В последние десятилетия. экспорт государственного капитала стал несколько ослабевать. На первое место вышли транснациональные банки, но важная роль государства на международном рынке ссудных капиталов сохраняется. Основное отличие государственного кредитования от частного в том, что государство стремится, прежде всего, к защите своих политических интересов, а не к получению максимальной прибыли. Подобное изменение характера деятельности финансово-кредитных институтов и государства происходит под влиянием научно-технической революции, инфляции, появления и усиления коллективных валют и нефтедолларов, изменения структуры вывоза капитала.

Одним из основных факторов развития международного рынка капиталов стала неолиберальная модель глобализации. Расширению процесса глобализации способствовала проводимая промышленно развитыми государствами политика поощрения и пропаганды либерализации (так называемый Вашингтонский консенсус).

В.Л.Почекин,
Белорусский государственный университет информатики и радиоэлектроники (г.Минск)

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНОМ БИЗНЕСЕ

Система защиты информации и обеспечения безопасности виртуального бизнеса призвана решать те же проблемы, что и системы безопасности для традиционных видов деятельности. Если не рассматривать действия злоумышленника, приводящие к физическому уничтожению предприятия, то совокупность угроз, с которыми сталкивается система безопасности, включает:

- утечку конфиденциальной информации коммерческой, финансовой, научно-технической деятельности предприятия;
- несанкционированный доступ к системам управления предприятием и технологическими процессами;
- подделку различного рода документов;
- мошенничество при проведении торговых и финансовых операций.

Следует заметить, что оформление договоров, удаленная работа с клиентами, заказ и доставка товаров и услуг, управление предприятием, получение кредитов напрямую связаны с обменом документами в электронном виде. В расчетной системе при проведении платежей происходят по существу два процесса – идентификация сторон и передача сообщений, снабженных определенными атрибутами, т.е. процессы, типичные для электронного документооборота. Даже производство продуктов и предоставление услуг в области обработки, хранения и передачи информации может быть сведено к работе с электронными документами. В этом смысле передача данных в компьютерных сетях есть нечто иное, как обмен сообщениями специального формата, а любой законченный продукт (видеофильм, электронный учебник, программное обеспечение), размещенный на каком-либо носителе или помещенный в электронный банк данных, по смыслу сразу становится электронным документом.

Правовые методы направлены *на создание защитного иммунитета*, основанного на угрозе применения репрессивного инструмента в отношении нарушителя интересов собственника информации *(источников угроз)* – с одной стороны, и установление механизмов применения определенных санкций в отношении этих нарушителей – с другой. Эти методы в основном ориентированы *на устранение угроз*, реализуемых источниками *антропогенного* характера, и являются базисом для реализации всех остальных методов защиты.

Вопросы нрава в этой сфере еще не решены полностью, однако имеющейся правовой базы достаточно для того, чтобы успешно начать применять для целей защиты интересов собственника информационных ресурсов все способы защиты гражданских прав, предусмотренные законом. К примеру, за правонарушения при работе с информацией и несоблюдение режима конфиденциальности, установленного собственником информации, предусмотрена ответственность (в том числе и материальная). Попытки овладения информацией, для которой установлен режим конфиденциальности, похищение документов, подкуп персонала, угрозы или иное, даже если не наступили какие-либо последствия, расценивается законом как преступление. Лица, незаконными методами получившие конфиденциальную информацию, в том числе сотрудники и контрагенты, обязаны возместить причиненные убытки.

Экономические методы также воздействуют на *антропогенные источники* угроз и, в совокупности с правовыми методами, позволяют не только сократить число этих источников, но и ввести в действие *механизмы ликвидации* последствий реализации угроз. К примеру, возможно применение системы коэффициентов и надбавок, которая создаст особые льготы сотрудникам, работающим с конфиденциальной информацией, и стабилизирует контингент; страхование информации (информационных рисков) для обеспечения полной и скорой компенсации ущерба.

Организационные методы в основном ориентированы на работу с персоналом, выбор местоположения и размещения объектов информатизации; организацию систем физической и противопожарной защиты; контроль выполнения принятых мер; возложение персональной ответственности за реализацию мер защиты. Эти методы применимы для *уменьшения числа внутренних антропогенных, техногенных* и *стихийных источников угроз*, а *также уменьшения влияния уязвимостей*. Как правило, они уже частично реализованы на действующих объектах информатизации. Их применение дает значительный эффект и сокращает общее число возможных реализаций угроз.

Инженерно-технические методы связаны с оптимальным построением зданий, сооружений, сетей инженерных коммуникаций, транспортных магистралей с учетом требований безопасности информации. Это довольно дорогостоящие методы, но они, как правило, *реализуются еще на этапе строительства* или *реконструкции объекта информатизации*, способствуют повышению его общей живучести и дают высокий эффект при устранении источников угроз. А некоторые источники угроз, например обусловленные стихийными бедствиями или техногенного характера, вообще не устранимы

другими методами. Кроме того, инженерно-технические методы позволяют ослабить влияние большого количества объективных и случайных уязвимостей.

Технические методы основаны на применении специальных технических средств защиты информации и контроля обстановки и дают значительный эффект при устранении угроз, связанных с действиями криминогенных элементов *(внешние антропогенные источники угроз)* по добыванию информации незаконными техническими средствами. Кроме того, некоторые методы, например резервирование средств и каналов связи, оказывают значительный эффект при устранении воздействия некоторых техногенных источников угроз и ослабляют влияние объективных, субъективных и случайных уязвимостей.

Программно-аппаратные методы в основном нацелены на *устранение проявления угроз, непосредственно связанных с процессом обработки* и *передачи информации*. Без этих методов невозможно построение целостной комплексной подсистемы информационной безопасности. В этой группе объединяются такие методы, как: ограничение доступа к средствам обработки и объектам защиты, разграничение доступа пользователей, управление потоками информации, маскирование структуры и назначения информационной сети, подтверждение подлинности информации, преобразование информации при ее передаче и хранении, блокирование неиспользуемых сервисов, мониторинг целостности программного обеспечения, конфигурации информационной сети, разрушающих воздействий и др.

Сопоставление актуальных угроз и методов их парирования позволяет определить, какими методами, какие угрозы наиболее целесообразно устранять, и рассчитать соотношение в распределении финансовых средств, выделенных на обеспечение безопасности информации.

Таким образом, анализ составных частей защиты информации виртуального бизнеса позволяет сделать принципиальный вывод, что ***система безопасности виртуального бизнеса по своей сути представляет собой систему безопасности электронного документооборота***.