

А. Ю. Каснерик, А. Д. Туфатулина

Институт бизнеса БГУ, Минск, Беларусь

Научный руководитель – Д. Г. Гончерёнок, старший преподаватель

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В статье рассматриваются вопросы экономической безопасности организации в условиях цифровой трансформации. Определяются ключевые угрозы экономической безопасности, такие как кибератаки и утечка информации. Анализируется взаимосвязь между цифровизацией и экономической безопасностью с акцентом на новых возможностях и угрозах, возникающих в процессе цифровой трансформации предприятий.

Ключевые слова: *экономическая безопасность, цифровая трансформация, риски и угрозы*

В современных условиях, когда внешняя и внутренняя среда предпринимательской деятельности становятся все более сложными и изменчивыми, обеспечение экономической безопасности становится важнейшей задачей для любого хозяйствующего субъекта. Республика Беларусь, как и многие другие страны, столкнулась с рядом специфических вызовов. На уровне предприятий это проявляется в необходимости адаптации к новым условиям рынка, усилении конкуренции и появлении новых рисков. Внешние угрозы экономической безопасности предприятия могут быть связаны с изменениями на международных рынках, колебаниями валютных курсов, санкциями или ограничениями, а также с обострением конкуренции. Внутренние – касаются, прежде всего, финансовой стабильности предприятия, его управленческого контроля, кадровой политики и соблюдения нормативно-правовых требований. Таким образом, в современных условиях вопрос обеспечения экономической безопасности предприятия выходит на первый план. Однако, что стоит за данным понятием?

Понятие «экономическая безопасность» имеет весьма широкое значение, поскольку его составляющие содержат в себе одновременно два аспекта: экономика и безопасность. По этой причине под экономической безопасностью объекта необходимо понимать такое состояние, которое обеспечивает его защиту от опасности в экономической сфере [9]. Экономическая безопасность организаций характеризуется уровнем защиты от внешних и внутренних угроз при эффективном использовании всех видов ресурсов для стабильного непрерывного развития. Можно выделить следующие функциональные составляющие экономической безопасности организации, охватывающие ключевые аспекты ее деятельности [13]:

- финансовую: контроль и балансирование доходов и расходов хозяйствующего субъекта;
- интеллектуальную и кадровую: снижение рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом;
- технико-технологическую: создание и использование современного оборудования, технической базы и основных средств производства, а также разработку эффективных технологий и бизнес-процессов;
- политико-правовую: всестороннее юридическое обеспечение деятельности организации, грамотную правовую работу с контрагентами и властью, решение иных правовых вопросов;
- экологическую: соблюдение национальных и международных стандартов минимально допустимого содержания вредных веществ в окружающей среде;

- информационную: обеспечение конфиденциальности, целостности и кибербезопасности;
- силовую: физическая охрана объектов, противодействие криминалу, взаимодействие с правоохранительными и другими государственными органами.

Для повышения экономической безопасности предприятиям нужно проанализировать текущее состояние и процессы в бизнесе на предмет рисков и потенциальных угроз и найти пути для их минимизации и предупреждения возможных убытков. Повышать уровень безопасности и уменьшать возможные убытки можно с помощью прописанных процессов, правил и регламентов, а также, используя физические инструменты. Их можно разделить на 3 группы: управление рисками (страхование, диверсификация, хеджирование и т.д.), средства технической защиты (контрольно-пропускные пункты, системы видеонаблюдения, системы пропусков) и финансовые инструменты (бюджетирование, планирование, ведение управленческого учета, мониторинг финансовых показателей).

На сегодняшний день, ведение бизнеса неразрывно связано с цифровой трансформацией, поскольку она стала ключевым фактором выживания и развития компаний в условиях глобальной конкуренции и быстро меняющихся технологий. Данный процесс предполагает использование передовых технологий и цифрового опыта для совершенствования бизнес-процессов, целей и стратегий при одновременном улучшении рабочего процесса и качества обслуживания клиентов [5]. В отличие от цифровизации, цифровая трансформация влечет за собой изменения не только на уровне ИТ, но и на уровнях бизнес-модели, взаимоотношений с клиентами и сотрудниками, а также конкретные процессы. Цифровая трансформация охватывает все процессы компании (цифровую бизнес-модель, цифровой актив, цифровую культуру) [8] и подразумевает изменение мышления в организации, вслед за которым идет перестройка бизнеса. Среди основных трендов цифровой трансформации бизнеса в 2024 г. можно выделить следующие: экосистемность, персонализация, IoT и 5G, применение искусственного интеллекта, а также планирование ресурсов предприятия. Их внедрение приносит множество преимуществ для организаций, экономики и общества в целом, среди них – повышение эффективности предприятий, улучшение взаимодействия с клиентами, снижение затрат, возможность быстро адаптироваться к изменяющимся рыночным условиям, сохранение конкурентоспособности и др. Однако цифровая трансформация связана с определенными угрозами для бизнеса. Угроза – это совокупность негативных факторов и условий, возникающих в ходе взаимодействия бизнеса с окружающими объектами, которые наносят ущерб компании [10]. Среди них можно выделить – кибератаки и утечку данных.

Кибератака – это воздействие на информационную систему с целью повредить ее, получить или ограничить к ней доступ, собрать конфиденциальные данные. Чтобы совершить кибератаку, злоумышленники ищут уязвимости в информационной системе [5]. По данным СФО в 2024 г. 85 % специалистов по кибербезопасности связывают рост кибератак с использованием злоумышленниками генеративного ИИ, 75 % – отмечают рост кибератак за последний год [1]. По данным Statista в 2023 г. 72,7 % всех организаций во всем мире стали жертвами атаки программ-вымогателей [7].

