Кришталюк А.Н.

ПРАВОВЫЕ АСПЕКТЫ СИСТЕМЫ БЕЗОПАСНОСТИ

курс лекций

Академия МАБИВ
www.mabiv.ru

Александр Кришталюк

Правовые аспекты системы безопасности

МОО "Межрегиональная общественная организация "Академия безопасности и выживания""

2014

Кришталюк А. Н.

Правовые аспекты системы безопасности / А. Н. Кришталюк — МОО "Межрегиональная общественная организация "Академия безопасности и выживания"", 2014

Обеспечение безопасной деятельности необходимо для любых предприятий и учреждений, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются для обеспечения их безопасности.Предназначено для преподавателей и студентов вузов специальностей по направлению безопасности, специалистов по безопасности, руководителей и менеджеров компаний.

Содержание

Александр Кришталюк
Правовые аспекты системы безопасности
Курс лекций

Рецензент:

кандидат технических наук, доцент кафедры «Электроника, вычислительная техника и информационная безопасность» ФГБОУ ВПО «Госуниверситет – УНПК» А. В. Артемов

* * *

А. Н. Кришталюк, руководитель Национального социального проекта «Здоровая Нация», аспирант кафедры «Туризм, рекреация и спорт» ФГБОУ ВПО «Госуниверситет – УНПК»

Лекция 1. Состояние проблемы обеспечения безопасности

Учебные вопросы:
1. Современные угрозы безопасности предприятия.
2. Анализ современного состояния проблемы безопасности.

Вопрос 1. Современные угрозы безопасности предприятия

Обеспечение безопасной деятельности необходимо для любых предприятий и учреждений, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются для обеспечения их безопасности.

Поэтому, анализируя современное состояние проблемы защиты, необходимо выбрать такой объект, в котором «аккумулировались» бы все основные особенности защиты. Одним из таких объектов является банковская система. Банк является наиболее разветвленным, постиндустриальным субъектом экономики, концентрирующим в себе огромный экономический потенциал и, естественно, привлекающий внимание злоумышленников (ЗЛ).

Прежде чем приступить к анализу современного состояния проблемы безопасности, необходимо определить, что подлежит защите и каким основным принципом следует пользоваться. По сложившейся международной практике безопасности объектами защиты с учетом их приоритетов являются:

1) личность;

2) информация;

3) материальные ценности.

Если приоритет сохранения безопасности личности является естественным, то приоритет информации над материальными ценностями требует более подробного рассмотрения. Это касается не только информации, составляющей государственную или коммерческую тайну, но и открытой информации.

Рыночные отношения с их неотъемлемой частью – конкуренцией обязательно требуют противодействия внешним и внутренним угрозам. Объекты защиты в большей или меньшей степени, в зависимости от целей ЗЛ и от конкретных условий, могут подвергаться различным нападениям, угрозам или находиться в ситуации, в которой они по объективным причинам подвергаются опасности.

Понятие "безопасная деятельность" любого предприятия или организации включает в себя:

1. Физическую безопасность, под которой понимается обеспечение защиты от посягательств на жизнь персонала.

2. Экономическую безопасность.

3. Информационную безопасность.

4. Материальную безопасность, т. е. сохранение материальных ценностей от всякого рода посягательств, начиная от их краж и заканчивая угрозами пожара и других стихийных бедствий.

1.1. Угрозы экономической безопасности

Угрозы экономической безопасности деятельности банка могут быть самыми различными, но мы выделим только основные угрозы, которые входят в компетенцию СБ.

К данному виду угроз в первую очередь относятся угрозы от:

1) отдельных сотрудников банка;

2) криминальных российских структур;

3) криминальных зарубежных структур;

4) международных криминальных структур.

Несмотря на очевидность данных угроз, проиллюстрируем их на наиболее ярких конкретных примерах.

В феврале 1995 года обанкротился крупный английский банк «Беринге». Это произошло потому, что работник банка Ник Лисон проводил незаконные сделки через счет, который был открыт еще в 1992 году. Убытки в 830 млн. фунтов стерлингов накапливались в течение долгого времени. Ни руководство банка, ни аудиторы, ни контролеры не выявили за это время никаких нарушений. Одной из причин явилось то, что Ник Лисон отвечал как за торговые операции, так и учетную документацию по операционной деятельности, а руководство банка не осуществляло должный контроль за раздельным ведением клиентских и собственных счетов брокеров.

В 1994 году пресечена деятельность преступной группы, состоящей из работников РКЦ ГУ ЦБ по Новосибирской области, Сибирского филиала Инкомбанка и представителей фиктивной коммерческой фирмы Группа путем перечисления денег по фальшивым платежным документам на счет этой фирмы похитила почти 1,4 миллиарда рублей.

В тяжелых условиях становления рынка положение банков усугубляется мощным и все возрастающим давлением со стороны криминального мира. Ни для кого не является секретом, что многие коммерческие фирмы прямо или косвенно связаны с мафиозными структурами или существуют за счет их средств.

Происходит постепенное сращивание российского и зарубежного преступного мира.

В условиях политической и экономической нестабильности и при наличии различного рода угроз (от неплатежеспособности до мошенничества) является естественным объединение усилий коммерческих структур для сохранения их экономической безопасности. Примером этому является соглашение между банками «Империал», "Столичный" и другими, направленное на сотрудничество и деятельность по предотвращению недобросовестной конкуренции, что, несомненно, повысит степень их экономической защищенности.

