Скрипина А.А., аспирант
Белгородский государственный технологический университет им. В.Г. Шухова

ВЛИЯНИЕ ФАКТОРА ИНФОРМАЦИИ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РЫНКА

skr-ana@yandex.ru

В настоящее время хозяйствующие субъекты осуществляют свою деятельность в условиях открытой глобальной экономики, в которой растет интенсивность конкуренции. Эта открытость способствует росту и таким образом является потенциально позитивной для экономики. Тем не менее, в условиях международного экономического кризиса повышается уровень риска для компаний и для российской экономики в целом. Поэтому первоочередная задача - идентифицировать эти риски и предотвратить их. Новым ведущим фактором развития экономики становится информация. Повсеместное внедрение информационных технологий приносит как новые возможности, так и качественно новые угрозы. В современном обществе в рамках экономической безопасности актуальной проблемой для всех отраслей экономики, в частности для строительной отрасли, становится обеспечение информационной безопасности.

Ключевые слова: *экономическая безопасность, информация, информационная безопасность, информатизация, факторы риска.*

Понятие безопасность весьма емкое и включает в себя множество аспектов. В самом общем смысле безопасность – это отсутствие каких-либо угроз, а также возможность противостоять им без получения вреда. В рамках данной работы, нас интересует понятие экономической безопасности.

Проблема экономической безопасности активно исследовалась как иностранными, так и российскими учеными. В. Паньков описывает экономическую безопасность следующим образом: «Это такое состояние национальной экономики, которое характеризуется ее устойчивостью, «иммунитетом» к воздействию внутренних и внешних факторов, нарушающих нормальное функционирование процесса общественного воспроизводства, подрывающих достигнутый уровень жизни населения и тем самым вызывающих повышенную социальную напряженность в обществе, а также угрозу существованию государства» [1].

Сущность экономической безопасности – это состояние экономики и институтов власти, при котором обеспечивается гарантированная защита национальных интересов, социально направленное развитие страны в целом, достаточный оборонный потенциал даже при наиболее неблагоприятных условиях развития внутренних и внешних процессов [2].

Выделяют следующие объекты экономической безопасности:

- государство в целом и его институты;
- регионы и отрасли;
- хозяйствующие субъекты;
- личность.

Экономическая безопасность предполагает защиту от определенных угроз. Такие угрозы можно классифицировать следующим образом.

Рис. 1. Классификация угроз экономической безопасности

Как мы видим в данном списке угроз есть такой фактор, как информация. В связи с процессом информатизации роль информации в

экономической безопасности стала одним из важнейших объектов защиты. Все уровни, все этапы и отрасли, указанные выше, пронизаны информационными технологиями и данными, что придает фактору информации первостепенную значимость.

В результате этого, в экономической безопасности появляется новый сложный и объемный раздел, называемый информационной безопасностью.

Информационная безопасность – состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере [6].

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации [4].

Информация может являться предметом собственности и подлежит защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Однако с расширением компьютерных сетей, все больше людей имеют доступ к информационно-вычислительным ресурсам систем обработки данных. Возможность связи территориально удаленных друг от друга пользователей обостряет проблему защиты данных от несанкционированного доступа и съема информации при ее обработке, хранении и передаче. Это требует увеличения затрат на средства защиты. На настоящий момент такие издержки могут составлять половину всех средств, направленных на создание и поддержание работы информационных систем.

В то же время объемы информации и информационные технологии выросли настолько, что связанные с ними отношения требуют регулирование со стороны государства. Принят ряд законодательных актов, основными задачами которых становятся регулирование отношений, которые возникающих при создании и использовании информационных технологий и средств их обеспечения, и защита граждан и прав субъектов, участвующих в информатизации. В РФ базовым законом, регламентирующим работу с информацией и информационными технологиями является «Федеральный закон об информации, информатизации и защите информации» от 10 января 2003 г. № 15-ФЗ.

Как уже сказано выше, информация – это преимущественно объект интеллектуального труда. Поэтому все формы ее воплощения регулируются Законом Российской Федерации «Об авторском праве и смежных правах».

В то же время информация может быть государственной, служебной или коммерческой тайной. Разглашение государственной тайны рассматривается как преступление, виновный в котором подвергается наказанию, предусмотренному статьей 283 УК РФ. Гражданский кодекс РФ придает информации статус служебной или коммерческой тайны, когда:

• она приносит действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;

• она не находится в свободном доступе;

• собственник информации принимает меры по обеспечению ее конфиденциальности.

