УДК 004.056.5

КИБЕРБЕЗОПАСНОСТЬ В КОНТЕКСТЕ ИКТ-СТРАТЕГИЙ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ

И. В. Сержант[1)], К. Д. Акалович[2)], Е. В. Шелютин[3)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, ivan.sergant2005@gmail.com*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, zyplikzy@gmail.com*
[3)] *студент, Белорусский государственный университет, г. Минск, Беларусь, shellliaegor@gmail.com*

Научный руководитель: **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, shandoranatasha@tut.by

В условиях стремительного развития информационно-коммуникационных технологий кибербезопасность становится одним из ключевых аспектов в стратегическом управлении организацией. С ростом объема цифровых данных, распространением облачных технологий и увеличением числа кибератак возникает необходимость внедрения комплексных решений для защиты информации. В этом контексте ИКТ-стратегии играют важную роль, обеспечивая платформу для эффективного принятия решений в условиях цифровизации бизнеса.

Ключевые слова: кибербезопасность; ИКТ; киберугрозы; защита данных; принятие решений.

CYBERSECURITY IN THE CONTEXT OF ICT STRATEGIES FOR DECISION MAKING

I. V. Sergeant[1)], K. D. Akalovich[2)], E. V. Shelyutin[3)]

[1)] *student, Belarusian State University, Minsk, Belarus, ivan.sergant2005@gmail.com*
[2)] *student, Belarusian State University, Minsk, Belarus, zyplikzy@gmail.com*
[3)] *student, Belarusian State University, Minsk, Belarus, shellliaegor@gmail.com*

Supervisor: **N. I. Shandora**

senior lecturer, Belarusian State University, Minsk, Belarus, shandoranatasha@tut.by

In the conditions of rapid development of information and communication technologies, cybersecurity becomes one of the key aspects in the strategic management of the organization. With the growth of digital data, the spread of cloud technologies and the

increasing number of cyberattacks, there is a need to implement comprehensive solutions to protect information. In this context, ICT strategies play an important role by providing a platform for effective decision making in a digitized business environment.

Keywords: cybersecurity; ICT; cyber threats; data protection; decision-making.

Кибербезопасность – это процесс защиты информации, информационных систем и сетей от кибератак, несанкционированного доступа, утечек и других угроз. Она включает в себя множество направлений, таких как обеспечение конфиденциальности, целостности и доступности данных, управление рисками и инцидентами, а также развитие механизмов противодействия киберугрозам [2].

- Конфиденциальность – защита информации от несанкционированного доступа.
- Целостность – обеспечение точности и полноты данных.
- Доступность – обеспечение возможности доступа к информации для авторизованных пользователей.
- Управление инцидентами – процессы, направленные на выявление, анализ и устранение последствий кибератак.

Правовое регулирование в сфере кибербезопасности направлено на создание нормативной базы, обеспечивающей защиту информации на уровне государства и международного сообщества [1]. Среди ключевых нормативных актов можно выделить:

- Указ Президента Республики Беларусь № 40 от 14 февраля 2023 года «О кибербезопасности». Документ устанавливает правовую основу для создания и функционирования национальной системы кибербезопасности, направленной на защиту государственных органов, организаций и критической информационной инфраструктуры от кибератак [3].
- Общую директиву по кибербезопасности Европейского Союза (NIS Directive), которая задает стандарты для государств-членов ЕС по защите критической инфраструктуры.
- Закон США о кибербезопасности (Cybersecurity Act), направленный на защиту данных и снижение рисков кибератак на национальном уровне.
- Национальные стандарты и руководства: например, ГОСТ Р в России, ISO 27001 и другие международные стандарты, регулирующие защиту информационных систем и управление рисками.

ИКТ-стратегии (информационно-коммуникационные технологии) представляют собой комплекс мероприятий и подходов, направленных на использование цифровых технологий для повышения эффективности бизнеса. Они играют важную роль в управлении процессами, ресурсами и коммуникациями внутри организации, что делает их критически важными для обеспечения безопасности и устойчивого развития [6].

