Л.С. Винарик,
А.Н. Щедрин

СПОСОБЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ ОНЛАЙНОВОГО ЭЛЕКТРОННОГО БИЗНЕСА

Несмотря на влияние мирового финансово-экономического кризиса на экономическое развитие страны, рост объема товарооборота во внутренних и внешних сделках, рост количества участников экономической деятельности в стране и на мировом рынке, деятельность органов государственной власти по управлению и регулированию экономических и финансовых потоков в настоящее время невозможны без широкого применения системы онлайнового электронного бизнеса (ОЭБ).

Процесс внедрения ОЭБ в экономическую деятельность субъектов хозяйствования порождает ряд проблем, связанных с безопасностью его функционирования и требует совершенствования и дальнейшего развития систем защиты.

Любой субъект хозяйствования может добиться успехов в современной экономической среде только в том случае, если его система управления соответствует ряду требований, наиболее важными из которых являются следующие:

прозрачность бизнеса и его «аналитичность», позволяющие не только владеть электронными информационными ресурсами о текущей ситуации, но и анализировать возможные причины – следственные связи, делать выводы и принимать на их основе экономически обоснованные управленческие решения;

управляемость и эффективное распределение полномочий и ответственности внутри субъекта хозяйствования, что обеспечивает эффективное использование преимуществ централизации одних управленческих функций и децентрализации других;

обеспечение «интервенции» информационно-телекоммуникационных технологий во все сферы жизни, что усиливает прозрачность бизнеса, способствует развитию так называемого третьего сектора экономики, возникновению новых форм ведения бизнеса, принципиальному изменению организации труда в пользу децентрализации управления, временного найма работников и создания виртуальных рабочих мест, появлению новых форм потребления и досуга, т.е. появлению ОЭБ, который объединяет разнообразные возможности взаимодействия поставщиков и потребителей, кроме того, он делает их независимыми, не привязанными к стационарным устройствам, предоставляя возможность осуществить покупку, провести платежи, принять участие в аукционе при наличии всего лишь мобильного телефона или карманного компьютера. Услугами ОЭБ можно воспользоваться всегда, независимо от времени или места нахождения.

Проведенный анализ деятельности ОЭБ позволяет выявить следующие особенности его становления и функционирования:

ОЭБ базируется на 5 и 6 технологических укладах, в которых господствующие позиции занимают информационно-телекоммуникационные технологии, средства космической связи, а глобальная информационная сеть является необходимым условием существования;

ISSN 1562-109X

в ОЭБ между различными индивидуумами устанавливаются прямые горизонтальные связи, что позволяет легко общаться;

поскольку электронные информационные ресурсы в сети распространяются очень быстро, то для ОЭБ характерна почти мгновенная динамика спроса и предложения, причём ценность ряда товаров проявляется не столько в их редкости, сколько, наоборот, в их массовости.

Наступление ОЭБ выглядит как неизбежность, поскольку в своей экономической нише он более эффективен, чем другие формы экономической деятельности. Возможные социальные потери в процессе его расширения необходимо предвидеть и по возможности нейтрализовать за счет дальнейшего исследования его свойств и моделирования возможных последствий его развития.

Мы живём в период, когда развивающиеся страны мировой экономической системы формируют и используют системы ОЭБ – это одна из форм постиндустриальной стадии развития человечества. В этих условиях степень использования электронных информационных ресурсов и информационных технологий становится одним из основных показателей развития, особенно общества и государства. Поэтому в различных субъектах хозяйствования возникают потребности в электронных информационных ресурсах, например, для борьбы с конкурентами, которые получают путём использования информационных средств и технологий. Всё это и порождает проблему безопасности ОЭБ, которая имеет общенациональный и региональный аспекты.

Соперничество конкурентов в борьбе за электронные информационные ресурсы приводит к нарушениям их конфиденциальности, полноты, достоверности и своевременности, что в свою очередь приводит к нарушению ритма и качества управления субъектом хозяйствования за счет ошибочных и неполных электронных информационных ресурсов.

Несмотря на проводимые исследования данной проблемы в различных аспектах: технических, технологических и организационных (О. Безмалый, В. Дубницкий, О. Котелев, Г. Лозикова, Г. Резго, В. Скиба, Г. Солнцева, В. Ульянов, У. Швартау, С. Шляхтина и др.), её важность сейчас с точки зрения оценки эффективности возможных систем защиты, к сожалению, очевидна далеко не всегда и не для всех. Тем не менее даже небольшого анализа достаточно, чтобы понять важность этой проблемы, которая возникает как из сложности и разновидности современных информационных систем, так и из необходимости комплексного подхода к безопасности с привлечением законодательных, административных, программно-технических мероприятий.

Целью статьи является предложение способов оценки безопасности ведения бизнеса в онлайне, т.е. ОЭБ, позволяющих по возможности нейтрализовать социальные потери, возникающие в данной системе.

