УДК 33

А. П. Соколов
ФБГОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», Владимир;
ФБГОУ ВО «Финансовый университета при Правительстве Российской Федерации», Москва, e-mail: sap9556565@gmail.com

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Ключевые слова: безопасность, информация, хозяйствующий субъект, информационная безопасность.

В статье раскрывается многообразие существующих инструментов в сфере управления защитой информации, и обосновано, что каждому предприятию требуется самостоятельно определять и устанавливать соответствующие приложения, в зависимости от потребностей. Кроме того, автором аргументирована необходимость предприятию при разработке защиты информации учитывать масштабы деятельности, отрасль, уникальность продукта и технологии, рынок, финансовые ресурсы и др. В частности обосновано, что для субъектов хозяйствования, которые функционируют на рынке недобросовестной конкуренции, применение инструментов информационной защиты является обязательным. Исходя из того, что все более очевидной становится зависимость общего уровня экономической безопасности предприятия от информационной составляющей, доказано, что условия неопределенности и значительной динамичности окружающей среды требуют от предприятий внедрения механизмов информационного обеспечения в системах управления, которые бы гарантировали значительную гибкость, открытость к внешней среде, способность своевременного совершенствования. Определены сущность и основные составляющие информационной безопасности предприятия, разработана проектная структура информационно-аналитической службы и осуществлено формирование рекомендаций по повышению уровня информационной безопасности отечественных предприятий.

A. P. Sokolov
Vladimir State University named after Alexander Grigoryevich and Nikolai Grigoryevich Stoletov, Vladimir;
Financial University under the Government of the Russian Federation, Moscow,
e-mail: sap9556565@gmail.com

INFORMATION COMPONENT MANAGEMENT IN THE SYSTEM OF ECONOMIC SECURITY OF THE ENTERPRISE

Keywords: security, information, business entity, information security.

The article reveals the variety of existing tools in the field of information security management, and proves that each enterprise needs to independently identify and install appropriate applications, depending on needs. In addition, the author argues for the need for an enterprise to take into account the scale of activity, industry, uniqueness of the product and technology, market, financial resources, etc. when developing information security. In particular, it is proved that for business entities that operate in the market of unfair competition, the use of information protection tools is mandatory. Based on the fact that the dependence of the general level of economic security of an enterprise on the information component is becoming more and more obvious, it is proved that the conditions of uncertainty and significant dynamism of the environment require enterprises to introduce information support mechanisms in management systems that would guarantee significant flexibility, openness to the external environment, and the ability to improve in a timely manner. The essence and main components of the information security of the enterprise are defined, the design structure of the information and analytical service is developed and recommendations for improving the level of information security of domestic enterprises are formed.

Введение

Под экономической безопасностью в контексте распространенной в настоящее время концепции устойчивого развития определена сбалансированность внутренней структуры открытой социально-эколого-экономической системы, в результате которой она стабильно функционирует, воспроизводится и развивается, а также гармоничное взаимодействие системы с внешней средой.

Экономическая безопасность государства, регионов, видов экономической

деятельности, предприятий является системным понятием с присущими свойствами целостности, синергизма, иерархичности и др. Как на макро -, так и на микроуровнях обеспечение экономической безопасности достигается путем реализации экономической стратегии, успешность которой зависит, в том числе от четко определенных составляющих элементов безопасности.

В современном научном мире исследованию экономической безопасности посвящен ряд научных работ. К наиболее значимым исследованиям в этом направлении следует отнести труды И.А. Сергеевой С.В. Белова, В.И. Каракеяна, Н.А. Пименова, Е.И. Кузнецовой, В.Ш. Уразгалиева, Р.А. Мошковой, В.В. Шлыкова, А.Е. Суглобова и др.

Экономическая безопасность исследуется учеными на различных иерархических уровнях экономической системы, но больше внимания уделяется микроуровню, где все еще дискуссионным остается вопрос составляющих экономической безопасности.

