УДК 004.056

ЦИФРОВИЗАЦИЯ И КИБЕРБЕЗОПАСНОСТЬ: ВЫЗОВЫ И РЕШЕНИЯ ДЛЯ БИЗНЕСА

Д. И. Гордиенко[1)], Е. А. Варвашеня[2)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, gordirnkoda19@gmail.com*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, elisavetta2007@gmail.com*

Научный руководитель **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, shandor@bsu.by

Цифровизация бизнеса в Республике Беларусь развивается стремительно, охватывая всё больше отраслей и процессов. Однако вместе с ростом цифровых решений усиливаются и киберугрозы, которые становятся всё более разнообразными и сложными. Цифровая трансформация белорусского бизнеса является объективной и необходимой реальностью. Текущая ситуация характеризуется высокой активностью злоумышленников, использующих преступные методы от получения информации до нанесения финансового ущерба.

Ключевые слова: кибербезопасность; киберугрозы; фишинг; социальная инженерия.

DIGITALIZATION AND CYBERSECURITY: CHALLENGES AND SOLUTIONS FOR BUSINESS

D. I. Hardzienka[1)], E. A. Varvashenia[2)]

[1)] *student, Belarusian State University, Minsk, Belarus, gordirnkoda19@gmail.com*
[2)] *student, Belarusian State University, Minsk, Belarus, elisavetta2007@gmail.com*

Supervisor **N. I. Sandora**

senior lecturer, Belarusian State University, Minsk, Belarus, shandor@bsu.by

The digitalization of business in the Belarus is developing rapidly, encompassing an ever-increasing number of industries and processes. However, along with the growth of digital solutions, cyber threats are also increasing, becoming increasingly diverse and complex. The digital transformation of Belarusian businesses is an objective and necessary reality. The current situation is characterized by high levels of activity by criminals using criminal methods ranging from obtaining information to causing financial damage.

Keywords: cybersecurity; cyber threats; phishing; social engineering.

В условиях активной цифровизации белорусского бизнеса киберугрозы становятся всё более значимыми. По данным Kaspersky за 2024 год, Беларусь занимает второе место в мире по доле пользователей, подвергшихся интернет-атакам – 43,4 %, что подчёркивает уязвимость организаций и необходимость системного подхода к информационной безопасности [1].

Фишинг остаётся наиболее распространенной угрозой: злоумышленники маскируются под банки, госорганы или партнеров, использую реалистичные письма и сайты. Социальная

инженерия также набирает обороты – злоумышленники используют поддельные подписи, номера и дипфейки, чтобы получить доступ к внутренней информации или инициировать переводы. Белорусские компании сталкиваются с фишингом, DDoS-атаками, вредоносными ПО, утечками персональных данных и даже саботажем инфраструктуры.

Одной из ключевых проблем, тормозящих эффективную цифровую трансформацию, является дефицит квалифицированных специалистов. Особенно остро это ощущается в регионах, где нехватка ИТ-кадров приводит к ошибкам, слабой защите систем и низкому уровню эксплуатации цифровых решений.

Дополнительным барьером становится использование устаревшего оборудования и программного обеспечения, часто зависимого от иностранных поставщиков. Это создаёт сложности с техподдержкой, обновлениями и совместимостью, особенно в условиях санкционного давления и ограниченного доступа к зарубежным сервисам

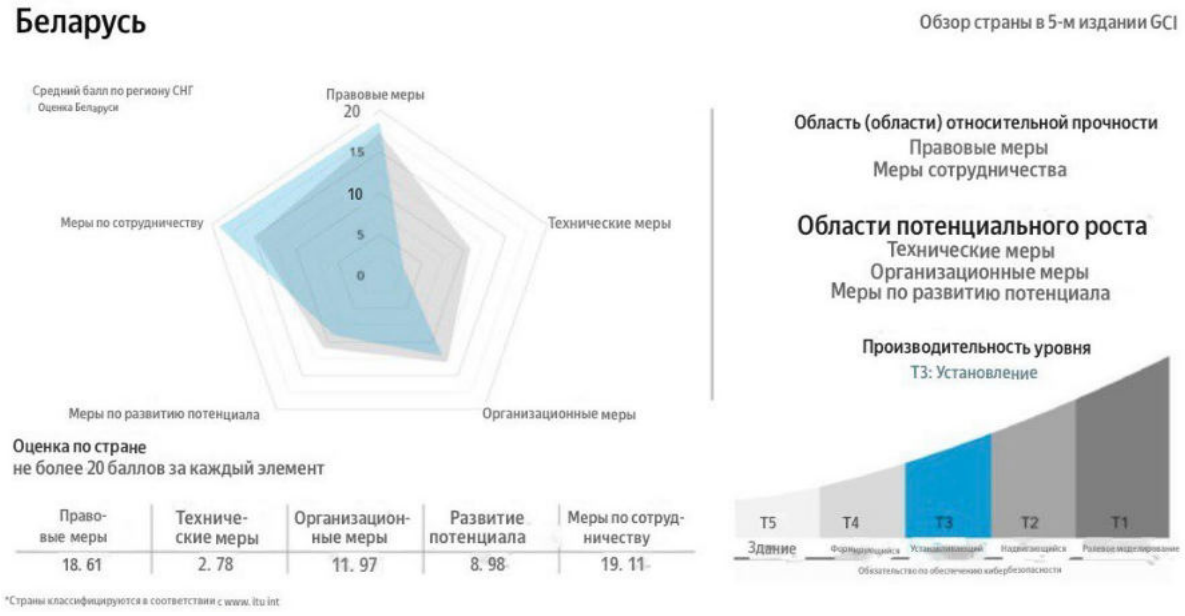
Без преодоления кадрового ограничения и без интеграции кибербезопасности в каждый этап цифровой трансформации бизнес рискует не только потерять данные, но и доверие клиентов, партнёров и государства.

