СИСТЕМА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: НОВЫЕ ВЫЗОВЫ И РИСКИ

Бабина Н. А., аспирант

Abstract. *In the article the economic is given values of concept "System of economic security of enterprise". Modern risks are selected and threat in the system of economic security of enterprise. The features of support of informative safety of enterprise are described.*

Keywords: *economic security, system of economic security of enterprise, informative safety, economic risk.*

В условиях экономики переходного периода организации, получившие широкую хозяйственную самостоятельность, столкнулись с необходимостью принципиально новых подходов к обеспечению собственной экономической безопасности, что потребовало коренного преобразования всей системы защиты экономических интересов.

В процессе становления рыночных отношений, создания правовой основы цивилизованного предпринимательства, усиления недобросовестной конкуренции и криминализации отдельных сегментов экономики основная тяжесть этих проблем легла на организации, которые во многих случаях оказались не подготовленными к их решению.

Проблема оценки экономической безопасности предприятия в последнее время приобрела особую актуальность. Обобщая мнение многих авторов [1-6], среди проблем экономической безопасности предприятия, требующих безотлагательного решения, необходимо выделить:

-отсутствие определенности в выборе составляющих экономической безопасности предприятия;

-наличие значительных затруднений формализованного описания динамических свойств предприятия с точки зрения обеспечения его экономической безопасности во взаимосвязи с действиями дестабилизирующих факторов;

- затруднения с определением состава оценочных критериев составляющих экономической безопасности;

-отсутствие общепризнанных отечественных методик оценки уровня составляющих экономической безопасности предприятия, поскольку подходы, получившие признание в зарубежной практике, не всегда можно применить в условиях переходной экономики.

Таким образом, проблема экономической безопасности предприятия требует комплексного подхода, осуществление которого достаточно сложно.

В условиях не всегда цивилизованных конкурентных отношений, несовершенства действующего законодательства, произвола фискальных органов и т.д., необходимо предусмотреть еще на стадии создания предприятия (при составлении его бизнес-плана и проекта устава) меры обеспечения экономической безопасности предприятия, позволяющие предотвратить либо минимизировать негативное влияние внешних и внутренних угроз, а также их вредные последствия.

Экономическая безопасность предприятия — это состояние его защищенности от негативного влияния внешних и внутренних угроз, дестабилизирующих факторов, при котором обеспечивается устойчивая реализация основных коммерческих интересов и целей уставной деятельности.

Для каждого предприятия «внешние» и «внутренние» угрозы сугубо индивидуальны. Вместе с тем, на наш взгляд, указанные категории включают отдельные элементы, которые приемлемы практически к любому субъекту хозяйственной деятельности.

Так, ко внешним угрозам и дестабилизирующим факторам можно отнести противоправную деятельность криминальных структур, конкурентов, фирм и частных лиц, занимающихся промышленным шпионажем либо мошенничеством, несостоятельных деловых партнеров, ранее уволенных за различные проступки сотрудников предприятия, а также правонарушения со стороны коррумпированных элементов из числа представителей контролирующих и правоохранительных органов [1].

К внутренним угрозам и дестабилизирующим факторам относятся действия или бездействия (в том числе умышленные и неумышленные) сотрудников предприятия, противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба компании, утечка или утрата информационных ресурсов (в том числе сведений, составляющих коммерческую тайну и/или конфиденциальную информацию), подрыв ее делового имиджа в бизнес-кругах, возникновение проблем во взаимоотношениях с реальными и потенциальными партнерами (вплоть до утраты важных контрактов), конфликтных ситуаций с представителями криминальной среды, конкурентами, контролирующими и правоохранительными органами, производственный травматизм или гибель персонала и т.д. [2].

