

КИБЕРБЕЗОПАСНОСТЬ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

А. А. Яблокова

*студент, Витебский государственный технологический университет, г. Витебск, Беларусь,
yblokovaanastasia2@gmail.com*

Научный руководитель О. П. Советникова

*кандидат экономических наук, доцент, Витебский государственный технологический университет,
г. Витебск, Беларусь, sovetnikova@bk.ru*

Информационная среда как компонент бизнес-среды характеризуется существенными киберугрозами и требует киберзащиты. Целью статьи является анализ сущности кибербезопасности как фактора финансовой безопасности предприятия. Автором рассмотрены понятия кибербезопасности и киберугроз, выявлена их взаимосвязь и влияние на финансовые потери бизнеса. Сделан вывод о необходимых мерах кибербезопасности, защите информационных ресурсов предприятий и предотвращении несанкционированного вмешательства в деятельность предприятий.

Ключевые слова: кибербезопасность; кибератаки; цифровизация; экономическое развитие; механизм защиты; экономическая стабильность

CYBERSECURITY AS A FACTOR OF ECONOMIC SECURITY OF ENTERPRISES

A. A. Yablakava

student, Vitebsk State Technological University, Vitebsk, Belarus, yblokovaanastasia2@gmail.com

Supervisor O. P. Sovetnikova

*PhD in economics, associate professor, Vitebsk State Technological University, Vitebsk, Belarus,
sovetnikova@bk.ru*

The information environment as a component of the business environment is characterized by significant cyber threats and requires cyber protection. The purpose of the article is to analyze the essence of cyber security as a factor in the financial security of an enterprise. The author considers the concepts of cyber security and cyber threats, identifies their relationship and impact on financial losses of business. A conclusion is made on the necessary cyber security measures, protection of information resources of enterprises and prevention of unauthorized interference in the activities of enterprises.

Keywords: cybersecurity; cyber attacks; digitalization; economic development; defense mechanism; economic stability

В современных реалиях процесс успешного функционирования и экономического развития предприятий во многом зависит от совершенствования их деятельности в области обеспечения экономической безопасности. Кибербезопасность становится одним из важнейших внутренних факторов экономической безопасности предприятий, когда цифровые технологии являются неотъемлемой частью бизнеса и требуют постоянного взаимодействия с информационными системами, облачными сервисами и удаленными рабочими процессами. Однако вместе с преимуществами технологий приходят новые вызовы и проблемы, в частно-

сти это связано с тем, что многие предприятия недооценивают важность инвестирования в кибербезопасность до тех пор, пока непосредственно не столкнутся с кибератаками, рост числа которых увеличивается ежегодно вместе с их усложнением. Недостаточно проработанные механизмы защиты, устаревшие программы и отсутствие должного уровня подготовки у сотрудников приводят к тому, что злоумышленники получают доступ к конфиденциальной информации, нарушают работу систем и наносят значительный ущерб предприятию в различных аспектах.

Эффективная защита от киберугроз позволяет предприятию сохранить конкурентные преимущества, избежать финансовых потерь и минимизировать репутационные риски, так как кибербезопасность напрямую влияет на устойчивость бизнес-процессов, финансовую стабильность и доверие клиентов и партнеров. Поэтому исследование кибербезопасности как фактора экономической безопасности становится актуальным для выявления рисков, разработки эффективных стратегий защиты от них и управления ими, а также для повышения общей устойчивости предприятия в условиях возрастающих цифровых угроз.

В эпоху цифровых трансформаций, кибератаки являются не только технологической проблемой, но и серьезной угрозой для экономики. Доверие к онлайн-транзакциям может быть подорвано нарушениями безопасности, что приведет к экономической стагнации. Последствия кибератак выходят за рамки прямых финансовых потерь, включая репутационный ущерб, сбои в работе и потерю интеллектуальной собственности. Ведущие технологические компании, такие как Microsoft, играют жизненно важную роль в обеспечении этого доверия, инвестируя в кибербезопасность. Поэтому защита цифровых систем имеет решающее значение не только для отдельных компаний, но и для стабильности и устойчивости мировой экономики в целом.

Для того, чтобы рассмотреть и предложить возможные меры по защите от киберпреступлений необходимо определить, что понимается под киберпреступлением и под кибербезопасностью. Так как данные понятие получили многогранную трактовку от различных авторов, можно предложить авторское определение: «Киберпреступление – это незаконная деятельность, осуществляемая с использованием компьютерных систем, сетей или интернета, которая направлена на причинение вреда, кражу информации, получение финансовой выгоды или другие противоправные цели».