Комплексная оценка состояния кибербезопасности Республики Беларусь по данным пятого издания Глобального индекса кибербезопасности (Global Cybersecurity Index, GCI) отражает, что Беларусь обладает прочной правовой основой и активно участвует в международном сотрудничестве, однако для перехода на более высокий уровень необходимо сосредоточиться на техническом оснащении, организационной зрелости и развитии кадрового потенциала.

В центре анализа – пять ключевых направлений: правовые меры, меры сотрудничества, организационные меры, технические меры и меры по развитию потенциала. Каждое направление оценивается по 20-балльной шкале.

На радарной диаграмме видно, что Беларусь получила 18,61 – юридические аспекты, 19,11 – международное сотрудничество, что свидетельствует о наличии развитой нормативной базы и активной интеграции в глобальные инициативы. Организационные меры оценены в 11,97 балла, технические – в 2,78, а развитие потенциала – в 8,98 балла.

В нижней части графика указано, что страна классифицирована в Tier 3 – «Установление», что означает наличие базовых элементов системы, но ещё не достигнут уровень зрелости, характерный для более развитых стран в области кибербезопасности (рисунок) [2].



Состояние кибербезопасности Республики Беларусь.
Источник: [2]

Цифровизация бизнеса в Беларуси сопровождается активным внедрением инструментов информационной безопасности, среди которых ключевую роль играют SIEM-системы, криптография, стандарты ISO и государственная поддержка.

SIEM-системы позволяют организациям централизованно собирать и анализировать события из различных источников – от операционных систем до антивирусов. Они выявляют инциденты на основе логических правил, фильтруют события по критичности, хранят данные для ретроспективного анализа и формируют отчётность. Банки Беларуси уже накопили значительный опыт в их внедрении, адаптируя решения под национальные требования и бизнес-процессы [3].

Создание отраслевых стандартов информационной безопасности (ИБ) для малого и среднего бизнеса в Республике Беларусь является важным шагом на пути к формированию устойчивой цифровой экономики.

Важным элементом реализации этой инициативы является партнёрство с Парком высоких технологий (ПВТ), который обладает уникальной экспертизой в сфере ИТ и подготовки кадров. ПВТ может стать платформой для обмена опытом, внедрения лучших международных практик и поддержки стартапов, работающих в области кибербезопасности.

В то же время в стране формируется комплексная система противодействия эти вызовам. Развивается нормативно-правовая база, внедряются современные технические средства защиты (SIEM, криптография), реализуются масштабные государственные программы и активно применяются международные стандарты информационной безопасности. Это создает прочный фундамент для построения бизнеса, способного противостоять современным угрозам.

Кибербезопасность не может быть периферийной функцией или разовой мерой. Она должна быть интегрирована в стратегию развития компании и стать неотъемлемой частью корпоративной культуры на всех уровнях.

Библиографические ссылки

1. Какие киберугрозы испытали на себе белорусы в 2024 году и как от них защититься в 2025 году // ibMedia : сайт. URL: https://ibmedia.by/news/kakie-kiberugrozy-ispytali-na-sebe-belorusy-v-2024-godu-i-kak-ot-nih-zashhititsya-v-2025-godu/ (дата обращения 15.09.2025).

2. Беларусь получила уровень Tier в Cybersecurity Index 2024 // Noventiq : сайт. URL: https://noventiq.by/about/news/belarus-poluchila-uroven-tier-3-v-global-cybersecurity-index-2024?ysclid=mft9l5wk16459280866 (дата обращения 16.09.2025).

3. Как мы внедряем SIEM // МультиТек Инжиниринг Информационная безопасность : сайт. URL: https://mte-cyber.by/mte-blog/kak-my-vnedryaem-siem/ (дата обращения 16.09.2025).