Количественный и качественный анализ перечисленных выше угроз позволяет сделать вывод о том, что надежная защита экономики любой компании возможна только при комплексном и системном подходе к ее организации. В связи с этим в лексиконе профессионалов, занимающихся обеспечением безопасности бизнеса коммерческих структур, появился термин «система экономической безопасности» предприятия [3]. С нашей точки зрения, системой экономической безопасности предприятия (СЭБ) является комплекс организацион- ноуправленческих, режимных, технических, профилактических и пропагандистских мер, направленных на качественную реализацию защиты интересов предприятия от внешних и внутренних угроз.

К числу основных задач СЭБ любой коммерческой структуры относятся [3; 4]:

— защита законных прав и интересов предприятия и его сотрудников;

— сбор, анализ, оценка данных и прогнозирование развития обстановки;

— изучение партнеров, клиентов, конкурентов, кандидатов на работу в компании;

— своевременное выявление возможных устремлений к предприятию и его сотрудникам со стороны источников внешних угроз безопасности;

— недопущение проникновения на предприятие структур экономической разведки конкурентов, организованной преступности и отдельных лиц с противоправными намерениями;

— противодействие техническому проникновению в преступных целях;

— выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников предприятия в ущерб его безопасности;

— защита сотрудников предприятия от насильственных посягательств;

— обеспечение сохранности материальных ценностей и сведений, составляющих коммерческую тайну предприятия;

— добывание необходимой информации для выработки наиболее оптимальных управленческих решений по вопросам стратегии и тактики экономической деятельности компании;

— физическая и техническая охрана зданий, сооружений, территории и транспортных средств;

— формирование среди населения и деловых партнеров благоприятного мнения о предприятии, способствующего реализации планов экономической деятельности и уставных целей;

— возмещение материального и морального ущерба, нанесенного в результате неправомерных действий организаций и отдельных лиц;

— контроль за эффективностью функционирования системы безопасности, совершенствование ее элементов.

С учетом перечисленных задач, условий конкурентной борьбы, специфики бизнеса предприятия строится его система экономической безопасности. Необходимо отметить, что СЭБ каждой компании также сугубо индивидуальна. Ее полнота и действенность во многом зависят от имеющейся в государстве законодательной базы, выделяемых руководителем предприятия материаль- но-технических и финансовых ресурсов, понимания каждым из сотрудников важности обеспечения безопасности бизнеса, а также от знаний и практического опыта начальника СЭБ, непосредственно занимающегося построением и поддержанием в «рабочем состоянии» самой системы.

К основным элементам СЭБ предприятия относятся [1; 3; 4]:

1) защита коммерческой тайны и конфиденциальной информации;

2) компьютерная безопасность;

3) внутренняя безопасность;

4) безопасность зданий и сооружений;

5) физическая безопасность;

6) техническая безопасность;

7) безопасность связи;

8) безопасность хозяйственно-договорной деятельности;

9) безопасность перевозок грузов и лиц;

10) безопасность рекламных, культурных, массовых мероприятий, деловых встреч и переговоров;

11) противопожарная безопасность;

12) экологическая безопасность;

13) радиационно-химическая безопасность;

14) конкурентная разведка;

15) информационно-аналитическая работа;

16) пропагандистское обеспечение, социально-психологическая, предупредительно-профилактическая работа среди персонала и его обучение по вопросам экономической безопасности;

17) экспертная проверка механизма системы безопасности.

В наши дни все большую актуальность приобретает защита интересов предприятия от противоправной деятельности коррумпированных представителей контролирующих и правоохранительных органов. В связи с этим, данное направление работы многими начальниками служб экономической безопасности коммерческих структур выделяется в качестве отдельного элемента СЭБ.

Основной смысл подобной системы состоит в том, что она должна носить упреждающий характер, а основными критериями оценки ее надежности и эффективности являются:

— обеспечение стабильной работы предприятия, сохранности и приумножения финансов и материальных ценностей;

— предупреждение кризисных ситуаций, в том числе различных чрезвычайных происшествий, связанных с деятельностью «внешних» и/или «внутренних» недоброжелателей.

Особенностью при построении системы экономической безопасности является тот факт, что ее действенность практически полностью зависит от человеческого фактора.

