Казахский национальный университет им. аль-Фараби

УДК 341:004.056 + 342.7:004.8 На правах рукописи

**БИСАЛИЕВ МАРЛЕН САКЕНОВИЧ**

# Международно-правовые аспекты защиты личной информации в глобальном и национальном информационном пространстве

8D04201 - Международное право

ДИССЕРТАЦИЯ
на соискание степени доктора философии (PhD)

Отечественный научный консультант:
доктор юридических наук, профессор
Шакиров Каримжан Нурумович

Зарубежный научный консультант:
доктор юридических наук, профессор школы управления, права и общества
Таллиннского Университета
Март Сюзи (Mart Susi)

Республика Казахстан
Алматы, 2025

**СОДЕРЖАНИЕ**

**НОРМАТИВНЫЕ ССЫЛКИ** ..... **3**
**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ** ..... **4**
**ВВЕДЕНИЕ** ..... **6**
**1 ТЕОРЕТИЧЕСКИЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ МЕЖДУНАРОДНО-ПРАВОВОЙ ЗАЩИТЫ ЛИЧНОЙ ИНФОРМАЦИИ** ..... **21**
1.1 Понятие личной (персональной) информации и границы охраны ..... 21
1.2 Источники и принципы международно-правовой защиты личной информации ..... 30
1.3 Методологические основы исследования защиты персональных данных . 43
**2 МЕЖДУНАРОДНО-ПРАВОВОЙ И НАЦИОНАЛЬНЫЙ РЕЖИМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ** ..... **58**
2.1 Международно-правовой статус субъектов отношений по защите персональных данных ..... 58
2.2 Международно-правовые инструменты и проблемные аспекты защиты персональных данных ..... 69
2.3 Стратегические вызовы для правового режима защиты персональных данных: искусственный интеллект и «нормативная турбулентность» ..... 85
2.4 Судебная практика в Республике Казахстан и пробелы правоприменения в сфере защиты персональных данных ..... 96
**3 ЭФФЕКТИВНОСТЬ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И НАПРАВЛЕНИЯ ЕГО СОВЕРШЕНСТВОВАНИЯ** ..... **109**
3.1 Понятие, условия и критерии эффективности правового регулирования защиты персональных данных ..... 109
3.2 Направления совершенствования правового регулирования защиты персональных данных ..... 121
3.3 «Правовая технология обеспечения защиты персональных данных» как механизм имплементации международных стандартов ..... 134
**ЗАКЛЮЧЕНИЕ** ..... **150**
**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** ..... **156**

## НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диссертации использованы ссылки на следующие стандарты:

1. ГОСТ 7.32-2001. Отчет о научно-исследовательской работе. Структура и правила оформления.

2. ГОСТ 7.1-2003. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

| | |
|---|---|
| АППК РК | Административный процедурно-процессуальный кодекс Республики Казахстан |
| АТЭС | Азиатско-Тихоокеанское экономическое сотрудничество (Asia-Pacific Economic Cooperation) |
| ВДПЧ | Всеобщая декларация прав человека |
| ВЭФ | Всемирный экономический форум |
| ГК РК | Гражданский Кодекс Республики Казахстан |
| ГТС | Акционерное общество «Государственная техническая служба» |
| ЕКПЧ | Европейская конвенция о защите прав человека и основных свобод |
| ЕС | Европейский союз |
| ЕСПЧ | Европейский суд по правам человека |
| ЗРК | Закон Республики Казахстан |
| ИИ | искусственный интеллект |
| ИКТ | информационно-коммуникационные технологии |
| КИБ | Комитет по информационной безопасности |
| КМП ООН | Комиссия международного права Организации Объединенных Наций |
| КНР | Китайская Народная Республика |
| КоАП РК | Кодекс Республики Казахстан об административных правонарушениях |
| МВД | Министерство внутренних дел |
| МПГПП | Международный пакт о гражданских и политических правах |
| МРП | месячный расчетный показатель |
| МФЦА | Международный финансовый центр «Астана» |
| МЦРИАП | Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан |
| НБ РК | Национальный Банк Республики Казахстан |
| НКО | некоммерческая организация |
| НК РК | Налоговый Кодекс Республики Казахстан |
| ООН | Организация Объединенных Наций |
| ОЭСР | Организация экономического сотрудничества и развития |
| ПД | персональные данные |
| ПОД/ФТ | противодействие отмыванию денег и финансированию терроризма |
| СЕ | Совет Европы |
| СНГ | Содружество Независимых Государств |
| ТРИПС | Соглашение по торговым аспектам прав интеллектуальной собственности |
| УК РК | Уголовный Кодекс Республики Казахстан |
| УПК РК | Уголовно-процессуальный кодекс Республики Казахстан |
| ЦАРКА | Центр анализа и расследования кибератак |
| ШОС | Шанхайская организация сотрудничества |

| | |
|---|---|
| ЭТП | электронная торговая площадка |
| ЭЦП | электронная цифровая подпись |
| Big Data | Большие данные |
| CCPA | California Consumer Privacy Act |
| CPPA | California Privacy Protection Agency |
| CPRA | California Privacy Rights Act |
| DPIA | Data Protection Impact Assessment (оценка воздействия на защиту персональных данных) |
| DPO | Data Protection Officer (уполномоченное лицо по защите персональных данных) |
| eGov.kz | веб-портал «электронного правительства» Республики Казахстан |
| GDPR | General Data Protection Regulation (Общий Регламент ЕС о защите персональных данных) |
| GLBA | Gramm-Leach-Bliley Act |
| HIPAA | Health Insurance Portability and Accountability Act |
| ISO | International Organization for Standardization |
| NIST | National Institute of Standards and Technology (Национальный институт стандартов и технологий США) |
| PII | Personally Identifiable Information |
| PIPIA | Personal Information Protection Impact Assessment (оценка влияния на защиту персональной информации) |
| PIPL | Personal Information Protection Law (Закон Китайской Народной Республики «О защите персональной информации» от 20 августа 2021 года) |

# ВВЕДЕНИЕ

**Общая характеристика работы.** Диссертационное исследование направлено на комплексный международно-правовой анализ теоретических и практических аспектов защиты личной (персональной) информации в глобальном и национальном информационном пространстве. Исследование охватывает эволюцию концепции личной информации и становление правовых механизмов ее защиты, анализ действующих международных договоров и национального законодательства (включая ЕС, США, КНР и др.), а также практики их применения. Особое внимание уделено современным вызовам цифровой эпохи, таким, как применение технологий искусственного интеллекта (ИИ), технологий обработки больших данных, трансграничная передача персональных данных и их влияние на правовые режимы защиты персональных данных. По результатам проведенного исследования сформулирован комплекс научно обоснованных предложений по совершенствованию законодательства Республики Казахстан о персональных данных и их защите с учетом передовых международных стандартов (Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. (Конвенция 108+), Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС) (Общий Регламент ЕС о защите персональных данных - GDPR). Он включает: системные поправки для устранения «нормативной турбулентности»; учреждение независимого уполномоченного органа по защите персональных данных; внедрение риск-ориентированного подхода и подотчетности (оценка воздействия на защиту персональных данных, реестры обработки персональных данных, защиты персональных данных на этапе проектирования и по умолчанию); расширение прав субъектов (переносимость, возражение против автоматизированных решений); уточнение ключевых дефиниций; обновление механизмов трансграничной передачи персональных данных (адекватность, стандартные оговорки, корпоративные правила) и усиление ответственности.

Дополнительно в диссертационном исследовании сформулирован комплекс практических рекомендаций по совершенствованию правового регулирования защиты персональных данных в Республике Казахстан. В частности, предлагается проведение фундаментальной институциональной реформы, направленной на создание независимого надзорного органа по защите персональных данных, наделенного достаточными полномочиями (включая аудит алгоритмических систем). Обосновывается необходимость системной имплементации в национальное законодательство передовых международных стандартов, включая риск-ориентированный подход (в частности, обязательную оценку воздействия на защиту персональных данных), принцип подотчетности (в том числе ведение реестров операций обработки персональных данных) и «защиту данных на этапе проектирования и по умолчанию». Кроме того,

рекомендации включают модернизацию понятийного аппарата (профилирование, псевдонимизация) и расширение прав субъектов (в частности, закрепление права на переносимость данных и права на возражение против решений, основанных исключительно на автоматизированной обработке). В сфере международного сотрудничества аргументируется необходимость приоритетного присоединения Республики Казахстан к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. Отдельный блок рекомендаций посвящен разработке специализированного регулирования искусственного интеллекта (ИИ) в рамках проекта Цифрового кодекса РК, основанного на классификации систем ИИ по уровням риска (с запретом «неприемлемых» систем и установлением императивных требований для «высокорисковых» систем).

**Актуальность настоящего исследования** обусловлена необходимостью совершенствования режимов (или механизмов) защиты персональных данных в условиях современных вызовов.

Во-первых, это вызовы, обусловленные развитием и применением технологий искусственного интеллекта (ИИ), технологий обработки больших данных, автоматизированного профилирования и технологий распределенного реестра (блокчейн). Эти инновационные инструменты способны осуществлять сбор и обработку значительных объемов персональных данных, относящихся к субъектам (физическим лицам). В результате формируются так называемые «цифровые следы», которые зачастую включают онлайн-идентификаторы и сведения о поведении субъектов в сети. Исследование «цифровых следов» является значимым фактором обеспечения безопасности обработки персональных данных и важным элементом практики цифровой криминалистики [1, с. 82]. Стремительное развитие систем ИИ ставит под сомнение способность существующих правовых норм поддерживать адекватный уровень защиты персональных данных в сфере информатизации [2, с. 96].

Во-вторых, актуальны международно-правовые вызовы, связанные с отсутствием гармонизации подходов различных государств к правовому регулированию в сфере защиты персональных данных. Это особенно важно, поскольку, как отмечает Т. А. Полякова, «транснациональность угроз и уровень ущерба при их реализации заставляют ставить проблему обеспечения информационной безопасности как глобальную, требующую усилий всего мирового сообщества» [3, с. 5]. Наблюдается расхождение моделей: от концепции ЕС, воплощенной в Общем регламенте ЕС о защите персональных данных (Регламент (ЕС) 2016/679 - GDPR) [4], до государственно-ориентированной системы КНР и секторального подхода США. Проблема конфликта юрисдикций была отмечена еще на заре становления интернет-права. В частности, в работе В. Б. Наумова отмечается, что отсутствие специализированных международных коллизионных норм вынуждает государства применять национальные концепции, что неизбежно приводит к столкновению правовых систем [5, с. 10-13]. Современная фрагментация регуляторных подходов контрастирует с ранними попытками формирования

глобального консенсуса. Знаковым документом этого периода стала Окинавская Хартия глобального информационного общества (2000 г.) [6], принятая лидерами G8. В ней отмечается необходимость создания «предсказуемой, транспарентной и недискриминационной» нормативной базы, которая обеспечивала бы эффективную защиту приватности при обработке персональных данных, одновременно сохраняя свободный поток информации. Хартия заложила политический фундамент для последующих дискуссий о балансе между инновациями и защитой прав личности в глобальном масштабе. Подобная фрагментация создает правовую неопределенность в сфере трансграничной передачи персональных данных и приводит к феномену «нормативной турбулентности» - ускоренной, но зачастую несистемной реакции национальных юрисдикций на технологические вызовы [7, с. 21]. Этот конфликт обусловлен фундаментальной природой глобального информационного пространства: как отмечено В. А. Копыловым, отсутствие географических границ в трансграничных сетях неизбежно ведет к «столкновению» и «ломке» национальных правовых режимов [8, с. 22]. Нормативная турбулентность, характеризующая современный этап развития права в сфере информатизации, проявляется в том, что законодатели стремительно принимают новые правовые нормы в ответ на технологические вызовы, не успевая сформировать системный подход к их регулированию. Это обусловлено тем, что объективное усиление зависимости общества от глобальной информационной инфраструктуры и свободы трансграничного информационного обмена порождает угрозу использования этой зависимости во вред интересам личности и общества [9, с. 3]. Современный этап развития информационного общества характеризуется такой нестабильностью нормативной среды, требующей проактивных подходов к правотворчеству.

В-третьих, данная проблематика обладает особой значимостью для Республики Казахстан. Перед Республикой Казахстан, находящейся на пересечении геополитических и экономических интересов и активно реализующей стратегию цифровой трансформации [10], стоит задача выработки сбалансированной национальной модели защиты персональных данных. На высшем государственном уровне этот вектор подтвержден Посланием Президента Республики Казахстан Касым-Жомарта Токаева от 8 сентября 2025 года «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» [11], где поставлена задача повсеместного внедрения ИИ в экономику и государственное управление. В числе институциональных мер объявлены создание Министерства искусственного интеллекта и цифрового развития РК и придание городу Алатау специального статуса как пилотной цифровой территории. Указом Президента РК от 18 сентября 2025 г. № 997 Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан преобразовано в Министерство искусственного интеллекта и цифрового развития Республики Казахстан, при этом функции по инновационной политике переданы в Министерство науки и высшего образования, а права и обязанности распределены между правопреемниками по передаваемым функциям [12].

Стратегический курс на технологическую интеграцию получил практическое подтверждение в ходе саммита «Центральная Азия - США» в ноябре 2025 г. Заключение пакета соглашений, направленных на масштабное внедрение передовых систем искусственного интеллекта, развитие спутниковой связи и создание Центра компетенций по цифровым платежам и кибербезопасности, свидетельствует об ускоренной интернационализации технологической инфраструктуры Казахстана [13]. Данный процесс неизбежно влечет рост трансграничной обработки персональных данных и актуализирует необходимость обеспечения регуляторной совместимости национального правового режима с юрисдикциями ключевых технологических партнеров, в частности США, для минимизации коллизионных рисков и гарантии прав субъектов персональных данных. Такая модель должна, с одной стороны, соответствовать передовым международным стандартам (например, принципам Конвенции 108+ [14]), а с другой - учитывать национальные интересы и особенности существующей в стране правовой системы. Недостатки в системе обеспечения информационной безопасности в Республике Казахстан уже привели к ряду масштабных нарушений безопасности персональных данных. В частности, в 2024-2025 гг. имели место масштабные нарушения безопасности персональных данных: от распространения базы, содержащей персональные данные (около 16 млн. записей [15]) до неправомерного разглашения персональных данных клиентов финансовых организаций и субъектов в сфере образования [16]. Эти случаи стали предметом широкого общественного обсуждения, подтвердив необходимость безотлагательных изменений в законодательстве о персональных данных и их защите. Укрепление правового режима в сфере защиты персональных данных, включая актуализацию положений Закона РК «О персональных данных и их защите», приобретает особую актуальность. В этих условиях комплексное международно-правовое исследование механизмов защиты личной информации (персональных данных) на глобальном и национальном уровнях, учитывающее технологические и регуляторные аспекты, является не только своевременным, но и практически востребованным.

В-четвертых, инциденты в сфере информационно-коммуникационных технологий (ИКТ), имеющие трансграничные последствия, влекут применение норм международного права об ответственности государств за международно-противоправные деяния. Ключевым вопросом в таких ситуациях является присвоение (вменение) [17, с. 36-37] противоправного деяния государству, в частности, как деяния его органов либо лиц [17, с. 135-150], действующих под его руководством или контролем [17, с. 159-166, 180-188]. В этой связи применение положений Проекта статей об ответственности государств за международно-противоправные деяния [18; 19, с. 38-53] представляется обоснованным методологическим ориентиром для анализа трансграничных инцидентов с персональными данными. При интерпретации этих положений применительно к киберпространству авторитетным источником выступает «Таллиннское руководство 2.0 о международном праве, применимом к кибероперациям» [20, с. 2, 79-167]. Несмотря на свой академический статус, этот

документ служит важным ориентиром для государств при квалификации трансграничных инцидентов и анализе вопросов суверенитета, юрисдикции и ответственности в киберпространстве (сфере ИКТ). Указанные статьи (ст. 4-11) устанавливают критерии присвоения поведения государству. Это позволяет определить, когда деяния, повлекшие трансграничные инциденты с персональными данными, могут повлечь международную ответственность государства вследствие нарушения им международного обязательства (например, ст. 17 Международного пакта о гражданских и политических правах) [21, с. 878, 879]. Это особенно актуально для правового регулирования в цифровую эпоху, где государства стремятся обеспечить баланс между свободным обращением информации и защитой персональных данных. Нормы Проекта статей об ответственности государств позволяют определить, когда деяния в сфере ИКТ следует квалифицировать как международно-противоправное деяние государства. Принципиальным правовым аспектом является присвоение деяния государству - установление того, что за кибер-инцидентом или нарушением безопасности персональных данных стоят органы данного государства либо лица (или группы лиц), действующие в действительности по указаниям либо под руководством или контролем этого государства. Такое присвоение деяния имеет не только доктринальное, но и практическое значение - оно является основанием для привлечения государства к международно-правовой ответственности и, при соблюдении установленных условий, для применения контрмер.