Воздействие на информацию либо на ее носители, а также неправомерное использование информации может нанести ущерб субъекту информационных отношений. Этот ущерб может быть прямым или косвенным, материальным или моральным. Поэтому все субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности (в различной степени в зависимости от величины ущерба, который им может быть нанесен).

Как известно, средой, в которой существует информация, является информационная система – совокупность данных, программно-аппаратных средств и персонала, обеспечивающая хранение, обработку и выдачу информации для решения прикладных задач. Из определения безопасности информации следует, что основными формами нарушения безопасности информации, которые может понести субъект в результате ее нарушения, являются:

1) нарушение доступности информации вследствие полной или частичной утраты работоспособности системы. Очевидно, что вывод из строя или недопустимое изменение режимов работы компонентов системы обработки информации может приводить к получению неверных результатов расчетов, отказам системы и/или отказам в обслуживании конечных пользователей;

2) нарушение целостности информации, которое может быть вызвано ее полным или частичным уничтожением, а также преднамеренным или случайным искажением;

3) нарушение конфиденциальности информации. Для закрытой информации это означает ее раскрытие, а для открытой – ее несанкционированное тиражирование.

Все виды информационных угроз можно разделить на две большие группы [5]:

- отказы и нарушения работоспособности программных и технических средств;

- преднамеренные угрозы, заранее планируемые злоумышленниками для нанесения вреда.

Выделяют следующие основные группы причин сбоев и отказов в работе компьютерных систем [6]:

- нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине старения или преждевременного износа их носителей;
- старения или преждевременного износа;
- нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине некорректного использования компьютерных ресурсов;
- нарушения, возникающие в работе аппаратных средств из-за неправильного использования или повреждения, в том числе из-за неправильного использования программных средств;
- неустраненные ошибки в программных средствах, не выявленные в процессе отладки и испытаний, а также оставшиеся в аппаратных средствах после их разработки.

Все перечисленные угрозы в той или иной степени характерны для всех отраслей экономики. Однако для строительной отрасли можно выделить следующие особенности:

- необходимость защиты ноу-хау и патентов. Так как в строительной отрасли большое значение имеет поиск новых материалов, использование которых дает предприятию конкурентные преимущества, следует обезопасить процесс их разработки и внедрения от утечек информации.
- необходимость защиты интеллектуальной собственности, такой как чертежи, планы, схемы и сметы. Кроме экономической угрозы, которую влечет распространение технических документов, существует угроза физической безопасности объектов при попадании таких документов в чужие руки (в особенности информации о производственных, общественных и правительственных объектах)
- защита средств программного обеспечения, в том числе и от человеческого фактора. Вся документация и виртуальные модели, прошедшие согласование и утверждение в соответствующих органах, должны быть защищены от случайного или преднамеренного изменения.

Государственные ведомства, отвечающие за экономическую безопасность, ежегодно выявляют почти 1000 враждебных актов против экономических субъектов. На самом деле, некоторые нарушения могут быть никогда не обнаружены. В качестве примера можно привести случаи кибер-атак: Троянский конь или любой другой вирус могут быть определены лишь через несколько месяцев или даже лет, успев нанести при этом значительный вред. Бывает и так, что беспокоясь о своей репутации, предприятия-жертвы не сообщают о незаконных вмешательствах в свою деятельность.

Любая компания, независимо от ее размера, может стать объектом атаки, начиная с момента, когда она переходит в инновационный сектор с высокой конкуренцией. Малые и средние предприятия у которых не всегда есть средства, чтобы достаточно обеспечить собственную систему безопасности, особенно подвержены подобным атакам.

Акты вмешательства имеют самые различные формы: вторжения (незаконные или разрешенные), организованное ослабление безопасности предприятия (судебное преследование, незаконное присвоение клиентов и т.д.), нарушения в сфере ноу-хау (пиратство, присвоение патента и т.д.), финансовые нарушения (агрессивный перехват контроля и др.), компьютерные атаки (в сфере средств массовой информации, вторжения в компьютерные системы и т.д.), эксплуатация человеческих слабостей (давление, общественные беспорядки и т.д.), разрушение имиджа и репутации компании.

Большая часть подобных актов, возможно, могут или смогут быть предотвращены благодаря осознанию реальности этой угрозы и путем введения практик соответствующего поведения из мирового опыта.

