УДК 339

Жукова Евгения Вадимовна
Российская академия народного хозяйства и
государственной службы при Президенте РФ
г. Санкт-Петербург
ms.zhukova12@mail.ru

СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ РИСКОВ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Данная статья посвящена системе раннего обнаружения нарушений информационной безопасности и отражена необходимость ее использования. Проведен анализ рисков и угроз информационной безопасности предприятий. Обоснована необходимость внедрения системы раннего предупреждения рисков.

Ключевые слова: информационная безопасность, риски, угрозы, система раннего обнаружения.

Zhukova Evgeniya Vadimovna
Russian Presidential Academy of National Economy and Public Administration
North-West Institute of Management

RISK EARLY WARNING SYSTEM AS AN ELEMENT OF INFORMATION SECURITY

Abstract: This article is devoted to the system of early detection of information security violations and reflects the need for its use. The analysis of risks and threats to information security of enterprises is carried out. The necessity of implementing an early risk warning system is justified.

Keywords: information security, risks, threats, early detection system.

Современная жизнь характеризуется активным использованием цифровых и электронных технологий. Они активно внедряются как в повседневную деятельность граждан, так и в производственные процессы предприятий, что обуславливает значимость развития цифровой экономики в мире.

Современный бизнес немыслим без использования информационных технологий. Практически все сферы деловой активности информатизированы, что обеспечивает их максимально эффективное и динамичное развитие. [1]

В XX веке информационные технологии начали активно внедряться в человеческую жизнь, а также использоваться в производственных процессах. Деловая активность подразумевает использование или преобразование посредством соответствующих технологий неких ресурсов. Однако, как сами ресурсы, так и технологии имеют уязвимости, которые могут быть реализованы, с той или иной степенью вероятности, как внешними или внутренними злоумышленниками, так и природными (стихийными) или техногенными негативными факторами. Это обусловило повышение рисков для информационной безопасности.

Сущность информационной безопасности заключается в защите данных в процессе передачи их по электронным каналам связи, что особенно актуально для цифровой экономики. Чаще всего в условиях цифровой экономики контрагенты осуществляют операции посредством использования электронных интернет-платформ. Наиболее типичным примером является купля-продажа товаров на сайтах интернет-магазинов, при этом оплата происходит при помощи банковских карт.

Система управления рисками является важной составляющей управления предприятием, поскольку в условиях цифровой экономики позволяет обеспечить информационную безопасность предприятия, стабильность и успешность его развития, поддержать репутацию благонадежного контрагента и поставщика. В таблице 1 представлены основные риски цифровой экономики для предприятия.

Исходя из таблицы 1 видно, что наибольшее внимание необходимо уделять внутренним рискам, а именно рискам, связанным с работой с контрагентами, конфиденциальной информацией, а также угрозам, которые возникают при работе по электронным каналам, в частности при продаже через интернет.

После того, как были определены основные и самые важные риски, была проведена оценка уровня их воздействия, и важнейшими рисками в цифровой

экономике в сфере информационной безопасности выделены:

– появление конкурентов, обладающих более совершенными цифровыми технологиями;

– рост кибепреступности;

– утечка конфиденциальной информации;

– несвоевременная поставка материалов оборудования и другого из-за технологического сбоя.

Таблица 1 – Основные риски цифровой экономики

Риск	Влияние на деятельность предприятия
Несвоевременная поставка материалов, оборудования и другого	Увеличение срока производства продукции
Рост кибепреступности, утечка конфиденциальной информации	Кража важных данных о продукции, технологиях
Недостаточный уровень защиты конфиденциальных данных, коммерческой информации, снижение количества заявок	Усиление позиции конкурентов, получивших доступ к технологической информации предприятия
Снижение цен конкурентов	Снижение цен
Появление новых конкурентов, обладающих более совершенными цифровыми технологиями	Снижение уровня продаж
Повышение цен у поставщиков	Падение чистой прибыли
Чрезвычайные обстоятельства (пожар, наводнение и другие)	Потеря средств
Финансовая нестабильность контрагента	Задержка поставки, потеря клиентов
Нарушение контрактных обязательств	Перебои и задержки поставок
Низкое качество поставляемых услуг или материалов	Низкое качество выпускаемой продукции
Уход поставщика с рынка	Расходы на поиск нового поставщика

Источник: составлено автором на основе. [2]

Вышеуказанные факторы определяют, что обеспечение информационной безопасности является главной проблемой в условиях цифровой экономики, поэтому рекомендуется внедрение системы раннего обнаружения нарушений безопасности данных.

