

Комплаенс и юридическая ответственность при инцидентах кибербезопасности

Profit Industry & Energy Day 2025

Август 2025

Информация, содержащаяся в настоящей презентации, носит общий характер и подготовлена без учета конкретных обстоятельств того или иного лица или организации

Предпринимать какие-либо действия на основании такой информации можно только после консультаций с соответствующими специалистами и тщательного анализа конкретной ситуации





Agenda

01

Проблематика

Глобальные утечки данных, важность и проблемы правового регулирования

02

Нормативно-правовое регулирование

Акты и положения, регулирующие вопросы кибербезопасности

03

Ответственность

Административная, уголовная, дисциплинарная

04

Судебная практика

05

Меры реагирования при утечке

06

Вопросы и ответы

Глобальные утечки данных

Июль 2025: в открытом доступе оказались данные 16,3 млн граждан Республики Казахстан (ФИО, ИИН, адреса, телефоны)

Масштаб инцидента – беспрецедентный для страны

Это часть глобального тренда:

- 2024 – архив MOAB, 26 млрд записей
- 2023 – утечка ≈10 млрд паролей
- 2021 – база на 8 млрд паролей

Новые утечки происходят практически ежемесячно

ПРОБЛЕМАТИКА

- ✗ Разрозненность и пробелы в правовом регулировании
- ✗ Многие организации не вводят положения, регулирующие вопрос кибербезопасности
- ✗ Последствия: огромные штрафы, репутационные риски, утрата данных

Нормативно-правовые акты

1. Закон Республики Казахстан «О персональных данных и их защите» («Закон о ПД»)
2. Закон Республики Казахстан «Об информатизации» («Закон об информатизации»)
3. Кодекс Республики Казахстан «Об административных правонарушениях» («КоАП РК»)
4. Уголовный кодекс Республики Казахстан («УК РК»)
5. Приказы Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан
6. Внутренние правила / политики компаний, регулирующие вопросы сбора и обработки персональных данных, кибербезопасности («Внутренние правила / политики»)

Закон РК «О персональных данных»

Базовый акт по регулированию сбора и обработки ПД

Закон о ПД закрепляет правовые основы работы с персональными данными и устанавливает обязанности для операторов

Определение персональных данных

ПД – сведения, относящиеся к определенному или определяемому лицу.

Перечень таких данных утверждает оператор в зависимости от целей деятельности

Виды персональных данных

К ПД могут относиться: ФИО, дата рождения, ИИН, паспортные данные, медицинская информация, банковские реквизиты, биометрия и др.

Согласие субъекта

Является обязательным условием для сбора и обработки

С 2022 г. включает: сведения об операторе, сроки согласия, вопрос передачи 3-м лицам, трансграничность. Допускается электронная форма (гос/негос-сервисы)

Закон РК «Об информатизации»

Объекты защиты

Закон об информатизации регулирует безопасность электронных ресурсов, ПО, интернет-ресурсов и ИК-инфраструктуры. Эти объекты должны быть защищены от несанкционированного или случайного доступа

Ключевые меры защиты

Предотвращение и выявление попыток доступа, минимизация последствий, восстановление ресурсов, предотвращение вмешательства и информирование регулятора о киберинцидентах

Виды мер

Правовые меры: законы, стандарты, ответственность

Организационные: режим доступа, разграничение полномочий

Технические: сертифицированные средства защиты, системы контроля и регистрации

Вывод

Закон об информатизации обязывает собственников информационных систем самостоятельно принимать меры для защиты ресурсов

Принимаемые меры не должны причинять вред людям, имуществу или государству

Ответственность за киберинциденты (утечку данных)

Административная

Ст. 79 КоАП РК: штрафы за незаконный сбор или обработку ПД – от 30 МРП (физлица) до 2000 МРП (крупные компании)

Ст. 641 КоАП РК: нарушения ИБ – 50 МРП (физлица) до 1000 МРП (крупные компании)

Неоповещение о киберинциденте – до 100 МРП, при повторе – до 200 МРП

Уголовная

Ст. 147 УК РК:

несоблюдение мер защиты – штраф до 3000 МРП или лишение свободы до 2 лет

незаконный сбор/обработка – до 5000 МРП или 3 года

с использованием служебного положения – до 5 лет

незаконное распространение сведений о частной жизни – от 3 до 7 лет

**Применяется только к физическим лицам*

Дисциплинарная

Согласно Трудовому кодексу РК, за нарушения внутренних положений, работодатель вправе применить дисциплинарное взыскание в виде: 1) замечания, 2) выговор, 3) строгого выговора или 4) увольнения

Увольнение возможно за повторное ненадлежащее исполнение обязанностей (пп. 16) п. 1 ст. 52 ТК РК)

Суды подтверждают законность увольнения при наличии дисциплинарного взыскания и нового нарушения

Судебная практика в Республике Казахстан в сфере кибербезопасности

Микрофинансовая организация

1

5 марта 2024 г. – утечка более 2 млн ПД граждан из открытого источника (GitHub). В МЦРИАП поступило более 5200 жалоб

2

Санкция

Компания оштрафована по ст. 79 КоАП РК: штраф 1000 МРП (фактически уплачено 500 МРП в сокращенном порядке)

Крупные компании Республики Казахстан

1

На GitHub опубликованы данные, предположительно утекшие в результате атаки. Содержали служебную информацию операторов связи и данные граждан

2

Санкция

Компании привлечены к ответственности по ст. 641 КоАП РК за нарушение законодательства об информатизации

Действия при утечке



1. Немедленно зафиксировать факт

Сохранить все данные:
дата, время, обстоятельства



2. Заблокировать данные

Принять меры во избежание
дальнейшего распространения



3. Уведомить уполномоченный орган

В случае утечки, необходимо в
течение одного рабочего дня
уведомить уполномоченный
орган



4. Провести внутреннее расследование

Порядок проведения расследований и
оформление их результатов не
регулируются законодательством, а
внутренними правилами / политикой



5. Обучение сотрудников

Провести обучение сотрудников по
безопасному использованию внутренних
информационных систем

Q
&A



Контакты



Асель Казбекова

Директор KPMG Law

Тел. +7 (727) 298 08 98

Моб. +7 (777) 776 80 88

E-mail: akazbekova@kpmglaw.kz





kpmg.kz

Информация, содержащаяся в настоящем документе, носит общий характер и подготовлена без учета конкретных обстоятельств того или иного лица или организации. Хотя мы неизменно стремимся представлять своевременную и точную информацию, мы не можем гарантировать того, что данная информация окажется столь же точной на момент получения или будет оставаться столь же точной в будущем. Предпринимать какие-либо действия на основании такой информации можно только после консультаций с соответствующими специалистами и тщательного анализа конкретной ситуации.

© 2025 г. ТОО «КПМГ Такс энд Эдвайзори», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, участник глобальной организации независимых фирм KPMG, входящих в KPMG International Limited, частную английскую компанию с ответственностью, ограниченной гарантиями своих участников. Все права защищены.

Наименование KPMG и логотип KPMG являются товарными знаками, используемыми по лицензии участниками глобальной организации независимых фирм KPMG.