Акты вмешательства, в основном, нацелены на три больших типа информации:

- Исследования и разработки. Результаты, предмет исследования и разрабатываемые программы содержат данные высокой ценности, как для предприятий, так и для научно-исследовательских учреждений. Часто их освоение конкурентом само по себе представляет угрозу компании или лаборатории.
- Торговая стратегия и маркетинг. Картотеки клиентов, осваиваемые рынки, ценовая политика, рекламные кампании, конкурентные стратегии, перспективы выхода на международный рынок – это те данные, которые при раскрытии третьей стороне способны причинить ущерб компании.
- Внутренняя среда компании. Персональные данные сотрудников, подробные схемы, планы помещений предприятия, информация о компьютерной системе и о системах безопасности – это очень ценная информация, которая может быть использована недобросовестным конкурентом или нарушителем, который хочет присвоить ценности компании или научно-исследовательской лаборатории.

После определения стратегической информации, которая подлежит защите, необходимо определить, как эта информация может быть получена третьими лицами. При всем множестве возможных путей особое внимание следует обратить на следующее:

• Физическая безопасность помещений. В любой компании или научно-исследовательском учреждении не должны воспринимать нормальным тот факт, что можно прийти и уйти в базы данных или в помещения предприятия, не имея специального приглашения. Должен быть разработан и исправно функционировать механизм внешней защиты (барьер, механизмы предотвращения несанкционированного проникновения, видеонаблюдение, соответствующее освещение). При этом стратегическая информация сама по себе становится объектом особых защитных мер. Должна быть внедрена эффективная система контроля перемещений внутри предприятия (ведение регистра, введение пропусков, обозначенный маршрут для посетителей, и т.д.). В сочетании с повышением бдительности персонала, это позволит выявить любые вмешательства в неположенные места.

• ИТ-безопасность. Анализ актов вмешательства, произошедших в последние годы, показывает, что злоумышленники искали, как войти на сервер предприятия, используя недостатки защиты, чаще всего обусловленные человеческой непредусмотрительностью, или собирали информацию, присваивая мобильные устройства (ноутбуки, USB-устройства, смартфоны и т.д.) Тем не менее, соблюдения некоторых простых правил безопасности часто достаточно, чтобы остановить нападающих или минимизировать последствия преступного деяния. Особенно это можно заметить при использовании сложных и часто изменяемых паролей, периодическом обновлении операционной системы и антивируса, установке брандмауэра, изоляции информации, несущей большое стратегическое значение, от открытого доступа в Интернете, использование выделенных ноутбуков во время путешествия, содержащих только необходимую информацию, благоразумие в использовании устройств USB, и т.д.

• Риски, обусловленные человеческим фактором. Совокупность дефектов и ошибок, вызванных деятельностью работников, зачастую с большим профессионализмом используются организаторами экономического вмешательства. Иногда гораздо проще положиться на небрежность или наивность сотрудников, работающих в компании, чтобы получить искомую стратегическую информацию.

Чтобы свести к минимуму небрежность и просчеты персонала, нужно сделать экономическую безопасность частью организационной культуры компании, придать ей не меньшее значение, чем безопасности труда. Она должна быть распространена среди всех сотрудников компании или научно-исследовательского учреждения. Ее организация и последующее управление должны включаться в список стратегических целей фирмы.

Когда сотрудники совершают деловые поездки (конференции, выставки, командировки), они становятся более уязвимыми, чем когда они находятся на самом предприятии. Для сохранения и обеспечения безопасности рабочей информации, которой обладает сотрудник, такие поездки должны стать объектом тщательной подготовки и сопровождаться подробными отчетами. И наоборот, при посещении организации посторонним человеком (член делегации, стажер, посетитель и т.д.) или группой лиц, их должны сопровождать и контролировать от первой до последней минуты.

• Коммуникации в компании и в научно-исследовательском учреждении. Тем не менее, с приходом открытой и свободно распространяемой информации возникает такое явление, как скрининг со стороны недобросовестных конкурентов. Поэтому крайне важно, чтобы информация, распространяемая в письменной форме, через Интернет или в ходе выставок и конференций, была точно отмерена и оценена на достаточно высоком уровне, чтобы взвесить все результаты такой степени освещения.