Учитывая высокий уровень латентности экономических преступлений, приведенные цифры лишь отчасти отражают процесс последовательного роста темпов криминализации экономики, сопровождающийся расширением масштабов проникновения в нее организованных преступных группировок, все более тесного смыкания с работниками органов государственного управления, в том числе на самом высоком уровне.

Прогнозы на ближайшее будущее предполагают появление новых и усиление общественно опасных форм преступной деятельности в сфере кредитно-денежных отношений (махинации с векселями, кредитными карточками, незаконная эмиссия ценных бумаг и т. п.).

В общем виде можно сформулировать основные угрозы экономической безопасности банка:

– плохая адаптированность существующей банковской системы к условиям рынка;

– общая неплатежеспособность;

– невозврат ссуд;

– лжепредпринимательство;

– мошенничество;

– подрыв доверия.

Наличие данных угроз обусловлено следующими видами риска:

1) риск утечки, уничтожения или модификации банковской информации;

2) риск отсутствия у руководства банка объективной информации о внутренней и внешней среде;

3) риск распространения конкурентами во внешней среде необъективной или опасной для банка информации.

Таким образом, обеспечение коммерческой деятельности банка или любой фирмы включает в себя не только защиту информации, но и сбор, классификацию, анализ, оценку и выдачу прогнозов для успешной коммерческой деятельности. Говоря другими словами, чем выше

информационное обеспечение банка, тем менее возможны угрозы его экономической деятельности.

1.2. Угрозы физической безопасности

В настоящее время участились случаи нападения на банкиров и служащих банка. Как правило, это прежде всего руководители коммерческих банков и фирм, которые в течение длительного времени (например, для запугивания, склонения к сотрудничеству и т. п.) или, наоборот, короткого промежутка времени (ограбление или убийство) являются объектом нападения со стороны преступников. Примеров тому достаточно.

Профессор А. В. Крысин в статье "Деятельность коммерческих банков (фирм) в условиях роста террористической угрозы" (см.: Частный сыск, охрана, безопасность, 1994, № 1) отмечает следующие методы воздействия на сотрудников коммерческих объектов:

– похищения и угрозы похищения главы и членов семьи;

– убийства, сопровождаемые насилием, издевательствами и пытками;

– психологический террор, угрозы, шантаж, вымогательство;

– публикация дезинформационных материалов о текущей деятельности некоторых коммерческих организаций, которые прямо направлены на их дискредитацию и компрометацию отдельных сотрудников;

– инспирация официальных заявлений от имени некоторых органов массовой информации и представителей исполнителей массовой власти, в которых подытоживается деловая репутация и наносится моральный и материальный ущерб отдельным коммерческим банкам, фирмам.

При этом выделяются следующие основные методы и приемы диверсионно-террористической деятельности:

– взрывы;

– обстрелы из автоматического оружия различных калибров и сигнальных ракетниц;

– минирования, в том числе с применением дистанционного управления;

– поджоги, броски канистр и иных емкостей с легко воспламеняющимися жидкостями и смесями;

– нападения, вторжения, захваты, пикетирования, блокирования;

– акты вандализма, повреждение входных дверей, решеток, ограждений, витрин, витражей, мебели, а также транспортных личных и служебных средств.

Цель подобных акций:

– откровенный террор в отношении коммерческих структур;

– нанесение им серьезного материального и морального ущерба, который в ряде случаев составляет десятки тысяч долларов США;

– срыв на длительное время, порой до нескольких месяцев, нормального функционирования коммерческого предприятия;

– вымогательство значительных сумм денег или каких-либо льгот (кредиты, отсрочки платежей и т. п.) перед лицом террористической угрозы.

Одной из реальных мер обеспечения физической безопасности является доведение до служащих защищаемого объекта, которым может угрожать опасность, обязательных правил поведения с учетом сложившейся обстановки, характера угрозы, возможного времени и места ее реализации и мероприятий, обеспечивающих их безопасность. Однако способы реализации угроз могут быть самые различные. Поэтому данные указания и советы могут носить лишь общий характер, поскольку преступники находят все новые и новые пути для достижения своих целей.

Резюмируя, можно сказать, что в настоящее время ни один человек не может чувствовать себя в безопасности. Различного рода преступления не получили бы такого широкого распространения, если бы банкиры уделяли должное внимание организации работы СБ. Обеспечение личной безопасности – напряженная работа. Банкир может попасть в "зону риска", и применение определенных методов охраны требует определенной системы поведения не только от охранников, но и от объекта охраны. Это обусловлено тем, что преступники предварительно собирают информацию о жертве, изучают "слабые места" и широко ими пользуются. Без необходимой информации об объекте нападения значительно увеличивается степень риска для преступников. Поэтому необходимо скрывать любую информацию, которую преступник может использовать при подготовке или совершении преступления. Важно отметить, что убийства, как правило, остаются нераскрытыми, что наводит на естественную мысль о хорошей организации и подготовке преступников.

