3. Увеличение мотивации и вовлеченности студентов.

ИИ может создавать интерактивные и увлекательные учебные материалы, предлагать игровые элементы и многое другое, что способствует повышению вовлеченности студентов.

4. Поддержка в обучении.

Виртуальные репетиторы могут отвечать на вопросы, предоставлять разъяснения по сложным темам и предлагать дополнительные ресурсы для изучения.

5. Сбор и анализ данных о процессе обучения.

Искусственный интеллект может эффективно собирать и анализировать данные о процессе обучения, что позволяет выявлять тенденции и проблемные области.

Как и любая другая система, ИИ не лишён определённых рисков и недостатков, для примера перечислим некоторые из них:

1. Конфиденциальность данных.

ИИ-системы собирают и обрабатывают большое количество информации об учащихся, включая их успеваемость, поведение и личные предпочтения. Это поднимает вопросы о конфиденциальности и безопасности данных.

2. Качество образования и возможные недостатки ИИ.

ИИ не всегда способен заменить человеческий подход. Преподаватели не только передают знания, но и вдохновляют, поддерживают и мотивируют студентов.

3. Социальные и экономические последствия.

Внедрение ИИ в образование может привести к социальным и экономическим изменениям, включая возможные сокращения рабочих мест для преподавателей.

Будущее образования с ИИ – это путь к новым возможностям, но оно будет зависеть от того, как мы сможем сбалансировать все аспекты. Важно развивать технологии с учетом потребностей всех участников образовательного процесса, чтобы обеспечить инклюзивную и качественную учебную среду.

Список использованной литературы

1. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. MA, USA, 2019, 242 p.

2. Luckin R., Homles W, Griffiths M, Forcier L. Intelligence Unleashed. An argument for AI in Education. London: Pearson, UCL Knowledge Lab, 2016, 60 p.

ИССЛЕДОВАНИЕ ВОПРОСОВ ЗАЩИТЫ ДАННЫХ ПРИ ИХ ХРАНЕНИИ

Дорох Артём (УО МГПУ им. И.П. Шамякина, г. Мозырь)
Научный руководитель – В.В. Давыдовская, канд. физ.-мат. наук, доцент

Защита данных при их хранении является одной из ключевых задач в условиях роста киберугроз [1]. В современном цифровом пространстве утечки информации могут привести к финансовым потерям, репутационным

рискам и юридическим последствиям. В Республике Беларусь защита данных регулируется Законом «О защите персональных данных» и другими нормативными актами, однако одних законодательных мер недостаточно [2]. Необходимо внедрение современных технических решений и строгая дисциплина в работе с данными.

Для эффективной защиты персональных и корпоративных данных применяются методы шифрования, резервного копирования и контроля доступа. Использование алгоритма шифрования AES-256 позволяет обеспечить надежную защиту конфиденциальной информации [3]. Регулярное резервное копирование критически важно, при этом предпочтительно хранить резервные копии в зашифрованном виде как на локальных серверах, так и в облачных хранилищах [4].

Контроль доступа играет важную роль в обеспечении безопасности. Следует ограничивать число сотрудников, имеющих доступ к важным данным, и использовать двухфакторную аутентификацию. Государственные организации отдают предпочтение сертифицированным системам безопасности и отечественному программному обеспечению, что снижает риск утечки информации через иностранные сервисы.

Крупные организации в Беларуси применяют системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) для мониторинга сетевого трафика. Эти решения позволяют выявлять и блокировать попытки несанкционированного доступа. Однако малый и средний бизнес пока не всегда уделяет должное внимание таким мерам защиты. Даже базовые шаги, такие как своевременное обновление программного обеспечения и использование антивирусных решений, значительно уменьшают вероятность атак [5].

Одним из ключевых аспектов безопасности является мониторинг доступа к данным и ведение журналов событий. Это помогает оперативно выявлять подозрительные действия и предотвращать утечки. Внедрение систем DLP («Data Loss Prevention») позволяет отслеживать передачу конфиденциальных данных и блокировать их несанкционированную отправку [6].

Эффективная защита данных невозможна без сегментации сети. Разделение корпоративной сети на изолированные сегменты ограничивает распространение вредоносных программ в случае взлома. Например, рабочие станции сотрудников, серверные хранилища и финансовые системы должны быть расположены в разных зонах с разными уровнями безопасности [7].

Комплексный подход к защите данных требует регулярных аудитов безопасности, обучения сотрудников и внедрения современных технологий. Только системный подход позволит минимизировать риски и обеспечить надежную защиту информации в условиях постоянно меняющихся угроз.

Список использованной литературы

1. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. – New York : John Wiley & Sons, 2017. – 784 p.

2. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. – Boston : Pearson Education, 2020. – 800 p.
3. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. – Indianapolis : Wiley, 2020. – 1232 p.
4. Kaspersky, E. Cybersecurity Threats and Countermeasures / E. Kaspersky // Journal of Information Security. – 2019. – V. 10. – P. 67–82.
5. Bishop, M. Computer Security: Art and Science / M. Bishop. – Boston : Addison-Wesley, 2018. – 1144 p.
6. Tanenbaum, A.S. Modern Operating Systems / A.S. Tanenbaum, H. Bos. – Boston : Pearson, 2023. – 1136 p.
7. Schneier, B. Secrets and Lies: Digital Security in a Networked World / B. Schneier. – New York : Wiley, 2015. – 432 p.

ПУБЛИКАЦИЯ ПРИЛОЖЕНИЯ В СЕРВИСАХ GOOGLE PLAY

Зайковский Владислав (УО МГПУ им. И.П. Шамякина, г. Мозырь)
Научный руководитель – А.В. Макаревич, канд. физ.-мат. наук, доцент

Публикация приложений в магазине Google Play в настоящее время является актуальной, поскольку это главный магазин приложений для платформы Android. Его аудитория насчитывает более 2,5 миллиарда пользователей и предоставляет разработчикам доступ к мировому рынку, монетизацию (платные загрузки, подписки, реклама), доверие пользователей (безопасность, автоматические обновления), инструменты продвижения (ASO, реклама, аналитика через Play Console), карьерные и бизнес-возможности. Успешные приложения могут стать стартапом или стабильным доходом и т. д. [1–3].

Умение публиковать и продвигать приложения – ключевой навык для разработчиков, влияющий на коммерческий успех проекта. Ниже на основании проведенного в рамках данной работы анализа особенностей и возможностей реализации выполненных разработок перечислены основные аспекты публикации приложение в Google Play.

Для начала необходимо подготовить APK/AAB-файл, убедившись в его соответствии политикам Google Play, создать иконку, скриншоты и описание для ASO-оптимизации.

Ключ к приложению создается с помощью инструмента keytool, входящего в состав JDK. Этот ключ необходимо хранить в безопасном месте, так как его потеря может привести к невозможности обновления приложения. Далее в Android Studio можно настроить подписание APK через меню Build. В открывшемся контекстном меню выбрать Generate Signed Bundle/APK. После выбора ключа и ввода пароля Studio создаст подписанный APK-файл. Подписанный APK готов к загрузке в Google Play. При этом необходимо помнить, что для обновлений приложения необходимо использовать тот же ключ подписи.