

позволяющих своевременно обнаружить возможные потери, либо искажение информации, что, в свою очередь, может привести к снижению финансовых потерь.

Диапазон доступной информации дает возможность для разработки абсолютно новых методов и алгоритмов для анализа и работы с технологиями Big Data.

Список использованных источников

1. Konstantin B. Optimizations in computing the Duquenne–Guigues basis of implications / B. Konstantin // Annals of Mathematics and Artificial Intelligence. 2014. Vol. 70. No. 1-2. P. 5-24. doi

2. Obiedkov S. Modeling ceteris paribus preferences in formal concept analysis, in: Formal Concept Analysis / S.Obiedkov //Ed. by P. Cellier, F. Distel, B. Ganter. Vol. 7880. Berlin, Heidelberg: Springer, 2013. P. 188-202.

3. Жилияк Н.А. Обучающе-тестирующий модуль для студентов IT специальностей / Н.А. Жилияк, А.С. Кобайло // Дистанционное обучение: материалы IX Междунар. науч.-метод. конф. Минск, 3-4 декабря 2015 г. – Минск: БГУИР, 2015. – С. 99–101.

УДК 004.8

С.К. Жумагулова, Г.Б. Абилдаева, Ж.Е. Есим

Карагандинский университет имени академика Е.А. Букетова
Карагандинский технический университет имени Абылкаса Сагинова
Карагандинский высший колледж «Volashag»
Караганда, Казахстан

IT-ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ ВЗГЛЯДЫ

Аннотация. Данная статья охватывает современные тенденции в области IT и кибербезопасности. В контексте быстрого развития искусственного интеллекта и машинного обучения рассматриваются новые горизонты, открываемые перед IT-технологиями. Особое внимание уделяется вопросам кибербезопасности, представляя их как главную заботу современного мира.

S.K. Zhumagulova, G.B. Abildaeva, Zh.E. Yesim
Karaganda University named after academician E.A. Buketov
Karaganda Technical University named after Abylkas Saginov

IT TECHNOLOGIES AND SECURITY: MODERN VIEWS

***Abstract.** This article covers current trends in the field of IT and cybersecurity. In the context of the rapid development of artificial intelligence and machine learning, new horizons opening up to IT technologies are considered. Particular attention is paid to cybersecurity issues, presenting them as the main concern of the modern world.*

В наш информационный век, когда технологии становятся неотъемлемой частью повседневной жизни, вопросы безопасности IT-технологий приобретают особое значение. Целью исследования явились анализ ключевых аспектов современных IT-технологий и кибербезопасности и оценка их влияния на современное общество.

С развитием IT-индустрии открываются новые горизонты, меняются привычные структуры и появляются инновационные решения. Тенденция, наблюдаемая в последние годы, - это рост искусственного интеллекта и машинного обучения. Алгоритмы искусственного интеллекта не только значительно повышают производительность системы, но и создают новые возможности в различных областях, от медицины до финансов.

По мере увеличения объема цифровых данных растет и их ценность, что делает их привлекательными целями для киберпреступников. Основной задачей является обеспечение кибербезопасности. Расширение атак и совершенствование методов требуют постоянного совершенствования мер защиты, для этого сегодня, благодаря технологии блокчейн, имеются мощные инструменты, которые могут использоваться организациями для защиты своей цифровой инфраструктуры.

Сегодня бизнес-сектор становится все более уязвимым для киберугроз. Компании инвестируют в технологии для обнаружения и предотвращения атак, обучения персонала по кибербезопасности и разработки четких политик безопасности. Все данные меры необходимы как для защиты конфиденциальной информации, так и для обеспечения доверия клиентов.

Поскольку сегодня активно наблюдается рост количества устройств, подключенных к сети Интернет, все более серьезными становятся проблемы кибербезопасности. При этом тот факт, что устройства Интернета вещей могут быть использованы для кибератак, свидетельствует о том, что разработчикам необходимо с самого начала принимать надежные меры безопасности в целях минимизации рисков.

Применяемые в наши дни IT-технологии имеют немало преимуществ, однако одновременно с этим они угрожают кибербезопасности. Организации, разработчики и конечные пользователи должны быть в курсе последних тенденций и активно принимать участие в создании безопасного цифрового будущего. Лишь путем совместных усилий можно обеспечить стабильность и безопасность в мире, в котором технологии являются обязательной частью жизни современного общества.

Список использованных источников

1 Гладких А. В. Методы защиты от DDoS –атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность: материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 3-5.

2 Ефремов Н. А. Процессы информатизации экономики и информационная безопасность / Н. А. Ефремов, Т. В. Мужжавлева // Экономика и предпринимательство. - 2023. - № 3. - С. 287-294.

3 Полтавцева М. А. Комплексное организационное обеспечение управления информационной безопасностью субъекта КИИ = Comprehensive Organizational Support for Information Security Management of the CII Subject / М. А. Полтавцева, Е. А. Ворошин // Защита информации. Инсайд. - 2023. - № 2. - С. 7-13.

УДК 534.44

Е.Г. Зайцева, А.И. Занько, Р.А. Борисенок, М.А. Валай

Белорусский национальный технический университет
Минск, Беларусь

ИСПОЛЬЗОВАНИЕ ЗВУКОВОГО АНАЛИЗА ДЛЯ ИССЛЕДОВАНИЯ ДИНАМИКИ ДЫХАТЕЛЬНОЙ ФУНКЦИИ ЧЕЛОВЕКА И МОНИТОРИНГА ТЕХНИЧЕСКОГО СОСТОЯНИЯ ТЕХНИКИ

Аннотация. Обоснована возможность использования звукового анализа для исследования динамики дыхательной функции человека и мониторинга технического состояния техники. Разработаны методики проведения соответствующих измерений.