успеваемость студентов и подбирают учебные материалы в зависимости от их уровня подготовки и стиля обучения [3]. Такие подходы позволяют повысить мотивацию учащихся и эффективность образовательного процесса. Более того, чат-боты на основе обработки естественного языка предоставляют студентам круглосуточную поддержку и помогают решать учебные вопросы в интерактивной форме.

Интеграция искусственного интеллекта в прикладные приложения открывает новые горизонты для развития человеческого общества. В медицине ИИ спасает жизни, в финансах – обеспечивает безопасность и устойчивость, а в образовании – делает процесс обучения более гибким и доступным. Однако для успешного внедрения необходимо уделять внимание этическим вопросам, конфиденциальности данных и прозрачности алгоритмов. В будущем роль ИИ будет только возрастать, и от того, насколько ответственно человечество подойдет к его использованию, зависит эффективность и безопасность цифрового прогресса [2].

Литература

1. Кудрявцев, А. И. Искусственный интеллект и машинное обучение: современные тенденции и приложения / А. И. Кудрявцев. – М. : Наука, 2021. – 256 с.
2. Новиков, Д. А. Технологии искусственного интеллекта в экономике и управлении / Е. В. Смирнова. – СПб. : Питер, 2022. – 304 с.
3. Смирнова, Е. В. Цифровизация образования: роль искусственного интеллекта / Е. В. Смирнова // Образовательные технологии и общество. – 2023. – № 2. – С. 60–70.

МЕТОДЫ ЗАЩИТЫ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

А. М. Хамраев

Государственный энергетический институт Туркменистана, г. Мары

Рассмотрены ключевые методы защиты данных, применяемые в телекоммуникационных системах. Особое внимание уделено криптографическим технологиям, аутентификации, контролю доступа и новым направлениям – гомоморфному шифрованию и дифференциальной приватности. Цель исследования – определить наиболее эффективные подходы к обеспечению безопасности данных в условиях возрастающих угроз и усложняющихся сетевых архитектур. Методика основана на анализе современных публикаций и практического опыта специалистов отрасли. Результаты показывают, что комплексное сочетание классических и инновационных методов защиты позволяет повысить устойчивость сетей к несанкционированному доступу и утечкам информации.

Ключевые слова: телекоммуникации, защита данных, шифрование, аутентификация, приватность.

METHODS OF DATA PROTECTION IN TELECOMMUNICATION NETWORKS

A. M. Hamrayev

The State Energy Institute of Turkmenistan, Mary

This paper discusses key data protection methods used in telecommunication systems, focusing on cryptography, authentication, access control, and emerging approaches such as homomorphic encryption and differential privacy. The study aims to identify the most effective strategies to ensure data security amid growing cyber threats. The methodology is based on a review of current literature and industry practices. The results demonstrate that combining traditional and innovative protection techniques significantly enhances network resilience against unauthorized access and data leaks.

Keywords: telecommunications, data protection, encryption, authentication, privacy.

Современный этап развития информационного общества характеризуется стремительным ростом телекоммуникационных технологий и объемов передаваемых данных. Телефонная связь, интернет, облачные сервисы и мобильные приложения объединены в сложные распределенные системы, функционирующие в режиме реального времени. Однако вместе с технологическим прогрессом возросли и угрозы безопасности: утечки информации, перехват трафика, вредоносные вмешательства и нарушение конфиденциальности стали повседневной реальностью операторов связи [1, с. 17].

Проблема защиты данных в телекоммуникационных сетях выходит за рамки чисто технической задачи. Это комплексный вопрос, включающий криптографические, организационные и правовые аспекты. Цель данного исследования – рассмотреть существующие и перспективные методы защиты данных, выявить их преимущества и ограничения, а также предложить направления повышения уровня информационной безопасности телекоммуникационных систем.

Ключевым элементом выступает криптография, обеспечивающая защиту данных на уровне каналов связи и протоколов. Использование симметричных алгоритмов (AES, ChaCha20) в сочетании с асимметричными (RSA, ECC) дает высокий уровень безопасности. Тем не менее, как подчеркивает Габидулин [1, с. 22], эффективность криптографических средств зависит не только от алгоритма, но и от правильного управления ключами, длины ключей и защиты программной реализации. Ошибки в этих аспектах часто становятся причиной компрометации систем.

Не менее важным направлением является аутентификация и управление доступом. Без четкой системы разграничения прав даже самая надежная криптография не сможет предотвратить внутренние угрозы. В современных телекоммуникационных компаниях применяются механизмы двухфакторной аутентификации, цифровые сертификаты и системы управления ролями (RBAC). Они позволяют ограничить действия пользователей в зависимости от их статуса и ответственности.

