УДК 007.52

ЭТИКА И КОНФИДЕНЦИАЛЬНОСТЬ В БИЗНЕС-АНАЛИТИКЕ

А.И. Миркина, 3 курс
Научный руководитель – **С.А. Демьянов**, магистр геогр. наук
Полесский государственный университет

Успешное управление организацией невозможно без принятия решений на основе фактов, и бизнес-аналитика, обеспечивающая сбор и обработку данных, является ключевым элементом для эффективного развития любой компании. Анализ данных в бизнесе опирается на различные инструменты, каждый из которых предназначен для решения конкретных задач [1].

Среди этих инструментов выделяются OpenAI Analytics для анализа веб-трафика, Microsoft Excel для начальной обработки данных, SQL для управления структурированными данными, SAS для расширенной аналитики, R для статистического анализа, Tableau и Power BI для визуализации данных, Python с библиотеками Pandas, NumPy и SciPy для комплексного анализа, а также Hadoop и Spark для обработки больших данных [2].

Выбор инструмента определяется конкретными задачами бизнеса, характером данных и целями исследования. Важно учитывать, что именно нужно узнать, с какими данными предстоит работать и какова конечная цель анализа, поскольку для прогнозирования продаж, оптимизации маркетинговой кампании, выявления рыночных тенденций или создания интерактивной панели мониторинга требуются разные аналитические подходы и инструменты.

Каждый инструмент бизнес-аналитики обладает уникальными возможностями и ограничениями: Excel прост, но не подходит для больших данных; Python гибок, но требует программирования; Hadoop и Spark сложны, но необходимы для обработки огромных объёмов информации. Правильный выбор инструмента гарантирует эффективность анализа [3, с. 193].

С развитием технологий роль бизнес-аналитики в принятии управленческих решений возрастает, но одновременно возникают этические вопросы, связанные с конфиденциальностью данных и их использованием. Этика обеспечивает достоверность, объективность и ответственное использование данных в бизнес-процессах.

Основные аспекты этической ответственности включают [4, с. 56]:

- Целостность данных: соблюдение законов о конфиденциальности при сборе, безопасное хранение и обработка данных.
- Объективность и беспристрастность: проведение анализа без искажений и учета личных предпочтений.
- Прозрачность: ответственность за точность выводов и их понятное объяснение с указанием ограничений.
- Социальная ответственность: учет потенциального влияния на общество и минимизация негативных последствий, избегая дискриминации.
- Экологическая ответственность: осознание и минимизация негативного воздействия на окружающую среду, которое может возникнуть в результате решений, основанных на анализе данных.

Законодательная база, регулирующая обработку персональных данных, варьируется в зависимости от страны. Однако существуют общие принципы и ключевые международные законодательные акты, которые необходимо учитывать при проведении бизнес-аналитики:

- Общий регламент по защите данных (GDPR) Европейского Союза. Один из самых строгих и всеобъемлющих законов о защите данных в мире. GDPR устанавливает единые правила для всех компаний, обрабатывающих персональные данные граждан ЕС, независимо от их местоположения.
- Белорусский закон от 07.05.2021 г. № 99-З «О защите персональных данных». Данный Закон регулирует правовые отношения, связанные с защитой персональных данных при их обработке, осуществляемой с использованием или без использования средств автоматизации, если при этом обеспечиваются поиск персональных данных и (или) доступ к ним по определенным критериям (картотеки, списки, базы данных, журналы и другое).
- Федеральный закон «О персональных данных» № 152-ФЗ Российской Федерации. Закон регулирует отношения, связанные с обработкой персональных данных на территории России, а также устанавливает требования к сбору, хранению, использованию и уничтожению персональных данных.
- Законы штатов США. В США защита персональных данных регулируется на уровне штатов, что приводит к разнообразию законодательства. Некоторые штаты имеют свои собственные законы о конфиденциальности, которые дополняют федеральные законы.

Таким образом, каждая страна имеет собственные законы о защите персональных данных, которые необходимо учитывать при проведении бизнес-аналитики на международном уровне.