Для Республики Казахстан, интегрирующейся в глобальную сферу ИКТ, юридическая квалификация инцидентов с персональными данными в соответствии с нормами международного права имеет особую значимость. Это позволяет государству эффективно защищать права субъектов персональных данных в случаях, когда их персональные данные подвергаются неправомерной обработке (или нарушению безопасности) в результате деяний других государств или лиц, действующих под их руководством или контролем. Учет критериев, закрепленных в Проекте статей об ответственности государств за международно-противоправные деяния, при разработке и применении национального законодательства позволяет обеспечить соответствие внутренних механизмов международным стандартам. Это снижает риск возникновения международной ответственности Республики Казахстан за трансграничные нарушения в сфере персональных данных, если соответствующее поведение может быть присвоено государству. В этой связи обращение к положениям Проекта статей (в частности, ст. 4-11) обусловлено необходимостью соотнести задачи национального регулирования с условиями возникновения международной ответственности (такими как присвоение деяния, нарушение международного обязательства и обстоятельства, исключающие противоправность). Это повышает обоснованность и актуальность анализа трансграничной защиты персональных данных.

**Цель диссертационного исследования** заключается в проведении комплексного международно-правового анализа теоретических и практических аспектов защиты личной (персональной) информации (персональных данных) в

глобальном и национальном информационном пространстве и в выработке на этой основе научно обоснованных предложений по совершенствованию международно-правовых и национальных механизмов регулирования в данной сфере.

Для достижения указанной цели были поставлены следующие **задачи**:

- раскрыть понятие, сущность и границы правовой охраны личной (персональной) информации как объекта международно-правовой защиты;
- проанализировать эволюцию, источники и принципы международно-правовой защиты личной информации;
- обосновать методологические основы исследования защиты персональных данных, включая совокупность общенаучных и частнонаучных методов познания;
- определить и охарактеризовать правовой статус основных субъектов отношений по защите персональных данных в международном и национальном праве;
- исследовать международно-правовые инструменты и механизмы (технологии) защиты персональных данных, выявив их проблемные аспекты в международном и национальном информационном пространстве;
- изучить стратегические вызовы правовому обеспечению защиты персональных данных, включая влияние искусственного интеллекта и «нормативной турбулентности»;
- проанализировать судебную практику в Республике Казахстан и выявить пробелы правоприменения в сфере защиты персональных данных;
- сформулировать критерии и условия, определяющие эффективность правового регулирования защиты персональных данных;
- разработать направления совершенствования правового регулирования защиты персональных данных;
- сформулировать концепцию «правовой технологии обеспечения защиты персональных данных» как механизм имплементации международных стандартов;
- на основе проведенного анализа обосновать конкретные предложения по совершенствованию законодательства Республики Казахстан в области защиты персональных данных и выработать рекомендации по гармонизации национальных подходов с передовыми международными стандартами.

**Объектом диссертационного исследования** являются международные и внутригосударственные общественные отношения, возникающие в процессе сбора, обработки, хранения, использования и трансграничной передачи персональных данных. Эти отношения охватывают широкий спектр взаимодействий - от деятельности государств и корпораций по обращению с персональными данными до поведения индивидуальных субъектов в сфере информатизации.

**Предметом диссертационного исследования** выступают нормативные правовые положения международного права, законодательство Республики Казахстан и зарубежных стран (включая ЕС, США, КНР и др.), судебная практика и доктринальные подходы, касающиеся защиты персональных данных.

В предмет исследования входит анализ международных договоров и актов (универсальных и региональных) по защите персональных данных, норм национального законодательства о персональных данных, соответствующей прецедентной и правоприменительной практики, а также рекомендаций и концепций, предлагаемых в научной литературе.

**Методологическую основу диссертационного исследования** составляет комплексный междисциплинарный подход, базирующийся на диалектическом методе познания и принципах постнеклассической рациональности. Исследование опирается на методологический плюрализм и интегративную парадигму правопонимания. Применен широкий спектр общенаучных методов: анализ и синтез, индукция и дедукция, моделирование и правовое прогнозирование. Среди частнонаучных методов ключевую роль играют формально-юридический и сравнительно-правовой методы (анализ моделей ЕС, США, КНР и РК), а также технико-правовой анализ. Особое внимание уделено методам международного права: толкованию договоров (согласно Венской конвенции 1969 г.), анализу «мягкого права», а также анализу вопросов международно-правовой ответственности государств и проблем присвоения поведения государству в киберпространстве (с опорой на Проект статей КМП ООН и авторитетные доктринальные исследования, такие как Таллиннское руководство 2.0 о международном праве, применимом к кибероперациям) и практику ЕСПЧ и Суда ЕС. Центральным элементом методологии выступает специализированная комплексная модель, включающая следующие взаимодополняющие подходы: системный, функциональный, аксиологический, социально-психологический. Системный и функциональный анализ позволяют исследовать структуру и эффективность правового режима в условиях «нормативной турбулентности». Аксиологический подход выявляет ценностные основания регулирования. Социо-психологический метод учитывает поведенческие аспекты и феномен «цифровых следов». Применение комплекса указанных методов обеспечило всесторонность, объективность и достоверность полученных результатов.

**Теоретическую (нормативную и эмпирическую) основу диссертационного исследования** составляют международные и национальные нормативные правовые акты, регулирующие защиту персональных данных, включая ключевые глобальные и региональные соглашения (например, Конвенцию Совета Европы 108+ и Общий регламент ЕС о защите персональных данных и проч.), а также законодательство Республики Казахстан и других государств в данной сфере. В исследовании использованы научные разработки в виде монографий, диссертаций, научных статей, аналитических отчетов, а также документы международных организаций (ООН, ОЭСР, Совет Европы, ЮНЕСКО и др.), затрагивающие вопросы защиты личной информации (персональных данных). Эмпирическую базу исследования составили материалы правоприменительной практики (включая решения международных юрисдикционных органов и акты национальных государственных органов), официальная информация и статистические сведения, а также сведения о фактах

нарушений безопасности персональных данных, имеющие непосредственное отношение к предмету исследования.

**Степень научной разработанности темы исследования и теоретическая основа диссертационного исследования.** Комплексный характер международно-правовых аспектов защиты персональных данных в глобальном и национальном информационном пространстве обусловил формирование обширного корпуса доктринальных исследований, находящихся на пересечении международного публичного, международного частного и информационного права.

Фундаментальную теоретико-методологическую основу диссертационного исследования составили труды классиков правовой и философской мысли, исследовавших природу права, государства и власти, в частности Г. В. Ф. Гегеля (G. W. F. Hegel), Ф. Энгельса и Г. Л. А. Харта (H. L. A. Hart). При формировании методологии исследования и анализе эволюции международно-правовых явлений важное значение имели работы ведущих ученых в области теории права и методологии науки на постсоветском пространстве, таких как Д. А. Керимов, В. С. Нерсесянц, А. В. Венгеров, В. В. Лазарев, В. С. Степин. Применение методов сравнительного правоведения было основано на доктринальных подходах, разработанных Р. Давидом (R. David), Р. Майклсом (R. Michaels) и Д. Ю. Полдниковым. Аксиологические и социологические аспекты права рассматривались с опорой на труды В. Дзедзяка (W. Dziedziak), Р. Банакара (R. Banakar) и М. Трэверса (M. Travers).

Вопросы защиты личной информации (персональных данных) изучались в рамках общей теории права, конституционного, гражданского, информационного и уголовного права. Фундаментальные основы права на частную жизнь были заложены еще в конце XIX века - так, в 1890 году Сэмюэл Уоррен и Луис Брэндейс охарактеризовали право на неприкосновенность частной жизни как «право быть оставленным в покое» [22, с. 205]. Впоследствии данный концепт получил развитие в трудах таких классиков, как Алан Вестин [23, с. 234] и Дэниел Солов [24, с. 57], и стал неотъемлемой частью доктрины прав человека. В современной зарубежной литературе проблемы персональных данных анализируются в контексте деятельности международных организаций (Совета Европы, Европейского Союза и др.) и реализации международных договоров в области приватности. Существенный вклад в разработку вопросов цифровой приватности внесли исследования в сфере права ЕС (например, практики применения GDPR) и сравнительно-правовые работы по защите личных (персональных) данных в различных юрисдикциях.

Анализ механизмов власти и социального контроля, основанных на наблюдении, нашел фундаментальное отражение в трудах М. Фуко (M. Foucault), чьи концепции дисциплинарной власти и «паноптизма» оказали значительное влияние на последующее осмысление проблем приватности и осуществления суверенных полномочий в информационном обществе. Классические критические взгляды были представлены в работах Дж. Оруэлла (G. Orwell) и Ф. Кафки (F. Kafka). В современную эпоху анализ социальных последствий «датафикации» проводился в рамках теории наблюдения

К. Д. Хаггерти (K. D. Haggerty) и Р. В. Эриксона (R. V. Ericson). Критический анализ трансформации экономических моделей под воздействием глобальной «датафикации» был предложен Ш. Зубофф (S. Zuboff) в рамках ее концепции «надзорного капитализма». Философия информации и цифровая этика были глубоко исследованы Л. Флориди (L. Floridi). Экономические и поведенческие аспекты приватности изучались А. Аквисти (A. Acquisti), Л. Брандимарт (L. Brandimarte), Г. Лёвенштейном (G. Loewenstein), С. Коколакисом (S. Kokolakis), Р. Талером (R. H. Thaler) и К. Санстейном (C. R. Sunstein).

Анализ темы исследования в контексте международного публичного права основывался на фундаментальных трудах ведущих представителей современной доктрины международного права. Ключевое значение для анализа вопросов государственного суверенитета, юрисдикции в киберпространстве и международно-правовой ответственности государств имеют работы Я. Броунли (I. Brownlie) и Дж. Кроуфорда (J. Crawford).

В контексте регулирования глобального информационного пространства особое значение приобрели теории глобального административного права, разработанные Б. Кингсбери (B. Kingsbury), Н. Кришем (N. Krisch), Р. Б. Стюартом (R. B. Stewart) и Э. Бенвенисти (E. Benvenisti), а также концепции транснационального частного регулирования и роли неформального правотворчества, мягкого права, которые развивали Ф. Кафаджи (F. Cafaggi), К. Скотт (C. Scott), Л. Сенден (L. Senden) и Й. Паувелейн (J. Pauwelyn).

Формирование глобального и региональных режимов защиты личной информации (персональных данных) находилось в центре внимания ведущих юристов-международников и компаративистов. Ключевыми теоретиками, определившими современный дискурс, выступили Д. Дж. Солов (D. J. Solove), разработавший таксономию приватности и концепцию вреда (в соавторстве с Д. К. Ситрон (D. K. Citron)), и Л. А. Байгрейв (L. A. Bygrave). Проблемы трансграничной передачи персональных данных, экстерриториального применения национального права и разрешения коллизий глубоко исследовались К. Кунером (C. Kuner), П. М. Шварцем (P. M. Schwartz) и Г. Гринлифом (G. Greenleaf). Феномен глобального регуляторного влияния ЕС («Брюссельский эффект») был концептуализирован А. Брэдфорд (A. Bradford), тогда как вопросы цифрового суверенитета и «национализма данных» анализировал А. Чандер (A. Chander).

Детальный анализ правопорядка ЕС, включая применение GDPR и развитие доктрины «цифровых прав человека», отражен в работах М. Суси (M. Susi), В. Г. Восса (W. G. Voss), Б. Ван дер Слота (B. Van der Sloot), Д. Эрдоса (D. Erdos), К. Докси (C. Docksey) и С. Де Тервань (C. De Terwangne). Специфика регулирования КНР и ее международно-правовые аспекты исследовались в работах Р. Кремерса (R. Creemers), М. Цзоу (M. Zou), Я. Ван (Y. Wang) и С. Мильорини (S. Migliorini).

Новый этап исследований связан с вызовами, обусловленными повсеместным внедрением технологий искусственного интеллекта (ИИ) и растущим влиянием глобальных онлайн-платформ. Влияние технологической

архитектуры на формирование правовых норм (концепции «Lex Informatica» и «Code is Law») исследовали Дж. Р. Райденберг (J. R. Reidenberg) и Л. Лессиг (L. Lessig). Правовые и этические аспекты ИИ, проблемы алгоритмической прозрачности и подотчетности были отмечены в работах С. Вахтер (S. Wachter), Б. Миттельштадта (B. Mittelstadt), М. Вила (M. Veale) и Ф. З. Боргесиуса (F. J. Z. Borgesius). Проблемы адаптации международного и национального права к темпам технологического развития («Pacing Problem») проанализировали Г. Е. Марчант (G. E. Marchant), Б. Р. Алленби (B. R. Allenby), Дж. Р. Херкерт (J. R. Herkert) и Р. Браунсуорд (R. Brownsword). Вопросы глобальной безопасности ИИ обсуждались ведущими мировыми техническими экспертами как Й. Бенжио (Y. Bengio), Дж. Хинтоном (G. Hinton), Я. Лекуном (Y. LeCun) и Р. В. Ямпольским (R. V. Yampolskiy). Вопросы правового регулирования деятельности транснациональных онлайн-платформ и ответственности информационных посредников (акторов) исследовали К. Клоник (K. Klonick) и Э. Дуэк (E. Douek); международные антимонопольные аспекты цифровых рынков были исследованы Л. Хан (L. Khan).

Значительное внимание в литературе было уделено современным регуляторным инструментам: концепции «приватность по умолчанию» («Privacy by Design»), разработанной А. Кавукян (A. Cavoukian); имплементации риск-ориентированного подхода, который изучали Дж. Блэк (J. Black) и М. Эберс (M. Ebers); принципу подотчетности, который анализировали А. Мантелеро (A. Mantelero), Т. Карьялайнен (T. Karjalainen), Д. Бутен (D. Butin), Д. Ле Метайе (D. Le Métayer); а также механизмам экспериментальных правовых режимов («регуляторных песочниц»), исследованным Х. Дж. Аллен (H. J. Allen), Д. А. Цечше (D. A. Zetzsche), Т. Буоц (T. Buocz) и Дж. Труби (J. Truby).

Фундаментальный вклад в развитие доктрины информационного права на постсоветском пространстве и в рамках ЕАЭС внесли: И. Л. Бачило, В. А. Копылов, В. Н. Лопатин, В. Б. Наумов, А. А. Стрельцов, Т. А. Полякова, М. А. Федотов. Публично-правовые и международные аспекты цифровизации, защиты данных и цифровой идентификации в регионе были исследованы в работах Э. В. Талапиной, М. А. Егоровой, А. Н. Мочалова, Е. Р. Россинской.

В отечественной науке международного, конституционного и информационного права вопросы правового регулирования информационного пространства и защиты личной информации исследовали такие казахстанские ученые, как Н. М. Габдыжамалов, Р. Б. Джилкишиев, Т. К. Ерджанов, Н. Е. Жексембаева, С. К. Жетписов, А. Сман, Д. В. Татаринов, Л. Ф. Татаринова, М. А. Шакенов, К. Н. Шакиров. Анализ их трудов позволяет выделить несколько ключевых направлений исследований.

Конституционно-правовые основы и трансформация информационных прав человека. Значительное внимание в отечественной науке уделяется фундаментальным аспектам правового положения личности и гарантиям прав человека. В работе А. Сман рассмотрены вопросы взаимоотношений государства и личности как центральную проблему современного конституционализма. В работе представлен комплексный анализ механизма конституционно-правового гарантирования прав и свобод человека, а также отмечена актуальность проблем

международно-правовой защиты прав и свобод в связи с процессами глобализации [25, с. 4-10]. Детальному анализу права на неприкосновенность частной жизни и механизмов его судебной защиты посвящены работы С. К. Жетписова. В работе рассматривается это право как фундаментальное право личности [26, с. 13-33] и отмечается, что приведение законодательства РК в соответствие с международными стандартами в сфере института тайны является приоритетной задачей, поскольку международное право задает высокий стандарт понимания права на конфиденциальность [27, с. 113, 115]. Трансформация информационных прав человека в цифровую эпоху исследуется в работе Н. Е. Жексембаевой. В работе анализируется влияние цифровизации на объем и содержание информационных прав, включая право на защиту персональных данных, и предлагаются пути совершенствования национального законодательства. Особое внимание уделяется вопросам обеспечения баланса между свободой слова и защитой неприкосновенности частной жизни [28, с. 50-64].