Киберпреступления могут принимать различные формы, включая, но не ограничиваясь, взломом систем, распространением вредоносного программного обеспечения, фишингом, кражей личных данных, атакой на системы организации (например, DDoS-атаки) и мошенничеством в онлайн-среде. В настоящее время количество киберпреступлений в Беларуси продолжает расти. Если за 2023 год в Беларуси совершено 85 374 преступления, из них 18 321 – по линии противодействия киберпреступности (21,5 %), то за первые шесть месяцев 2024 года из совершенных 36 155 преступлений 10 099 относятся к киберпреступлениям, что составляет уже 27,9 %. По оценке аналитиков, наибольшую угрозу для клиентов белорусских банков в 2024 году представляют киберугрозы, связанные с телефонным мошенничеством (вишингом) с использованием социальной инженерии [1].

Кибербезопасность в рамках предприятия представляет собой совокупность процессов, технологий и контролей, направленных на защиту компьютерных систем, сетей и данных от киберугроз и несанкционированного доступа. Это включает в себя применение мер предосторожности для предотвращения кибератак, обеспечение конфиденциальности, целостности и доступности информации, а также управление инцидентами в случае их возникновения.

Экономическая безопасность предприятия напрямую связана с кибербезопасностью, под которой понимается совокупность методов, технологий и процессов, предназначенных для защиты целостности сетей, программ и данных от цифровых атак.

Глобальный индекс кибербезопасности (Global Cybersecurity Index, GCI) является надежным справочником, который измеряет приверженность стран кибербезопасности на глобальном

уровне. Специалисты оценивают компьютерную безопасность всех стран мира по пяти параметрам: юридическая, техническая, организационная подготовленность, готовность к сотрудничеству, развитие образовательного и исследовательского потенциала страны.

В GCI 2024 используется новая методика анализа, которая позволяет отметить достижения в области информационной безопасности каждой страны. 46 стран отнесены к первому, самому высокому, из пяти уровней. В группу вошли страны Европы, США, Гана, Кения, Маврикий, Марокко, Руанда. Вторая группа – «Развитие» – объединила 29 стран, включая Китай, Россию, Казахстан, Швейцарию, Канаду и другие. Большинство стран находятся на этапах «Становления» (уровень 3–49 государств) и «Формирование» (уровень 4–56 государств). Эти страны значительно расширили цифровые услуги и возможности подключения, но им всё ещё необходимо интегрировать меры информационной безопасности. Наибольшей поддержки международного сообщества требуют 14 стран пятой группы («Создание»). По данным GCI 2024, с 2021 года наибольшего прогресса в области кибербезопасности добился Африканский континент. Развивающиеся страны, не имеющие выхода к морю, и малые островные развивающиеся государства продолжают сталкиваться с нехваткой ресурсов и возможностей для обеспечения кибербезопасности [2].

Организации сталкиваются с многочисленными типами инцидентов кибербезопасности.

Кибератаки могут крайне негативно влиять на основные атрибуты безопасности: целостность, доступность и конфиденциальность, что приводит к нарушению или задержке услуг или действий, финансовым потерям и общему недоверию к электронным транзакциям.

Кибератаки продолжают развиваться, и для того, чтобы поддерживать данные и системы в защищенном состоянии, необходимо принимать значительные и эффективные меры.

Меры, направленные на контроль риска кибербезопасности, носят не только технический характер. Правовые, нормативные и организационные меры также необходимо учитывать, чтобы иметь действительно эффективный подход. Эти меры должны включать адекватные законы; обязательные правовые или отраслевые стандарты; программы повышения осведомленности и объявления общественной службы; программы развития навыков; распространение передового опыта; создание специализированных агентств; эффективные формы международного сотрудничества правоохранительных органов.

Таким образом, кибербезопасность является решающим фактором в обеспечении экономической стабильности в цифровом мире. Она требует целостного подхода, объединяющего технологии, человеческие навыки и сотрудничество для обеспечения безопасного цифрового будущего. Приоритетным направлением в совершенствовании информационной безопасности Республики Беларусь является работа над нормативно-правовой базой, а также улучшение механизма государственного регулирования деятельности в данной сфере. Профилактические беседы с населением также являются неотъемлемым звеном в решении вопроса информационной безопасности как страны в целом, так и отдельного человека в частности.

Библиографические ссылки

1. Киберпреступления в Беларуси // Myfin : сайт. URL: <https://myfm.by/article/biznes/eksperty-rasskazali-o-kolicestve-kiberprestuplenij-v-belarusi-33983> (дата обращения: 07.04.2025).
2. Global Cybersecurity Index 2018. URL: Global Cybersecurity Index 2024 *Subtitle report* (itu.int) (дата обращения: 25.03.2025).