1.3. Угрозы информационной безопасности

Как считают западные специалисты, утечка 20 % коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы. Ни одна даже преуспевающая фирма США не просуществует более трех суток, если ее информация, составляющая коммерческую тайну, станет известной. Таким образом, экономическая и информационная безопасность банка или фирмы тесно взаимосвязаны.

Уменьшение угрозы экономической деятельности банка предусматривает получение информации о конкурентах. Поэтому, вполне естественно, уменьшение данной угрозы для одних банков влечет за собой увеличение угрозы экономической деятельности для других банков. Это стало возможным из-за наличия промышленного и, в частности, банковского шпионажа.

Ущерб от деятельности конкурентов, использующих методы шпионажа, составляет в мире до 30 % всего ущерба, а это – миллиарды долларов. Точную цифру убытков указать нельзя по следующей причине: ни ЗЛ, ни пострадавшие не стремятся предать гласности совершенные действия. Первые, боясь ответственности за содеянное, а вторые – из-за боязни потерять имидж. Этим объясняется высокий уровень латентности правонарушений и отсутствие о них информации в открытой печати. Поэтому до читателей доходит менее 1 % от всех случаев нарушений, которые обычно имеют уголовный характер и которые скрыть нельзя.

Банковский шпионаж использует самые разнообразные приемы: «классические» методы шпионажа (шантаж, подкуп и т. п.), методы промышленного шпионажа, несанкционированное использование средств вычислительной техники, аналитические методы. Возможность использования указанных методов появилась потому, что банковская информация имеет различные формы представления (документ, человеческая речь, машинный носитель и т. п.) и, следовательно, различные способы ее передачи, хранения и обработки. Поэтому спектр угроз информационной безопасности весьма широк.

Промышленный шпионаж достаточно развит в западных странах. Сотни фирм специализируются на изготовлении средств технической разведки и на проведении мероприятий по промышленному шпионажу. В последнее время он получил распространение и в нашей стране. Масштабы промышленного шпионажа можно оценить хотя бы по следующему факту – на проходившей в 1995 году выставке-продаже зарубежных и отечественных средств технической разведки было продано 70 тыс. единиц средств добывания информации и только единицы их поиска и борьбы с ними. А всего на выставке было представлено более 2000 видов различных устройств. В настоящее время около 200 российских и зарубежных фирм торгуют на территории России и стран СНГ средствами промышленного шпионажа и контршпионажа. Рост конкуренции стимулирует спрос на оборудование промышленного шпионажа.

За последнее время накопилось немало примеров, когда потери коммерческих структур от утечки информации за счет промышленного шпионажа превосходили размеры прямых потерь от краж или разбойных нападений. Нельзя недооценивать возможности промышленного шпионажа и ущерб, который он может принести банку или фирме. Страшно представить, какой ущерб может принести банку закладное устройство стоимостью всего $10 в случае его удачного размещения. Примеров тому достаточно – читатель сам знает о них, а исходя из ранее сказанного они (примеры) не приводятся.

Используют средства и методы промышленного шпионажа, как правило, либо недобросовестные конкуренты, либо мафиозные структуры. Причем последние, в отличие от примитивной уголовщины, имеют свою собственную разведку и контрразведку, а на их техническое оснащение новейшими и дорогостоящими средствами не жалеют денег.

Противодействие получению информации с помощью технических средств разведки (ПДТР) достаточно сложно и по силам только специалистам, имеющим практический опыт. Это объясняется следующими основными причинами:

– в общем случае неизвестно, кто, когда, в каком месте и каким образом попытается получить информацию;

– приобретение средств промышленного шпионажа не вызывает затруднений;

– правовая регламентация использования средств промышленного шпионажа несовершенна. С помощью средств промышленного шпионажа не только различными способами подслушивают или подсматривают за действиями конкурентов, но и получают информацию, непосредственно обрабатываемую в средствах вычислительной техники. Это уже стало повседневным явлением (например, съем информации с дисплеев или линий связи ЭВМ). Однако наибольшую опасность здесь составляет непосредственное использование ЗЛ средств вычислительной техники, что породило новый вид преступлений – компьютерные преступления, т. е. несанкционированный доступ к информации (НСД), обрабатываемый в ЭВМ.

Рис 1. Проблемы и направления обеспечения безопасности

По мнению зарубежных экспертов, ущерб, нанесенный банкам США за счет несанкционированного использования вычислительных сетей путем введения и «навязывания» ложной информации из Москвы и Санкт-Петербурга российскими мафиозными структурами, только за I квартал 2005 года составил $300 млн.

Контрольные проверки, проведенные несколько лет назад по просьбе ряда банков Москвы специалистами Гостехкомиссии России и Российского центра «Безопасность», показали, что при использовании вычислительных сетей относительно просто войти в базы данных, считать и изменять их содержимое, подделывать переводы и т. п.

Приведенные примеры показывают, что использование средств вычислительной техники раскрывает новую область для промышленного шпионажа. При этом ЗЛ могут не только

получить доступ к открытой информации, но и к информации, содержащей коммерческую и государственную тайну. Если студент-хакер может войти в сеть НАТО, как это было совсем недавно, и получить секретную ключевую информацию, то в коммерческую вычислительную систему может войти и программист-профессионал, оставшийся без работы и нанятый конкурентами или мафиозными структурами. А если можно войти в вычислительную систему, то можно не только получить информацию, но и всю ее уничтожить, модифицировать или манипулировать. В силу этого банк или фирма потерпят убытки или станут на грани финансового краха из-за невозможности выполнения своих функций.