Развитие национального информационного законодательства и регулирование информационного пространства. Существенный вклад в теоретическое осмысление, анализ становления и развития казахстанского информационного права внесли Д. В. Татаринов и Т. К. Ерджанов. Д. В. Татаринов проанализировал ранний период развития законодательства (1992-2012 гг.), выявив его нестабильность и отсутствие системного подхода, что привело к неконтролируемому обороту личной информации [29, с. 146]. В работе концептуально обосновано формирование права на защиту персональных данных как нового элемента конституционного права на неприкосновенность частной жизни в эпоху глобальных сетей [29, с. 148]. Т. К. Ерджанов продолжил анализ проблем защиты неприкосновенности частной жизни в период становления информационного права (2013-2016 гг.), также оценивая фрагментарность законодательства того времени [30, с. 937-938]. Особую значимость представляют его предложения по системному реформированию законодательства, включая идею принятия консолидированного закона о регулировании Интернета [31, с. 259-260]. Комплексные вопросы правового регулирования информационных отношений исследовал М. А. Шакенов. В работе рассмотрено информационное пространство как объект правового регулирования, проанализированы принципы и методы этого регулирования, а также предложены меры по обеспечению информационной безопасности и защите персональных данных в условиях глобализации [32, с. 34-83].

Специфические вызовы защиты прав в сфере информатизации. Казахстанские ученые также фокусировались на конкретных проблемах, возникающих в глобальных сетях, включая защиту чести и достоинства, вопросы анонимности и цифровых следов. Т. К. Ерджанов и Л. Ф. Татаринова одними из первых указали на процессуальные и юрисдикционные пробелы при защите чести и достоинства в цифровой среде. Т. К. Ерджанов отметил сложность привлечения к ответственности анонимных нарушителей в социальных сетях [33, с. 137-138]. В работе детально исследованы пределы «права на анонимность» (при этом аргументируется, что оно не является абсолютным

[34, с. 85, 87]), а также предложено внедрение механизмов идентификации пользователей [34, с. 87-88]. В работах Л. Ф. Татариновой отмечаются проблемы, связанные со сложностью установления ответчика при распространении порочащей информации в сети Интернет [35, с. 206]. Феномен цифровых следов и их значение для защиты персональных данных анализируется в работе К. Н. Шакирова. В работе рассматриваются международно-правовые и национальные подходы к определению и защите персональных данных, а также отмечается необходимость адаптации правовых механизмов к новым реалиям в сфере информатизации [1, с. 82-83, 93-94].

Информационная безопасность и противодействие киберпреступности. Проблемы информационной безопасности в условиях региональной и международной интеграции отмечены в исследовании Н. М. Габдыжамалова. В работе предлагаются пути укрепления системы информационной безопасности Казахстана в контексте интеграционных процессов [36, с. 61-109]. Комплексное криминалистическое исследование проблем расследования преступлений в сфере информационных технологий проведено в работе Р. Б. Джилкишиева. В работе представлен детальный анализ современного состояния киберпреступности (2021-2025 гг.), свидетельствующий о ее стремительном росте и низкой раскрываемости [37, с. 15-21]. Особую значимость имеют предложения по совершенствованию уголовного законодательства (введение в УК РК ст. 212-1 «Цифровое мошенничество», использование ИИ как квалифицирующего признака) [37, с. 43-45].

Несмотря на значительный объем доктринальных исследований, динамичное развитие технологий и трансформация глобального информационного пространства требуют дальнейшего комплексного международно-правового анализа проблем защиты личной информации с учетом национальных интересов Республики Казахстан.

**Научная новизна диссертационного исследования** определяется как актуальностью постановки проблемы, так и полученными результатами. Данная работа представляет собой одно из первых в отечественной науке международного права монографических исследований, посвященных защите персональных данных в условиях цифровой глобализации. В исследовании объединены перспективы международного публичного, информационного и сравнительного права, учитываются современные технологические реалии (ИИ, большие данные, интернет вещей и др.), что само по себе является новым шагом для комплексного осмысления темы.

В процессе разработки темы исследования были сформулированы и обоснованы **основные положения, выносимые на защиту:**

1. Введено и обосновано понятие «нормативной турбулентности» как характеристики современного международно-правового регулирования в глобальном информационном пространстве. Предлагается авторское определение данного феномена для описания состояния правовой неопределенности, вызванного системным разрывом между трансграничным характером цифровых технологий (включая ИИ) и территориальным характером юрисдикций. Нормативная турбулентность проявляется в фрагментации

глобальной регуляторной среды, возникновении коллизий национальных режимов и усилении фактического нормотворчества частных акторов («самонормативности»). Данное понятие позволяет концептуализировать вызовы, стоящие перед гармонизацией международно-правовых стандартов защиты персональных данных.

2. Предложена концепция трансформации «вторичных» (процедурных) норм в «первичные» (субстантивные) как условие реализации фундаментальных прав человека в глобальном информационном пространстве. Обосновано, что в условиях трансграничной обработки данных и алгоритмического принятия решений процедурные гарантии (принципы прозрачности, подотчетности, информированности) приобретают фундаментальное значение. Этот вывод подтверждается эволюцией международно-правовых стандартов (в частности, GDPR, Конвенция 108+), где соблюдение данных принципов становится самостоятельным условием законности обработки персональных данных и необходимым элементом эффективной экстерриториальной защиты права на неприкосновенность частной жизни.

3. Разработано авторское определение «цифровых следов» с учетом их трансграничной природы и международно-правового значения. Сформулировано понятие цифровых следов как комплексной информационно-правовой и криминалистической категории, объединяющей сведения о действиях субъектов в глобальной сети. Предложенное определение акцентирует двойственную международно-правовую природу цифровых следов: с одной стороны, как объекта правовой охраны (элемент персональных данных, требующий защиты независимо от юрисдикции), а с другой - как транснационального средства доказывания, сбор и использование которого требуют международного сотрудничества и гармонизации процессуальных стандартов (в частности, в контексте Будапештской конвенции о компьютерных преступлениях).

4. Обоснована невозможность распространения международно-правового режима персональных данных на сведения о юридических лицах. На основе анализа универсальных и региональных международно-правовых инструментов (МПГПП, Конвенция 108+, GDPR) и доктрины международного права прав человека доказано, что субъектом права на защиту персональных данных является исключительно физическое лицо. Аргументировано, что право на информационное самоопределение является неотъемлемым атрибутом человеческого достоинства. Распространение данного режима на организации противоречит сложившемуся международному консенсусу и телеологическому толкованию соответствующих норм; защита информационных активов юридических лиц обеспечивается иными международно-правовыми институтами.

5. Сформулировано понятие «правовой технологии обеспечения защиты персональных данных» как механизма имплементации международных обязательств. Предложена оригинальная концепция правовой технологии защиты персональных данных, понимаемой как интегрированная совокупность правовых, организационных и технических средств и процедур (проведение

оценки воздействия на защиту персональных данных, ведение реестров операций и инвентаризацию массивов персональных данных, защита персональных данных на этапе проектирования), направленных на реализацию прав субъектов персональных данных. Данная модель выступает необходимым инструментом для эффективной имплементации международных стандартов в национальный правопорядок, обеспечивая регуляторную совместимость и достижение «адекватного уровня защиты», необходимого для законных трансграничных потоков персональных данных в глобальном информационном пространстве.

**Теоретическая значимость диссертационного исследования** заключается в развитии научных представлений о международно-правовых основах (режиме) защиты персональных данных. Выводы и положения диссертации дополняют теорию международного права и информационного права, особенно в части соотношения (или взаимодействия) международных норм и концепции цифрового (информационного) суверенитета. Введенные в научный оборот понятия (такие как «нормативная турбулентность», «цифровые следы» в юридико-доктринальном смысле, «правовая технология защиты данных» и др.) обогащают понятийно-категориальный аппарат юридической науки. Они создают основу для последующих научных исследований на стыке прав человека и технологий, международного регулирования и национальной цифровой политики.

**Практическая значимость исследования** состоит в применимости разработанных подходов и рекомендаций для совершенствования международно-правового и национального режима защиты персональных данных в Республике Казахстан. Предложенные решения могут использоваться: 1) в нормотворчестве Парламента и Правительства при подготовке системных поправок и Цифрового кодекса, гармонизации Закона РК «О персональных данных и их защите» с Конвенцией о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. и Регламентом (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС; 2) в правоприменении уполномоченных органов (включая перспективный независимый орган по защите персональных данных) для контрольно-надзорной деятельности, разработки методик оценки рисков и стандартов подотчетности; в работе судов и прокуратуры при разрешении споров и оценке электронных доказательств; 3) в международно-правовой деятельности МИД РК и иных органов при формировании позиции по трансграничным потокам персональных данных, кибербезопасности и искусственному интеллекту, атрибуции инцидентов и присоединении к договорам; 4) в образовании - при разработке междисциплинарных программ. Дополнительно обоснованы практические меры: проект комплексных поправок; учреждение независимого уполномоченного органа по защите персональных данных; внедрение оценки воздействия на защиту персональных данных, ведение реестров операций с

персональными данными и концепции защиты персональных данных на этапе проектирования и по умолчанию; расширение прав субъектов персональных данных; уточнение дефиниций; современные механизмы трансграничной передачи персональных данных (решения об адекватности, стандартные договорные условия, обязательные корпоративные правила); усиление ответственности; процессуальные новации об электронных доказательствах и развитие «регуляторных песочниц». Реализация предложений повышает совместимость правовых режимов и доверие к цифровым услугам.

**Апробация результатов исследования.** Основные положения и результаты диссертационного исследования прошли апробацию в форме научных публикаций и публичных выступлений. Ключевые идеи работы изложены в ряде статей, опубликованных в отечественных и зарубежных изданиях, включая журналы, индексируемые в международных наукометрических базах (Scopus, Web of Science), в частности «Convergence between and among the Chinese, the EU and Kazakhstan Approaches towards Personal Data Protection against the AI in the Digital Sphere» [7], написанной в соавторстве. Отдельные результаты докладывались на международных и республиканских научно-практических конференциях, что позволило получить ценные замечания и учесть их при доработке исследования. Общий объем публикаций по теме диссертации отражает полноту проведенного исследования и подтверждает его научную новизну. Диссертантом в процессе проведенного исследования получено пять авторских свидетельств.

Диссертация обсуждена на расширенном заседании кафедры международного права факультета международных отношений Казахского национального университета им. аль-Фараби.

**Структура диссертационного исследования.** Структура диссертационной работы соответствует целям и задачам исследования. Диссертационное исследование включает введение, три раздела основного содержания (разделенные на подразделы), заключение и список использованных источников. В первом разделе рассматриваются теоретико-правовые основы понятия личной информации (персональных данных) и исторические аспекты формирования международно-правового режима их защиты. Второй раздел посвящен комплексному анализу этих правовых режимов. В разделе последовательно рассматриваются международно-правовой статус субъектов отношений по защите персональных данных, международно-правовые инструменты и проблемные аспекты их применения, стратегические вызовы, обусловленные развитием искусственного интеллекта и феноменом «нормативной турбулентности», а также анализируется судебная практика в Республике Казахстан и пробелы правоприменения. В третьем разделе исследуются проблемы эффективности и направления развития правовых средств защиты персональных данных, представлены авторские концепции и практические рекомендации. Завершают работу выводы, обобщающие результаты исследования и предлагающие конкретные меры по улучшению международно-правового и национального регулирования оборота персональных данных.

# 1 ТЕОРЕТИЧЕСКИЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ МЕЖДУНАРОДНО-ПРАВОВОЙ ЗАЩИТЫ ЛИЧНОЙ ИНФОРМАЦИИ

## 1.1 Понятие личной (персональной) информации и границы охраны

**Эволюция понятия приватности и личной информации.** Исторической отправной точкой современного понимания права на неприкосновенность частной жизни принято считать статью американских юристов Сэмюэла Уоррена и Луиса Брэндайса «Право на неприкосновенность частной жизни» [22, с. 205]. В этом труде, написанном в ответ на технические новшества конца XIX века (связанные с появлением фотографической фиксации и средств массовой информации), впервые сформулирована идея о самостоятельном «праве быть оставленным в покое» - требовании охранять частную жизнь лица от произвольного и (или) незаконного вмешательства. В работе отмечается, что в условиях усложнения общественных отношений и развития технологий, адекватная защита частной жизни приобретает особую актуальность. Право должно эволюционировать, обеспечивая охрану не только физической неприкосновенности лица, но и его чести, достоинства и личной тайны.

На протяжении первой половины XX века в правовой доктрине преобладал именно такой «пассивный» подход к праву на неприкосновенность частной жизни, заключавшийся в его охране от постороннего вмешательства. Однако с развитием информационно-коммуникационных технологий, сбор и обработка сведений приобрели масштабный характер. В этих условиях стала очевидной недостаточность прежнего «пассивного» подхода к защите права на неприкосновенность частной жизни. Существенный сдвиг произошел в 1960-х годах, благодаря исследованиям Алана Вестина. В фундаментальной работе «Privacy and Freedom» [23, с. 234] было предложено активное определение приватности: право индивидов самостоятельно решать, когда, как и в каком объеме информация о них распространяется. Эта концепция сместила акцент с пассивной защиты на активный контроль субъекта над информационными потоками о себе, заложив философский фундамент современных законов о защите персональных данных [38]. Следует отметить, что каждая из классических концепций приватности имеет свои ограничения. Идея Сэмюэла Уоррена и Луиса Брэндайса о «праве быть оставленным в покое» отражала реалии эпохи печатных СМИ и обеспечивала лишь пассивную защиту, поэтому она не предвидела масштабов современного сбора данных. Подход Алана Вестина, определяющий приватность через активный контроль индивида над информацией о себе, сталкивается с трудностями в условиях цифровой экономики, когда объемы и скорость обработки данных делают эффективный личный контроль затруднительным.

Идея Алана Вестина получила свое наиболее полное развитие в Европе в виде (форме) принципа «информационного самоопределения» (в немецкой версии: «*Informationelle Selbstbestimmung*»), сформулированного Федеральным Конституционным Судом ФРГ в решении по делу о переписи населения (1983 г.) [39]. Суд постановил, что достоинство личности и право на

свободное развитие включают способность самостоятельно определять какие сведения о частной жизни раскрываются и в каких пределах. Этот принцип автономии личности в сфере информационно-коммуникационных технологий лег в основу модели защиты данных ЕС и был закреплен как в Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Конвенции Совета Европы № 108 (1981 г.)) [40], так и впоследствии в самом влиятельном акте - Регламенте (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент ЕС о защите персональных данных (GDPR)) [4].

**Новые вызовы цифровой эпохи.** Как отмечает Март Суси, перенос прав человека из традиционной (внецифровой, офлайн) сферы в цифровую (онлайн) среду не сохраняет их целостности. В сфере информатизации возникают искажения, нарушающие системную согласованность и предсказуемость правоприменения. Отсюда следует рассматривать цифровые права как особую конструкцию с иными связями между нормами и участниками регулирования, а не как продолжение традиционных институтов [41, с. 3-10]. Ускоренное развитие информационно-коммуникационных технологий, технологий обработки больших данных и искусственного интеллекта (ИИ) обусловило возникновение новых вызовов в сфере защиты персональных данных. Американский правовед Дэниел Солов в книге «The Digital Person: Technology and Privacy in the Information Age» наглядно показал, как разрозненные фрагменты сведений, собираемые государством, частным сектором и самими пользователями, формируются в подробные «цифровые досье», формируя цифровой образ человека [24, с. 44-49]. Это отмечает фундаментальную роль информации в современном мире, поскольку она обуславливает не только возможность социальной адаптации человека, но и развитие его личности, самореализацию и самоутверждение [9, с. 34]. На основе таких профилей принимаются решения (в том числе автоматизированные), влекущие юридические последствия для субъекта или аналогичным образом существенно затрагивающие его права - от оценки кредитоспособности и процедур найма до включения в контрольные списки. Для концептуализации исследуемых угроз настоящее исследование обращается к классическим образам, отражающим их природу. Речь идет, во-первых, о феномене тотального надзора, получившем наиболее яркое воплощение в антиутопии Джорджа Оруэлла [42, с. 3], и, во-вторых, об ощущении правовой беспомощности (или незащищенности) перед лицом непрозрачных, чрезмерно формализованных и умаляющих человеческое достоинство бюрократических процедур, детально проанализированных в произведениях Франца Кафки [43]. В этом контексте информационная безопасность человека состоит в невозможности нанесения вреда ему как личности, чья социальная деятельность во многом базируется на осмыслении получаемой информации и информационных взаимодействиях с другими индивидами [9, с. 34-35]. Данная аналитическая рамка дополняется обращением

к работам Мишеля Фуко, в частности, к его анализу дисциплинарной власти и паноптических механизмов социального контроля [44, с. 195-228].

В цифровом обществе практически всякая активность оставляет «цифровой след» - совокупность формализованных данных о действиях человека [45, с. 611-619]. Эти следы одновременно служат ценным материалом для криминологии и основой для формирования все тех же цифровых досье. Поэтому защита персональных данных в настоящее время выходит за рамки классического понимания права на неприкосновенность частной жизни и охватывает всю совокупность правоотношений субъекта в условиях информационного общества. Предоставляя данные о себе государственным органам и коммерческим организациям для участия в современных социально-экономических отношениях, субъект персональных данных, с одной стороны, реализует свои права и законные интересы, а с другой - рискует утратить контроль (такова цель «системы») над этими данными [46, с. 203-210]. Таким образом, вопрос заключается в установлении четких границ правовой охраны - что именно признается личной информацией и подлежит защите, а где заканчивается частная сфера и начинаются допустимые интересы государства и членов его общества. Таким образом, охрана личной информации (персональных данных) выступает как конкретизация права на неприкосновенность частной жизни, отражающая его информационно-ценностный аспект. Эта охрана является неотъемлемой целью обеспечения общей информационной безопасности, которая включает защиту конституционных прав субъектов на сохранение тайны частной жизни и конфиденциальности персональных данных, имеющихся в информационных системах [3, с. 19].