Рассмотрим ключевые понятия обозначенной цели.

Понятие *«безопасность»* трактуется как состояние, при котором отсутствует опасность, есть защита от неё.

«Безопасность» – это состояние, при котором отсутствует возможность причинения ущерба потребностям и интересам субъекта отношений.

«Угроза» определяется как непосредственная опасность. Опасность носит общий потенциальный характер, но так как противоречия между субъектами хозяйствования возникают постоянно, то и опасность может существовать постоянно.

С юридической точки зрения понятие «угроза» определяется как намерение нанести зло (ущерб).

При всем многообразии видов угроз все они взаимосвязаны и воздействуют на интересы, как правило, комплексно. Поэтому для их ослабления, нейтрализации и парирования создаётся система обеспечения безопасности.

Обеспечение безопасности – это особым образом организованная деятельность, направленная на сохранение внутренней устойчивости субъекта хозяйствования, его способности противостоять разрушительному агрессивному воздействию различных факторов, а также активное противодействие существующим видам угроз.

Применительно к ОЭБ определение безопасности можно сформулировать так: *«Безопасность ОЭБ – это состояние защищённости интересов субъектов хозяйствования и их отношений, совершающих коммерческие операции (сделки) с помощью технологий ОЭБ, от угроз материальных и других потерь».*

Обеспечение безопасности независимо от формы собственности необходимо для любых субъектов хозяйствования и учреждений как с государственных организаций, так и маленьких фирм. Различия будут состоять лишь в том, какие средства и методы, в каком объёме требуются для обеспечения их безопасности.

Опираясь на понятие безопасности, можно сказать, что безопасность любого субъекта хозяйствования или организации включает:

физическую безопасность, под которой понимается обеспечение защиты от посягательства на жизнь и личные интересы сотрудников;

экономическую безопасность, под которой понимается защита экономических интересов субъектов отношений. В рамках экономической безопасности также рассматриваются вопросы обеспечения защиты материальных ценностей от пожара, стихийного бедствия, краж и других посягательств;

информационную безопасность, под которой понимается защита информации от модификации (искажения, уничтожения) и несанкционированного использования.

Повседневная практика показывает, что к основным угрозам физической безопасности относятся:

психологический террор, запугивание, вымогательство, шантаж;

грабёж с целью завладения материальными ценностями или документами;

похищение сотрудников субъектов хозяйствования или членов их семей;

убийство сотрудников.

В экономической безопасности можно выделить следующие виды угроз:

общая неплатежеспособность;

утрата средств по операциям с фальшивыми документами;

подрыв доверия к фирме.

Обеспечение информационной безопасности является одним из ключевых моментов обеспечения безопасности
субъекта хозяйствования. Как считают зарубежные специалисты, утечка 20% коммерческой информации в 60 случаев из 100 приводит к банкротству субъекта хозяйствования, поэтому физическая, экономическая и информационная безопасность очень тесно взаимосвязаны.

Угрозы безопасности могут быть связаны с действиями факторов, значение и влияние которых практически всегда неизвестны. Присутствие такой неопределённости и ограниченность доступных ресурсов и средств не позволяют создать абсолютно безопасную систему. Поэтому при создании системы безопасности ОЭБ необходимо минимизировать степень риска возникновения ущерба исходя из особенностей угроз безопасности и конкретных условий субъекта хозяйствования, занимающегося ОЭБ.

Можно выделить два основных критерия, позволяющих оценить эффективность системы защиты:

отношение стоимости системы

защиты (включая текущие расходы на поддержание работоспособности этой системы) к убыткам, которые могут возникать при нарушении безопасности;

отношение стоимости системы защиты к стоимости взлома этой системы с целью нарушения безопасности.

Смысл указанных критериев заключается в том, что мероприятия по обеспечению безопасности считаются эффективными, если стоимость системы защиты, обеспечивающей заданный уровень безопасности, оказывается меньше затрат по возмещению убытков в результате нарушения безопасности.

Уровень безопасности при этом в силу объективной неопределённости факторов, влияющих на безопасность, оценивается, как правило, вероятностными показателями.

Оценку эффективности системы безопасности ОЭБ целесообразно осуществлять при помощи обобщённого показателя. Для выбора обобщённого показателя (O_n) состояния защищённости i-го ($i \epsilon j$) субъекта хозяйствования при проведении j-й ($i \epsilon j$) коммерческой операции на рынке ОЭБ будем исходить из следующего.

Состояние защищённости будем характеризовать степенью риска получения i-м субъектом хозяйствования материального или иного ущерба в денежном выражении ($Д_в$) не выше заданного (требуемого) уровня ($Д'_В$) при совершении коммерческой операции.