В настоящее время в зарубежных странах появились информационные брокеры, которые с помощью хакеров взламывают СЗИ, получают информацию, а затем ее продают. Покупателями могут быть как конкуренты пострадавшей фирмы, так и сама пострадавшая фирма.

Понятие "компьютерная преступность" включает в себя несколько позиций. В него входят несанкционированное проникновение в сети, хищение времени ЭВМ и изменение информации ("логической бомбы", вирусы и т. д.), также противоправные действия с использованием компьютерной техники:

– различные виды мошенничества, связанные с неправомерным использованием пользовательских терминалов, осуществление международных денежных переводов (вследствие чего фирмы несут убытки, исчисляемые сотнями тысяч долларов), незаконное изготовление и подделка электронных средств платежа и их использование для хищения наличных средств из банкоматов;

– несанкционированное тиражирование компьютерных продуктов и т. д. (компьютерное пиратство);

– компьютерный саботаж;

– распространение по международным информационным сетям материалов порнографического содержания, экономический шпионаж и пр.

Более подробно о преступлениях в сфере компьютерной информации, согласно российскому законодательству, см.: Комментарий к уголовному кодексу РФ. М., Юрист, 1997 г., ст. ст. 272–274.

В части компьютерных преступлений Россия не отстает от зарубежных стран. В 2001 году начальник отдела автоматизации неторговых операций вычислительного центра Внешэкономбанка совершил кражу на сумму $12500 США. Из материалов уголовного дела, возбужденного по факту кражи, следует, что хищение валютных средств было выполнено с помощью несанкционированного изменения не только программного обеспечения, но и манипуляций с данными по счетам клиентов банка. Имея возможность доступа к ЭВМ по роду своих служебных обязанностей, начальник отдела автоматизации незаконным путем создал излишки валютных средств (резерв) на некоторых счетах, которые впоследствии, также незаконным путем, перераспределялись на другие счета, в том числе открытые по поддельным документам. Информация на машинных носителях ЭВМ о движении средств по этим счетам впоследствии корректировалась с целью пополнения на них запасов валютных средств. Компьютерная система банка в данном случае служила инструментом, аналогичным по функциональному назначению средствам, обычно используемым для подделки документов.

Необходимость совершенствования защиты банковской информации и телекоммуникационных систем подтверждается растущим числом фактов незаконного обладания финансовой информацией.

ЦБ России в 2006 году выявил подделанных финансовых документов на сумму около 450 млн. рублей. Это стало возможным благодаря использованию новой СЗИ компьютерной и телекоммуникационной сети. Точной цифры потерь российских коммерческих банков, обусловленных недостаточностью внимания к безопасности информации, не знает никто. Однако есть все основания предполагать, что они большие.

Противодействовать компьютерной преступности сложно, что главным образом объясняется:

– новизной и сложностью проблемы;

– сложностью своевременного выявления компьютерного преступления и идентификации ЗЛ;

– возможностью выполнения преступлений с использованием средств удаленного доступа, т. е. ЗЛ на месте преступления нет;

– трудностями сбора и юридического оформления доказательств компьютерного преступления.

Учитывая большой ущерб от компьютерных преступлений, в настоящее время стали широко внедряться криптографические средства защиты информации, которые обладают гарантированной стойкостью защиты. Однако и они не являются панацеей для защиты информации, т. к. защищают только часть спектра, а не весь спектр угроз информационной безопасности.

Промышленный шпионаж широко использует опыт военной разведки, из которого известно, что 90 % информации о противнике можно получить косвенным путем. При этом источниками информации о конкурентах являются:

– информация, содержащаяся в средствах массовой информации, целенаправленная на исследуемый объект;

– сведения, распространяемые непосредственно конкурентом, его служащими или клиентами;

– финансовые отчеты, проспекты, брошюры, рекламные издания, запросы и т. д.;

– переговоры со служащими и клиентами конкурента;

– непосредственное наблюдение за объектами конкурентов. Сбор подчас многочисленных и отдельно взятых незначительных сведений позволяет получить практические прогнозы и нередко – достоверные выводы об экономическом состоянии конкурента для принятия тактических и стратегических решений в целях обеспечения собственной экономической безопасности. Например, регулярные наблюдения за автомашинами, подъезжающими к зданию банка-конкурента, позволяют выявить его клиентов, их взаимоотношения с банком, деловую активность банка и т. д.

Знания о покупках программного обеспечения для средств вычислительной техники позволяют направить исследования с целью выявления недокументированных функций и последующее их использование для нарушения работы средств вычислительной техники.

Незначительная на первый взгляд информация при значительном объеме обеспечивает переход количества в качество при ее обобщении и аналитической обработке.

1.4. Угрозы материальной безопасности

В последние годы участились нападения на банки и их филиалы.

Особую проблему составляет обеспечение безопасности при перевозке денежных средств. Один из фактов: в Екатеринбурге совершено нападение – пропали сотрудники УБРР и один миллиард рублей. Этот пример показывает высочайшую подготовку и прекрасное информирование преступников о деятельности СБ.