**Международно-правовые стандарты права на неприкосновенность частной жизни.** На универсальном уровне базовые международные акты закрепляют право на неприкосновенность частной жизни, хотя прямо не определяют понятие личной информации. Так, ст. 12 Всеобщей декларации прав человека 1948 года [47] и ст. 17 Международного пакта о гражданских и политических правах 1966 года [48] провозглашают право каждого на защиту от произвольного или незаконного вмешательства в личную и семейную жизнь. Это означает, что вмешательство в частную жизнь не должно быть произвольным или незаконным. Однако ни документы ООН, ни практика Комитета ООН по правам человека не содержат исчерпывающего перечня сведений или аспектов, формирующих содержание права на неприкосновенность частной жизни.

На региональном уровне в Европе ключевое значение имеет ст. 8 Европейской конвенции о защите прав человека и основных свобод (ЕКПЧ) [49], гарантирующая право на уважение частной и семейной жизни, жилища и корреспонденции. Европейский суд по правам человека неоднократно указывал, что понятие «частная жизнь» по смыслу ст. 8 ЕКПЧ включает защиту персональных данных и иной личной информации лица. Любая обработка персональных данных государственными органами рассматривается через призму этой нормы и требует соблюдения критериев законности, наличия законной цели и необходимости в демократическом обществе. Практика ЕСПЧ выработала важные подходы к балансированию права на приватность с

публичными интересами и правом на информацию, став ориентиром для национальных правопорядков. Например, в решениях ЕСПЧ отмечается, что хранение органами власти данных о частной жизни должно быть предусмотрено законом и соразмерно преследуемой цели (дело Rotaru v. Romania, 2000 г. [50], S. And Marper v. The United Kingdom, 2008 г. [51] и др.). Тем самым международное право в общем виде признает неприкосновенность личной информации как составной элемент права на приватность, возлагая на государства обязательство обеспечивать их защиту от произвольного или незаконного вмешательства.

**Универсальное определение персональных данных в современном международном праве.** В ответ на вызовы цифровой эпохи международное сообщество разработало специальные нормы, детально регламентирующие обработку персональных данных. Наибольшее влияние оказала Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. (Конвенция 108+) [14]. В пп. «а» ст. 2 Конвенции 108+ и в пп. 1) ст. 4 GDPR содержится универсальное определение: «персональные данные - любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу…». Попытки сформулировать широкое определение, основанное на критерии возможности прямой или косвенной идентификации субъекта персональных данных посредством ссылки на различные факторы (физические, экономические, социальные), предпринимались и в ранних законопроектах стран СНГ, что свидетельствует о раннем осознании многогранности этого понятия [5, с. 33]. Идентифицируемым считается лицо, которое возможно опознать прямо или косвенно, в частности, по таким идентификаторам как имя, номер документа, данные о локации, онлайн-идентификатор, либо по одному или нескольким признакам, отражающим физическую, физиологическую, генетическую, психическую, экономическую, культурную или социальную идентичность. Данное определение предельно широкое и технологически нейтральное. Оно охватывает огромный спектр сведений, которые на первый взгляд могут не считаться «личными», - от IP-адресов и файлов «cookie» до истории поисковых запросов и геолокационных данных, поскольку через них в совокупности человек также может быть идентифицирован. Границы охраны при таком подходе проводятся по критерию идентифицируемости. Если информация привязана к конкретному индивиду или позволяет его идентифицировать, то она подпадает под правовой режим защиты персональных данных. Напротив, анонимизированные (обезличенные) данные, не позволяющие установить личность субъекта, формально выходят за пределы объекта охраны.

Различные правовые системы имплементировали данную концепцию с учетом своих особенностей. Европейский союз сформировал всеобъемлющую модель: она включает признание защиты данных личного характера фундаментальным правом (ст. 8 Хартии ЕС об основных правах) [52]), закрепление ключевых принципов в GDPR и расширенный комплекс прав субъектов (право на доступ, исправление, удаление, возражение, переносимость

данных и др.). Нарушение требований влечет строгие санкции (административные штрафы в размере до 20 млн. евро или (для предприятий) до 4 % от общего мирового годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше), что подчеркивает высокий приоритет защиты персональных данных в ЕС.

США исторически пошли по секторальному пути регулирования: единого федерального закона о защите персональных данных нет; действует «фрагментарное» сочетание федеральных и штатных норм [53]. Вместо единого понятия используются разные определения: в здравоохранении HIPAA защищает «Protected Health Information (PHI)» [54], в финансовом секторе GLBA - «Nonpublic Personal Information (NPI)» [55], а COPPA регулирует сбор информации о несовершеннолетних «Personal Information» [56]; термин «Personally Identifiable Information (PII)» применяется преимущественно в стандартах и рекомендациях (например, NIST 800-122 [57, с. C1-C2]). В последние годы наблюдается сдвиг к унификации законодательства на уровне штатов (в частности, калифорнийские CCPA/CPRA и работа Калифорнийского агентства по защите приватности CPPA [58]), однако модель США остается более узкой по охвату и с менее высокими максимальными санкциями по сравнению с GDPR.

Модель защиты персональной информации (персональных данных) КНР сложилась совсем недавно и представляет особый интерес ввиду иной правовой культуры. На протяжении длительного времени в Китае не существовало всеобъемлющего закона о защите персональных данных, однако в ответ на рост цифровой экономики и общественный запрос в 2021 году был принят Закон КНР о защите личной информации (Personal Information Protection Law, PIPL) [59]. Его понятие «личной информации» близко к европейскому - любые сведения, связанные с идентифицированным или идентифицируемым физическим лицом, исключая обезличенные данные. При этом подход КНР сочетает элементы модели ЕС (например, требования согласия на обработку, права субъектов на доступ, исправление, удаление) с акцентом на общественное благо и национальную безопасность. В КНР создана многоуровневая система регулирования: помимо PIPL действуют Закон КНР о кибербезопасности (2017 г.) [60] и Закон КНР о безопасности данных (2021 г.) [61], устанавливающие строгие требования к хранению данных внутри страны и контролю над трансграничной передачей. Государственные органы получают широкие полномочия доступа к персональным данным, что отражает коллективистские ценности и приоритет государственной безопасности над неприкосновенностью частной жизни. Тем не менее, закрепление на законодательном уровне обязанностей частных организаций (операторов) по защите персональных данных и права субъектов подавать жалобы и требовать возмещения вреда свидетельствуют о формировании и в Китае культуры защиты персональных данных. Таким образом, несмотря на различные акценты - права человека в ЕС, свобода предпринимательства в США, государственные интересы в Китае - прослеживается общая тенденция к сближению стандартов личной информации под влиянием глобальных цифровых рисков. Во всех трех

моделях отмечается признание того, что эффективная защита персональных данных необходима для устойчивого развития информационного общества.

**Правовые основы защиты персональных данных в Республике Казахстан.** Конституция Республики Казахстан закладывает фундамент охраны личной информации. В частности, ст. 18 Конституции РК гарантирует право каждого на неприкосновенность частной жизни, личную и семейную тайну, а также защиту чести и достоинства [62]. Запрещается сбор, хранение и распространение сведений о частной жизни лица без его согласия, кроме случаев, предусмотренных законом [63] (эти положения согласуются с международными стандартами). Одновременно Конституция РК (ст. 20) провозглашает право на свободу получения и распространения информации, что создает потенциальный конфликт интересов между гласностью и приватностью. Правоведы обращают внимание на эту коллизию [64, с. 32-35]: с ростом информационного общества важно обеспечить баланс между правом человека (личности) на доступ к сведениям и правом на тайну личной жизни. В научных работах (например, Е. А. Миндровой) отмечается необходимость ясно разграничить, где заканчивается общественное право знать и начинается личная тайна [65, с. 11]. Ключевым законом выступает Закон РК «О персональных данных и их защите» от 21.05.2013 № 94-V [66], который закрепляет определение персональных данных и устанавливает основы их обработки. Согласно пп. 2) ст. 1 данного Закона, персональные данные - «это сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе». Данное определение практически воспроизводит европейский подход, что скорее свидетельствует о влиянии концепций GDPR и Конвенции № 108. При этом законодательство РК имеет и особенности. В отличие от GDPR, Закон РК не выделяет «генетические данные» в самостоятельную категорию - геномная и дактилоскопическая информация относится к персональным данным ограниченного доступа и подлежит конфиденциальной обработке. Биометрические данные в национальном праве определены как персональные данные о физиологических и биологических особенностях, позволяющих установить личность, при этом поведенческие признаки к биометрическим не относятся [67]. В практическом плане к биометрическим данным обычно относят, например, изображение лица и голос - именно когда они используются для идентификации. В результате, понятие персональных данных охватывает широкий спектр сведений, позволяющих прямо или косвенно идентифицировать физическое лицо (субъекта), включая современные цифровые (онлайн) идентификаторы. Закон также подразделяет персональные данные по режиму доступа на общедоступные и ограниченного доступа. В отношении общедоступных персональных данных не применяются требования по обеспечению их конфиденциальности, тогда как данные ограниченного доступа подлежат защите, и их обработка допускается лишь при наличии законных оснований и в соответствии с заявленными целями.

В последние годы Казахстан реализовывал масштабную программу цифровизации («Цифровой Казахстан», утв. в 2017 г. [68]), направленную на

активное внедрение электронных услуг, технологий обработки больших данных и ИИ в деятельность государственных органов и частного сектора. Проекты электронного правительства (веб-портал «электронного правительства» (eGov.kz) [69], базы данных в сфере строительства e-Qurylys [70], ЖКХ e-Shanyraq [71] и др.) накопили значительные массивы персональных данных. С одной стороны, государство провозглашает защиту персональных данных неотъемлемой частью конституционного права на неприкосновенность частной жизни. С другой стороны, цифровая трансформация предполагает их активную обработку в целях оптимизации государственного управления и предоставления услуг. В результате персональная информация (персональные данные) в Казахстане обрела двоякую роль. Она является нематериальным благом, связанным с достоинством личности и охраняемым законом, но одновременно - необходимым ресурсом для реализации гражданских прав и получения услуг, элементом правосубъектности индивида в информационном обществе [72, с. 46]. Отечественные исследователи отмечают, что сочетание потребности государства в достоверных данных и развития ИКТ создает новые уязвимости для неприкосновенности частной жизни [1, с. 82; 73, с. 70]. Случаи нарушений безопасности персональных данных (включая массовые нарушения безопасности персональных данных из государственных и негосударственных информационных систем), имевшие место в РК в последние годы, подтверждают наличие рисков неправомерного доступа и обуславливают необходимость совершенствования мер по их защите [74].

Законодатель и надзорные органы РК страны предпринимают шаги к усилению защиты персональных данных. Так, в 2019-2020 гг. нормативная правовая база была дополнена положениями, устанавливающими обязанность собственников и (или) операторов уведомлять уполномоченный орган об инцидентах информационной безопасности (включая факты неправомерной передачи персональных данных), а Правительство РК назначило Министерство цифрового развития, инноваций и аэрокосмической промышленности (МЦРИАП; ныне - Министерство искусственного интеллекта и цифрового развития РК) ответственным за политику в этой сфере [75; 76].

Однако сравнительно-правовой анализ национального законодательства Республики Казахстан и положений GDPR выявляет наличие существенных пробелов в правовом регулировании РК. В законе РК прямо не предусмотрены такие права субъектов, как право на переносимость персональных данных или право возражать против автоматизированного решения (составление профиля), которые являются столпами европейского режима защиты персональных данных. Режим ответственности также мягче: штрафы за нарушения в РК несопоставимо ниже, чем в ЕС, что снижает превентивный эффект норм. Как отмечают отечественные [77, с. 205-208] и зарубежные [78, с. 77-79] ученые, отсутствие в национальной правовой системе Казахстана независимого уполномоченного органа по защите персональных данных (аналогичного в английской версии: *Data Protection Authority - DPA* [79]) представляет собой существенный институциональный дефицит. Данный пробел не восполняется деятельностью существующей Комиссии по доступу к информации. Анализ

полномочий Комиссии, проведенный в том числе Организацией экономического сотрудничества и развития (ОЭСР), показывает, что ее компетенция ограничена вопросами доступа к информации [80, с. 19]. Все это ограничивает признание Казахстана как страны с «адекватным уровнем защиты» по стандартам ЕС и затрудняет международный обмен персональными данными. Таким образом, национальное право стоит перед задачей не только формально перенять передовые нормы, но и внедрить их, учитывая отечественные реалии, чтобы найти баланс между стремлением к цифровизации и фундаментальным правом на частную жизнь.

**Границы правовой охраны и современные подходы.** На основании приведенного анализа возможно заключить, что понятие личной информации как объекта правовой охраны в XXI веке - достаточно сложный многоуровневый феномен. Он включает традиционные идентификаторы личности (ФИО, документы, удостоверяющие личность, адрес проживания), сведения частной жизни (семейная, медицинская, финансовая тайна), а также обширный массив цифровых данных об активности человека (поведенческие данные, онлайн-идентификаторы, биометрия, метаданные коммуникаций и пр.) - все то, что составляет «цифровой профиль» современного индивида. Законодательная охрана распространяется на всю эту информацию, если она позволяет выявить личность, хотя режим защиты дифференцируется (особо охраняются биометрические и чувствительные данные, смягчен режим для общедоступных сведений). В то же время право не является абсолютным - границы приватности обозначены там, где возникают превалирующие законные интересы государства, общества или иных лиц. Международные акты и национальные законы допускают ограничения права на неприкосновенность личной жизни в целях защиты национальной безопасности, общественного порядка, прав других лиц - но такие ограничения должны быть предусмотрены законом и необходимы в демократическом обществе (как требует ст. 8 ЕКПЧ). Например, обработка персональных данных без согласия субъекта допускается в целях осуществления правосудия или оперативно-розыскной деятельности, однако такая обработка строго регламентирована законом в целях предотвращения злоупотреблений. Применение новейших технологий (включая распознавание лиц, массовое видеонаблюдение и профилирование на основе технологий обработки больших данных) обуславливает необходимость переосмысления содержания и пределов права на неприкосновенность частной жизни. Европейские надзорные органы и Совет Европы призывали запретить наиболее опасные практики, такие как автоматическое распознавание лиц в реальном времени в общественных местах, чтобы не превратить общество в полностью «прозрачное» [81, с. 2-3, 12; 82].

Поэтому, обеспечение права на личную информацию в условиях глобальной цифровизации требует комплексного подхода. Необходимо сочетать философские принципы автономии личности (право человека контролировать свои данные), технологически нейтральные юридические определения, охватывающие новые виды данных, и эффективные механизмы правоприменения. Последние включают независимый надзор, ответственность за нарушения, международное сотрудничество и просвещение субъектов данных

об их правах. Только при наличии реальных гарантий, позволяющих человеку сохранять осознанный контроль над своей «цифровой личностью», провозглашенные нормы перестанут быть декларативными. Для РК приобщение к мировым стандартам в этой сфере означает не копирование зарубежных моделей, а их адаптацию к национальному контексту - создание устойчивого баланса между задачами развития цифрового государства и соблюдением фундаментальных прав и свобод личности. В конечном счете, эволюция понятия персональной информации и границ ее охраны отражает стремление правовой науки и практики обеспечить достоинство, свободу и безопасность личности в новой цифровой реальности.

*Таким образом,* по итогам анализа понятия личной (персональной) информации и границ ее охраны возможно сформулировать следующие выводы:

Эволюция международно-правовой доктрины свидетельствует о фундаментальной трансформации понимания приватности: от пассивной концепции «права быть оставленным в покое» к активному принципу информационного самоопределения. В условиях глобальной цифровизации защита персональных данных выступает в качестве ключевого правового института, конкретизирующего фундаментальное право на неприкосновенность частной жизни в сфере сбора и обработки данных.

В современном международном праве (Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. (Конвенция 108+), Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (GDPR)) утвердилось универсальное, технологически нейтральное определение персональных данных, основанное на критерии идентифицируемости физического лица. Данный подход позволяет распространить правовую охрану на широкий спектр сведений, включая цифровые идентификаторы и поведенческие данные, формирующие «цифровое досье». Границы охраны проводятся по признаку идентифицируемости; анонимизированные данные исключаются из объекта защиты.

Сравнительно-правовой анализ демонстрирует глобальную конвергенцию дефиниций личной информации, однако национальные модели (ЕС, США, КНР) существенно различаются в подходах к балансированию прав субъекта персональных данных, интересов бизнеса и государственной безопасности. Эффективность правовой охраны, в том числе в Республике Казахстан, зависит не только от имплементации международных норм, но и от наличия действенных институциональных гарантий, в частности, независимого надзорного органа по защите персональных данных.