Новым вызовом для системы экономической безопасности предприятия является увеличение количества преступлений в области информационных технологий, защиты информации, негласного съема (похищения) информации с цифровых носителей, кибер-атаки и т. д.

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т. п.) через Интернет, коммунальные объекты. Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество. В зарубежных государствах, в частности США, получили распространение аферы, связанные с продажей доменных имен.

Под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства [1].

Одним из видов компьютерной преступности можно считать компьютерное пиратство (пиратство в сфере использования информационных технологий).

По данным исследовательской компании IDC, уровень компьютерного пиратства в Украине составляет 83%. Это значит, что на 83% из 15 млн. работающих в стране компьютеров установлена хоть одна нелегальная копия како- голибо программного обеспечения, за которое хорошо было бы заплатить. В основном это продукты компании Microsoft — Windows и Office, компании Adobe— Photoshop, Illustrator и Pagemaker, а также других производителей, в частности игр [5],

По оценкам специалистов Microsoft, средний уровень электронного пиратства в Центральной и Восточной Европе (32 страны) составляет 70%.

Для определения уровня пиратства мы обращаемся к нескольким организациям и ассоциациям в данной отрасли — например, BSA, IDC. Здесь нужно отметить, что они, скорее, изучают уровень пиратства среди предприятий, а не среди потребителей. Это и малые предприятия, и очень крупные, включая госсектор. В таких отраслях экономики Украины, как телекоммуникации, банковский и финансовый сектор, страховые компании, уровень пиратства достаточно низок. Самый высокий уровень пиратства — в сфере малого бизнеса.

Одной из причин распространения пиратства называют высокую цену продуктов. Однако довольно часто пиратству подвергаются дешевые продукты, например, в игровой индустрии.

У пиратства много причин, и не только ценовых. Их нужно рассматривать в комплексе. Главное — чтобы чиновники, бизнесмены и обычные пользователи начали понимать, что такое право интеллектуальной собственности.

Microsoft стала одним из двигателей борьбы с компьютерным пиратством в Украине, России и других странах Восточной Европы. Компания инициировала программу льготной легализации программного обеспечения в школах и государственных учреждениях. Была создана рабочая группа по легализации и правам интеллектуальной собственности. Однако реальных результатов почти нет.

Разрабатывается методология оценки информационных технологий для того или иного предприятия. Условно говоря, на крайней левой позиции этой шкалы предприятие рассматривает программное обеспечение как инструмент своей деятельности, с которым связаны затраты. Крайняя правая позиция — когда организация рассматривает информационные технологии как свой стратегический актив, составляющий часть ее капитала. В течение своего жизненного цикла каждая организация перемещается от крайней левой позиции к крайней правой [б].

Сейчас в России зарегистрировано около 35 млн. активных пользователей Интернет, в Украине — почти 10 млн. пользователей, постоянно увеличивается и количество пользователей ПК. Индустрия высоких технологий растет на 40% в год. Рынок становится зрелым. Эксперты высказывают мнение, что российская и украинская экономики не слишком подвержены основным угрозам информационной безопасности — вирусным и хакерским атакам, краже персональных данных, потому что уровень развития высоких технологий в этих экономиках достаточно низкий.

Во многих странах возникают серьезные скандалы, когда происходят взломы баз данных кредитных карт или похищается другая приватная информация.

Или коммерческие секреты попадают в руки конкурентов. Также есть вопросы безопасности детей, которые находятся в Интернете. Правительство должно озаботиться интересами информационной безопасности государства в целом и граждан в частности.

Жизнь каждой страны зависит от киберсистем, которые на сегодняшний день являются чрезвычайно уязвимыми для атак, в том числе — террористических.

В то же время, многие из этих систем являются простым. Это означает высокий уровень их уязвимости — подвернуть их атаке довольно просто. Возможны атаки на телекоммуникации, на интернет, мобильные системы связи. В мире нет страны, которая были бы защищена от компьютерных атак. Специфика кибератак состоит в том, что их можно организовать легко и дешево — достаточно нескольких инженеров.