Защита банков и инкассаторов от ограбления в значительной степени зависит от их технической оснащенности. Если защита банков традиционна, то техническое оснащение инкассаторов требует специальных автомашин-сейфов, закрывающихся кодовыми замками, которые невозможно открыть в пути. Поэтому деньги можно похитить только вместе с машиной.

Следует особо отметить, что нападения на инкассаторов в большинстве случаев совершаются при участии или наводке сотрудника ограбленной коммерческой структуры. Таким

образом, СБ должна вести работу с персоналом для выявления их сомнительных связей и т. п. Подобная деятельность носит название "обеспечение внутренней безопасности".

Годы труда могут пойти прахом за считанные секунды. Выживание или крах коммерческой организации часто зависит от степени готовности СБ к различного рода неожиданностям. Приведем лишь три примера.

В 1989 г. небольшой пожар в помещении страховой компании Penn Mutual уничтожил информацию в компьютерном зале компании, т. к. 15 млн. литров воды залили его.

Аналогичный пример пожара в 1995 г. имел место в Москве в Промстройбанке, где погиб один человек и был нанесен ущерб в размере 10 млн. долларов. По словам председателя правления, банковская информация не пострадала, однако он признал, что банк не готов к подобным чрезвычайным последствиям (МП) с точки зрения ее защиты.

В мае 1996 г. пожар во французском банке "Кредит лионз" нанес ущерб в 350 млн. долларов.

Следует обратить внимание на высокий процент ущерба от пожаров, связанных с поджогами. Так, в США поджог – самый быстрорастущий вид преступления, и каждый второй пожар вызван поджогом. Как показали исследования, такая статистика типична для многих стран и не зависит от типа политического или государственного устройства.

Журнал «Survivel» сообщает, что 150 из 350 деловых организаций, функционировавших в Международном торговом центре до взрыва в 1993 г., спустя год прекратили свое существование.

Бедствия, такие как пожары, взрывы, ураганы, наводнения, землетрясения, нарушения электропитания и т. п. трудно предсказуемы, хотя и относительно редкие, но могут привести к значительным убыткам. Но восстановление деловой активности после подобных ситуаций должны быть четко спланированы СБ. Централизованное управление процессом восстановления важно для поддержания деятельности организации, ее способности предоставить заказчикам хотя бы минимум услуг, иначе коммерческий крах неизбежен.

Вопрос 2. Анализ современного состояния проблемы безопасности

Обобщая и анализируя вышеприведенные примеры угроз безопасности, можно выделить три основные составляющие проблемы безопасности:

1. Правовая защита.
2. Организационная защита.
3. Инженерно-техническая защита.

Раскроем содержание каждого направления. Смысл обеспечения правовой защиты ясен из самого названия. Организационная защита включает в себя охрану и режим работы объекта. Под инженерно-технической защитой понимается совокупность инженерных, программных и других средств, направленных на исключение угрозы безопасности.

Вполне естественно, что для каждого вида угроз безопасности должны использоваться различные правовые, организационные и инженерно-технические мероприятия. Это обусловлено различным характером угроз. Целью анализа является рассмотрение возможности СБ предупредить, выявить и «устранить» ЗЛ.

Анализ зафиксированных фактов и уголовных дел, связанных со всеми видами безопасности, свидетельствует о стремительном росте правонарушений. Убийства, мошенничество, промышленный шпионаж и т. п. уже превратились в реальный фон деятельности как государственных, так и коммерческих структур. Положение можно охарактеризовать, как напряженное, что обусловлено:

– крайне тяжелой экономической обстановкой в стране, расслоением общества на "очень богатых" и "очень бедных", падением уровня социальной защиты населения;

– отсутствием должной координации деятельности правоохранительных органов, специальных служб, суда, прокуратуры и негосударственных СБ;

– сложностью учета правонарушений в экономической сфере;

– отсутствием необходимого опыта выявления и пресечения новых видов преступлений в экономике;

– ухудшением криминогенной обстановки.

Учитывая международный характер и масштабы преступлений, их предотвращение и борьба с ними требует активных международных усилий. Даже самое идеальное решение правовых и законодательных вопросов обеспечения безопасности не обеспечит ее сохранения, если не будет работать организационный механизм, претворяющий в жизнь данные положения. В настоящее время такой механизм только зарождается, его развитию препятствует политическая и экономическая нестабильность.

Анализ возможностей технического обеспечения блокирования угроз безопасности (инженерно-техническая защита) может быть проведен из расчета того, что ЗЛ (конкуренты и мафиозные структуры) и СБ обладают одинаковыми возможностями в оснащении.

Мировой уровень технического состояния противодействия попыткам нарушения безопасности достаточно высок. Однако для практической деятельности необходимо выполнение двух основных условий:

– наличие средств на закупку и эксплуатацию СЗ,

– наличие необходимого уровня подготовки персонала.

При наличии этих основных условий можно противостоять любым попыткам злоумышленных действий, однако в настоящее время главный акцент в деятельности СБ коммерческих структур пока грешит силовым подходом к проблеме безопасности в целом, делая ставку на мускулы охранников, а не на интеллект и техническую оснащенность. Попутно отметим, что

имеющийся сейчас силовой подход имеет низкий уровень подготовки, который не соответствует сложившейся криминогенной обстановке и международной практике.