Далее проведем анализ источников и принципов международно-правовой защиты личной информации (подраздел 1.2).

## 1.2 Источники и принципы международно-правовой защиты личной информации

**Международные источники права на неприкосновенность личной информации.** Как было описано в предыдущем подразделе, право на защиту частной жизни и личной информации закреплено на универсальном уровне в актах ООН. Всеобщая декларация прав человека (ВДПЧ) 1948 года [47] провозглашает, что «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции…» (ст. 12 ВДПЧ). Юридически обязующим стало аналогичное положение ст. 17 МПГПП 1966 года. Каждому гарантируется защита закона от незаконного или произвольного вмешательства в частную жизнь, посягательств на честь и репутацию [48]. Эти нормы заложили фундамент международно-правовой защиты личной информации как элемента права на частную жизнь. Государства-участники обязаны обеспечить реализацию данного права во внутренних правопорядках, в том числе посредством принятия соответствующих законов и механизмов защиты. В юридической доктрине по кибербезопасности источники правового регулирования понимаются шире, чем традиционные источники права: помимо международных договоров, а также универсальных и региональных международных актов, во внимание принимаются конституционные нормы и акты «мягкого права», включая модельные законы. При этом основу такого регулирования составляет национальное законодательство [83, с. 16]. Было также отмечено, что на региональном европейском уровне ключевым источником права является Европейская конвенция о защите прав человека и основных свобод 1950 года (ЕКПЧ) [49]. В частности, обращено внимание, что ст. 8 ЕКПЧ гарантирует право на уважение личной и семейной жизни, жилища и корреспонденции, и европейские суды распространили эту защиту на сферу персональных данных. В прецедентной практике Европейского суда по правам человека право на защиту персональных данных рассматривается как неотъемлемая часть права на частную жизнь, нарушение которого возможно лишь при соответствии строгим требованиям законности, законной цели и необходимости в демократическом обществе. Таким образом, ЕКПЧ (ст. 8) фактически обязывает государства обеспечить в национальном праве надлежащие гарантии защиты персональных данных, рассматриваемой как неотъемлемый элемент права на уважение частной жизни, в том числе от произвольной или незаконной обработки данных, касающихся частной жизни лица.

Помимо правозащитных договоров общего характера, сформировались специализированные международные соглашения в области защиты персональных данных. Первым глобальным многосторонним соглашением стал принятый Советом Европы в 1981 году договор - Конвенция № 108 о защите физических лиц при автоматизированной обработке персональных данных [40]. Эта Конвенция (открытая для присоединения не только государств - членов Совета Европы) установила базовые принципы обработки персональных

данных, обязательные для государств-участников. В частности, ст. 5 Конвенции требует, чтобы персональные данные собирались и обрабатывались справедливо и законно, хранились для определенных и законных целей и не использовались способами, несовместимыми с этими целями, были адекватными, релевантными и не избыточными по отношению к целям обработки, а также точными и при необходимости обновлялись, и хранились не дольше, чем это необходимо для указанных целей. Эти принципы законности, целевого ограничения, минимизации данных, точности и ограниченного срока хранения впоследствии легли в основу большинства национальных законов о персональных данных и региональных стандартов. Таким образом, базовые международные принципы получили воплощение в конкретных правовых нормах. Так, принцип ограничения цели прямо закреплен в пп. «b» п. 1 ст. 5 GDPR и воспроизведен в законодательстве многих государств, а принцип минимизации данных - в пп. «c» п. 1 ст. 5 GDPR, став общемировым стандартом. Универсальные нормы-принципы легли в основу современной нормативной базы защиты персональных данных в большинстве юрисдикций.

Конвенция № 108 предписывает государствам-участникам принять внутренние меры для реализации этих принципов, включая меры безопасности и правовые средства защиты лиц, чьи данные обрабатываются. В 2018 году была принята обновленная редакция Конвенции № 108 (так называемая Конвенция 108+), которая модернизировала положения договора с учетом современных вызовов - расширения сферы применения на неавтоматизированные данные, введения дополнительных гарантий прав субъектов данных и обязанностей государств по надзору за обработкой данных. Хотя Республика Казахстан не является участником Конвенции № 108, данный договор служит важным ориентиром для формирования национального законодательства, и многие положения закона РК о персональных данных и их защите 2013 г. перекликаются с международно-признанными стандартами Конвенции № 108 (например, разделение данных на общедоступные и ограниченного доступа, необходимость согласия субъекта и др.).

Другим значимым международным источником права является Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» [4] (Общий Регламент ЕС о защите персональных данных или GDPR), вступивший в силу в 2018 году. Хотя GDPR - это акт ЕС, его влияние носит глобальный характер, благодаря экстерриториальному применению и высокому стандарту защиты. GDPR кодифицировал современные принципы обработки персональных данных и детализировал права субъектов данных и обязанности контролеров (операторов) данных. В частности, GDPR устанавливает принципы законности, справедливости и прозрачности обработки; ограничения цели (персональные данные собираются для конкретных законных целей и не используются далее несовместимо с этими целями); минимизации данных (сбор только необходимого объема персональных данных); точности (актуальности); ограничения сроков хранения; целостности и конфиденциальности (обеспечение

безопасности персональных данных) и принцип подотчетности (ответственности) контролера за соблюдение всех перечисленных принципов. Эти принципы во многом развивают положения Конвенции № 108 и дополняют их такими требованиями, как прозрачность (обязательное информирование субъекта о целях и способах обработки) и подотчетность (обязанность контролера не только соблюдать, но и уметь доказать соблюдение правил). Необходимость поиска баланса между защитой частной жизни при обработке личных данных и обеспечением свободного потока информации была зафиксирована еще в «Окинавской Хартии Глобального информационного пространства» (G8, 2000 г.), ставшей важным международным ориентиром [5, с. 39-41]. В GDPR также закреплены конкретные механизмы для обеспечения практической реализации указанных принципов, такие как: обязанность проведения оценки воздействия на защиту персональных данных, обязанность уведомления надзорного органа и субъектов о нарушениях безопасности персональных данных, а также институт (обязанность назначения) уполномоченного лица по защите персональных данных и др. Несмотря на то, что Казахстан не связан требованиями GDPR напрямую, данный Регламент рассматривается как лучший международный опыт [84, с. 77; 85, с. 24, 69]. При разработке национальных реформ и новых норм (например, проектов поправок в закон о персональных данных и их защите, внедрения концепции «Цифровой Казахстан») учитываются положения GDPR, особенно в контексте трансграничной деятельности и обмена данными с организациями ЕС.

Помимо законодательства в сфере защиты персональных данных, важную роль играет Будапештская конвенция о компьютерных преступлениях 2001 г. (Конвенция Совета Европы № 185) [86]. Этот документ направлен на противодействие преступлениям в сфере информатизации (киберпреступности) и устанавливает составы уголовных правонарушений (такие как неправомерный доступ к компьютерным данным, вмешательство в данные или системы, компьютерное мошенничество), а также определяет механизмы международного правового сотрудничества компетентных органов. Опосредованно Будапештская конвенция способствует защите персональных данных, требуя криминализации деяний, связанных с неправомерным получением или иным злоупотреблением персональными данными. Государства-участники обязаны принять законодательство, предусматривающее ответственность, например, за неправомерный доступ к информационным системам и неправомерный перехват персональных данных. Хотя Казахстан пока не присоединился к данной Конвенции (по состоянию на август 2025 г. Казахстан имеет статус наблюдателя и предпринимает шаги к возможному вступлению [87; 88; 89]), ее положения используются страной как модель при разработке национальных норм об уголовной ответственности за киберпреступления. Одним из первых шагов по гармонизации законодательства на постсоветском пространстве стал Модельный закон СНГ «О персональных данных» (1999 г.), целью которого было определение правового режима использования персональных данных [5, с. 26-27]. Следует отметить, что Казахстан в декабре 2019 года ратифицировал Соглашение СНГ о сотрудничестве в борьбе с

киберпреступностью [90], что свидетельствует об осознании проблем защиты информации в сфере информатизации на региональном уровне. Таким образом, многоуровневая система международных источников права - от универсальных норм о праве на частную жизнь до специализированных конвенций (Совета Европы, ЕС, СНГ) - формирует правовую основу для защиты личной информации во всем мире. Эти источники права определяют принципы, обязательства и стандарты, которые государства имплементируют в национальное законодательство.

**Принципы защиты персональных данных в международном праве.** Международно-правовой режим обработки персональных данных основан на общепризнанных принципах, сформированных десятилетиями развития законодательства и практики. Уже в 1980 году Организация экономического сотрудничества и развития (ОЭСР) приняла Основные положения по защите неприкосновенности частной жизни и международных обменов персональными данными. В 1981 году в этой сфере был заключен первый юридически обязывающий международный договор - Конвенция Совета Европы № 108 «О защите частных лиц в отношении автоматизированной обработки персональных данных». Указанные акты закрепили фундаментальные принципы (точность персональных данных, ограничение цели, надлежащая безопасность, прозрачность и др.), которые затем получили развитие в GDPR и национальных законодательствах; впоследствии данная Конвенция была модернизирована Протоколом 2018 г. («Конвенция 108+»).

Важным этапом в формировании глобальной повестки стало принятие Окинавской Хартии глобального информационного общества (2000 г.) [6]. Являясь политической декларацией лидеров G8, Хартия стала влиятельным актом «мягкого права», закрепившим видение развития ИКТ на международном уровне. Принципиальное значение для темы исследования имеет положение Хартии о том, что развитие информационного общества должно сопровождаться мерами по укреплению доверия и безопасности. Документ признал необходимость международного сотрудничества для преодоления «цифрового разрыва» (в английской версии: *«digital divide»*) и особо выделил задачу обеспечения защиты конфиденциальности и персональных данных потребителей, а также необходимость «бороться со злоупотреблениями, подрывающими целостность сети». Таким образом, Окинавская Хартия стала одним из первых документов высокого уровня, связавших развитие глобальной информационной инфраструктуры с необходимостью обеспечения информационной безопасности и защиты прав личности в цифровой среде, что способствовало легитимации этой проблематики на международном уровне.

Помимо европейских стандартов, действует и азиатско-тихоокеанский подход (АТЭС). Так, в 2004 году (с обновлением в 2015 году) на уровне АТЭС была утверждена Рамочная программа конфиденциальности данных (в английской версии: *APEC Privacy Framework*), нацеленная на согласование общих принципов защиты данных без строгой унификации законодательства [91, с. 7, 20; 92, с. 4]. В рамках этой системы функционирует Система трансграничных правил конфиденциальности (в английской версии:

*APEC Cross-Border Privacy Rules System - CBPR*), позволяющий организациям на добровольной основе подтверждать соответствие единым стандартам приватности с целью облегчения трансграничной передачи персональных данных [93, с. 1-3]. Такой гибкий подход мягкого права призван сбалансировать свободный поток данных и защиту частной жизни. Этот поиск баланса был артикулирован ранее на уровне «Большой восьмерки» в Окинавской хартии Глобального информационного общества (2000 г.) [6], где отмечалась необходимость развития механизмов защиты личной жизни при одновременном обеспечении свободного потока информации.

Далее кратко раскроем содержание ключевых принципов на материале права ЕС (GDPR), опираясь в том числе на современную доктрину и комментарий под редакцией Кристофера Кунера, Ли Байгрейва и Кристофера Докси [94, с. 309-320]. В основе этой деятельности лежит принцип гуманизма, заключающийся в обеспечении прав и свобод человека при осуществлении противодействия информационным угрозам и недопущении произвольного вмешательства в его частную жизнь, личную и семейную тайны [9, с. 43].

**1. Принцип законности, справедливости и прозрачности.** Обработка персональных данных должна осуществляться на принципах законности, справедливости и прозрачности по отношению к субъекту. Законность означает наличие у контролера правового основания для каждой операции с данными (согласие субъекта, исполнение договора, законное обязательство, защита жизненно важных интересов, публичный интерес или законные интересы контролера). Принцип справедливости требует учитывать разумные ожидания субъекта данных и не действовать обманным или угнетающим образом. Прозрачность обязывает предоставлять субъектам ясную и доступную информацию о том, какие их данные собираются, с какой целью, кто их получает, как долго они хранятся и какие права имеет субъект. Согласно комментариям экспертов, принцип прозрачности выступает гарантией того, что субъекты могут контролировать свои персональные данные, а непрозрачная скрытность обработки рассматривается как нарушение основополагающего доверия между субъектом и обрабатывающей организацией [95, с. 314].

**2. Принцип ограничения цели.** Персональные данные должны собираться для конкретных, заранее определенных и законных целей и не могут далее использоваться несовместимо с этими целями. Данный принцип препятствует расширяющейся, неопределенной обработке данных: организация обязана четко формулировать, зачем нужны данные (например, для предоставления определенной услуги, для учета кадров и т. д.), и не вправе потом использовать их для иных чуждых целей без дополнительного основания. Ключевым требованием является законность целей и способов обработки, а также соответствие объема и характера обрабатываемых персональных данных заявленным целям [9, с. 84]. В комментарии к GDPR отмечается, что последующее изменение целей обработки возможно лишь при наличии новой правовой основы и с учетом совместимости с изначальной целью [95, с. 315]. Для реализации принципа целевого ограничения требуется организационно

закреплять перечень целей обработки персональных данных в политиках конфиденциальности и уведомлять субъектов персональных данных при любом изменении этих целей.

**3. Принцип минимизации данных.** Обрабатываемые персональные данные должны быть адекватными, релевантными и ограничиваться тем, что необходимо для целей их обработки. Иными словами, не допускается обработка персональных данных, являющихся избыточными по отношению к заявленным целям их обработки. Например, если осуществляется сбор персональных данных для цели регистрации субъекта на информационном ресурсе, то требование предоставить его домашний адрес или ИИН будет рассматриваться как избыточное и, следовательно, нарушающее принцип минимизации данных. В контексте GDPR данный принцип тесно связан с пропорциональностью вмешательства в частную жизнь: сбор данных должен быть соразмерен нуждам и не чрезмерен [95, с. 317]. Практическое применение минимизации - это регулярный пересмотр форм и полей сбора данных, удаление лишних граф и ограничение перечня собираемой информации самыми необходимыми категориями.

**4. Принцип точности (актуальности).** Личная информация должна быть точной и при необходимости обновляться. Неточные или неактуальные персональные данные могут повлечь принятие ошибочных решений в отношении субъекта (например, неправомерный отказ в предоставлении услуги на основе недостоверных данных). Поэтому контролер обязан принимать разумные меры для исправления или удаления персональных данных, если они неверны или неактуальны. GDPR закрепляет право субъекта на исправление (ст. 16) и право на удаление «устаревших» данных (ст. 17, «право на забвение» что отражает данный принцип [95, с. 317]. В законодательстве РК также предусмотрена обязанность операторов обеспечивать точность персональных данных и своевременно их актуализировать, хотя механизм реализации этого принципа пока недостаточно развит (например, процедуры уведомления субъекта о необходимости обновить информацию).

**5. Принцип ограничения срока хранения.** Персональные данные должны храниться в форме, позволяющей идентифицировать субъекта, не дольше, чем это необходимо для целей, ради которых данные собирались. По достижении цели данные должны быть уничтожены либо обезличены [95, с. 318]. Международная практика рекомендует устанавливать конкретные сроки хранения для разных категорий данных (например, бухгалтерские данные - 5 лет, данные неактивных пользователей - 1 год и т. п.) и по истечении сроков проводить безопасное удаление. В Казахстане данному аспекту уделено мало внимания. Закон РК «О персональных данных и их защите» 2013 г. не содержит прямых норм о максимальных сроках хранения, ограничиваясь указанием на необходимость прекратить обработку при отсутствии необходимости (ст. 10). Это указывает на пробел в правовом регулировании: на практике собственники и (или) операторы зачастую осуществляют хранение персональных данных сверх сроков, необходимых для достижения целей их обработки. Подобная

практика увеличивает риски неправомерного доступа или распространения персональных данных.

**6. Принцип целостности и конфиденциальности.** Необходимы надлежащие меры безопасности для защиты персональных данных от утраты, несанкционированного доступа, изменения или разглашения. Это включает принятие оператором необходимых организационных и технических мер, в том числе использование шифровальных (криптографических) средств, для защиты данных от неправомерного или случайного доступа, уничтожения, изменения и распространения [9, с. 88]. Этот принцип возлагает на контролеров обязанность технической и организационной защиты данных: использовать шифрование, парольную защиту, ограничение доступа сотрудников, резервное копирование, аудит безопасности [95, с. 318]. Международные стандарты (например, ISO 27001) и GDPR (ст. 32) требуют проведения оценки рисков и применения мер, соответствующих рискам и характеру данных (особо чувствительные персональные данные требуют усиленной защиты). Принцип конфиденциальности означает, что доступ к персональной информации должны иметь лишь уполномоченные лица, необходимые для обработки, и сами данные не раскрываются третьим лицам без законного основания. Закон РК «О персональных данных и их защите» (ст. 24-26) возлагает на собственников и (или) операторов обязанность принимать необходимый комплекс мер по защите персональных данных, в том числе от неправомерного распространения и доступа. Однако на практике в Казахстане неоднократно фиксировались масштабные нарушения безопасности персональных данных (в том числе из государственных и негосударственных информационных систем). Это указывает на недостатки в практической реализации установленных мер защиты и на необходимость совершенствования системы обеспечения информационной безопасности.

