Защита на экспорт? Строго по лицензии!

Сетевой журнал №12.2000

Сергей Вихорев, директор департамента ОАО "ЭЛВИС-ПЛЮС"
В последнее время все более актуальными становятся проблемы трансграничного распространения криптографических продуктов.

Вместо предисловия

В последнее время все более актуальными становятся проблемы трансграничного распространения криптографических продуктов. Иногда можно наблюдать даже некоторую эйфорию в этом вопросе. Законодатель вроде бы дает собственнику информации право самому определять степень защиты своих ресурсов, но умалчивает, что правила игры для применения некоторых средств защиты, в частности криптографических, устанавливаются другими нормами. Пользуясь своим конституционным правом на сохранение тайны переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, каждый человек, естественно, желает обезопасить себя применением криптографических средств, как наиболее надежных для защиты информации в каналах связи.
На территории России в обороте находится большое количество криптографических продуктов иностранного производства. Складывается обманчивое впечатление, что возможно их широкое использование. Некоторые публикации еще больше подогревают интерес к этой проблеме. «Правительство Соединенных Штатов Америки приняло новые правила экспорта программных продуктов и разрешило поставки средств со 128-битным ключом шифрования за пределы страны».Ура! «Компания RSA Security объявила о публикации своего алгоритма шифрования для свободного распространения».Многократное ура!
Однако российским пользователям упрощение процедуры вывоза или открытая публикация алгоритма ничего существенного недаст: для использования в нашей стране средств шифрования как зарубежного, так и российского производства нужны разрешения ФАПСИ. Но если вы думаете, что живете в самой зарегулированной стране, то глубоко заблуждаетесь.

Немного истории

Россия не единственная страна, которая вводит ограничения на использование шифровальных средств защиты информации. В принципе, это устоявшаяся международная практика. Законодательное регулирование вопросов защиты информации на государственном уровне характерно для большинства развитых стран мира.
В этой области наиболее разработанное законодательство - в США. Первый закон о защите информации там принят еще в 1906 году, и к настоящему времени число законодательных актов в данной сфере достигло 500. Информационная безопасность рассматривается американской администрацией как один из ключевых элементов национальной безопасности. В США, где администрация всячески содействует внедрению шифровальных средств в коммерческий сектор, продажа шифровального оборудования, а также алгоритмов шифрования и средств обеспечения безопасности компьютеров другим странам законодательно ограничивается, что дает государству возможность контролировать за передачу в эти страны научной и технической информации и продукции. Практически все криптографические средства, производимые в США, включаются в список военного имущества, продажа которого осуществляется в соответствии с правилами международной торговли. Государственным

подрядчикам разрешено использовать только шифровальную технику, либо изготовленную по заказу Агентства национальной безопасности (АНБ), либо прошедшую сертификацию в этом агентстве. Фирмы - изготовители средств шифрования не должны находиться в иностранном владении или под иностранным влиянием. Выдача лицензий на продажу шифровальных средств входит в сферу компетенции Министерства торговли и Государственного департамента США, которые координируют свою деятельность с АНБ. На практике же основная роль в решении проблемы экспорта таких средств принадлежит АНБ, которому предоставлено право вето и которое самостоятельно может запретить их продажу за рубеж.

При этом однозначно установлено, что вывозимые криптографические средства не должны служить препятствием для органов электронной разведки США при добывании ими информации. Необходимо отметить, что экспорт из США стандартных криптографических алгоритмов разрешается для использования их только финансовыми учреждениями или субсидируемыми США фирмами. Все другие криптографические устройства могут экспортироваться, если они предназначены только для проверки целостности данных, но не для их шифрования. АНБ разрешает также фирмам США продавать за рубеж криптосистемы с собственными алгоритмами при условии их одобрения АНБ. При этом АНБ имеет право требовать модификации таких алгоритмов до выдачи лицензии на экспорт. До недавнего времени законодательство США позволяло экспортировать программы шифрования с длиной ключа не более 56 бит, и то лишь в том случае, если производители соглашались создавать в своих продуктах систему «депонирования ключа», что дает возможность сотрудникам американских правоохранительных органов при необходимости расшифровывать данные. Сейчас, под давлением фирм производителей, правительство США приняло новые правила экспорта программных продуктов и разрешило поставки за пределы страны средств со 128-битным ключом шифрования.