Основные компоненты ИКТ-стратегий:

- Инфраструктура ИКТ: создание и поддержание инфраструктуры для обмена данными и управления бизнес-процессами.

- Программное обеспечение: использование приложений для автоматизации бизнес-процессов.

- Управление данными: процессы сбора, хранения и анализа данных.

- Кибербезопасность: защита информации от угроз и несанкционированного доступа.

На сегодняшний день множество компаний внедряют эффективные ИКТ-стратегии, интегрирующие кибербезопасность как один из ключевых элементов. Примером успешной реализации таких стратегий может служить компания Google, которая использует многофакторную аутентификацию и шифрование данных для защиты информации своих пользователей.

Другой пример – Microsoft, которая активно разрабатывает и внедряет облачные решения с встроенными механизмами безопасности, такими как Azure Security Center. Эти подходы позволяют компаниям снижать риски кибератак и обеспечивать защиту данных при их обработке и хранении в облачных сервисах.

Киберугрозы являются одной из основных проблем для современных организаций. Вредоносные программы, фишинг, кибершпионаж и атаки типа «отказ в обслуживании» (DDoS) могут нанести серьезный ущерб не только инфраструктуре, но и репутации компании [4].

Последствия DDoS атак:

- Утечка конфиденциальных данных.

- Финансовые потери из-за кибератак.

- Невозможность выполнения бизнес-задач из-за перебоев в работе информационных систем.

В контексте ИКТ-стратегий эти риски оказывают прямое влияние на процесс принятия решений. Например, руководство компании может быть вынуждено пересмотреть свою стратегию цифровой трансформации или внести изменения в политику управления информацией для снижения киберугроз.

Для минимизации рисков и обеспечения устойчивости организации на практике используются различные инструменты и методологии. Среди них:

- Шифрование данных: один из ключевых методов защиты информации от несанкционированного доступа.

- Многофакторная аутентификация: дополнительный уровень безопасности для идентификации пользователей.

- Управление уязвимостями: регулярный аудит и устранение уязвимостей в системах [5].

Важным аспектом кибербезопасности является также образование и подготовка сотрудников, поскольку человеческий фактор остается одним из слабых звеньев в защите информации.

В ходе исследования было показано, что кибербезопасность играет критическую роль в успешной реализации ИКТ-стратегий. Современные компании должны интегрировать защиту информации в процессы принятия решений для обеспечения устойчивого роста и минимизации рисков, связанных с киберугрозами.

ИКТ-стратегии, включающие элементы кибербезопасности, становятся неотъемлемой частью эффективного управления в цифровую эпоху. Будущее кибербезопасности лежит в постоянном развитии технологий, а также в обучении и повышении осведомленности сотрудников о киберугрозах. Для дальнейших исследований важно рассматривать новые технологические решения и их влияние на принятие решений в бизнесе.

Библиографические ссылки

1. *Коваленко Э. В., Урусов З. Х.* Проблемные вопросы обеспечения кибербезопасности // Право и управление. 2023. С. 256–258.

2. *Назарова А. Д., Шведов В. В.* Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации // Столыпинский вестник. 2023. С. 12–20.

3. О кибербезопасности [Электронный ресурс]. URL: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g (дата обращения: 24.09.2024).

4. *Рыбаков Д. А.* Развитие и применение кибербезопасности в сфере информационных технологий // Вестник науки. 2023. С. 267–271.

5. Стратегические риски и проблемы кибербезопасности [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/strategicheskie-riski-i-problemy-kiberbezopasnosti (дата обращения: 24.09.2024).

6. Цифровая трансформация – шаг в будущее : материалы IV Междунар. науч.-практ. конф. молодых ученых, Минск, 13 окт. 2023 г. / Белорус. гос. ун-т ; редкол.: И. А. Карачун (гл. ред.), А. А. Королёва, Б. Н. Паньшин. Минск : БГУ, 2023. С. 331–333.