Цель статьи заключается в идентификации сущности защищенности предприятия и её основных составляющих, факторов влияния на формирование и возможных угроз, определении места и роли информационной составляющей в структуре его экономической безопасности.

Материалы и методы исследования

В процессе исследования использован последовательный механизм, инструменты которого направлены на формирование экономической безопасности предприятия, предполагая существование гибкой системы управления, способной оперативно выявлять изменения во внешней среде и реагировать их, делая возможным функционирование хозяйствующего субъекта в любых условиях.

В процессе исследования ключевыми методами выступили систематизация, группировка, абстрагирование с целью определения информационной безопасности хозяйствующего субъекта с учетом предоставления мер правовой гарантии на уровне государства и предприятия, регулирования информационного потока, программно-технической поддержки с целью предотвращения незаконной утечки информации.

Результаты исследования и их обсуждение

Наиболее распространенным подходом к выделению составляющих экономической безопасности на микроуровне являются функциональный. Например, М.В. Алябьева [1], выделяет следующие составляющие: интеллектуальную, кадровую, финансовую, технико – технологическую, политико-правовую, экологическую, информационную и силовую. Аналогичного мнения придерживается и В.В. Шлыков [15] добавляя к ним рыночную, а также интерфейсную составляющую, характеризующих надежность взаимодействия с экономическими контрагентами предприятия А.П. Козырев [9] выделяет всего четыре составляющие: социальную, финансовую, производственную и сбытовую. В трудах Р.А. Мошковой [11] обоснован набор составляющих экономической безопасности, среди которых социально-экономическая, финансовая, производственная, экологическая, силовая, организационно-управленческая, материально-техническая, информационно-правовая.

Т.В. Зырянова [6], исследуя экономическую безопасность на различных иерархических уровнях отечественной экономики (экономическая безопасность государства, региона, предпринимательства как сектора экономики, предприятия, предпринимательской деятельности) выделяет ее составляющие также по функциональному признаку, элементами которой выступают обеспечивающие жизнеспособность предприятия как первичного звена:

– финансовая устойчивость и независимость;

– конкурентоспособность;

– эффективность управления, правовой защиты;

– защита информационной среды;

– безопасность персонала, имущества и коммерческих интересов.

По мнению Н.А. Денисовой [4] в составляющие экономической безопасности не следует включать те, которые носят не экономический характер, а именно финансовая, внутренне экономическая, внешнеэкономическая и социально-экономическая.

На основании обзора источников отметим, что наиболее существенными являются следующие структурные элементы экономической безопасности предприятий (расположено в убывающем порядке по количеству упоминаний):

– интеллектуально-кадровая (или социально-экономическая),

– финансовая,

– производственная (или технико-технологическая),

– экологическая.

Обозначенный набор составляющих соответствует распространенной в настоящее время концепции устойчивого развития.

Однако, часто применяемый подход включения в структуру экономической безопасности всех возможных составляющих считаем не достаточно обоснованным и перегруженным для целей управления. Соглашаемся частично с позицией Л.К. Ивановой, по мнению которой в составляющие экономической безопасности не следует включать те, которые носят не экономический характер [7].

Автор отрицает необходимость включения в составляющие экономической безопасности силовую, информационную, интеллектуальную, экологическую, политико-правовую составляющие.

Действительно, в структуру экономической безопасности не целесообразно включать политико – правовую, силовую и информационную составляющие, поскольку, по мнению автора статьи, это даже не составляющие, а больше предпосылки, необходимые для обеспечения и поддержания экономической безопасности.

Например, государственная регистрация, правовое обеспечение, соблюдение требований действующего законодательства, постоянное отслеживание законодательных изменений – обязательные и необходимые условия, которые должны выполнять все субъекты хозяйствования для осуществления хозяйственной деятельности. Силовая защита предприятий от, например, рейдерских захватов больше касается вопросов их охраны. Необходимо также отметить, что не все предприятия создают собственные службы безопасности или нанимают охрану со стороны.