На смену традиционным методам защиты приходят инновационные технологии, такие как гомоморфное шифрование. Этот подход позволяет обрабатывать данные в зашифрованном виде, что особенно актуально для операторов, проводящих аналитические расчеты и прогнозирование нагрузки сети. Исследование Ванга и соавторов [2, с. 45] показывает, что использование гомоморфного шифрования в сочетании с атрибутным управлением доступом повышает безопасность без существенного снижения производительности.

Кроме того, все большее значение приобретает дифференциальная приватность – технология, позволяющая анализировать большие массивы данных без раскрытия информации об отдельных пользователях. По мнению Манды [3, с. 13], именно этот метод станет ключевым элементом защиты в эпоху 5G и 6G, где телекоммуникационные компании обрабатывают терабайты персональных сведений ежедневно.

Результаты исследования показывают, что защита данных в телекоммуникационных сетях невозможна без комплексного подхода. Отдельные технологии, такие как криптография, аутентификация или приватные вычисления, эффективны лишь в сочетании друг с другом. Для обеспечения устойчивости к современным киберугрозам требуется интеграция технических и организационных мер, регулярное обновление алгоритмов защиты, а также учет международных стандартов и нормативов.

В ближайшие годы ключевыми тенденциями станут развитие постквантовой криптографии, использование искусственного интеллекта для мониторинга сетевой безопасности и дальнейшее внедрение методов приватных вычислений. Только системное применение этих технологий позволит создать доверенную цифровую среду, где данные пользователей и компаний будут надежно защищены на всех уровнях телекоммуникационной инфраструктуры.

Литература

1. Габидулин, Э. М. Защита информации в телекоммуникационных сетях / Э. М. Габидулин // CyberLeninka. – 2013. – С. 17–24.
2. Privacy protection of communication networks using fully homomorphic encryption and attribute encryption / W. Wang [et al.] // Scientific Reports. – 2024. – P. 45–52.
3. Manda, J. K. Privacy-Preserving Technologies in Telecom Data Analytics / J. K. Manda // Telecom Review. – 2025. – P. 11–19.

ОПТИМИЗАЦИЯ АКТИВОВ ПРЕДПРИЯТИЯ КАК КЛЮЧЕВОЙ ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПЕРСОНАЛА

Л. В. Мартинович, В. А. Самец, Т. А. Петровская

Белорусский национальный технический университет, г. Минск

Повышение эффективности персонала как ключевого актива любого предприятия имеет огромное значение для оптимального функционирования организаций. В статье описаны способы оптимизации структуры персонала, используя современное программное обеспечение.

Ключевые слова: активы предприятия, персонал, оптимизация, программное обеспечение.

OPTIMIZATION OF THE COMPANY'S ASSETS AS A KEY FACTOR IN INCREASING STAFF EFFICIENCY

L. V. Martsinovich, V. A. Samets, T. A. Petrovskaya

Belarusian National Technical University, Minsk

Increasing the efficiency of personnel as a key asset of any enterprise is of great importance for the optimal functioning of organizations. The article describes ways to optimize the personnel structure using modern software.

Keywords: company assets, personnel, optimization, software.

К активам предприятия относится все, чем владеет компания, от наличных денег до оборудования и интеллектуальной собственности. Активы компании представляют собой ресурсы, которые могут быть использованы для создания прибыли.

Структура активов оказывает значительное влияние на инвесторов, политиков и на сам объект хозяйствования, а именно на его устойчивость, конкурентоспособность и способность к росту. Для любой компании оптимизация структуры активов может повысить прибыльность, снизить финансовые риски и заложить основу устойчивого роста. Инвесторам понимание структуры активов компании может помочь оценить инвестиционные риски и потенциальную доходность. Следовательно, необходимо оптимизировать деятельность компании с точки зрения структуры активов.

В условиях динамично меняющейся экономической среды компании сталкиваются с необходимостью оптимизации своих активов также для повышения эффективности, достижения стратегических целей, минимизации рисков и максимизации доходов [1].

Оптимизация состава активов — процесс определения соотношения отдельных видов активов, обеспечивающего наилучшие условия производственно-коммерческой деятельности при высоком уровне ликвидности [2].

Для начала процесса оптимизации необходимо провести анализ структуры активов.

Оптимизация активов на предприятии может проводится следующим образом:

1. Аудит или проверки, которые помогают обнаружить устаревшие или неактуальные активы.