тивные услуги по гигиене, на лабораторные анализы, борьбу с болезнями животных и т.п. Следует при этом иметь в виду, что заинтересованность сельхозтоваропроизводителей в продаже молока перерабатывающим предприятиям по новым ценам, учитывающим потребительскую ценность продукта, обеспечит более полную загрузку предприятий и снижение себестоимости молочной продукции, а также позволит постепенно нивелировать потери от более высоких закупочных цен.

Рассмотренная концепция является далеко не единственным направлением совершенствования системы ценообразования в АПК, но применение ее на практике, как показывают реалии сегодняшнего дня, необходимо – это позволит осуществить конкретные позитивные сдвиги в решении данной проблемы.

Литература

Боев В.Р., Серков А.Ф., Романов А.Е. Основные результаты аграрной реформы // Экономика с.-х. и перераб. предприятий. – 1996. – № 6.

Гасанов А.Т. Резервы увеличения производства молока и молочных продуктов. – М.: Агропромиздат, 1990. – 241 с.

Кириллова Г.М., Камышова Я.Т., Тихонова Н.А. Пути выхода молочной отрасли из кризисного состояния // Экономика с.-х. предприятий. – 2000. – № 1. – С. 35-36.

Коган М.Ю. и др. Ценообразование в АПК зарубежных стран. – М., 1990. – 56 с.

Молоко коровье. Требования при закупках: ГОСТ 13264-88. – М.: Госкомитет СССР по стандартизации, 1988. – 6 с.

Счастливцева Л.В., Губанова Н.В. Ценовая ситуация на аграрном рынке России и ее государственное регулирование // Экономика с.-х. и перераб. предприятий. – 1998. – № 5. – С. 18-21.

УДК 336.76

К.А. Филиппов

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА РЫНКЕ ЦЕННЫХ БУМАГ РОССИИ

Комплексный характер проблемы и компьютерная преступность на рынке ценных бумаг

В настоящее время актуальность проблемы обеспечения информационной безопасности связана с тем, что информационная и деловая активность все более перемещается в область кибернетического пространства. Масштабы последствий преднамеренного или непреднамеренного нарушения нормального функционирования автоматизированных систем могут варьировать от небольших сбоев для пользователей до экономической катастрофы в масштабах всей страны.

Концепция защиты информации на рынке ценных бумаг строится на основе принципов защиты, по которым работает сеть передачи данных "Деловая сеть России". В этой сети большое внимание уделено решению вопросов надежной защиты передаваемой, хранимой и обрабатываемой информации от несанкционированного доступа, вопросов контроля ее целостности и подлинности на базе современных информационных технологий.

Общее понятие комплексной безопасности включает в себя:

- физическую безопасность (защита зданий, помещений, подвижных средств и т.п.);
- безопасность аппаратных средств (защита средств вычислительной техники, сетевого оборудования и т.п.);
- безопасность программно-математического обеспечения (защита от программных вирусов, "троянских коней", логических бомб, хакеров и т.п.);
- безопасность связи (защита каналов связи от внешних воздействии любого вида);
- безопасность сети в целом (дополнительные меры защиты, вызванные особенностью сети).

Применительно к специфике создаваемой информационной инфраструктуры рынка ценных бумаг России безопасность программно-аппаратных средств и сети в целом в современном толковании последних проработок ФАПСИ следует трактовать как защиту от "информационного оружия" (ИО).

При этом должна реализовываться защита:

- от комплексного воздействия, направленного на нарушение функционирования непосредственно телекоммуникационной среды;
- от несанкционированного доступа к технологической (служебной) и иной информации, связанной с работой сети;

- от разрушения программных средств защиты с целью получения доступа к содержанию информации, передаваемой абонентами.

Нарушение функционирования телекоммуникационной среды может осуществляться за счет воздействия на аппаратно-программные средства путем передачи несанкционированных служебных команд, осуществления вирусных атак на системное и прикладное программное обеспечение (ПО), операционные системы, базы данных, пользовательскую и иную информацию, активизации аппаратно-программных закладок.

Несанкционированный доступ может осуществляться путем неправомерного использования ресурсов сети, в том числе при помощи чтения, записи данных, инициирования выполнения несанкционированных команд и программ, а также путем снятия информации техническими средствами.