Компании обязаны принимать юридические, технические и организационные меры для защиты персональных данных от несанкционированного доступа, раскрытия, изменения или уничтожения.Компании обязаны принимать юридические, технические и организационные меры для защиты персональных данных. Обеспечение конфиденциальности стало одной из наиболее актуальных задач, и компании активно разрабатывают технические методы защиты данных, опираясь на триаду «конфиденциальность-целостность-доступность».

Принцип конфиденциальности ограничивает доступ к информации с помощью шифрования, контроля доступа и аутентификации. Целостность данных гарантирует неизменность информации с помощью механизмов проверки данных, таких как контрольные суммы.

Принцип доступности гарантирует, что информация будет доступна авторизованным пользователям, используя механизмы резервного копирования и восстановления данных для предотвращения потерь. Катастрофы, требующие таких механизмов, включают как естественные (пожары, наводнения), так и искусственные (отказы оборудования, кибератаки, ошибки пользователей) события.

Современная защита персональных данных строится на принципах недоверия, многоуровневой проверки и интеллектуального анализа. Подход нулевого доверия подразумевает отсутствие доверия ни к одному устройству или пользователю. Многофакторная аутентификация (пароль, отпечаток пальца, код на телефоне) повышает безопасность учётных записей. Искусственный интеллект и машинное обучение применяются для анализа данных, выявления подозрительной активности и предотвращения кибератак.

Для надежной защиты данных электронной почты от фишинга и несанкционированного доступа организации используют DMARC для аутентификации и отслеживания почты, SPF для авторизации почтовых серверов и DKIM для добавления цифровых подписей. Шифрование данных (сквозное шифрование) обеспечивает недоступность информации для посторонних, а модель управления доступом на основе ролей (RBAC) ограничивает доступ пользователей к необходимой информации.

Решения для предотвращения потери данных (DLP) защищают от утечек, сегментация сети снижает риск распространения вредоносных программ, непрерывный мониторинг безопасности обеспечивает своевременное обнаружение угроз, регулярное резервное копирование позволяет восстанавливать данные, а тестирование на проникновение и управление исправлениями безопасности устраняют уязвимости.

Сегментация сети изолирует отдельные ее части, таким образом снижая риск распространения вредоносных программ. Непрерывный мониторинг безопасности позволяет своевременно обнару-

живать и реагировать на угрозы. Регулярное резервное копирование данных обеспечивает возможность восстановления персональной информации в случае ее потери. Тестирование на проникновение и оценка уязвимостей помогают выявить и устранить слабые места в системе безопасности. Управление исправлениями безопасности позволяет своевременно устранять уязвимости в программном обеспечении [5].

Этика и конфиденциальность данных являются неотъемлемыми аспектами бизнес-аналитики. Соблюдение этических принципов и обеспечение безопасности данных не только способствует укреплению доверия клиентов, но и создает конкурентное преимущество для организации.

Список использованных источников

1. Чигаревская Е.П. Бизнес-анализ как современный инструмент управления бизнесом // Научные стремления. 2016. № 20. С. 204–205. eDn yrMJAr.

2. Шнайдер О.В., Лапаев П.Ю. теоретические аспекты бизнес-анализа // Балтийский гуманитар ный журнал. 2014. № 2 (7). С. 89–90. eDn sIrDMl.

3. Баврилeнко, В. И. Основы бизнес-анализа: учебно-методическое пособие / В. И. Баврилeнко. – Москва : КНОРУС, 2018. – 270 с.

4. Системы управления эффективностью бизнеса: Учебное пособие / Н.М. Абдикеев, С.Н. Брускин, Т.П. Данько и др.; Под научн. ред. Н.М. Абдикеева и О.В. Китовой. М., 2015. 282 с.

5. Брускин С.Н. Системы поддержки принятия решений в корпоративном планировании с использованием информационной бизнес-аналитики: практика и перспективы// Современные информационные технологии и ИТ-образование. Т. 1 (№ 11), МГУ им. М.В. Ломоносова - М., 2015 г. - с.593-598.