Система раннего обнаружения нарушений безопасности позволит защитить не только конфиденциальную информацию, но и информацию интернет-магазинов, что особенно важно для платежных данных. Интенсивные

темпы роста электронной торговли приводят к увеличению денег в обороте, а, соответственно, и к росту кибепреступности в данной отрасли.

Система раннего обнаружения нарушений информационной безопасности на основе технологий является инновационной по причине того, что включает в себя подсистемы, которые ранее не использовались вместе, они существовали по отдельности. [3] Представленная концептуальная модель объединяет несколько подсистем:

– подсистема сбора и предобработки так называемых больших данных (Big Data);

– подсистема обнаружения и фиксации отклонений в событийном потоке;

– подсистема обработки данных и знаний для выявления потенциальных угроз, основанная на технологии интеллектуального анализа данных;

– подсистема раннего предупреждения о нарушениях информационной безопасности – это так называемая система обнаружения, предупреждения и ликвидации последствий компьютерных атак или центров реагирования на инциденты компьютерной безопасности.

Далее было проведено сравнение систем раннего обнаружения нарушений безопасности разных производителей, которое представлено в (табл. 3).

Таблица 3 – Сопоставление систем раннего обнаружения нарушений безопасности

Показатель	PT Anti-APT	Heimdal Security	Signavio
Наличие веб-приложения	Нет	Нет	Да
Возможность бесплатного использования (тестовый период)	Нет	Нет	Да
Совместимость с популярными операционными системами	Да	Да	Да

Согласно данным таблицы, для разработки в внедрения на предприятие бизнес-процессной модели обеспечения информационной безопасности в процессе электронной торговли, Signavio является наилучшим веб-приложением

для моделирования и симуляции бизнес-процессов.

Главным преимуществом является то, что для его работы нет необходимости устанавливать программное обеспечение, данное приложение является облачным, что значительно облегчает процесс хранения и передачи данных. Signavio предоставляет возможность бесплатного использования программы на 30 дней для тестирования. [4]

Внедрение блока обеспечения информационной безопасности в бизнес-модель позволит свести к минимуму вероятность пострадать от угроз киберпреступности, потери персональных данных. Использование на предприятии Signavio позволит уменьшить количество сбоев в поставке материалов посредством оптимизации бизнес-процессов, повысить уровень защиты конфиденциальных данных, коммерческой информации от утечек и киберпреступности. Разработка бизнес-процессной модели с помощью данного графического облачного редактора позволит облегчить процесс хранения и передачи конфиденциальных данных, повысить их уровень защиты, предотвратить утечку важной производственно-технологической информации.

Экономическая эффективность от деятельности определенной системы является важнейшей составляющей внедрения данной системы в функционирование организации. Показатели экономической эффективности характеризуют целесообразность произведенных на ее создание и функционирование затрат. Предлагаемая система помогает предприятиям увеличивать базу клиентов, защищает личные данные каждого пользователя и является эффективным примером программного обеспечения для защиты информации в условиях цифровой экономики.

Таким образом, по результатам исследования, проведенного в рамках научной статьи, сделаны следующие выводы. Важнейшей проблемой предприятий в цифровой экономике является защита конфиденциальной информации от киберпреступников. В связи с этим в целях совершенствования электронной торговли рекомендуется внедрение на предприятии бизнес-процессной модели, обеспечивающей защиту информации.

Суть ее заключается в действии системы раннего обнаружения нарушений информационной безопасности после стадии поступления заявки, перед ее обработкой. Экономическая эффективность рекомендуемого мероприятия будет получена, когда начальные инвестиции будут покрыты полностью полученными доходами. После внедрения рекомендуемого программного обеспечения повысится уровень защиты конфиденциальной информации предприятия, количество обработанных заявок, что в итоге приведет к росту доходов предприятия, а, следовательно, к росту прибыли.

Цифровизация экономики требует от хозяйствующих субъектов постоянного отслеживания инноваций, внедрения усовершенствованных технологий, программного обеспечения, чтобы функционировать на рынке успешней конкурентов. Это обуславливает актуальность и важность проведенного исследования.

Список литературы

1. Цифровая экономика: социально-психологические и управленческие аспекты / Е.В. Камнева, А.И. Гретченко, Н.П. Дедов и др.; под ред. Е.В. Камневой, М.М. Симоновой. – Москва : Прометей, 2019.

2. Аракелян С. Цифровая экономика: стратегия развития и новые технологии достижения, риски, угрозы // Экономист. – 2018. – №6.

3. Указ Президента Российской Федерации от 13 мая 2017г. №208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_216629/ (дата обращения: 5.12.2020).

4. Указ Президента Российской Федерации от 9 мая 2017г. №203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 5.12.2020).