ЗАЩИТА ИНФОРМАЦИИ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Ясенев В. Н.

Глобальные социальные изменения, произошедшие в мире в конце XX в., требуют объективного анализа информационной среды мирового сообщества. Следует отметить, что ранее проблема обеспечения информационной безопасности в нашей стране не только не рассматривалась, но и фактически игнорировалась. При этом считалось возможным ее решение путем введения тотальной секретности и различных ограничений. И только в последние годы в России была осознана вся важность данного вопроса: в составе Совета безопасности РФ создана Межведомственная комиссия по информационной безопасности. Разработан проект ее доктрины, в которой отражены методы и средства защиты жизненно важных интересов личности, общества, государства в мировом информационном пространстве.

В рамках обеспечения информационной безопасности следует рассмотреть на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности;
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

К первой группе следует отнести в первую очередь главу 28 ("Преступления в сфере компьютерной информации") раздела IX новой редакции Уголовного кодекса. Эта глава достаточно полно охватывает основные угрозы информационным системам, однако обеспечение практической реализуемости соответствующих статей пока остается проблематичным.

Закон "0б информации, информатизации и защите информации (приложение №1) можно причислить к этой же группе. Правда, положения этого закона носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно.

К группе направляющих и координирующих законов и нормативных актов относится целая группа документов, регламентирующих процессы лицензирования и сертификации в области информационной безопасности. Главная роль здесь отведена Федеральному агентству правительственной связи и информации (ФАПСИ) и Государственной технической комиссии (Гостехкомиссии) при Президенте Российской Федерации.

В области информационной безопасности законы реально преломляется и работают через нормативные документы, подготовленные соответствующими ведомствами.

Самое важное на законодательном уровне — создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Конечно, законы не могут опережать жизнь, но важно, чтобы

отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Хотелось бы обратить особое внимание на желательность приведения российских стандартов и сертификационных нормативов в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности.

Главное же, чего не хватает современному российскому законодательству (и что можно почерпнуть из зарубежного опыта), это позитивная (не карательная) направленность. Информационная безопасность — это новая область деятельности, здесь важно научить, разъяснить, помочь, а не запретить и наказать. Общество должно осознать важность данной проблематики, понять основные пути решения соответствующих задач, должны быть скоординированы научные, учебные и производственные планы так можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- ориентация на созидательные, а не карательные законы;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Проблемам информационной безопасности в последние годы было уделено определенное внимание в монографиях, научных статьях, учебных пособиях.

Прежде всего это труд Мартина Либики «What is Information warfare?»являющейся основополагающий среди трудов, относящихся к теме "Информационные войны", а также его книга «Defending the Cyberspace. » Кроме этого, из зарубежных источников можно выделить книгу Давида С. Альбертса «Defensive information warfare».

Что касается отечественных источников, то, к сожалению, в настоящее время эта проблема мало отражена. Среди них можно назвать лишь такие работы, как "Новые информационные технологии и современные международные отношения" Д. Г. Балуева, а также его работа "Завоевание будущего. Внешняя политика России на рубеже веков".

Проблемам обеспечения защиты информационных объектов предприятия (фирмы) посвящены труды В. Б. Зубик, Г. А. Титоренко, Вехова В. Б., Н. В. Макаровой и др. Несмотря на несомненную и бесспорную теоретическую и практическую значимость указанные исследований, в них не рассматривается в комплексе характеристика информационных компьютерных преступлений, а также четко не выделены проблемы, касающиеся совершенствования практики их раскрытия и предупреждения. Это в конечном итоге оказывает негативное влияние на качественный уровень профессиональной подготовки сотрудников правоохранительных органов, аудиторов, бухгалтеров и др. специалистов.

Угрозы безопасности информационным объектам подразделяются на 4 группы.

1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналом связи. Информация, обрабатываемая на компьютерах или передаваемая по локальным сетям передачи данных, может быть снята через технические каналы утечки.

2. Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой.

3. Угрозы доступности данных. Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации.

4. Угрозы отказа от выполнения транзакций. Возникают в том случае, когда легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность.

Транзакция — это передача сообщений с подтверждением об их передаче и приеме.

