

# **Социальные и профессиональные вопросы информатики и ИТ**

## **Вариативное задание 6. Нарушения норм и правил в ИТ-разработках**

**Автор:**

**Воложанин В.О.**

**4 курс, ИВТ 1.2**

**Задание 6.1.** Нарушения в сфере создания новых продуктов и использования информационных ресурсов и технологий.

### **Основные нарушения в сфере информационных технологий**

- Нарушение безопасности данных: Утечка или несанкционированный доступ к данным пользователей.
- Неэтичное использование данных: Использование данных без согласия пользователей, нарушение конфиденциальности.
- Нарушение лицензионных соглашений: Использование нелегального ПО или несоответствие условий лицензий.
- Кибератаки и мошенничество: Вирусы, фишинг, социальная инженерия, кибершантаж.
- Недостаточная прозрачность алгоритмов: непонимание или непрозрачность действий алгоритмов ИИ, что может привести к дискриминации.

### **Меры борьбы с нарушениями**

- Ужесточение санкций за утечку данных или их неправильное использование.
- Принятие законов, регулирующих использование ИИ и машинного обучения.
- Обеспечение более четкой регуляции обработки персональных данных (например, как в GDPR).
- Регулярные курсы по безопасности данных, этике и защите прав пользователей.
- Повышение квалификации в области соблюдения норм безопасности и защиты от кибератак.
- Шифрование данных, многослойная защита, двухфакторная аутентификация.
- Внедрение систем контроля доступа и журналов аудита для мониторинга действий.
- Формирование корпоративной культуры, ориентированной на защиту данных и соблюдение норм конфиденциальности.
- Привлечение сотрудников к осознанию важности соблюдения правил безопасности.

### **Этические нормы и законы, способствующие разрешению нарушений**

Защита данных и конфиденциальности:

- Разработка и соблюдение законов, защищающих персональные данные (например, GDPR).
- Ответственность за утечку или несанкционированное использование данных.

Прозрачность алгоритмов и ИИ:

- Принятие законов, требующих от разработчиков ИИ объясняемости и справедливости алгоритмов.
- Прозрачность в процессе принятия решений алгоритмами, чтобы минимизировать дискриминацию.

Ответственность за манипуляции с данными:

- Введение строгих наказаний за манипуляции с данными, кражу интеллектуальной собственности и нарушение авторских прав.

### **Повышение ответственности ИТ-специалистов**

Индивидуальная ответственность:

- Введение личной ответственности для ИТ-специалистов за нарушение стандартов безопасности и этики.
- Включение обязательных сертификаций и квалификаций, подтверждающих способность следовать этическим и правовым нормам.

Механизмы воздействия:

- Введение внутренней дисциплинарной ответственности на уровне компании.
- Применение независимых аудитов для оценки поведения ИТ-специалистов.

Законодательная ответственность:

- Разработка законов, предусматривающих ответственность ИТ-специалистов за нарушение норм безопасности и этики.

- Включение ответственности за недобросовестные действия в контракты с работниками.

### **Предложения по нормализации работы с ИТ**

- Введение обязательных внешних и внутренних аудитов, которые помогут оперативно выявлять нарушения.
- Создание системы "красных флажков" для раннего обнаружения угроз безопасности.
- Разработка и внедрение стандартов безопасности, чтобы действия ИТ-специалистов были прозрачными и контролируруемыми.
- Применение санкций за нарушение законов в сфере ИТ на уровне государственных и корпоративных структур.
- Введение обязательной сертификации для всех ИТ-специалистов, которая подтверждает их знания в области этики и безопасности.
- Регулярные курсы повышения квалификации и сертификация в области защиты данных.