Тогда обобщённый показатель (O_n) может быть представлен в виде вероятности

$$O_n = P(Д'_В \le Д_В), \qquad (1)$$

где O_n – показатель оценки состояния защищённости i-го ($i \epsilon j$) субъекта хозяйствования при проведении j-й коммерческой операции ($i \epsilon j$);

P – количество функций, выполняемых информационной системой;

i-e – множество субъектов хозяйствования, участвующих в ОЭБ;

j-e – множество коммерческих операций на рынке ОЭБ.

Очевидно, что различные значения показателя O_n будут характеризовать различное состояние защищённости i-го субъекта хозяйствования, совершающего j-ю операцию во множестве видов коммерческой деятельности ОЭБ, и может быть представлено критерием оценки безопасности (W) в следующем виде:

$$W = \begin{cases} \text{Гарантированная, если } O_n \le 0{,}99 \\ \text{Высокая, если } 0{,}99 < O_n \le 0{,}8 \\ \text{Средняя, если } 0{,}8 < O_n \le 0{,}5 \\ \text{Низкая, если иначе.} \end{cases} \qquad (2)$$

Выделяют следующие группы факторов, определяющие безопасность ОЭБ:

состояние правового обеспечения рынка;

эффективность действующего в стране правоприменения;

грамотность и продуманность действий участников рынка ОЭБ.

Исходя из методических соображений целесообразно все факторы, определяющие условия проведения операций конкретного коммерческого вида на рынке ОЭБ, рассматривать в двух аспектах:

общие для всех участвующих в операциях субъектов хозяйствования;

частные, т.е. сопровождающие операции конкретного субъекта хозяйствования.

Это позволит проводить оценку безопасности j-х операций ОЭБ с учетом влияния только общих факторов с последующей корректировкой этих оценок применительно к конкретному i-му субъекту хозяйствования. При таком подходе оценка безопасности может проводиться в два этапа.

На первом этапе определяется совокупность всех возможных в ОЭБ операций (с учетом принадлежности их частей к различным видам коммерческой деятельности) и проводится их типизация. Для каждой из этих типовых коммерческих операций осуществляется оценка безопасности с использованием предложенных показателей и критерия с учётом влияния только общих факторов

применительно к гипотетическому субъекту хозяйствования.

На втором этапе каждый конкретный субъект хозяйствования идентифицирует свою коммерческую операцию с одной из типовых и для неё проводит
корректировку оценок безопасности путём учета влияния частных факторов.

Важнейшим полем деятельности является решение вопроса безопасности ОЭБ – это наведение порядка в управлении субъектами хозяйствования, организациями, банками. Сейчас сотни украинских субъектов хозяйствования выходят на мировой рынок, что требует правильной организации работ, качества планирования, эффективных технологий для принятия менеджерами управленческих решений как по вертикали, так и по горизонтали.

Для обработки электронных информационных ресурсов создаются компьютеризированные системы управления, которые используют зарубежные и отечественные вычислительные средства. С внедрением их осваиваются новые технологии организации бизнес-процессов.

Основу безопасности субъектов хозяйствования при использовании систем ОЭБ составляет безопасность индивидуальная, групповая и массовая. Не осведомлённость работников о наличии информационных угроз, к которым в первую очередь важно отнести психологическое влияние на электронные информационные ресурсы, на информационные потоки, приводит к ликвидации или искажению этих ресурсов, к изменению информационных потоков и другим негативным последствиям.

Процесс обеспечения безопасности систем ОЭБ в Украине развивается крайне не равномерно. Большая часть областей, в том числе и особенно важных, остаются белым пятном. Позитивные смены проходят очень вяло. В то же время при правильной организации дела, состояние, связанное с безопасностью ОЭБ, можно кардинально изменить за короткий срок. Для этого необходима государственная программа наивысшего уровня и воля руководства страны, чтобы был создан Комитет по информатизации, который координировал бы, направлял и контролировал ход работ, в том числе и по вопросам безопасности ОЭБ.

Литература

1. Илляшенко С. Факторы риска целевых рынков / С. Илляшенко // Бизнесинформ. – 1998. – № 3. – С. 68-76.

2. Информатика: учебник / под ред. проф. И.В. Макаровой. – 2-е изд. – М.: Финансы и статистика, 1998. – 768 с.

3. Котелев О.А. Электронная коммерция / О.А. Котелев, Г.Я. Резго, В.И. Скиба. – М.: Перспектива, 2003. – 428 с.

4. Солнцева Г.И. Человеческий фактор в обеспечении безопасности информационной инфраструктуры / Г.И. Солнцева // Информационное общество. – 2000. – № 3. – С. 34-37.

5. Чурков А.М. Информационное общество и эмпирическая социология / А.М. Чурков. – М.: Радио и связь, 2003. – 631 с.

6. Швартау У. Как обеспечить информационную безопасность / У. Швартау // Глобальные сети и коммуникации. – 2000. – № 8. – С. 11-15.