Представляет интерес сравнение объема финансирования СБ стран Западной Европы и России. Первые расходуют от 15 до 25 % годовой прибыли. Анализ средств, расходуемых на содержание СБ коммерческими банками России, показывает, что многие из них тратят менее 1 % от годовой прибыли. Дальнейшее ухудшение криминогенной ситуации в России неизбежно приведет российских бизнесменов к необходимости тратить на безопасность фирмы или банка столько же, сколько их западные коллеги, если не больше.

Вывод: обеспечение безопасности является одним из базовых факторов, определяющих как саму возможность экономической деятельности, так и ее стратегические направления.

Несовершенство правового законодательства и, как следствие, отсутствие единого отлаженного механизма обеспечения безопасности коммерческой деятельности приводит к тому, что основная тяжесть данной проблемы ложится непосредственно на коммерческие структуры.

Однако в настоящее время появилась тенденция к стабилизации положения в области безопасности коммерческой деятельности.

Лекция 2. Правовые вопросы обеспечения безопасности

Учебные вопросы:

1. Основные условия успешного решения проблем правового обеспечения деятельности в области безопасности.
2. Государственная политика обеспечения безопасности.
3. Организационно-правовое обеспечение защиты информации.

Вопрос 1. Основные условия успешного решения проблем правового обеспечения деятельности в области безопасности

Ряд экспертов в области безопасности, исходя из опыта развития ситуации в последние 30–40 лет, пришли к заключению, что в качестве основополагающих предпосылок успеха в решении проблем правового обеспечения деятельности в этой сфере можно выделить следующие три, приведенные ниже.

1. Совершенствование законодательства.

В передовых странах с развитыми системами имущественного страхования большинство людей беспечно относится к вопросам охраны своей собственности в силу того, что уверены в получении страхового возмещения в случае кражи имущества. Это обстоятельство существенным образом облегчает задачу для потенциального преступника. С другой стороны, легкость достижения преступной цели толкает многих на неправедный путь.

На вопрос, над которым ломает голову общественность, кто больше виноват: собственник ли, беспечно и легкомысленно оставивший имущество без присмотра, или воришка, соблазнившийся на легкую добычу, в последнее время юристы склонны отвечать теорией о так называемой обоюдной ответственности. Человек слаб и зачастую не в силах устоять перед искушением, за малым прегрешением следует более серьезное, правонарушитель превращается в преступника, в результате криминогенная ситуация в обществе обостряется.

В настоящее время у специалистов-правоведов не вызывает сомнения, что разработка и принятие законодательных норм, предписывающих обязательное для собственника осуществление минимума мер в области обеспечения безопасности любых объектов собственности, способствовало бы сокращению преступных посягательств против собственности.

Понятие тайны, секрета тесно связано с понятием собственности. В рыночной экономике каждый собственник, в том числе и любой хозяйствующий субъект, обладает естественным правом за свой собственный счет охранять свои имущественные интересы и права (в том числе право на коммерческую тайну), естественно, без ущерба правам и интересам других собственников и общества в целом. Охранять это право – дорогостоящее дело. Обеспечивать безопасность объектов собственности, к примеру, засекречивать информацию "с запасом" объявляя ее коммерческой тайной, просто невыгодно. Коммерческая тайна наряду с рекламой – элемент маркетинга, и никто, кроме самого собственника и управляющего предприятием, отвечающих за получение прибыли и упущенную выгоду, не может определить необходимые объемы информации, требующие защиты, и соответствующие затраты, которые можно себе для этого позволить.

Казалось бы, противоречие неразрешимо? И все же специалисты склоняются к необходимости учитывать универсальный принцип о том, что право вообще и право собственности, в частности, неразрывно связаны и с определенными обязательствами, налагаемыми на их обладателей.

Так, ряд специалистов в нашей стране полагают, что внесение, к примеру, в банковское законодательство положений об обязательности принятия определенного минимума мер безопасности в наиболее уязвимых для преступных имущественных посягательств финансово-кредитных учреждениях, особенно привлекающих средства частных вкладчиков, способствовало бы сокращению преступности в этой сфере бизнеса. Этому способствовало бы и введение обязательного технического аудита систем защиты, без которого было бы нельзя получить лицензию на этот вид деятельности. Более того, корректировка в этом направлении

законодательных актов способствовала бы углублению в обществе понимания важности проблемы безопасности вообще.

2. Необходимость регулирования правоотношений в сфере производства систем и средств безопасности.

На Западе общественность уже давно склоняется к тому, чтобы в этой сфере было введено государственное регулирование и лицензирование (как это уже имеет место в Израиле и некоторых штатах США). Одним из элементов государственного регулирования должно быть создание необходимой организационно-правовой и научно-технической базы лицензирования и сертификации, специальных аттестационных и сертификационных центров и лабораторий для проведения тестирования, чтобы пользователь мог иметь возможность отличить хорошее от дурного. Несомненно, что внедрение государственного регулирования в этой области является важным шагом на пути обуздания преступности.

3. Совершенствование систем страхования, связанного с обеспечением безопасности.