Угрозы могут быть обусловлены естественными факторами (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины); человеческими факторами, которые в свою очередь подразделяются на:

• пассивные угрозы (угрозы, носящие случайный, неумышленный характер). Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной "утечкой умов", знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т. п.);

• активные угрозы (угрозы, обусловленные умышленными, преднамеренными действиями людей). Это угрозы, связанные с передачей, искажением, и уничтожением научных открытий, изобретений, секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); просмотром и передачей различной документации, просмотром "мусора"; подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной "утечкой умов", знаний, информации (например, в связи с получением другого гражданства по корыстным мотивам); человеко-машинными и машинными факторами, подразделяющимися на:

• пассивные угрозы. Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.); с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

• активные угрозы. Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и других материалов, просмотр вводимых данных, распечаток, просмотр "мусора"); угрозы, реализуемые бесконтактным

способом (электромагнитных излучений, перехват сигналов, наводимых в цепях, визуально-оптические способы добычи информации). Способы воздействия угроз на информационные объекты подразделяются на:

- информационные;
- программно-математические;
- физические;
- радиоэлектронные;
- организационно-правовые.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;
- несанкционированный доступ к информационным ресурсам;
- манипулирование информацией (дезинформация, сокрытие или сжатие информации);
- нарушение технологии обработки информации.

Программно-математические способы включают:

- внедрение компьютерных вирусов;
- установка программных и аппаратных закладных устройств;
- уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты информации;
- воздействие на персонал;
- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

- невыполнение требований законодательства о задержке с принятием необходимых нормативно-правовых положений в информационной сфере;
- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Безопасность информационной системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности ресурсов системы.

Систему обеспечения безопасности информации можно разбить на следующие подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компью-

тера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений и разглашения.

Безопасное программное обеспечение представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается принятием мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в отчет на телекоммуникационный запрос. К объектам информационной безопасности на предприятии относят:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;
- средства и системы информатизации — средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления предприятиями, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

Анализ существующих технологий и средств сбора и транспортировки финансовой информации выявил ряд их особенностей и перспектив:

- отсутствуют сквозные технологии обработки данных, имеются функциональные разрывы между отдельными задачами;
- до настоящего времени не создана единая транспортная сеть, обеспечивающая надежную доставку финансовой информации;
- сбор и обработка значительной части информации дублируется различными ведомствами и организациями (налоговой инспекцией, таможенным комитетом, внебюджетными фондами, региональными и отраслевыми органами управления и др.);
- отсутствуют централизованно утвержденные нормативные документы, определяющие информационное взаимодействие (с использованием электронных носителей) между экономическими ведомствами;
- используемые информационные технологии устарели, не соответствуют современному уровню.

Защита информации в автоматизированных системах экономического объекта должна строиться исходя из следующих основных принципов:

- обеспечение физического разделения областей, предназначенных для обработки секретной и несекретной информации;
- обеспечение криптографической защиты информации;
- обеспечение аутентификации абонентов и абонентских установок;
- обеспечение разграничения доступа субъектов и их процессов к информации;
- обеспечение установления подлинности и целостности документальных сообщений при их передаче по каналам связи;
- обеспечение защиты от отказов от авторства и содержания электронных документов;

• обеспечение защиты оборудования и технических средств системы, помещений, где они размещаются, от утечки конфиденциальной информации по техническим каналам;

• обеспечение защиты шифротехники, оборудования, технических и программных средств от утечки информации за счет аппаратных и программных закладов;

• обеспечение контроля целостности программной и информационной части автоматизированной системы;

• использование в качестве механизмов защиты только отечественных разработок;

• обеспечение организационно-режимных мер защиты. Целесообразно использование и дополнительных мер по обеспечению безопасности связи в системе;

• организация защиты сведений об интенсивности, продолжительности и графиках обмена информацией;

• использование для передачи и обработки информации каналов и способов, затрудняющих ее перехват;

• реализация безопасного администрирования финансовой системы.

К механизмам обеспечения защиты информации в автоматизированных системах относятся:

• контроль доступа к информационным ресурсам;

• шифрование данных (криптографическая защита);

• электронная цифровая подпись;

• обеспечение целостности и достоверности данных;

• обеспечение аутоидентификации (подтверждение подлинности отправителя и получателя информации);

• маскировка графика (затруднение анализа потоков информации без ее вскрытия).

Особенностью системного подхода к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам программно-технические, правовые. организационно-экономические. Организация подобный защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы.

Системный подход к защите информации базируется на следующих методологических принципах:

• конечной цели — абсолютного приоритета конечной (глобальной) цели;

• единства — совместного рассмотрения системы как целого и как совокупности частей (элементов);

• вязности — рассмотрения любой части системы совместно с ее связями с окружением;

• модульного построения — выделения модулей и системе и рассмотрения ее как совокупности модулей.

• иерархии — введения иерархии частей (элементов) и их ранжирования;

• функциональности — совместного рассмотрения структуры н дикции с приоритетом функции над структурой;

• развития — учета изменяемости системы, ее способности к развитию, расширению, заменению частей, накапливанию информации;

• децентрализация — сочетания к принимаемых решениях и управлении централизации и децентрализации;

• неопределенности — учета неопределенностей и случайностей в системе.

Комплексная защита информации в автоматизированных системах достигается за счет безусловного выполнения требований нормативных документов, регламентирующих деятельность в области защиты информации.