**7. Принцип подотчетности.** Это сравнительно новый, но ключевой принцип, означающий, что контролер (оператор) персональных данных несет ответственность за соблюдение всех перечисленных принципов и должен быть способен продемонстрировать такое соблюдение. В GDPR принцип подотчетности закреплен в п. 2 ст. 5 и реализуется через требования документировать процессы обработки, вводить политики и процедуры, назначать ответственных лиц, проводить оценку воздействия на защиту персональных данных и т. п. Смысл подотчетности - сдвиг от формального соответствия к реальной проактивной ответственности: организация должна не ждать проверки, а сама регулярно оценивать свою деятельность на соответствие принципам и готовить доказательства (отчеты, журналы, документы) [95, с. 318].

Кристофером Докси в комментарии отмечается, что принцип подотчетности превращает защиту персональных данных из набора статичных правил в динамический процесс управления рисками, требуя от организации культуры соблюдения и готовности отчитаться за каждое действие с персональными данными [96, с. 557, 560, 568]. В законодательстве РК принцип подотчетности явно не обозначен, однако отдельные элементы присутствуют: например, ст. 22 Закона РК «О персональных данных и их защите» обязывает операторов

при передаче персональных данных третьим лицам удостовериться в обеспечении ими конфиденциальности, а п. 7 Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных [97] требует вести журнал обращения к информационной системе персональных данных. Тем не менее, отсутствует институт независимого контроля (специализированного уполномоченного органа по защите персональных данных) и обязанность операторов регистрировать базы данных или сообщать о нарушениях безопасности, что в международной практике рассматривается как пробел в реализации принципа подотчетности.

Подводя итог, международно-правовые принципы обработки персональных данных: законность, справедливость, прозрачность, ограничение цели, минимизация, точность, ограничение хранения, целостность и конфиденциальность, подотчетность образуют единый свод требований, направленных на обеспечение баланса между свободным обращением персональных данных и защитой прав личности. Эти принципы признаны на глобальном уровне и должны приниматься во внимание государствами при разработке национального законодательства. В основе этого регулирования лежит законодательное закрепление принципов «сбалансированности интересов личности, общества и государства и их взаимной ответственности» [3, с. 10].

**О правовом режиме защиты персональных данных в Казахстане с учетом вышеизложенных положений.** Республика Казахстан, учитывая общемировые тенденции, сформировала свою систему правовых источников защиты личной информации на конституционном, законодательном и подзаконном уровнях. Основы заложены в Конституции РК 1995 года, которая хотя прямо и не упоминает «персональные данные», но содержит нормы о неприкосновенности частной жизни и тайнах личности. Так, пп. 1, 2 ст. 18 Конституции РК гласят: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Каждый имеет право на тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений…» [62]. Эти положения соответствуют международным стандартам (ст. 12 ВДПЧ, ст. 17 МПГПП) и фактически признают право на частную жизнь и конфиденциальность коммуникаций на конституционном уровне. Кроме того, ст. 20 Конституции РК гарантирует свободу получения и распространения информации, но с оговоркой о возможности ограничений, не допускающих разглашения охраняемой тайны. Таким образом, уже в Конституции закреплен принцип, что сведения личного характера относятся к тайне, охраняемой законом.

После обретения независимости Казахстан длительное время не имел специального закона о персональных данных, и защита личной информации осуществлялась фрагментарно через нормы о тайне переписки, врачебной тайне, банковской тайне и т. д. Лишь в 2013 году был принят комплексный Закон РК «О персональных данных и их защите» № 94-V [66] - ключевой закон, регулирующий сбор, обработку и защиту персональных данных. В преамбуле этого Закона прямо указано, что он определяет цель, принципы и правовые

основы деятельности, связанные со сбором, обработкой и защитой персональных данных, а его целью является «…обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных.». В данном Законе закреплено определение «персональных данных» - это «сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе». Также введены категории специальных данных, например «биометрические данные» (сведения о физиологических и биологических особенностях человека, позволяющие установить его личность). Закон подразделил персональные данные по доступности на общедоступные (распространяемые с согласия субъекта либо не требующие конфиденциальности по закону) и данные ограниченного доступа (охраняемые законом персональные сведения). В теории информационного права классификация информации по степени доступа к ней (открытая и ограниченного доступа) является базовой, при этом персональные данные однозначно относятся к категории ограниченного доступа [8, с. 47]. В целом, в Законе 2013 года нашли отражение многие международные принципы: в ст. 5 закреплены, в частности, принципы законности целей и способов обработки персональных данных, минимизации их объема, а также обеспечения безопасности. Таким образом, формально национальное законодательство провозгласило те же ориентиры, что и мировые стандарты.

Важную роль играет Закон РК «Об информатизации» № 418-V от 24.11.2015 г. [98]. Закон регулирует отношения в сфере создания и использования информационных систем и ресурсов. В числе принципов государственного регулирования в сфере информатизации Закон провозглашает «соблюдения прав, свобод и законных интересов физических лиц, а также прав и законных интересов юридических лиц;» (пп. 2) п. 2 ст. 3). В Законе (ст. 36) электронные информационные ресурсы, содержащие персональные данные, отнесены к категории ресурсов ограниченного доступа, и установлено, что их сбор и обработка должны осуществляться в соответствии с законодательством о персональных данных. Таким образом, законодательство об информатизации взаимосвязано с законом о персональных данных, обеспечивая технологическую основу соблюдения режима защиты персональных данных (например, при интеграции государственных информационных систем и предоставлении государственных услуг в электронной форме должны соблюдаться требования по защите персональных данных).

Кроме профильных законов, нормы о защите персональных данных находят отражение в других отраслях права Казахстана. В ст. 115 ГК РК [99] предусматривается нематериальное право на тайну частной жизни, охраняемую гражданско-правовыми средствами. Субъекты персональных данных (физические лица) вправе обращаться за защитой своих прав как в уполномоченный орган (в административном порядке), так и в суд. В судебном (гражданско-правовом) порядке они вправе требовать пресечения незаконного сбора или распространения сведений об их частной жизни, а также возмещения (компенсации) морального вреда, причиненного нарушением их прав на защиту

персональных данных. Уголовный кодекс РК [100] устанавливает уголовную ответственность за деяния, посягающие на неприкосновенность частной жизни. Незаконный сбор или распространение сведений о частной жизни регулируется ч. 2 ст. 147 УК РК - за эти деяния предусмотрены, в зависимости от части, штраф до 5 000 МРП или лишение свободы (до 3-х лет). Одновременно ст. 211 УК РК охватывает неправомерное распространение электронных информационных ресурсов ограниченного доступа (включая ресурсы с персональными данными) - это самостоятельный состав с иными санкциями. Кроме того, за нарушения требований закона о персональных данных предусмотрена административная ответственность по ст. 79 КоАП РК. Отдельно усилена ответственность за незаконное распространение персональных данных, совершенное должностными лицами. Такое деяние квалифицируется по ст. 147 УК РК, предусматривающей признак использования служебного положения. При причинении существенного вреда возможна дополнительная квалификация по ст. 361 УК РК (для должностных лиц) или ст. 250 УК РК. Параллельно, Кодекс РК об административных правонарушениях (КоАП РК) [101] содержит ст. 79, устанавливающую административную ответственность за нарушение законодательства о персональных данных и их защите (штрафы для физических лиц от 30 до 100 МРП, для должностных - до 200, для юридических - до 2 000 МРП). Таким образом, в национальном праве существует двухуровневая система ответственности. Нарушения законодательства Республики Казахстан о персональных данных и их защите, не содержащие признаков уголовно наказуемого деяния, влекут административную ответственность, тогда как посягательства на неприкосновенность частной жизни влекут уголовную ответственность. Уголовно-процессуальный кодекс также содержит гарантии защиты личной информации (ст. 14, 16) [102]. Например, в ходе расследования запрещается сбор сведений о частной жизни лица, не относящихся к делу, а получение информации из каналов связи (перехват телефонных переговоров, осмотр корреспонденции) допускается только с санкции суда и при наличии достаточных оснований (ст. 231, 232, 243, 246 УПК РК).

На уровне государственной политики в Казахстане приоритет защиты персональных данных в цифровую эпоху определен и институционализируется. В 2017 году была принята Государственная программа «Цифровой Казахстан» (2018-2022 гг.) [68], целью которой было развитие цифровой экономики и электронного правительства. В рамках этой программы уделялось внимание созданию надежной инфраструктуры кибербезопасности и защиты данных физических лиц при предоставлении электронных услуг. Кроме того, была утверждена Концепция кибербезопасности «Киберщит Казахстана» [103], где в качестве угроз национальной (и информационной) безопасности определены киберпреступность и утечки информации, а также отмечены уязвимости, обусловленные несовершенством законодательства в сфере защиты персональных данных. В Концепции была обозначена необходимость совершенствования законодательства об информатизации и разработки эффективной системы защиты персональных данных в условиях «электронного правительства». Реализация этой концепции привела к принятию ряда мер:

созданию государственных технических служб кибербезопасности, развитию Центра анализа и расследования кибер-инцидентов (ЦАРКА), запуску сервиса мониторинга обращений к персональным данным в госорганах и др. В 2020 году, отечественные ученые, анализируя ситуацию в Казахстане, приходят к выводу, что действующий Закон Республики Казахстан «О персональных данных и их защите» «носит общий характер и нуждается в конкретизации». Они также отмечают, что «ряд важных аспектов, имеющих непосредственное отношение к обеспечению конфиденциальности персональных данных», в 2020 году был «не регламентирован» [104, с. 55].

**Проблемные аспекты и недостатки действующего законодательства Республики Казахстан.** Несмотря на значительное развитие нормативной базы, национальное регулирование в сфере персональных данных сталкивается с рядом вызовов и характеризуется неполной гармонизацией с передовыми международными стандартами. В научной литературе отмечается отсутствие целостной системы и согласованной государственной политики в этой сфере: нормативно-правовая база остается фрагментарной, а институциональные механизмы защиты недостаточно эффективны [105, с. 31]. В частности, возможно выделить следующие недостатки:

**1. Отсутствие независимого надзорного органа по защите персональных данных.** Во многих странах (включая государства ЕС) действуют уполномоченные органы - комиссии или инспекторы по защите персональных данных, контролирующие соблюдение законодательства, рассматривающие жалобы субъектов персональных данных, налагающие санкции. В Республике Казахстан функции государственного контроля в сфере защиты персональных данных распределены между различными государственными органами. Так, Министерство искусственного интеллекта и цифрового развития РК (ранее - МЦРИАП) реализует функции уполномоченного органа в сфере информатизации. Правоохранительные органы, в свою очередь, осуществляют досудебное расследование по фактам нарушений безопасности персональных данных. При этом в Республике Казахстан отсутствует институт специализированного, независимого органа (омбудсмена) в сфере защиты персональных данных.

**2. Пробелы в нормативном закреплении прав субъектов (ограниченный объем прав).** По сравнению с GDPR, где закреплен широкий перечень прав (доступ, исправление, удаление, ограничение, возражение, переносимость), в праве РК набор прав сформулирован иначе. Закон РК закрепляет право субъекта на получение информации (право на доступ) о наличии у оператора его персональных данных и порядке их обработки, а также право требовать их изменения и дополнения, требовать их блокирования или уничтожения в случае, если сбор и обработка произведены с нарушением законодательства, а также право на отзыв согласия (за исключением случаев, предусмотренных законом). Вместе с тем, отдельного права на переносимость (аналог ст. 20 GDPR) нет, а «право на удаление» носит условный характер - действует, в частности, при незаконной обработке или истечении сроков хранения; право на возражение против обработки выражено опосредованно

через отзыв согласия. Процедуры исполнения детализированы. Контролер обязан предоставить ответ в течение трех рабочих дней, а в подтвержденных случаях внести изменения/блокировать/уничтожить данные - в течение одного рабочего дня, направив мотивированный ответ при отказе. Механизмы защиты включают обращение к уполномоченному органу (административные меры) наряду с судебной защитой. При этом на практике сохраняются риски формального подхода (массовые «типовые» согласия и недостаточная информированность субъектов), что ограничивает фактическую осуществимость прав.

**3. Терминологическая несогласованность и коллизии со смежными правовыми режимами.** Значимость точных и законодательно закрепленных терминологий и определений отмечается в доктрине юридической (законодательной) техники. Эта проблема актуальна и на международном уровне. Как отмечает И. Л. Бачило, правовые дефиниции следует разрабатывать и закреплять прежде всего в базовых законах соответствующих институтов, а терминологию - инвентаризировать и управлять ею, обеспечивая единообразие во всех разрабатываемых нормативных правовых актах [106, с. 97]. Терминологическая несогласованность и отсутствие единства терминов порождает разночтения, затрудняет правоприменение и информационно-поисковую работу. Закон РК «О персональных данных и их защите» различает общедоступные и ограниченного доступа персональные данные. Доступ к последним ограничен законом, а распространение общедоступных персональных данных допускается при наличии согласия субъекта либо в случаях, прямо установленных законом. При этом действуют специализированные режимы охраны информации (государственная, банковская, медицинская тайна), которые пересекаются с регулированием персональных данных (например, банковская тайна - ст. 50 Закона «О банках и банковской деятельности» [107]; сведения о здоровье, врачебная тайна - ст. 273 Кодекса РК «О здоровье народа и системе здравоохранения» [108]). Сведения о состоянии здоровья являются персональными данными, составляющими медицинскую тайну, но не относятся к биометрическим данным (биометрия - признаки, используемые для идентификации). В части «открытых данных» законодательство обязывает публиковать только общедоступные сведения (пп. 12) п. 1 ст. 9 ЗРК «О доступе к информации») [109]. Включение персональных данных ограниченного доступа недопустимо, а опубликованные персональные данные с нарушением законодательства подлежат исключению из общедоступных источников по запросу субъекта (ст. 6 ЗРК «О персональных данных и их защите»).

**4. Недостаточная эффективность режима реагирования на нарушения безопасности персональных данных.** В 2023-2025 годах в Казахстане фиксировались крупные инциденты с персональными данными [110]. Вместе с тем, с 2024 года действует обязанность - при нарушении безопасности персональных данных собственник или оператор в течение одного рабочего дня уведомляет уполномоченный орган, после чего через инфраструктуру электронного правительства осуществляется уведомление субъектов

персональных данных. Это позволяет своевременно реагировать на инциденты информационной безопасности и минимизировать их последствия. По конструкции норма сопоставима с требованием уведомления о нарушениях безопасности данных в ст. 33-34 GDPR.

**5. Несоразмерность ответственности и ее недостаточный сдерживающий (превентивный) эффект.** Административные санкции за нарушения законодательства о персональных данных в РК зависят от состава правонарушения и категории субъекта предпринимательства. По ч. 4 ст. 79 КоАП РК максимальный штраф для крупного бизнеса достигает 2 000 МРП (для среднего - до 1 000 МРП, для малого и НКО - до 750 МРП), при этом по базовым составам размеры заметно ниже (30-200 МРП). Параллельно действуют уголовно-правовые механизмы: ст. 147 УК РК (нарушение неприкосновенности частной жизни и законодательства о персональных данных) и ст. 211 УК РК (неправомерное распространение электронных информационных ресурсов ограниченного доступа). По отдельным частям предусмотрены штрафы до 200 МРП и лишение свободы от трех до семи лет. Открытая статистика по применению этих норм ограничена, дел относительно немного, что затрудняет оценку превентивного эффекта санкций. В сравнении с правом ЕС различие остается существенным: GDPR допускает штрафы до 20 млн. евро или 4 % мирового годового оборота компании, что обеспечивает более высокий сдерживающий эффект.

Очевидно, что в условиях цифровизации (программа «Цифровой Казахстан») правовая система должна была обеспечивать «баланс» между развитием информационных технологий и охраной приватности физических лиц [111, с. 249, 252]. Отсутствие надлежащих гарантий защиты персональных данных снижает общественное доверие к электронным услугам и государственным информационным системам. В то же время, избыточное правовое регулирование (непропорциональные ограничения) может препятствовать инновациям. Поэтому требуется сбалансированный подход - адаптировать лучшие международные практики (в том числе принципы и механизмы GDPR, положительный опыт государств Европы и СНГ), учитывая национальные особенности и конституционные ценности.