Ввиду резкого роста экономических преступлений в настоящее время (и в нашей стране это особенно) имущественное страхование становится все более рискованным и менее прибыльным. Очевидна взаимосвязь между страхованием имущества от всевозможных рисков, в том числе связанных с преступными посягательствами и положением дел в области производства и внедрения эффективных средств и систем защиты. Беспечный и легкомысленный собственник, оставляющий раскрытыми настежь двери и окна пустующего дома, провоцирующий тем самым преступника на совершение противоправных деяний, вряд ли может рассчитывать в случае совершения кражи на автоматическое страховое возмещение в полном объеме. Иначе выплата этого возмещения фактически означала бы прямое субсидирование криминального бизнеса. Процесс страхования поэтому сочетается с мерами, побуждающими собственника-страхователя обеспечивать необходимую безопасность своего имущества.

Размеры страховых взносов (премий), сумм возмещений и другие условия договоров имущественного страхования должны напрямую зависеть от эффективности мер безопасности, предпринимаемых страхователем, разумный обязательный минимум которых было бы целесообразно закрепить законодательно. Кроме того, желательно страхуемому собственнику одновременно с выдачей страхового полиса обеспечить возможность получения специальной подготовки и консультаций (плата за которые входила бы в стоимость полиса), относительно выбора в зависимости от существования тех или иных рисков и угроз подходящего оборудования и систем безопасности, а также их последующего внедрения. В ряде стран (США, Канада, Израиль) такого рода механизм уже запущен, что способствует сдерживанию роста преступлений против личности и собственности.

В условиях нынешней российской действительности, когда страховой рынок лишь формируется, главной заботой многих страховых компаний, к сожалению, является выдача страхового полиса и получение премии. О возможных финансовых последствиях заключенного страхового соглашения страховщики задумываются не всегда, да и порой недосуг, так как подвергать серьезной оценке принимаемые на страхование объекты некогда: того и гляди клиента перехватит менее разборчивый страховщик. Такая ситуация продлится недолго, еще несколько крупных убытков и отечественные страховщики также поймут, что выгоднее прибегнуть заблаговременно к услугам квалифицированных экспертов для оценки страхуемого риска, чем страховать объекты, состояние которых, в том числе эффективность систем обеспечения их безопасности, остается для страховой компании тайной за семью печатями.

Вопрос 2. Государственная политика обеспечения информационной безопасности

2.1. Принципы государственной политики

Информация и информационные ресурсы, как продукты общественного производства, являются объектами права собственности и, следовательно, имеют своих собственников и потребителей (пользователей).

Государственная политика обеспечения информационной безопасности основывается на следующих принципах:

– государство обеспечивает контроль за созданием, сохранностью и использованием национальных информационных ресурсов, а также способствует предоставлению гражданам доступа к мировым информационным ресурсам;

– государство обеспечивает право граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

– засекречивание есть исключение из общего права на доступ к информации; рассекречивание информации осуществляется в установленном законом порядке;

– ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируется;

– любое юридическое или физическое лицо, собирающее, накапливающее и обрабатывающее персональные и любые другие конфиденциальные данные, несет ответственность перед законом за их сохранность и использование;

– перечни сведений, могущих быть отнесенными к конфиденциальной информации или, наоборот, не могущие быть отнесены к таковым, определяются установленным законом порядком;

– интересы собственников, владельцев и распорядителей информационных ресурсов охраняются законом.

Для претворения в жизнь изложенных принципов необходима соответствующая инфраструктура информационной безопасности.

2.2. Деятельность государства по обеспечению информационной безопасности

Характерной особенностью настоящего этапа развития информационной безопасности является переход от ведомственных, в основном технократических подходов, к комплексному государственному. Возглавляет данную работу Совет Безопасности Российской Федерации. Он поднимает вопрос о разработке конституционных законов в сфере информатизации и информационной безопасности.

Для выработки государственной политики и координации организационно-правовой деятельности в данной сфере в соответствии с Законом РФ "О безопасности" в Совете Безопасности Российской Федерации создана Межведомственная комиссия по информационной безопасности.

Межведомственная комиссия формирует общегосударственный механизм выявления угроз и защиты интересов России в информационной сфере. При этом выделяются три основных направления ее деятельности, а именно обеспечение:

– защищенности системы формирования информационных ресурсов;

– необходимого уровня защищенности применяемых технологий передачи и обработки информации;

– конституционных прав и свобод граждан, законных интересов государства и общества в сфере информатизации.

Таблица 1.

Основные отличия информационного права

Правовые понятия	Вещное право	Исключительное право		Информационное право	
Объект	вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права	результаты интеллектуальной деятельности		информация	
Детализация объектов	недвижимые и движимые вещи, плоды, продукция и доходы, животные, деньги, валютные ценности, ценные бумаги	авторское право	интеллектуальная собственность и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.)	необщедоступная конфиденциальная информация: коммерческая тайна, банковская тайна, тайна страхования, тайна связи, иная служебная тайна, персональные данные	личная и семейная тайна
Характер права	публичное	частное	публичное	публичное	частное
Оборотоспособность	могут свободно отчуждаться или переходить от одного лица к другому	неотчуждаемы	ограниченно оборотоспособные	ограниченно оборотоспособные	неотчуждаемая