Однако считаем, что интеллектуальная составляющая должна быть включена в состав экономической безопасности, причем в связи с инновациями (объекты авторского права, интеллектуальной и промышленной собственности, наличие которых защищает предприятие с юридической точки зрения, а использование дает возможность получать экономическую выгоду). Экологическая составляющая может быть объединена с производственной (технико-технологической) составляющей, поскольку вопросы экологии, охраны труда, безопасности окружающей среды и т. д. несут в себе производственный характер и не существуют отдельно сами по себе. Также в условиях рыночных отношений и жесткой конкуренции целесообразно включить в структуру экономической безопасности маркетинговую и инновационную составляющие, о чем речь будет идти ниже.

Таким образом, к составляющим экономической безопасности отнесены: маркетинговая, инновационная, производственная (технико-технологическая), социально-экономическая, финансовая. Подчеркнем, что все эти составляющие взаимосвязаны и взаимодействуют друг с другом, не могут существовать друг без друга, то есть имеют системный характер. Кроме того, в состав экономической безопасности включены элементы, связанные с продукцией (работами, услугами), реализация которой (которых) позволяет получать доход и, за вычетом осуществленных расходов, – прибыль, то есть имеют непосредственное отношение именно к экономическим отношениям хозяйствующих субъектов.

Отметим также, что достижение экономической безопасности обеспечивается благодаря эффективному использованию потенциала. Использование-это действие, процесс.

В контексте данного исследования повышение эффективности использования потенциал рассматривается как цель, достижение которого является положительным результатом.

Соответственно, экономическая безопасность является результатом эффективного использования потенциала и зависит от него, а формирование экономической безопасности предприятия включает комплекс мер, направленных на защиту каждой из составляющих.

Следовательно, информационная составляющая играет одну из главных ролей в обеспечении экономической безопасности хозяйствующего субъекта.

Таким образом, главные составляющие экономической безопасности предприятия, сущность и задачи его информационной безопасности приведена на рис. 1.

Рис. 1. Инструменты экономической безопасности предприятия

Следовательно, одной из важнейших составляющих в структуре экономической безопасности предприятия является информационная часть, предусматривающая создание единой системы данных о его деятельности, а основная задача для руководства заключается в разработке мер по ее обеспечению.

Исследуя информационную безопасность предприятия как объекта административно-правовой охраны, Н.А. Лукашук отмечает, что само понятие «информационная безопасность предпринимательства» означает совокупность мероприятий, определенных на уровне нормативно-правовых актов, регламентирующих предпринимательскую деятельность и определяющих особенности защиты информации субъектами хозяйствования в России, и внутренних правил конкретного предприятия, направленных на защиту их информационного ресурса, нейтрализацию и ликвидацию угроз эффективному функционированию информационной системы субъекта хозяйственной деятельности в частности и деятельности этого субъекта в целом [10].

Составляющие информационной безопасности предприятия систематизированы на рис. 2.

Рис. 2. Направления обеспечения информационной безопасности предприятия

Таким образом, информационная безопасность предприятия обеспечивается мерами правовой поддержки в отношении государственной политики в направлении правового поля, прав и обязанностей субъектов, в частности информационного права; организационного обеспечения, определяющего правила и меры поступления и обработки информации на предприятии; программно-технического обеспечения, делая возможной защиту информации с помощью технических средств, а также предоставляет возможность принятия технических решений.

Необходимо отметить, что правовое обеспечение формируется на уровне государства, а на уровне предприятия это предусматривает разработку и внедрение положения об информационной безопасности по направлениям: определение объектов, составляющих коммерческую тайну, меры по сохранению информации, ответственность за разглашение и т. д.

Для функционирования организационного обеспечения важную роль играет система бухгалтерского учета, регистрирующая факты хозяйственной жизни.

Взаимосвязь организационных мероприятий и программно-технического обеспечения проявятся в автоматизации соответствующих процессов.