В Европе, как и в США, экспорт шифровальных средств и ЭВМ с криптографической защитой без соответствующей лицензии запрещен даже в дружественные страны. Практически все спецслужбы ведущих стран мира обеспечили такой порядок, когда получить лицензию на экспорт очень трудно, а иногда и невозможно. Даже при реализации совместных проектов, например при создании сотовой телефонной системы GMS, органы безопасности США и Великобритании настояли на изъятии из системы шифровального алгоритма засекречивания речи А5, аналогичного американскому стандарту DES. Это было сделано под предлогом необходимости прослушивать разговоры преступников по телефонам подвижной связи.

Франция - страна с типичной и наиболее развитой нормативной базой, регулирующей процесс производства и продажи криптографических средств. В соответствии с французским законодательством, шифровальное оборудование предназначено в первую очередь, для обороны страны и обеспечения ее внешней и внутренней безопасности, поэтому по единой классификации шифровальная техника подпадает под определение «военное оборудование второго класса, содействующее эффективному использованию оружия в боевых условиях». Следовательно, изготовление, использование и экспорт такого оборудования автоматически становится предметом контроля государства. Для производства криптографических средств и уж тем более торговли ими требуется специальное разрешение правительства. Если такое оборудование производится для частных целей, то необходимы еще разрешения Министерства связи и Министерства обороны. Импорт шифровальной техники на территорию Французской Республики вообще запрещен, за исключением некоторых специально предусмотренных случаев (например, для использования в международных платежных системах). Экспорт такого оборудования возможен только с разрешения Премьер-министра страны, выдаваемого после консультаций со специальным комитетом по военному оборудованию. Закон объявляет экспорт и снабжение криптографическими средствами без специального разрешения преступлением, которое наказывается штрафом в размере до 500 000 франков или тюремным заключением на срок от одного до трех месяцев. Суд может также запретить нарушителю заниматься производством шифровальной техники на срок до пяти лет.

В Китае, Израиле, Иране, Ираке, Вьетнаме, Пакистане использование криптографических программ может быть разрешено только после рассмотрения вопроса в государственной структуре, обладающей соответствующими полномочиями. В Тунисе разрешение на использование криптографии даётся только при условии, что копии ключей хранятся в банке данных или депозитарии у доверенного лица, уполномоченного государством («депонирование ключей»). Подобный же законопроект рассматривается в Великобритании.
Кроме стремления облегчить жизнь собственным органам электронной разведки, законы различных государств имеют целью охрану своих рынков от чрезмерно глубокого проникновения на них иностранных производителей.

Ситуация в России

В России, как и в других странах, экспорт-импорт шифровальных средств находится под контролем государства. При этом наша модель контроля по своей сущности достаточно близка к американской и во многом ее повторяет. Контроль осуществляется через механизм лицензирования. Эти операции могут совершаться только на основании лицензии Министерства торговли Российской Федерации, уполномоченного Правительством Российской Федерации на регулирование внешнеэкономической деятельности. Такая лицензия выдается на основании решения ФАПСИ на каждую конкретную ввозимую/вывозимую партию средств криптографии. При этом принимаются во внимание цель ввоза/вывоза криптографических средств, объем партии и производитель.
Необходимо обратить внимание, что любая деятельность, связанная с шифровальными средствами (независимо от того импортного или отечественного они производства) на территории Российской Федерации подлежит обязательному лицензированию. Поэтому в выдаче разрешения ФАПСИ на ввоз/вывоз шифровальных средств может быть и отказано, если у компании-экспортера/импортера отсутствует соответствующая лицензия ФАПСИ на деятельность в области защиты информации шифровальными средствами (эксплуатация, монтаж, настройка, реализация и т. д.). В виде исключения ФАПСИ может принять заявление о выдаче разрешения на ввоз/вывоз от организации, не имеющей лицензии, но подавшей документы на получение таковой в соответствии с Положением о лицензировании.
Как правило, разрешается ввоз в Россию оборудования, предназначенного для использования в международных платежных системах, обеспечения международного информационного обмена и связи зарубежных компаний или их филиалов со своими штаб-квартирами. При этом означенные организации должны принять на себя обязательства не передавать ввезенные криптографические средства другим организациям и не оказывать услуги по шифрованию информации для других юридических или физических лиц.
Для получения решения о ввозе/вывозе криптографических средств организации, занимающиеся экспортно-импортными операциями, должны обратиться в ФАПСИ для проведения экспертизы.
Это в свою очередь требует обязательного проведения технической экспертизы средств защиты информации, которая установить, являются ли эти средства шифровальными или нет. В задачи такой экспертизы не входит оценка качества средства защиты и обеспечиваемого им уровня защищенности информации (что, собственно, составляет суть сертификации). Она лишь определяет, к какому типу или виду относится данное средство.
Надо помнить, что интересы потребителя при использовании импортной продукции в информационных системах в соответствии с российским законодательством защищаются таможенными органами Российской Федерации. Эти органы сами могут обратиться в ФАПСИ для проведения такой экспертизы. Учитывая, что специалистов в области криптографии в Таможенном комитете не так много, можно предположить, что во всех спорных случаях такое