Утечка данных – это инцидент, при котором конфиденциальная, личная или коммерческая информация становится доступной неавторизованным лицам. Она включает в себя кражу личных данных (пароли, номера кредитных карт) или коммерческой информации (финансовые отчеты, патенты). С начала этого года хакеры запустили в сеть 286 млн уникальных телефонных номеров и 96 млн адресов электронной почты. Об этом в конце октября 2024 г. сообщает сервис разведки утечек данных и мониторинга даркнета Data Leakage & Breach

Intelligence (DLBI) [2]. Больше всего утечек зафиксировано из сектора электронной коммерции от всех попавших в открытый доступ данных. На втором месте стоят аптеки и медицинские сервисы, за ними идет сектор финансовых услуг и ретейлеры. По объему же слитых данных лидирует финансовый сектор. Таким образом, цифровая трансформация и экономическая безопасность бизнеса связаны так, что чем глубже интегрируются цифровые инструменты в бизнес, тем важнее становится обеспечение надежной экономической безопасности для защиты ресурсов, данных и устойчивости предприятий. Однако, для обеспечения эффективной экономической безопасности необходимы именно цифровая трансформация и внедрение новых технологий.

В белорусских компаниях цифровая трансформация происходит не так быстро, как в западных странах, но крупные предприятия и холдинги начинают активно применять новые технологии. Согласно Глобальному инновационному индексу за 2024 г., Республика Беларусь занимает 38 место по показателю «Доступ к ИКТ» (среди 133 стран) и 55 место по показателю «Использование ИКТ» (среди 133 стран) [11]. По данным Глобального инновационного индекса 2023 г. наша страна заняла 80 место из 132 стран, что соответствует третьему квартилю, наиболее сильными позициями являются «Человеческий капитал и научные исследования» и «Знания и технологии» [4]. Также Постановлением Совета Министров Республики Беларусь от 2 февраля 2021 г. № 66 утверждена программа «Цифровое развитие Беларуси» на 2021–2025 гг. [12]. Развитие цифровых технологий создает отличные перспективы для укрепления экономической безопасности в стране. Вместе с тем, статистические данные по экономическим преступлениям за последние годы подтверждают необходимость дальнейшего развития данной стратегии. Беларусь входит в тройку стран СНГ, на которую в 2023 г. и первой половине 2024 г. было совершено наибольшее количество кибернападений. Жертвами кибератак в Беларуси чаще всего становятся госучреждения (22 %), промышленные предприятия (14 %), финансовые компании (11 %) и организации из сферы науки и образования (8 %) [3].

В современных условиях обеспечение экономической безопасности является необходимым фактором для успешного функционирования предприятий. Сложности внутренней и внешней среды требуют от организаций адаптации и внедрения современных технологий. Соответственно, для обеспечения надежной экономической безопасности в Республике Беларусь крайне важно развивать и интегрировать цифровые технологии, что создаст прочный фундамент для стабильного роста и устойчивого развития бизнеса в условиях быстро меняющегося мира.

Список использованных источников

1. News for CFOs // CFO. – URL: <https://www.cfo.com/> (date of access: 17.10.2024).
2. DLBI – Поиск утечек данных и мониторинг даркнета. – URL: <https://dlbi.ru/> (дата обращения: 17.10.2024).
3. Жертвами кибератак часто становятся госучреждения и промышленные предприятия // GB.BY. – URL: <https://www.gb.by/novosti/> (дата обращения: 18.10.2024).
4. What is the future of innovation-driven growth // Global Innovation Index. – URL: <https://www.wipo.int/web/> (дата обращения: 19.10.2024).
5. Top 10 Digital transformation trends and strategies for 2023 and beyond // LinkedIn. – URL: <https://www.linkedin.com/> (date of access: 18.10.2024).
6. Что такое кибератаки и какие они бывают // Skillbox Media. – URL: <https://skillbox.ru/media/code/chto-takoe-kiberataki-i-kakie-oni-byvayut/> (дата обращения: 17.10.2024).
7. Statista – Global firms targeted by ransomware 2023. – URL: <https://www.statista.com/> (дата обращения: 20.10.2024).

8. Главные тренды 2024 года в области цифровизации // Бизнес-секреты Тинькофф. – URL: <https://secrets.tinkoff.ru/> (дата обращения: 17.10.2024).
9. *Гончерёнок, Д. Г.* Подходы к определению экономической безопасности организации // Бизнес. Образование. Экономика : Междунар. науч.-практ. конф., Минск, 2 апреля 2020 г. : сб. ст. в 2 ч. / редкол.: В. В. Манкевич (гл. ред.) [и др.]. – Минск : Институт бизнеса БГУ, 2020. – Ч. 2. – С. 18–21.
10. Экономическая безопасность предприятия: риски и угрозы // КонтурФокус. – URL: <https://focus.kontur.ru/site/news/> (дата обращения: 19.10.2024).
11. Рейтинги ИКТ // Министерство связи и информатизации Республики Беларусь. – URL: <https://mpt.gov.by/> (дата обращения: 20.10.2024).
12. Государственная программа «Цифровое развитие Республики Беларусь» на 2021–2025 годы // Министерство связи и информатизации Республики Беларусь. – URL: <https://mpt.gov.by/> (дата обращения: 21.10.2024).
13. *Резкин, П. Е.* Сущность и составляющие экономической безопасности организации / П. Е. Резкин, Н. Л. Белорусова // Вестник Полоцкого государственного университета. – 2013. – № 5. – С. 47–55.