Разрушение программных средств защиты может осуществляться путем активизации внедренных аппаратно-программных закладок. Закладки могут применяться для разрушения встроенных и внешних средств и систем защиты, нарушения целостности и функционирования распределенных систем управления, передачи и обработки информации, технических средств, системного и прикладного ПО, пользовательской и иной информации.

Защита от воздействия ИО должна обеспечиваться комплексом мероприятий на всех этапах разработки, ввода в действие, модернизации аппаратно-программных средств телекоммуникаций, а также при обработке, хранении и передаче по каналам связи информации с широким применением современных средств криптографической защиты. При этом необходимо учитывать дополнительную сложность и специфику решения задачи защиты при использовании импортного оборудования.

В состав задач обеспечения безопасности информации включаются:

- защита информации в каналах связи и базах данных криптографическими методами;
- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);
- обнаружение нарушений целостности объектов данных;
- обеспечение живучести сети шифросвязи при компрометации части ключевой системы;
- обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации;
- обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;
- защита от несанкционированных действий по каналу связи или от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов;
- организационно-технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

Особую актуальность в этих условиях приобретает обеспечение защиты информации, что является одной из основных составляющих автоматизированных технологий финансового рынка. При этом должна использоваться надежная комплексная защита финансовых документов специальными средствами, прошедшими сертификацию в соответствующих государственных службах.

В настоящее время можно выделить два основных направления воздействия на информационно-телекоммуникационные сети и электронные базы данных:

- незаконное проникновение в базы данных и системы кредитно-финансовых структур преступных групп с целью хищения денежных средств;
- применение экстремистскими группировками "информационного оружия" с целью уничтожения (искажения) баз данных, систем электронных банковских расчетов и иных компонентов кибернетического пространства для нанесения прямого экономического ущерба в масштабах государства. Материальные потери от подобного воздействия могут быть сравнимы с потерями от крупномасштабной военной агрессии.

Таким образом, компьютерная преступность вышла на уровень одной из самых серьезных международных проблем.

Ежегодные потери от компьютерной преступности составляют:

- в Великобритании – 2,5 млрд ф.ст. (4,45 млрд долл.);
- в странах Западной Европы – 30 млрд долл.;
- в США – 100 млрд долл.

При этом экономически развитые страны для защиты информации в кредитно-финансовой сфере используют исключительно национальные криптографические средства.

Таким образом, мировой опыт свидетельствует о том, что задача предупреждения компьютерной преступности является комплексной, а на защиту электронной информации требуются значительные затраты.

Обеспечение защиты информации на рынке ценных бумаг

Совокупность аппаратно-программных и организационно-технических средств, реализующих систему информационной безопасности ОТС, должна образовывать распределенный комплекс, функционирующий под управлением централизованной службы безопасности и возглавляемый администратором безопасности сети.

Служба безопасности сети должна обеспечивать:

- учет абонентов конфиденциальной связи;
- регистрацию и обработку ситуаций, связанных с нарушением безопасности;
- управление восстановлением конфиденциальной связи при компрометации ключей у абонентов сети;
- взаимодействие с центром управления безопасностью сети "Деловая сеть России";
- сбор статистики об информации, обрабатываемой средствами криптографической защиты (СКЗИ).

Для пользователей различных уровней защиты применяются различные механизмы распределения ключей.

Абонент конфиденциальной связи регистрируется администратором службы безопасности сети.

Для исключения возможности доступа несанкционированных пользователей к базам данных ОТС и дезорганизации работы системы внесение изменений в БД может производиться только персоналом, обслуживающим определенное оборудование (или администратором БД).

Функционирование телекоммуникационных средств сети обеспечивается персоналом службы управления сетью — администратором сети.

Служба безопасности и служба управления сетью совместно обеспечивают:

- защиту ресурсов сети;
- реконфигурацию сети;
- взаимодействие со службами управления сетью и безопасность базовой сети передачи данных ("Деловая сеть России").

Концепция безопасности в СПД "Деловая сеть России". При создании системы защиты информации на финансовом рынке целесообразно воспользоваться средствами защиты, предоставляемыми сетью передачи данных "Деловая сеть России" (ДСР), в рамках которой разработана концепция защиты информации и предоставления услуг. В ДСР особое место занимает решение вопросов обеспечения надежной защиты передаваемой, хранимой и обрабатываемой информации от несанкционированного доступа, контроля ее целостности и подлинности на базе современных информационных технологий.

ДСР должна обеспечивать структурам финансового рынка России комплексную безопасность за счет использования криптографических, алгоритмических и организационно-технических мер, средств и способов, гарантирующих безопасность информации.