*Таким образом,* по итогам анализа источников и принципов международно-правовой защиты личной информации возможно сформулировать следующие выводы.

В проведенном анализе отмечается формирование комплексной, но фрагментированной системы источников международно-правовой защиты личной информации. Данная система эволюционировала от универсальных норм о неприкосновенности частной жизни (МПГПП) к специализированным региональным режимам (Конвенция 108+, GDPR), обладающим выраженным экстерриториальным эффектом и определяющим глобальные стандарты.

Нормативную основу регулирования составляют основополагающие принципы обработки персональных данных: законность, справедливость и прозрачность, ограничение цели, минимизация данных, точность, ограничение хранения, целостность и конфиденциальность, а также подотчетность.

В РК имплементированы базовые международные подходы в национальное законодательство. Однако анализ выявил ряд системных пробелов, препятствующих эффективной реализации данных стандартов: отсутствие независимого специализированного надзорного органа по защите персональных данных (омбудсмена), ограниченный объем прав субъектов персональных данных (в частности, отсутствие права на переносимость) и недостаточный сдерживающий эффект санкций по сравнению с передовыми моделями (GDPR). Для обеспечения действенной защиты требуется дальнейшая гармонизация национального права с международными практиками, направленная на устранение выявленных коллизий и усиление институциональных гарантий. В условиях глобализации и возрастания новых угроз, необходима дальнейшая имплементация международных правовых актов и гармонизация законодательства государств в рамках региональных сообществ.

Рассмотрев ключевые источники и принципы международно-правовой защиты персональных данных, необходимо перейти к обоснованию научного инструментария данной работы. В подразделе 1.3 представлены методологические основы исследования защиты персональных данных.

## 1.3 Методологические основы исследования защиты персональных данных

Методологическая основа диссертационного исследования обусловлена сложностью, многоаспектностью и динамизмом объекта и предмета научного поиска. Таковыми выступают международно-правовые и внутригосударственные общественные отношения, возникающие в процессе обработки персональных данных в условиях глобальной цифровой трансформации. Исследование международно-правовых аспектов защиты персональных данных в условиях беспрецедентного технологического развития и связанной с ним адаптации (или эволюции) международного правопорядка, требует применения комплексной методологии, способной охватить как формально-юридические (догматические) основы правового регулирования, так и его функциональную эффективность, ценностные (аксиологические) ориентиры и технологический контекст.

Глобальное информационное пространство характеризуется трансграничностью информационных потоков, экстерриториальным применением (экстерриториальным охватом) норм отдельных юрисдикций, появлением новых влиятельных негосударственных акторов (глобальных цифровых платформ) и опережающим развитием технологий по отношению к нормативной базе. Это предопределяет необходимость методологического плюрализма, сочетающего достижения общей теории права, международного публичного права, информационного права, а также смежных гуманитарных и технических наук. Отказ от монометодологического подхода обусловлен тем, что ни один метод в отдельности не способен обеспечить полноту и глубину анализа столь комплексного феномена, как правовое регулирование обработки персональных данных в эпоху ИИ и больших данных.

Методологическая структура исследования выстроена иерархически и включает четыре взаимосвязанных уровня: 1) философско-мировоззренческий фундамент; 2) междисциплинарный подход; 3) систему общенаучных и частнонаучных (специальных юридических) методов; 4) специализированный комплексный подход к анализу предмета исследования.

**1. Философско-мировоззренческие основы исследования.** Философско-мировоззренческую основу диссертационного исследования составляет диалектический метод познания социально-правовой действительности [112, с. 49-50]. Данный метод позволяет рассматривать международно-правовой режим защиты персональных данных не как статичную совокупность норм, а как динамическую систему, развивающуюся под воздействием технологических, политических и социальных факторов. Применение диалектики обеспечивает соблюдение фундаментальных принципов научного исследования: объективности, всесторонности, конкретности и историзма. Диалектический метод ориентирует на изучение явлений в их развитии, взаимосвязи и противоречивости.

В частности, закон единства и борьбы противоположностей позволяет выявить внутренние движущие силы развития международно-правового регулирования обработки персональных данных. Диалектический подход обусловливает анализ ключевых противоречий, определяющих развитие исследуемой сферы:

а) Противоречие между глобальным характером потоков персональных данных и национальным (территориальным) характером правового регулирования. Глобальная сфера информационно-коммуникационных технологий, в силу своей трансграничной архитектуры, нивелирует территориальные ограничения для трансграничной передачи персональных данных. В то же время правовое регулирование остается преимущественно территориальным, основанным на Вестфальской системе суверенных государств. Это порождает сложные коллизии юрисдикций, проблемы экстерриториального применения национальных законов (например, Общего регламента ЕС о защите персональных данных (GDPR); Закона КНР «О защите персональной информации» и актуализирует международно-правовые дискуссии о содержании концепции «цифрового суверенитета» и пределах юрисдикции государства в киберпространстве. В исследовании анализируется, как государства стремятся восстановить контроль над потоками персональных данных через механизмы локализации данных, и какие международно-правовые последствия это влечет. Диалектический анализ позволяет исследовать эти противоречия как источник развития новых форм международного сотрудничества и гармонизации правовых режимов.

б) Противоречие между необходимостью свободного потока персональных данных и императивом защиты фундаментальных прав человека. Свободный поток персональных данных является условием инновационного развития, международной торговли и реализации свободы выражения мнения (концепция «свободного потока данных с доверием» - в английской версии: *Data Free Flow with Trust - DFFT*). Однако неконтролируемая обработка персональных данных,

особенно с применением технологий ИИ и технологий обработки больших данных, создает системные угрозы для права на неприкосновенность частной жизни, автономии и достоинства личности, а также для демократических институтов (риски манипулирования, алгоритмической дискриминации). Исследование направлено на поиск путей разрешения этого противоречия посредством выработки сбалансированных правовых решений и применения принципа пропорциональности как универсального метода оптимизации правового регулирования.

в) Противоречие между стремительным развитием технологий и инерционностью правотворческих процессов. Ускоренное развитие технологий ИИ, машинного обучения, Интернета вещей (в английской версии: *Internet of Things - IoT*) [113] и квантовых вычислений [114] опережает способность национальных правовых систем и международного права адаптироваться к этим новым вызовам. В результате возникает разрыв между уровнем технологического развития и существующей нормативно-правовой базой. Это приводит к феномену, определяемому в диссертации как «нормативная турбулентность», - состоянию ускоренного, но фрагментарного, зачастую реактивного и несистемного нормотворчества, сопровождаемого появлением пробелов и коллизий.

Закон перехода количественных изменений в качественные объясняет, как накопление технологических возможностей (рост вычислительных мощностей, объемов персональных данных) приводит к сдвигам в правовой реальности, требующим формирования новых правовых институтов и трансформации существующих принципов (например, перехода от принципа «согласия» к принципу «подотчетности») [115, с. 282-285; 116, с. 118-127; 117, с. 310].

Закон отрицания отрицания позволяет проследить развитие института защиты персональных данных - от первоначального понимания права на неприкосновенность частной жизни как «права быть оставленным в покое» [22, с. 205] (отрицание неограниченного вмешательства) к концепции активного контроля и права на информационное самоопределение [39] (отрицание пассивной защиты в условиях цифровизации), и далее - к формированию комплексных систем управления рисками (подход, основанный на оценке риска) и структурной защиты прав и свобод в эпоху ИИ [116, с. 135-140].

г) Противоречие между технологическими возможностями и ограниченными когнитивными способностями индивида (субъекта персональных данных). Рост сложности систем обработки персональных данных и непрозрачность алгоритмов создают фундаментальную информационную асимметрию между контролерами (операторами, государством, глобальными корпорациями) и субъектами персональных данных. Это затрудняет реализацию права на информационное самоопределение и ставит под сомнение эффективность традиционных правовых механизмов, таких как (информированное) согласие.

Эпистемологическая позиция исследования базируется на признании объективной реальности международно-правовых явлений и возможности их научного познания. Вместе с тем, исследование сферы информатизации ставит

перед юридической наукой новые онтологические и эпистемологические вопросы. Необходимо учитывать особый онтологический статус цифровых объектов (включая персональные данные, алгоритмы, цифровые следы), которые не обладают физической субстанцией, но оказывают реальное воздействие на правоотношения (в том числе связанные с обработкой и защитой персональных данных).

Учитывая высокую степень изменчивости сферы информатизации, нелинейность технологического развития и фундаментальную неопределенность, исследование опирается на принципы постнеклассической рациональности. Этот подход предполагает учет контекстуальности знания, междисциплинарности, влияния ценностных установок на процесс познания и необходимости постоянной рефлексии над методологическими основаниями [118, с. 641-697]. В условиях, когда технологии (в частности, технологии обработки персональных данных) не только являются объектом регулирования, но и сами выступают в роли регулятора (концепция «*regulation by design*»), правовая наука должна адаптировать свой инструментарий для анализа нормативности, встроенной в технологическую архитектуру.

Исследование исходит из комплексной парадигмы правопонимания, позволяющей сочетать инструментарий юридического позитивизма (при анализе действующих норм международного и национального права) с естественно-правовыми (при оценке ценностных оснований регулирования и его соответствия фундаментальным правам человека, включая право на защиту персональных данных) и социологическими подходами (при анализе эффективности правоприменения и социального контекста) [119, с. 26].

**2. Междисциплинарный подход к исследованию.** Объект диссертационного исследования носит выраженный междисциплинарный характер. Международно-правовая защита персональных данных не может быть исследована исключительно в рамках юридической догматики без учета технологического, социального, экономического и политического контекстов.

а) Взаимодействие права и технологий (технико-правовой анализ). Понимание правовых механизмов защиты персональных данных невозможно без осмысления технологических основ их обработки. Такие явления, как автоматизированное принятие решений (включая профилирование), машинное обучение, криптографическая защита (включая сквозное шифрование), децентрализованные реестры (блокчейн), непосредственно влияют на содержание и эффективность правовых норм. Исследование опирается на достижения теории информации и кибернетики для анализа таких категорий, как «цифровые следы», «идентифицируемость», «анонимизация» и «псевдонимизация», что позволяет обеспечить технологическую значимость правового анализа и избежать принятия юридически значимых решений на основе устаревших технологических представлений.

Особое место занимает технико-правовой анализ, направленный на изучение взаимовлияния правовых норм и технологической архитектуры. В рамках этого направления используется концепция «Lex Informatica» или «код - это закон» по Л. Лессигу (в английской версии: *«Code is Law»*), согласно

которой программный код и архитектура информационных систем сами по себе выступают формой регулирования поведения, зачастую более эффективной, чем традиционные правовые нормы [120, с. 553-556; 121, с. 1-8].

Технологическая архитектура может как способствовать защите прав субъектов персональных данных (например, через технологии повышения приватности), так и ограничивать их (например, через системы массового наблюдения или манипулятивные интерфейсы - «темные шаблоны» (в английской версии: «*dark patterns*») [122]. Технико-правовой анализ применялся для анализа принципов «защиты персональных данных на этапе проектирования и по умолчанию» (в английской версии: «*data protection by design and by default*», ст. 25 GDPR) как метода интеграции правовых требований в технологические процессы на стадии их проектирования [123, с. 2-5].

б) Взаимодействие права и международных отношений. Регулирование трансграничных потоков персональных данных является предметом геополитической конкуренции и международной политики. Различия в подходах ключевых юрисдикций (ЕС, США, КНР) обусловлены не только правовыми традициями, но и стратегическими интересами в сфере цифровой экономики, национальной безопасности и технологического лидерства. Исследование учитывает концепции цифрового суверенитета, информационной безопасности и регуляторной конкуренции для анализа процессов формирования международно-правового режима защиты персональных данных. Особого внимания требует анализ роли негосударственных акторов - глобальных цифровых платформ, которые обладают значительной нормативной властью и влиянием, сопоставимым с влиянием государств, что ставит вопросы об их международной правосубъектности (термин КМП ООН) и ответственности в рамках концепции «глобального управления» (в английской версии: «*Global Governance*») [18; 124, с. 16-23; 125, с. 3; 126, с. 25-68; 127, с. 18-21].

в) Взаимодействие права, экономики и социологии. Персональные данные приобрели значительную экономическую ценность, став ключевым активом цифровой экономики. В исследовании использовались элементы экономического анализа права для оценки регуляторного воздействия предлагаемых норм, анализа издержек соблюдения законодательства. Обращение к концепциям поведенческой экономики и социологии необходимо для анализа феномена «сетевых эффектов» [128, с. 424] и формирования монополий в «платформенной экономике», что напрямую влияет на распределение власти и рисков в сфере обработки персональных данных [129, с. 780-784].

г) Взаимодействие права и этики. Развитие технологий ИИ и технологий наблюдения актуализирует фундаментальные этические вопросы о границах допустимого вмешательства в частную жизнь, справедливости алгоритмических решений и автономии личности. Аксиологический фундамент исследования формируется с учетом современных этических концепций и документов «мягкого права» (например, Рекомендации ЮНЕСКО по этике ИИ, Принципы ОЭСР по ИИ), которые определяют ценностные ориентиры для

развития правового регулирования (включая сферу защиты персональных данных) и часто предшествуют принятию юридически обязывающих норм.

**3. Система методов научного познания.** Методологическая структура исследования представляет собой иерархическую систему общенаучных и частнонаучных (специальных юридических) методов, применяемых в комплексе для достижения поставленных целей и задач.

а) Общенаучные методы. К общенаучным методам, применяемым в диссертации, относятся:

1) Анализ и синтез. Анализ используется для декомпозиции сложных международно-правовых институтов (например, режима GDPR, механизма Конвенции 108+) на составные элементы. Синтез позволяет обобщить полученные данные и сформулировать целостные выводы и концепции.

2) Индукция и дедукция. Индуктивный метод применяется при обобщении материалов правоприменительной практики; дедуктивный метод используется для проверки теоретических гипотез и применения общих международно-правовых принципов к конкретным ситуациям.

3) Исторический метод. Применение исторического метода (в его общенаучном значении) позволяет проследить эволюцию технологических предпосылок и социальных запросов, обусловивших становление института правовой защиты персональных данных.

4) Логический метод. Логические приемы (определение понятий, классификация, систематизация, аргументация) используются для упорядочения понятийно-категориального аппарата исследования.

5) Метод аналогии применяется при анализе возможности применения существующих международно-правовых норм к новым явлениям в сфере информатизации.

6) Метод моделирования используется для построения идеализированных конструкций правовых механизмов (например, модели независимого надзорного органа) и прогнозирования последствий их внедрения [112, с. 510].

7) Метод правового прогнозирования. В условиях «нормативной турбулентности» данный метод позволяет формировать ожидания о предстоящих вызовах (например, влияние квантовых вычислений на криптографию и безопасность персональных данных) и выработать соответствующие правовые решения.

б) Частно-научные (специальные юридические) методы. Особое место в методологии диссертационного исследования занимают специально-юридические методы, обеспечивающие строгость и точность правового анализа.

1) Формально-юридический (догматический) метод. Данный метод является базовым и направлен на изучение внутреннего строения правовых норм, их толкование, систематизацию и классификацию [130, с. 79-99, 124-154]. Он включает анализ правовых дефиниций, юридико-технический анализ структуры нормативных актов (GDPR, Закон КНР «О защите персональной информации», Закон РК «О персональных данных и их защите») для выявления пробелов и коллизий, а также квалификацию новых правовых явлений. Этот метод применялся для обоснования невозможности распространения правового

режима защиты персональных данных на данные о юридических лицах, исходя из цели регулирования (защита прав физических лиц) и доктрины правосубъектности.

2) Сравнительно-правовой метод. В условиях глобализации и трансграничного характера общественных отношений в сфере обработки персональных данных сравнительно-правовой метод приобретает ключевое значение. Метод позволяет выявить общие закономерности, национальные особенности и лучшие практики правового регулирования защиты персональных данных. Применение сравнительно-правового метода основано на обоснованном выборе объектов сравнения, представляющих различные регуляторные модели (философии):

- Европейский Союз (ЕС). Представляет всеобъемлющую, правозащитную модель, основанную на защите фундаментальных прав (включая право на защиту персональных данных согласно ст. 1 GDPR). ЕС активно продвигает свои стандарты на глобальном уровне («Брюссельский эффект»).
- Соединенные Штаты Америки (США). Характеризуются секторальной (отраслевой), рыночно-ориентированной моделью с фрагментированным регулированием. Анализ США важен ввиду доминирования американских цифровых платформ.
- Китайская Народная Республика (КНР). Представляет государственно-ориентированную модель, где защита персональных данных тесно сопряжена с интересами национальной безопасности и концепцией цифрового суверенитета.
- Республика Казахстан (РК). Выступает как пример юрисдикции, активно осуществляющей цифровую трансформацию и ориентированной на имплементацию ключевых международных стандартов (в частности, положений GDPR и Конвенции 108+) в контексте евразийского пространства.

