and economics security are analysed, and ways of solving them are proposed.