ДСР обеспечивает выполнение требований, необходимых для обеспечения информационной безопасности абонентов в ОТС:

- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);
- обнаружение нарушений целостности объектов данных;
- живучесть сети связи при компрометации части ключевой системы;
- защиту технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации;
- защиту программных продуктов и средств вычислительной техники от внедрения программных вирусов и закладок;
- защиту от несанкционированного доступа к сети, в том числе и к средствам ее управления, предотвращающую снижение уровня защищенности информации;
- реализацию организационно-технических мероприятий, направленных на выполнение требований, регламентирующих эксплуатацию сети.

Задачи организации, обеспечения функционирования и безопасности СКЗИ, изготовления сертификатов открытых криптоключей для электронной цифровой подписи (ЭЦП), снабжения криптоключами в конкретной организации возлагаются на региональные центры управления безопасностью.

Общее руководство по вопросам деятельности всех центров управления безопасностью осуществляет главный центр управления.

Уровни зашиты информации и национальная политика России в области информационной безопасности

В ОТС должны использоваться как криптографические, так и организационные меры защиты информации пользователей, рекомендуемые к применению в сети ДСР.

Криптографические методы защиты информации реализуются на абонентском уровне путем использования следующих уровней защиты:

- уровень защиты А – комплексная защита по требованиям ФАПСИ, с ответственностью ФАПСИ за функционирование систем защиты информации;
- уровень защиты В – защита по требованиям ФАПСИ в части анализа программного окружения СКЗИ, специальной защиты, защищенности линейной передачи, а также в части требований к техническим средствам и помещениям. Предусматривается контроль ФАПСИ за функционированием систем защиты информации;
- уровень защиты С – криптографическая защита на уровне потребителя по требованиям ФАПСИ. Системы создаются пользователем на основе приобретаемых средств шифрования и ЭЦП, на которые имеется сертификат ФАПСИ. Встраивание средств шифрования и ЭЦП в прикладные системы должно происходить с выполнением определенных интерфейсных и криптографических протоколов для обеспечения взаимодействия системы с системами уровня

С. СКЗИ при построении системы не подлежит модификации. Пользователь приобретает сертифицированные СКЗИ, на которые имеется разрешение ФАПСИ, и несет ответственность за их использование в соответствии с рекомендациями разработчика.

Пользователям предоставляется возможность применять СКЗИ в следующих режимах:

- информация подписывается и шифруется;
- информация подписывается и не шифруется;
- информация не подписывается и шифруется;
- информация не подписывается и не шифруется.

Если абонентские комплексы (АК) принадлежат объектам различного уровня защищенности, то программно-техническими и организационными мерами должна быть исключена возможность отправки в АК сообщений с уровнем конфиденциальности выше уровня этого АК.

Обмен информацией между АК различных уровней защищенности может производиться только по инициативе абонента, имеющего более высокий уровень защиты.

Алгоритмы шифрования и их реализации в виде аппаратно-программных средств и реализация средств защиты от НСД должны быть только отечественного производства.

Состав и назначение программно-аппаратных средств в АК на базе отдельного ПК должны быть фиксированны и неизменны в течение всего времени его использования.

Для АК с уровнями защиты А, В и С система криптографической защиты программно-аппаратных средств шифрования должна осуществлять контроль целостности программ криптографической защиты.

Для АК с уровнями защиты А и В должны быть обеспечены изолированность операционной среды и контроль за исполняемыми файлами.

Для АК с уровнем защиты С программные продукты, работающие совместно со средствами защиты информации, должны соответствовать объявленным характеристикам, быть защищены от вирусных разрушающих воздействий, закладок и исследованы на наличие скрытых функциональных возможностей.

Ключи шифрования изготавливаются ФАПСИ и доставляются на АК по закрытым каналам связи, а также с помощью фельдъегерской связи.

Ключи-подписи юридических и физических лиц изготавливаются на специально организованных рабочих местах пользователей сети — сертифицированных ФАПСИ АРМах администраторов безопасности.

Национальная политика России в области информационной безопасности. Ориентация на кооперацию с зарубежными странами при развитии в России систем информационного обмена открывает возможность доступа в эти системы зарубежным пользователям. Недостаточное воздействие государства на функционирование и развитие рынка информационных продуктов и услуг в России может привести к появлению информации, утечка которой представляет угрозу для безопасности страны, в особенности при широкомасштабной и направленной деятельности на этом рынке зарубежных фирм.