Однако использование программно-технического обеспечения не гарантирует абсолютной защиты данных. В данном случае необходимо отметить, что защита конфиденциальной информации на предприятии становится все более актуальной проблемой, учитывая, что серьезные негативные последствия возникают в компаниях ИТ-сферы при потере информации (баз данных), результатов аналитических исследований, начальных кодов, программных продуктов, персональных данных клиентов, без которых дальнейшее продолжение бизнеса становится проблемным.

Как отмечает А.Отт, современная ИТ-структура подвергается большому количеству атак, наиболее актуальными из которых являются:

– фишинг (fishing) – способы перехвата паролей – номеров кредитных карт и т. п. с помощью техники социальной инженерии;

– Spyware – Malware – средства перехвата данных и установление контроля над компьютером;

– вирусы и другие вредоносные коды;

– Spam/SPIM-нежелательные сообщения, засоряющие электронную почту;

– утечка бизнес-информации, которая может нанести компании неисправимый ущерб;

– угроза судебного преследования, связанная с неправомерным использованием информации, которая защищена авторским правом [12].

Обозначенные тенденции свидетельствуют о необходимости усиления защиты информации, постоянного обновления программного обеспечения в соответствии с развитием технологий. Системы информационной защиты предприятия развиваются параллельно с развитием программ, которые имеют негативное влияние.

Основные инструменты по обеспечению информационной безопасности предприятия систематизировано в таблице.

Таким образом, наиболее распространенными являются средства идентификации и аутентификации пользователей, шифрования информации и средства антивирусной защиты. Использование таких программ предоставляет возможность контроля по действиям пользователей в информационной системе, в случае копирования данных не позволит другим пользователям понять полученную информацию за счет применения шифра, а средства антивирусной защиты обеспечат нейтрализацию вредоносных программ.

Таким образом, учитывая многообразие существующих инструментов по защите информации, каждое предприятие должно самостоятельно определять необходимость установки соответствующих приложений, в зависимости от потребностей.

Кроме того, необходимо учитывать масштабы деятельности предприятия, отрасль, уникальность продукта и технологии, рынок, финансовые ресурсы предприятия и др.

В частности, для субъектов хозяйствования, которые функционируют на рынке недобросовестной конкуренции, применение инструментов информационной защиты является обязательным.

Предприятиям, разрабатывающим уникальный продукт или услуги, также необходимо усилить информационную защиту, поскольку разглашение такой информации приведет к аналогам и повлияет на рыночную устойчивость предприятия. Кроме того, необходимо определить, каким образом обеспечивается информационная безопасность на предприятии – собственными силами учитывается ли с помощью вовлеченных организаций стоимость систем, которые внедряются в действие.

Инструменты обеспечения информационной безопасности предприятия

Инструмент	**Характеристика**
Средства идентификации и аутентификации пользователей	Первоочередная проверка пользователей. Идентификация за счет определения имени, аутентификации – проверка соответствия
Средства шифрования информации	Преобразование первичных данных в закодированную форму. В процессе используется шифр как общие принципы шифрования
Межсетевые экраны	Контроль доступа к информации со стороны пользователей других сетей
Виртуальные частные сети	Создание и настройка сети, позволяющей двум компьютерам обмениваться информацией
Средства контактной фильтрации	Технология комплексного контроля Интернет-ресурсов
Инструменты проверки целостности содержимого дисков	Позволяют обнаружить любые действия с информацией (открытие, изменение, копирование) и идентифицировать субъект влияния
Средства антивирусной защиты	Программы, обнаруживающие вирусные приложения нейтрализуют их воздействие
Системы обнаружения уязвимости сетей и анализаторы сетевых атак	Программы, направленные на выявление факта несанкционированного доступа к данным, воздействия на информационную базу. Системы предупреждают о подозрительной деятельности, начале атаки на сеть

Заключение

Предприятие, которое планирует усилить конкурентные позиции на рынке, улучшить показатели деятельности, должно оперативно реагировать на изменения и иметь гибкую систему управления. Наличие качественной информации и принятие на ее основе решений предоставляют такую возможность, которая определяет информационную составляющую экономической безопасности предприятия как приоритетную.

