Заключение

Цифровая экономика имеет потенциал значительно изменить экономический ландшафт развивающихся стран. Однако для достижения этого потенциала необходимо преодолеть существующие барьеры и создать условия для устойчивого развития. Важно, чтобы правительства, частный сектор и международные организации работали вместе для создания инклюзивной и динамичной цифровой экономики

Список использованных источников

1. World Bank. (2020). Digital Economy for Africa Initiative.
2. UNCTAD. (2019). Digital Economy Report 2019.
3. Brynjolfsson, E., McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.
4. OECD. (2016). Digital Economy Outlook 2017.
5. Tapscott, D., Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.
4. Ходжанепесов, К.А., & Шаханов, Г.Б., (2024). Инновационные методы и информационные технологии в развитии образования в Туркменистане. Журнал “Universum: технические науки”, 64-66.

УДК 004.056

Р.Р. Джурабаев
Казанский инновационный университет имени В.Г. Тимирясова
Казань, Россия

ВОПРОС О КИБЕРБЕЗОПАСНОСТИ И КАЧЕСТВЕ КАДРОВ ЕЁ ОБЕСПЕЧЕНИЯ

Аннотация. *В статье рассматриваются актуальные проблемы кибербезопасности и требования к качеству кадров, необходимых для обеспечения защиты информационных систем. Представлены подходы к подготовке специалистов в этой области.*

Dzhurabaev Ramil Ravilevich
Kazan Innovative University named after V. G. Timiryasov
Kazan, Russia

ON THE ISSUE OF CYBERSECURITY AND THE QUALITY OF PERSONNEL TO ENSURE IT

Abstract. *The article discusses current issues of cybersecurity and the requirements for the quality of personnel necessary to ensure the protection of information systems. Approaches to training specialists in this field are presented.*

Введение

Современное развитие информационных технологий и глобализация информационного пространства привели к значительному увеличению рисков, связанных с киберугрозами. Защита информации становится одной из ключевых задач для государственных и частных организаций. Качество кадров, обеспечивающих кибербезопасность, играет решающую роль в эффективности защиты от кибератак.

Цель и задачи работы

Цель данной работы - определить требования к качеству подготовки специалистов по кибербезопасности и предложить пути решения проблем, связанных с кадровым дефицитом в данной области. Задачи работы включают:

1. Анализ текущего состояния кибербезопасности и существующих угроз.
2. Определение ключевых компетенций специалистов по кибербезопасности.
3. Обзор существующих образовательных программ и курсов повышения квалификации.
4. Разработка рекомендаций по улучшению системы подготовки кадров.

Пути решения проблем

Анализ текущего состояния;

Современные киберугрозы разнообразны и сложны. Они включают в себя вирусные атаки, фишинг, DDoS-атаки, взломы и утечки данных. Анализ показывает, что большинство атак происходит из-за недостаточной подготовки персонала и отсутствия современных систем защиты.

Ключевые компетенции специалистов;

Для эффективной защиты информационных систем специалисты по кибербезопасности должны обладать следующими компетенциями:

- Глубокие знания в области информационных технологий и сетевой безопасности.
- Понимание методов и инструментов кибератак.
- Навыки разработки и внедрения защитных мер.
- Способность к быстрому реагированию на инциденты.

- Постоянное обучение и повышение квалификации.

Образовательные программы;

Важным аспектом подготовки специалистов является наличие качественных образовательных программ. В настоящее время существуют различные формы обучения, включая университетские курсы, специализированные тренинги и онлайн-курсы. Однако, многие из них не соответствуют современным требованиям рынка.

Новые идеи и результаты

Для улучшения качества подготовки кадров предлагается:

1. Создание междисциплинарных программ обучения, включающих технические, правовые и управленческие аспекты кибербезопасности.
2. Введение обязательных практических занятий и симуляций кибератак.
3. Сотрудничество с промышленностью для обновления программ обучения в соответствии с текущими угрозами.
4. Разработка и внедрение сертификационных программ, подтверждающих квалификацию специалистов.

Опыт внедрения

Некоторые образовательные учреждения уже начали внедрять новые подходы к обучению. Например, Казанский Инновационный Университет разработал программу, включающую практические занятия и сотрудничество с ведущими ИТ-компаниями. Результаты показывают, что такие программы значительно повышают уровень подготовки специалистов.

Выводы

Кибербезопасность требует высококвалифицированных кадров, обладающих широким спектром знаний и навыков. Современная система подготовки специалистов должна быть ориентирована на практическое обучение и постоянное обновление знаний. Только таким образом можно эффективно противостоять современным киберугрозам.

Список использованных источников

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
2. Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.

3. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
4. Stallings, W. (2018). Cryptography and Network Security: Principles and Practice. Pearson.
5. Whitman, M., & Mattord, H. (2017). Principles of Information Security. Cengage Learning.

УДК 004.657

С.К. Жумагулова, А.А. Шайкенова, А.Ж. Койшыбай
Карагандинский университет имени академика Е.А. Букетова
Караганды, Казахстан
Казахский национальный исследовательский университет имени К.И. Сатпаева
Алматы, Казахстан

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ОБЛАСТИ ГЕОФИЗИКИ

Аннотация. *В статье рассматриваются основные направления применения искусственных нейронных сетей в геофизике, подчеркивая их значимость в анализе данных и прогнозировании природных явлений. В условиях роста технологий глубокого обучения открываются новые возможности для более точной интерпретации геофизической информации и улучшения процессов поиска полезных ископаемых. Особое внимание уделено потенциалу нейронных сетей в сейсмическом мониторинге и предсказании природных катастроф, что способствует повышению безопасности и минимизации экологических рисков.*

S.K. Zhumagulova, A.A. Shaikenova, A.Zh. Koishybay
Karaganda University named after Academician E.A. Buketov
Karaganda, Kazakhstan
Kazakh National Technical University named after K.I.Satpaev
Almaty, Kazakhstan

THE USE OF ARTIFICIAL NEURAL NETWORKS IN THE FIELD OF GEOPHYSICS

Abstract. *This article examines the main applications of artificial neural networks in geophysics, highlighting their importance in data analysis and natural phenomena forecasting. With the advancement of deep learning technologies, new possibilities are emerging for more accurate interpretation of geophysical data and optimization of resource exploration processes. Special attention is given to the potential of neural networks in seismic monitoring and predicting natural disasters, contributing to enhanced safety and reduction of environmental risks.*