Необходимо также строго регулировать информацию, размещенную в социальных сетях субъектами всех уровней компании или научно-исследовательского учреждения. Анализ среды компании или индивидуального предприятия является основным способом получения информации третьими лицами. Благодаря социальным сетям и так называемым методам социальной инженерии, это работа предшествует любой экономической атаке, дает возможность разработать подробный план вмешательства и обеспечить тем самым его успех. Именно поэтому целесообразно вести политику неразглашения среди сотрудников, обладающих наиболее детальной и ценной информацией

Можно сделать вывод, что в условиях информатизации обеспечение экономической безопасности ставит перед собой новую задачу, имеющую приоритетное значение – защиту данных от несанкционированного вмешательства, распространение, утери и повреждения. Также необходимо разрабатывать мероприятия, которые позволят уменьшить последствия, в случае

подобного инцидента. Предприятиям нужно предусмотреть систему доступа к конфиденциальной информации только доверенных лиц. Любое несанкционированное вмешательство должно быть документировано, расследовано, а его причины должны становиться основой для улучшения информационной безопасности. Следует помнить, что затраты на создание, поддержание и совершенствование системы информационной безопасности значительно меньше, чем вред, который способна нанести хакерская атака или разглашение конфиденциальных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Барановская Т.П. [и др.]; под ред. В. И. Лойко. Информационные системы и технологии в экономике: учебник. 2-е изд., перераб. и доп. М.: Финансы и статистика, 2005. 416 с.

2. Баталов С. А. Информационные системы и технологии: [учебное пособие]. Уфа: УГАЭС, 2006. 480 с.

3. Благовещенская М.М., Злобин Л.А. Информационные технологии систем управления технологическими процессами: учебник для вузов. М.: Высшая школа, 2005. 768 с.

4. Богомолов О.Т. Мировая экономика в век глобализации: Учебник. М.: ЗАО «Издательство «Экономика», 2007. 359 с.

5. В. В. Брага [и др.]; под ред. Г. А. Титоренко. Автоматизированные информационные технологии в экономике: [учебник для студентов вузов]. М.: ЮНИТИ, 2005. 399 с.

6. Вечканов Г.С. Экономическая безопасность. СПб.: Вектор, 2009. 412 с.

7. Гайнанов Д.А., Изергина М.Э. Стратегия управления персоналом предприятия при внедрении корпоративной информационной системы: [монография]. Уфимский государственный авиационный технический университет. Уфа: УГАТУ, 2007. 246 с.

8. Дорошенко Ю.А., Кочеткова О.В. Экономическая безопасность: Учеб. пособие. Белгород: Изд-во БГТУ им. В.Г. Шухова, 2006. 180 с.

9. Дьяконов В.П. Новые информационные технологии: [учебное пособие для студентов высших учебных заведений и университетов]. М.: СОЛОН-Пресс, 2005. 640 с.

10.Рудычев А.А., Борачук В.В., Чижова Е.Н. Проблемы реформирования системы управления промышленным предприятием в условиях нестабильной внешней среды: монография. Белгород: Изд-во БГТУ, 2011. 185 с.

11.Рудычев А.А., Кузнецова И.А., Рябов А.А. Информационно-инновационная компонента формирования системы управления промышленным предприятием: монография. Белгород: Изд-во БГТУ, 2010. 9,0 п.л.

12.Румбешт В.В. Информационная безопасность: Учебное пособие. Белгород: Изд-во БелГУ, 2008. 216 с.

13.Суглобов А.Е, Хмелев С.А., Орлова Е.А. Экономическая безопасность предприятия: Учебное пособие для студентов вузов. М.: ЮНИТИ-ДАНА, 2013. 356 с.

14.Уткин В.Б., Балдин К.В. Информационные системы и технологии в экономике. М: ЮНИТИ-ДАНА, 2003. 335 с. (Серия «Профессиональный учебник: Информатика»).

15. Ярочкин, В.И. Информационная безопасность: Учебник. М.: Академический проект; Фонд «Мир», 2003. 640 с. (Серия «Gaudeamus).

Skripina A.A.

INFLUENCE OF THE INFORMATION FACTOR IN THE ECONOMIC SECURITY OF MARKET

Currently, the economic agents operate in an open global economy in which increasing the intensity of competition. This openness promotes growth and thus is potentially positive for the economy. However, in the context of the international economic crisis increases the risk level for the companies and for the Russian economy as a whole. Therefore, the first task is to identify these risks and prevent them. The new leading factor in the development of the economy becomes information. The widespread introduction of information technologies brings new opportunities and new threats. In modern society, within the framework of economic security is becoming urgent problem of information security for all sectors of economy, in particular for the construction industry.

Key words: *economic security, information, information security, informatization, risk factors.*

Скрипина Анастасия Анатольевна, аспирант кафедры экономики и организации производства.
Белгородский государственный технологический университет им. В.Г. Шухова.
Адрес: Россия, 308012, Белгород, ул. Костюкова, д. 46.
E-mail: skr-ana@yandex.ru