Субъект правоотношения	дееспособные физические и юридические лица	любые физические и юридические лица		любое лицо, обладающее сведениями или профессионально занимающееся их сбором и обработкой	любые физические лица
Основания охраны	закон	закон	регистрация	конфиденциальность	закон
Основания возникновения	сделка, наследование, реорганизация юридического лица, накопление, переработка, результат использования и другое предусмотренное законом	создание		установление режима доступа	от рождения
Сроки	до отчуждения, отказа и права, гибели или уничтожение имущества и другое предусмотренное законом	установлены законом или до отчуждения		устанавливаются собственником информации	пожизненно
Основания прекращения	отчуждение, отказ от права, гибель или уничтожение имущества и другое, предусмотренное законом	истечение срока или передача прав		когда информация становится общедоступной	по суду или с утратой дееспособности

Таблица 2.
Классификация защищаемой информации

Виды информации конфиденциального характера	Нормативные акты
Персональные данные	Федеральный закон "Об информации, информатизации и защите информации"
Тайна усыновления	Семейный кодекс Российской Федерации
Личная и семейная тайна	Гражданский кодекс Российской Федерации
Тайна следствия и судопроизводства	Уголовно-процессуальный кодекс Российской Федерации
Служебная тайна	Гражданский кодекс Российской Федерации
Служебная информация ограниченного распространения	Постановление Правительства Российской Федерации № 1233 от 3 ноября 1994 г.
Тайна связи	Федеральный закон "О связи"
Служебная информация	Федеральный закон "О рынке ценных бумаг"
Геологическая информация о недрах	Закон "О недрах"
Врачебная тайна	Основы законодательства Российской Федерации "Об охране здоровья граждан", Закон Российской Федерации "О трансплантации органов и (или) тканей человека"
Нотариальная тайна	Основы законодательства Российской Федерации "О нотариате"
Адвокатская тайна	Закон РСФСР "Об утверждении положения об адвокатуре"
Коммерческая тайна	Гражданский кодекс Российской Федерации
Банковская тайна	Гражданский кодекс Российской Федерации, Закон "О банках и банковской деятельности"
Тайна страхования	Гражданский кодекс Российской Федерации, Закон "О страховании"
"Ноу-хау"	Указ Президента России № 188 от 6 марта 1997г "Об утверждении перечня сведений конфиденциального характера"
Государственная тайна	Федеральный закон "О государственной тайне", Уголовный кодекс Российской Федерации

Межведомственной комиссией принят проект единой концепции информационной безопасности России, правовую основу которой составляют:

1. Конституция Российской Федерации.
2. Законы:

– "О безопасности";
– "О государственной тайне";
– "Об информации, информатизации и защите информации",
– "О коммерческой тайне";
– "О персональных данных".

Ключевым элементом концепции является отказ от взгляда на необходимость защиты только секретной информации и переход к осознанию необходимости защиты любого информационного ресурса, ценного для его владельца или собственника.

По оценке специалистов в сфере информации около 80 % составляет беспатентная неавторизованная часть, т. е. та информация, которая может быть защищена классическими средствами патентного права. В то же время среди информации этого типа существует такая, которую можно, при определенных условиях, использовать во вред законным интересам граждан, субъектов хозяйственной деятельности, государства и общества.

В зависимости от типа защищаемых информационных ресурсов система обеспечения информационной безопасности должна создаваться на соответствующих правовых и организационных основах (рис. 1.).

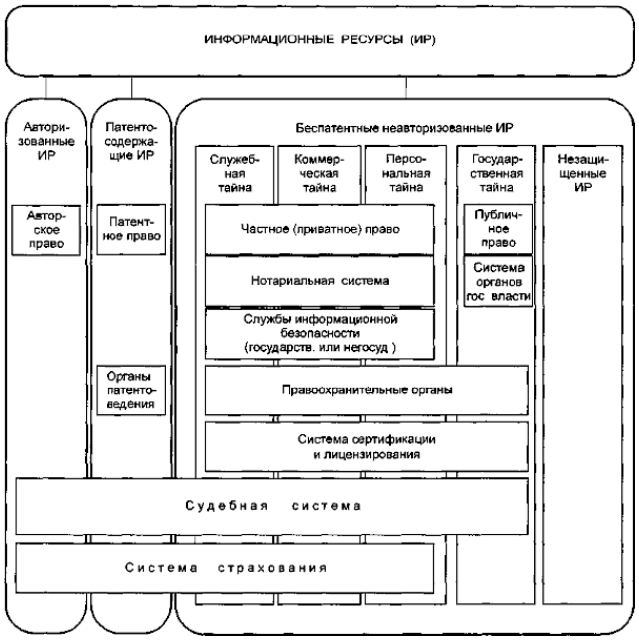

Рис. 1. Правовое и организационное обеспечение безопасности

Вопрос 3. Организационно-правовое обеспечение защиты информации

3.1. Правовое регулирование и организация работ по защите информации

Вопросы развития и внедрения безопасных информационных технологий тесным образом связаны не только с решением научно-технических проблем, но и с вопросами правового регулирования общественных отношений в процессе информатизации. При этом их решение в большей степени зависит не только от уровня развития вычислительной техники, но и от признания за информацией статуса товара, продукта общественного производства. Установление в законодательном порядке права собственности на информацию является важнейшим аспектом формирования информационной политики государства.

Конец ознакомительного фрагмента.