Финансовый рынок России остается и, видимо, будет оставаться самой притягательной сферой для организованной преступности. До приведения банковского и уголовного законодательства к реалиям сегодняшнего дня снижения уровня преступности в данном направлении ожидать не следует. Кроме того, преступные сообщества в Российской Федерации и за ее пределами не прекращают попыток осуществления крупномасштабных противоправных акций, которые могут существенно дестабилизировать кредитно-финансовую систему России и повлиять на деятельность коммерческих банков и участников рынка ценных бумаг.

В последние годы в Российской Федерации был принят ряд законодательных актов, направленных на решение вопросов защиты информации. Среди ранее принятых актов следует отметить в первую очередь законы "О государственной тайне", "Об информации, информатизации и защите информации", "О сертификации продукции и услуг", "О федеральных органах правительственной связи и информации".

В соответствии с Законом Российской Федерации "О федеральных органах правительственной связи и информации" ФАПСИ предоставлено право выдачи предприятиям и организациям независимо от форм собственности лицензий на создание и эксплуатацию шифровальных средств, а также на предоставление услуг шифровальной связи. Защита информации в Российской Федерации должна проводиться организациями, имеющими лицензию ФАПСИ, а средства защиты должны иметь сертификаты Федерального агентства.

Кроме того, ряд указов Президента и постановлений Правительства Российской Федерации регламентирует, в частности, порядок экспорта и импорта шифровальных средств. Указ Президента Российской Федерации № 334 от 3 апреля 1995 года "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" подытоживает комплекс разработанных и принятых законодательных и иных нормативных актов в данной области. Указ требует безусловного и ускоренного внедрения в жизнь предусмотренных предыдущими законами и постановлениями мер по наведению порядка в такой жизненно важной для любого государства сфере, как защита конфиденциальной информации; вводит в действие механизм реализации перечисленных выше законодательных актов, возлагая ответственность за их выполнение на правоохранительные, таможенные и налоговые органы страны. Данный Указ необходимо рас-

сматривать как составную часть ряда законодательных и нормативных актов, принятых в стране в 1993-1995 годах и направленных на формирование цивилизованных отношений в сфере защиты конфиденциальной информации.

Указ Президента Российской Федерации № 662 от 3 июля 1995 года "О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации" регламентирует условия функционирования электронной системы финансовых расчетов при формировании рынка ценных бумаг Российской Федерации.

Литература

Законодательные и нормативные акты:

О рынке ценных бумаг: Федеральный закон № 39-ФЗ от 22 апреля 1996 г. (принят ГД ФС РФ 20.03.96 г.) // СЗ РФ. – № 17. - Ст. 1918; Рос. газ. – 1996. – 25 апр. (№ 79).

Об утверждении концепции развития рынка ценных бумаг в Российской Федерации: Указ Президента РФ № 1008 от 1 июля 1996 г. // Рос. газ. – 1996. – 5 июля (№ 125); Рос. газ. (Ведомственное приложение). – 1996. – 6 июля. (№ 126); СЗ РФ. – 1996. – № 28. – Ст. 3356.

О Федеральной комиссии по рынку ценных бумаг: Указ Президента РФ № 1009 от 1 июля 1996 г. // СЗ РФ. – 1996. – № 28. – Ст. 3357; Рос. газ. – 1996. – 12 июля (№ 130); Рос. газ. (Ведомственное приложение). – 1996. – 13 июля (№ 131).

О предоставлении регистрационных форм профессиональными участниками рынка ценных бумаг: Распоряжение ФКЦБ России № 201-р. от 17 марта 1998 г. // http: www.fedcom.ru

О системе раскрытия информации на рынке ценных бумаг: Постановление ФКЦБ России №2 от 9 января 1997 г. // http: www.fedcom.ru

О системе раскрытия информации: Комментарии к Постановлению ФКЦБ №2 от 9 января 1997 г. // http: www.fedcom.ru

Специальная литература:

Генин М. Законы о раскрытии информации // Компьютерра. – 1998. – № 6. «Прозрачный» рынок – это выгодно // Дело. – 1998. – 10 апр. – № 7(75).

Левенчук А. Раскрытие информации государственных и частных организаций // Компьютерра. – 1998. – № 6.

Клещев Н.Т. и др. Рынок ценных бумаг: шаг России в информационное общество. – М.: Экономика, 1997.