Не исключено, что в будущем конфликты между государствами и организациями перейдут в киберпространство. В будущем кибератаки станут агрессивнее и будут проводиться не только с целью заработка или шпионажа, но и с целью демонстрации силы атакующих. Кроме того, увеличится количество угроз для пользователей мобильных и облачных технологий, а также для аудитории социальных сетей.

Мобильное рекламное ПО (madware, mobile advertising software) может не только сильно помешать процессу использования устройства, но и выдать злоумышленникам детали вашего местоположения, контактные данные, а также идентификационные данные устройства. Программа типа madware, незаметно попадающая на устройство при установке стороннего приложения, часто начинает заваливать пользователя всплывающими окнами, создает ярлыки, меняет настройки браузера и собирает его личные данные.

Специалисты отмечают, что пользователи с большим доверием относятся к социальным сетям, начиная от обмена личными данными и заканчивая покупкой игровой валюты и виртуальных подарков друзьям. По мере того, как с целью повышения уровня монетизации, социальные сети дают пользователям возможность дарить друг другу настоящие подарки, рост денежного оборота в социальных сетях дает злоумышленникам новые возможности для осуществления атак.

Эксперты ожидают роста числа атак, направленных на кражу платежных данных в социальных сетях и обман пользователей с целью заставить их сообщить эти и другие данные поддельным соцсетям. Сюда могут входить фальшивые извещения о подарках и электронные письма, требующие от пользователя указать свой домашний адрес и иную личную информацию. И хотя предоставление нефинансовой информации может показаться делом безобидным, злоумышленники торгуют и обмениваются ей, объединяя данные с уже имеющимися, что зачастую позволяет им получать доступ к по-настоящему ценной информации.

Кроме того, включение в корпоративные сети незащищенных устройств, собирающих информацию, которая после этого оседает на других облачных носителях, значительно повышает риск утечки или целенаправленного захвата дан-

ных. Установка пользователями все новых приложений, в конечном счете, неизбежно приводит к заражению.

Некоторые вредоносные мобильные программы дублируют функционал уже ранее существовавших угроз, например тех, что крадут информацию с устройств. Однако иногда появляется и что-то новое. Например, во времена dial-upмодемов существовали программы, которые звонили на 900 номеров, принадлежащих хакерам. Сегодня вредоносные программы отправляют платные смс-сообщения, и вырученные средства достаются злоумышленникам. В будущем можно будет наблюдать дальнейшее развитие мобильных технологий, что создаст новые возможности для киберприступников.

Набирающая популярность технология электронных кошельков eWallet неизбежно станет еще одной платформой, которую злоумышленники попытаются использовать в своих целях. А по мере повсеместного внедрения технологий мобильных платежей, мобильные устройства станут представлять еще большую ценность. По аналогии с угрозой Firesheep для перехвата чужих Wi-Fi-сессий, стоит ожидать появления программ, которые будут перехватывать платежную информацию пользователей. Некоторые платежные системы широко популярны среди технически неискушенных пользователей и могут иметь уязвимости, потенциально ведущие к краже информации.

Литература:

1. Экономическая безопасность национальной экономики: инвестицион- ноинновационный аспект [кол. монография]. — К.; КНУТД, 2012. — 430 с.

2. Экономическая безопасность предприятий, организаций и учреждений [учебное пособие для студ. вузов]. — К. : Правовое единство, 2009. — 544 с.

3. Экономическая безопасность Украины [Монография] / В. Т. Шлемко, И. Ф. Бинько. — К.: НИСИ, 1997. — 144 с.

4. Экономическая и имущественная безопасность предприятия и предпринимательства. Антирейдерство. — Тернополь : Терно-граф, 2008. — 424 с.

5. Преступления в сфере информационных технологий [электронный ресурс]. — http://ru.wikipedia.org/wiki

6. Дашян М. С. Право информационных магистралей (Law of information highways): Вопросы правового регулирования в сфере Интернет, — М: "Волтерс Клувер", 2007