Однако внедрение информационных технологий как способствует защите информации, так и требует усиления организационных мероприятий, увеличения расходов, привлечения соответствующих специалистов, свидетельствуя о взаимосвязи всех процессов на предприятии как единой системы, предусматривая в целом обеспечение его информационной и экономической безопасности.

Разработка и внедрение информационной безопасности с помощью программно-технического обеспечения должна учитывать стоимость программ и систем, необходимость привлечения специалистов или возможность создания службы информационной безопасности на предприятии. Главными факторами при определении необходимости внедрения инструментов информационной защиты являются масштабы деятельности, уникальность продукции или услуги, рынок и имеющиеся финансовые ресурсы предприятия, предназначенные для данных целей.

Библиографический список

1. Алябьева М. В. Экономический и маркетинговый анализ в системе обеспечения экономической безопасности предприятия и его совершенствование: монография / М. В. Алябьева, В. Г. Владимирова. – Москва : Ruscience, 2017. 153 с.

2. Глинская М.В. Обеспечение национальной энергетической безопасности как базовое условие повышения эффективности системы международных экономических отношений // Инновационная экономика. 2023. № 4 (37). С. 80-100.

3. Глинская М.В. Стратегические интересы в сфере международной энергетической безопасности // Мировая экономика в XXIвеке: глобальные вызовы и перспективы развития. Сборник материалов Международной научно-практической конференции в 2-х томах. Том 1. Москва, РУДН.2018. С. 20-22.

4. Денисова Н.А. Методика анализа кадрового потенциала как инструмент обеспечения экономической безопасности организации / Н.А. Денисова, А.М. Филипченко // Вестник Екатерининского института. 2020. № 3(51). С. 34-38.

5. Долгополов С.А. Информационная безопасность в системе экономической безопасности организации // Экономика и предпринимательство. 2019. № 3 (95). С. 175-178.

6. Зырянова Т.В. Моделирование учетного процесса в условиях автоматизации // Все для бухгалтера. 2007. № 24 (216). С. 35-47.

7. Иванова Л.К. Экономическая безопасность предприятия // Вестник Уфимского государственного авиационного технического университета. 2013. № 7 (60). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/ekonomicheskaya-bezopasnost-predpriyatiya-1. (дата обращения 1.02.2024).

8. Капустин Н. Экономическая безопасность отрасли и фирмы // Бизнес-информ. 2005. № 11-12. С. 45-47.

9. Козырев А.П. Экономическая безопасность: теория и практика управления: монография / А.П. Козырев, О.В. Бойко. М.: Инфра-М, 2014. 296 с.

10. Лукашук Н.А. Экономическая безопасность предприятия: сущность, оценка, факторы роста в контексте концепции устойчивого развития // Труды БГТУ. Минск: БГТУ, 2016. № 7 (189). С. 283–288.

11. Мошкова Р.А. Направления совершенствования управления экономической безопасностью транспортных предприятий: монография / Р.А. Мошкова. М.: Русайнс, 2021. 642 с.

12. Отт А. Современные тенденции в области контентной фильтрации/А. Отт // JetInfo. 2012. № 10. [Электронный ресурс]. URL: https://alexott.net/ru/writings/cf/index.html#sec5. (дата обращения 1.02.2024).

13. Самочкин В.Н. Экономическая безопасность промышленных предприятий // Известия ТулГУ. Экономические и юридические науки. 2014. № 3–1. С. 342–352.

14. Тарасова Н.В. Влияние информационных технологий на экономическую безопасность // Journal of Economy and Business. 2020. № 2-2 (60). С. 128-133.

15. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. М.: Алетейя, Санкт-Петербургский университет МВД России, Рязанский институт права и экономики МВД России, 2021. 144 с.