обращение гарантировано, а все время проведения экспертизы импортная продукция, вызвавшая сомнение, будет пылиться на полках таможенного склада.
Кроме того необходимо отметить, что не существует универсальной методики отнесения тех или иных средств к шифровальным, поэтому решение о том, является или нет данное средство шифровальным, принимается в каждом конкретном случае по результатам экспертизы документации и, как правило, образцов изделия (читай - как Бог на душу положит). Существенные трудности при этом создает проблема обеспечения авторских прав, поскольку полный комплект документации обычно не позволяет определить, какие алгоритмы использованы в конкретной технической реализации.
На сегодняшний день в области криптографической защиты информации пока не выработан единый, принятый во всей стране понятийный аппарат. Многие понятия и термины, которые вводятся законами и иными нормативными актами и используются различными органами, работающими в сфере защиты информации, или отдельными авторами, носят неоднозначный и противоречивый характер. В одни и те же термины часто вкладывается различное смысловое содержание.
ФАПСИ при проведении технической экспертизы руководствуется широким перечнем документов и понятий, в том числе определением шифровальных средств (средств криптографической защиты информации) и определением понятия шифра. В частности, к шифровальным средствам ФАПСИ относит: реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику; реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и электронной цифровой подписи; аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления ключевых документов для шифровальных средств независимо от вида носителя ключевой информации.
Как видно, определение достаточно широкое и размытое. При проведении экспертизы по отнесению средств защиты к классу криптографических, по мнению ФАПСИ, следует руководствоваться тремя критериями:

- наличием некоторого математического преобразования данных;
- наличием секретного параметра этого преобразования - ключа с мощностью ключевого множества, большего или равного двум;
- обратимость используемого математического преобразования данных.

Используя эти критерии, ФАПСИ к категории шифровального средства относит любое средство, независимо от его назначения и способа реализации, в котором реализован криптографический алгоритм, работающий под управлением ключа, в том числе средства, используемые для закрытия информации в канале связи, имитозащиты сообщения, аутентификации пользователей, средства электронной цифровой подписи, средства закрытия таблицы паролей и т. д. Кроме того, под эти критерии подпадают не только технические средства, но и ручные шифры, а также ключевая информация, предназначенная для шифрования.

То есть при желании любое современное устройство обработки информации в ходе экспертизы может быть отнесено к криптографическим средствам, что само по себе нонсенс. Особенно это касается современных программных продуктов западных производителей, так как большинство основных операционных систем в мире в той или иной форме используют криптосистемы.

Например, если строго следовать российским законам, одна из самых популярных операционных систем корпорации Microsoft новая Windows 2000 не может продаваться в России до тех пор, пока из нее не будут исключены функции шифрования. Однако системы шифрования настолько тесно интегрированы с ядром Windows 2000, что произвести изменения практически невозможно, даже если бы это не шло вразрез с коммерческими интересами Microsoft.

Можно также вспомнить, что программы Arj, Rar, Pkzip, WinZip и им подобные архиваторы позволяют создавать защищенные паролем архивы, популярная в России программа Netscape Communications имеет программу шифрования для своего браузера, продукты компании Trusted Information Systems, такие как Internet-брандмауэр Gauntlet, содержат алгоритмы шифрования DES. Продукты корпорации Microsoft типа Cryptographic Service Provider, поддерживают криптографический API-интерфейс для методов DES.

Не надо забывать и об аппаратных средствах, без которых невозможно построение современных информационных сетей. Прежде всего, это различного рода маршрутизаторы (например, Cisco) и межсетевые экраны (скажем, CheckPoint), содержащие криптографические модули, поддерживающие DES, и т. д.

Проведенный анализ показывает, что сейчас в области применения криптографических средств защиты информации больше вопросов, чем ответов.

Если мы строим действительно правовое государство, то законодательство в области использования криптографического оборудования требует определенной либерализации. Само понятие «двойные технологии» предполагает, что те или иные средства можно использовать как в государственных, так и в частных интересах. Поэтому необходимо очень аккуратно, но четко провести разграничение таких средств либо по признаку принадлежности (ограничения касаются только средств защиты государственных секретов), либо по критериям технических параметров (например, как в западных странах - по размеру закрытого ключа). Иначе будет действовать народная мудрость: строгость российских законов компенсируется необязательностью их исполнения.