УДК 338.001.36

КИБЕРБЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕДПРИЯТИЙ

Т. Н. Буренок[1)], А. Д. Волгина[2)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, tania.burenok@gmail.com*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, alexandra.volgina7@gmail.com*

Научный руководитель: **Т. А. Бронская**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, bronska.tatiana@yandex.ru

В научной работе описывается важность кибербезопасности в условиях цифровой трансформации предприятий, так как с развитием взаимосвязанных систем и облачных технологий увеличиваются риски кибератак, что требует внедрения комплексных стратегий защиты данных. Кибербезопасность включает технологии, методы и политику, направленные на предотвращение атак и защиту компьютерных систем, приложений, устройств и данных.

Ключевые слова: кибербезопасность, искусственный интеллект, цифровая трансформация.

CYBERSECURITY IN THE ERA OF DIGITAL TRANSFORMATION OF ENTERPRISES

T. N. Burenok[1)], A. D. Volgina[2)]

[1)] *student, Belarusian State University, Minsk, Belarus, tania.burenok@gmail.com*
[2)] *student, Belarusian State University, Minsk, Belarus, alexandra.volgina7@gmail.com*

Supervisor: **T. A. Bronskaia**

senior lecturer, Belarusian State University, Minsk, Belarus, bronska.tatiana@yandex.ru

The scientific work describes the importance of cybersecurity in the context of digital transformation of enterprises, since with the development of interconnected systems and cloud technologies, the risks of cyber-attacks increase, which requires the introduction of comprehensive data protection strategies. Cybersecurity includes technologies, methods, and policies aimed at preventing attacks and protecting computer systems, applications, devices, and data.

Keywords: cybersecurity, artificial intelligence, digital transformation.

В эпоху цифровизации компаний кибербезопасность стала важнейшим аспектом деятельности. С ростом взаимосвязанных систем и облачных технологий увеличиваются риски кибератак, что требует создания комплексных стратегий для защиты данных и обеспечения безопасности при цифровой трансформации.

Кибербезопасность – это любые технологии, методы и политика предотвращения кибератак или смягчения их последствий. Кибербезопасность направлена на защиту компьютерных систем, приложений, устройств, данных, финансовых активов и людей от программ-вымогателей и других вредоносных программ, фишинговых атак, кражи данных и других киберугроз.

Кибератаки оказывают огромное и растущее влияние на бизнес и экономику. По некоторым оценкам, к 2025 году киберпреступность будет обходиться мировой экономике в 10,5 трлн долларов США в год. Стоимость кибератак продолжает расти по мере того, как киберпреступники становятся все более изощренными [1].

Средняя стоимость утечки данных в США подскочила с 4,45 млн долларов США в 2023 году до 4,88 млн долларов США, что на 10 % больше, чем в прошлом году, и является самым высоким показателем с начала пандемии 2020 года.

На корпоративном уровне кибербезопасность является ключевым компонентом общей стратегии управления рисками организации. По данным Cybersecurity Ventures, в период с 2021 по 2025 год глобальные расходы на продукты и услуги в области кибербезопасности превысят 1,75 трлн долларов США.

В современном цифровом мире фишинг является одной из распространенных форм кибератак, при которой злоумышленники используют мошеннические электронные письма, чтобы обманом заставить пользователей перейти по вредоносным ссылкам или загрузить вредоносное ПО. Для борьбы с этим многие организации внедрили имитационные фишинговые упражнения как часть своей стратегии кибербезопасности. Пример такой инициативы произошел в реальной жизни в компании Tribune Publishing, крупной медийной компании в США [3]. В 2020 году компания провела внутренний тест, в ходе которого сотрудники получили электронное письмо с обещанием праздничной премии при переходе по ссылке. Это письмо было разработано таким образом, чтобы выглядеть достоверно, но являлось частью фишинговой кампании для повышения осведомленности. Когда сотрудники переходили по ссылке, их встречало уведомление, объясняющее, что они попались на фишинговую симуляцию, и им предоставлялись обучающие материалы о том, как распознавать фишинговые атаки.

Аудиты в области кибербезопасности и соблюдение законов о защите данных, таких как General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), Personal Information Protection and Electronic Documents Act (PIPEDA), Brazil's General Data Protection Law (LGPD), являются ключевыми элементами для обеспечения безопасности конфиденциальной информации и избежания юридических последствий [5]. Реальный пример, подчеркивающий важность кибераудитов и соблюдения законов о конфиденциальности, — это случай с компанией Equifax, одной из крупнейших кредитных бюро в США. В 2017 году Equifax подверглась масштабной утечке данных, в результате которой были скомпрометированы персональные данные 147 миллионов американцев, включая имена, номера социального страхования, даты рождения и адреса [2].

В условиях стремительного роста цифровизации и увеличения взаимосвязанных систем кибербезопасность становится неотъемлемой частью стратегического управления рисками для организаций. Кибератаки, становясь все более сложными и разрушительными, требуют внедрения комплексных и многослойных стратегий защиты, включающих физические, технические и административные меры. Эффективное управление атаками и восстановление после них играют ключевую роль в минимизации ущерба и восстановлении нормального функционирования организаций. Для этого необходимы оперативные планы реагирования, регулярные обновления систем безопасности и постоянный мониторинг уязвимостей.

Библиографические ссылки

1. What is Cybersecurity? [Электронный ресурс]. URL: https://www.ibm.com/topics/cybersecurity (дата обращения: 21.09.2024).

2. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach [Электронный ресурс]. URL: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach (дата обращения: 19.09.2024).

3. How a Phishing Awareness Test Went Very Wrong [Электронный ресурс]. URL: https://www.bankinfosecurity.com/blogs/how-phishing-readiness-test-goes-very-wrong-p-2948 (дата обращения: 22.09.2024).

4. 42 Cyber Attack Statistics by Year: A Look at the Last Decade [Электронный ресурс]. URL: https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/ (дата обращения: 21.09.2024).

5. Data Privacy Laws and Regulations Around the World [Электронный ресурс]. URL: https://securiti.ai/privacy-laws/ (дата обращения: 21.09.2024).