Сравнение проводилось на двух уровнях: микросравнение (сопоставление конкретных правовых институтов - например, правового режима согласия, объема прав субъектов персональных данных, механизмов трансграничной передачи) и макросравнение (анализ общих принципов и ценностных оснований правовых систем). Особое внимание уделено анализу экстерриториального применения (охвата) норм и выявлению тенденций к гармонизации или фрагментации правовых режимов, включая феномен «Брюссельского эффекта» [131, с. 25-65].

3) Историко-правовой метод. Применение данного метода направлено на исследование генезиса и эволюции международно-правового режима защиты персональных данных. Это позволяет выявить исторические предпосылки формирования современных стандартов, проследить логику их развития, включая эволюцию концепции права на неприкосновенность частной жизни (приватности), а также проанализировать этапы становления ключевых международных актов (ОЭСР, СЕ, ЕС и др.) [132, с. 25-26].

в) Методы, специфичные для науки международного права. Учитывая специализацию диссертационного исследования, особое внимание уделено методам, применяемым в доктрине международного права и при анализе международно-правовой практики.

1) Методы толкования международных договоров. При анализе международных актов (МПГПП, ЕКПЧ, Конвенция 108+, соглашения ВТО) применялись общепризнанные правила и способы толкования, кодифицированные в ст. 31-33 Венской конвенции о праве международных договоров 1969 года [133]: грамматическое (текстуальное), систематическое (контекстуальное) и телеологическое (целевое) толкование. Особое значение придается эволютивному (динамическому) толкованию. Применительно к договорам о правах человека, данный метод имеет решающее значение. Он предполагает толкование положений конвенции в свете современных условий (доктрина «живого инструмента»). Этот метод активно используется ЕСПЧ для адаптации ст. 8 ЕКПЧ к новым технологическим вызовам [134]. В диссертационном исследовании эволютивное толкование применяется для анализа механизма применения основных прав человека в цифровой среде.

2) Анализ формирования и содержания норм международного права и «мягкого права». В условиях отсутствия универсального кодифицированного договора, регулирующего ИКТ, исследуется вопрос о формировании международного обычного права в данной сфере. Применяется двухэлементный подход к выявлению (идентификации) международного обычая: анализ всеобщей практики и признания такой практики в качестве правовой нормы, как это определено в практике Международного Суда ООН [135] и кодифицировано КМП ООН. Анализируется роль актов «мягкого права» (резолюций международных организаций, кодексов поведения, этических принципов) как инструмента восполнения пробелов в условиях «нормативной турбулентности» и как стадии формирования предстоящих юридически обязательных норм (процесс «отверждения»).

3) Анализ международной ответственности государств и проблем присвоения (атрибуции) поведения. Особое внимание уделено анализу положений Проекта статей об ответственности государств за международно-противоправные деяния [18], разработанных КМП ООН, в частности, ст. 4-11, касающихся присвоения поведения государству, применительно к трансграничным инцидентам с персональными данными в киберпространстве. Проблема присвоения (атрибуции) является одной из центральных в международном праве применительно к киберпространству. Исследуются критерии «эффективного контроля» [136] и концепция «должной осмотрительности» (в английской версии: «*due diligence»*), обязывающая государства предотвращать использование своей территории для совершения международно-противоправных деяний в киберпространстве.

4) Анализ международной судебной и квазисудебной практики. Исследование опирается на анализ решений и консультативных заключений Международного Суда ООН, а также, в значительной степени, на практику ЕСПЧ и Суда ЕС. Практика ЕСПЧ по толкованию ст. 8 ЕКПЧ и практика Суда ЕС по применению GDPR (например, дела Schrems I и II) являются ключевыми источниками для понимания современных стандартов защиты персональных данных.

г) Эмпирические методы и анализ данных.

1) Качественный контент-анализ. В рамках настоящего исследования данный метод используется для многоуровневого анализа корпуса источников: международных договоров (Конвенция 108+), наднационального права (GDPR), национальных законодательных актов (КНР, США, РК), документов «мягкого права» (рекомендации ОЭСР, ЮНЕСКО), аналитических отчетов и материалов судебной практики (ЕСПЧ, Суд ЕС). Целью применения метода является не только фиксация явного содержания текстов, но и выявление смыслов, доминирующих концептуальных подходов и ценностных ориентаций. Посредством систематического кодирования и категоризации текста выявляются ключевые правовые дефиниции (например, подходы к определению «персональных данных», «идентифицируемости», «риска»), прослеживается эволюция международно-правовых принципов, а также идентифицируются пробелы и коллизии, характеризующие состояние «нормативной турбулентности».

2) Метод анализа конкретных случаев (кейс-стади). Применяется для углубленного, многоаспектного изучения наиболее значимых дел (судебной практики) и ситуаций, оказавших существенное влияние на развитие регулирования и правоприменительную практику. Выбор дел обусловлен их репрезентативностью и способностью проиллюстрировать сложные правовые коллизии или технологические вызовы. Ключевые международные судебные прецеденты, определившие вектор развития права (например, дела Schrems I и II в практике Суда ЕС, повлиявшие на режим трансграничной передачи персональных данных, или дело Delfi AS v. Estonia в практике ЕСПЧ об ответственности посредников). Масштабные инциденты нарушения безопасности персональных данных (включая случаи в РК в 2024-2025 гг., в частности, инцидент, затронувший данные 16 млн. субъектов), позволяющие выявить системные пробелы в национальном правоприменении и механизмах контроля. Данный метод позволяет исследовать функционирование правовых норм в реальном контексте, оценить эффективность существующих механизмов защиты и обосновать необходимость их совершенствования.

**4. Специализированный комплексный подход.** Для решения специфических задач диссертационного исследования, связанных с анализом права в условиях цифровой трансформации и «нормативной турбулентности», применяется комплексная методологическая модель, интегрирующая следующие взаимодополняющие подходы: системный, функциональный, аксиологический, социо-психологический и, в дополнении, риск-ориентированный. Эта модель позволяет преодолеть ограниченность сугубо формально-юридического (догматического) анализа и обеспечить междисциплинарный синтез. Поэтому автор уделяет основное внимание четырем ключевым методам: системному, функциональному, аксиологическому и социо-психологическому [137, с. 44].

а) Системный подход позволяет рассматривать сложные правовые явления как единую целостную систему, выявляя взаимосвязи между их элементами. В контексте настоящей работы это означает анализ защиты персональных данных в совокупности уровней и компонентов: международных норм, региональных

стандартов и национального законодательства, а также институциональных механизмов их реализации. Правовые нормы о персональных данных рассматриваются не изолированно, а как части единого международно-правового механизма, где, например, положения GDPR и национального законодательства (в том числе Казахстана) образуют связанную систему регулирования. Применение системного метода способствует формированию единой понятийно-категориальной базы и целостного представления о правовом явлении персональных данных. Так, персональные данные анализируются как правовое явление в системе международного и национального права, что помогает определить их место среди иных объектов правовой охраны и проследить структуру отношений, возникающих при их обработке. Системный анализ акцентирует необходимость комплексности и полноты исследования данной сферы. В работе с его помощью определяется архитектура «правовой технологии» защиты данных: выявляются все основные элементы (принципы, нормы, институты, процедуры) и их связь друг с другом [112, с. 47]. Например, системный подход позволяет отразить, как глобальные стандарты (такие как принцип информационного самоопределения в европейском праве) проникают в национальные правовые системы и требуют координации с местными нормами. Кроме того, системный метод применяется для оценки эффективности действующего законодательства: комплексный анализ показывает, достаточно ли согласованы между собой нормы разных уровней (международных конвенций, регламентов ЕС, национальных законов) и как они совместно функционируют для обеспечения права на неприкосновенность частной жизни. Таким образом, системный подход формирует базис исследования, позволяя увидеть защиту персональных данных как единый механизм с многоуровневой структурой и устранить фрагментарность в понимании проблемы.

б) Функциональный подход нацелен на изучение роли и назначения правовых норм и институтов, то есть тех функций, которые они выполняют в обществе и правовой системе [138, с. 342-348; 139, с. 50]. В сфере защиты персональных данных функциональный метод помогает выяснить, какие социальные потребности удовлетворяет правовое регулирование, и каковы практические результаты действия норм. В диссертации функциональный анализ применяется для оценки того, насколько эффективно действуют механизмы защиты персональных данных, и какие задачи они решают. Например, посредством функционального подхода анализируется, каким образом нормы GDPR обеспечивают реализацию прав субъектов данных (право на информацию, на исправление, на удаление данных и т. д.) и выполняется ли его функция по повышению уровня защиты права на защиту персональных данных в цифровой среде. Аналогично исследуется функциональная роль национальных институтов - например, Уполномоченного органа в сфере защиты персональных данных в Казахстане - в системе гарантий прав субъектов персональных данных. Такой анализ выявляет практические эффекты правовых норм: снижают ли они риски неправомерной обработки персональных данных, создают ли стимулы к справедливому поведению операторов, обеспечивают ли надлежащий баланс между свободой выражения мнения и информации и правом

на защиту персональных данных. Кроме того, функциональный метод применяется при рассмотрении феномена цифровых следов: выясняется, какую функцию они выполняют в правовом смысле - например, служат ли цифровые следы доказательствами в суде, индикатором уровня защищенности информации или основанием для новых правовых обязанностей. Анализ функций позволяет определить, требуют ли цифровые следы особого правового режима (с учетом их роли как потенциального источника угроз безопасности данных) или достаточно общего режима защиты персональных данных. В итоге функциональный метод в работе дает возможность оценить действенность существующих норм и институтов, обнаружить пробелы в механизме защиты (если какая-то функция не выполняется надлежащим образом) и сформулировать предложения по их совершенствованию.

в) Аксиологический (ценностный) подход позволяет рассматривать правовые явления через призму ценностей и целей, которые лежат в их основе [140, с. 53-60; 141, с. 51; 142, с. 778-782]. В сфере международно-правовой защиты персональных данных аксиологический метод фокусируется на тех ценностных основаниях, которые обуславливают особый режим охраны персональных данных. Неприкосновенность частной жизни (конфиденциальность), достоинство личности, автономия воли, безопасность и доверие - все эти ценности определяют содержание правовых норм о персональных данных. Посредством аксиологического анализа в диссертации уточняется смысл базовых понятий и принципов: в частности, понятие «персональные данные» раскрывается с учетом того, какое значение придается персональным данным в разных правовых системах и культурах. Например, право на защиту персональных данных в европейском правопорядке рассматривается как производное от фундаментального права на уважение частной и семейной жизни, отраженного в ст. 8 ЕКПЧ [49]. Это свидетельствует о высокой ценности частной жизни (приватности) в аксиологической системе европейского права.

В более широком контексте выявление ценностных оснований регулирования позволяет понять, как различия в ценностных приоритетах обуславливают фрагментацию национальных моделей регулирования (например, в подходах ЕС, США, КНР). Аксиологический подход позволяет не только выявить и сбалансировать эти противоречивые ценности, но и обосновать критерии пропорциональности и соразмерности при разрешении таких конфликтов, опираясь на практику международных судов.

Анализ ценностных ориентиров показывает эволюцию права на защиту персональных данных - от восприятия персональных данных как объекта экономического обмена к признанию их элементом личных неимущественных прав, охраняемых в том числе международным правом. Возможно отследить, как менялось отношение общества и государства к персональным данным (например, рост ценности частной жизни (приватности) в цифровую эпоху, появление концепции «право на информационное самоопределение» и др.), и как эти ценностные сдвиги влияют на содержание правовых норм. В частности, аксиологический анализ применяется при сопоставлении подходов ЕС и

Республики Казахстан: выявляются ценностные приоритеты (европейский акцент на защиту частной жизни и возможный акцент на государственную безопасность или экономическое развитие в национальном контексте) и оценивается, насколько эти различия препятствуют или, наоборот, стимулируют гармонизацию правовых стандартов.

Кроме того, данный подход используется для обоснования этико-правовых принципов регулирования новых технологий. Он позволяет обосновать концепцию трансформации «вторичных» (процедурных) норм в «первичные» (материальные) в цифровой среде (субстантивизация процедурных гарантий). В контексте теории Г. Л. А. Харта показывается, как под воздействием технологий ИИ обеспечение прозрачности и подотчетности приобретает фундаментальное значение, становясь не просто вспомогательной обязанностью, а самостоятельной юридической ценностью и условием законности цифровых решений [130, с. 79-123].

Таким образом, аксиологический метод углубляет теоретическую основу исследования, позволяя обосновать предлагаемые определения и правовые решения ссылкой на разделяемые обществом основополагающие ценности. Он же помогает определить направления совершенствования законодательства - исходя из идеалов справедливости, свободы и безопасности, которыми должно руководствоваться правотворчество в области цифровых прав.

г) Социологические и психологические подходы позволяют учесть социальный контекст функционирования норм о защите персональных данных, а также поведенческие аспекты субъектов персональных данных и иных участников их обработки (включая операторов и обработчиков) [143, с. 6-17; 144, с. 509-513]. При исследовании международно-правовых аспектов защиты персональных данных социо-психологический метод имеет существенное значение, поскольку реализация (и нарушение) прав субъектов персональных данных напрямую обусловлена поведением индивидов в информационном обществе.

Социологический компонент метода включает анализ эмпирических данных о практике обработки персональных данных. Сюда входит: статистика инцидентов безопасности и нарушений режима защиты персональных данных; анализ социального восприятия приватности, включая исследование отношения различных социальных групп к сбору и обработке персональных данных и учет феномена «парадокса приватности» (в английской версии: «*Privacy Paradox»*) [145, с. 126-130]; анализ правоприменительной (включая судебную) практики и комплаенс-практик операторов в сфере защиты персональных данных. Так, изучение общественного мнения выявляет противоречие между общественным запросом на информацию (интерес государственных органов, операторов и иных лиц в получении расширенного доступа к персональным данным) и потребностью индивидов в обеспечении конфиденциальности и реализации права на защиту своих персональных данных [146, с. 2-9; 147, с. 144, 150; 148, с. 5; 149].

Психологический аспект дополняет этот анализ, исследуя мотивацию и восприятие субъектов персональных данных. Это включает изучение мотивации

субъектов правоотношений, в частности психологических механизмов и когнитивных искажений, влияющих на принятие решений пользователями о предоставлении согласия на обработку данных. В частности, анализируется, как влияние дизайна интерфейсов (например, «теория подталкивания» (в английской версии: «*nudge theory»*) [150, с. 3, 83-86] и «темные шаблоны» [122]) сказывается на свободном волеизъявлении субъекта при получении согласия. Также психологический аспект объясняет, как фактор удаленности и виртуальности коммуникаций снижает восприятие угрозы и способствует раскрытию конфиденциальной информации. В рамках диссертационного исследования данный метод применяется, в частности, для анализа феномена «цифровых следов» - совокупности персональных данных, которую субъект оставляет о себе при использовании информационно-коммуникационных технологий. Ранее в работе было отмечено [1, с. 86], что эти данные («цифровые следы») могут стать объектом несанкционированного доступа или незаконной обработки со стороны третьих лиц в целях, нарушающих права субъектов персональных данных. Эти выводы обуславливают необходимость учета поведенческого фактора при разработке правовых средств защиты: важно понимать, как именно субъекты персональных данных предоставляют (или оставляют) свои данные и каковы ключевые уязвимости в этом процессе.

Социологический метод в исследовании также реализуется через сравнительный анализ правоприменительной практики различных юрисдикций. Изучение решений европейских надзорных органов по защите персональных данных (в частности, по делам о нарушении GDPR) и Уполномоченного органа Республики Казахстан в сфере защиты персональных данных позволяет выявить тенденции в соблюдении (или нарушении) законодательства о персональных данных. Это обеспечивает эмпирическую базу для выводов о социальных факторах, препятствующих эффективной защите (например, низкая правовая осведомленность субъектов данных, экономическая мотивация операторов), и о мерах, способных повлиять на поведение участников обработки персональных данных.

д) Риск-ориентированный подход. В качестве сквозного методологического инструмента, интегрированного из теории управления рисками в современное правовое регулирование (в частности, в GDPR и Регламент ЕС об ИИ), используется риск-ориентированный подход. Он предполагает классификацию регуляторных требований в зависимости от уровня риска для прав и свобод физических лиц, связанного с обработкой персональных данных или использованием системы ИИ [151, с. 530].

Применение данного подхода означает методологический сдвиг от предписывающего регулирования к проактивному управлению рисками со стороны операторов (контролеров) [152]. Этот подход лежит в основе таких правовых инструментов, как оценка воздействия на защиту персональных данных и классификация систем ИИ по уровням риска (в Регламенте ЕС об ИИ). Применение данного подхода позволяет сконцентрировать регуляторные и надзорные усилия на операциях обработки персональных данных, представляющих высокий риск, и обеспечить гибкость регулирования для

технологий с низким уровнем риска. Это особенно важно для поддержания баланса между эффективной защитой персональных данных и стимулированием технологических инноваций.

*Таким образом,* представленная методологическая основа обеспечивает комплексный и всесторонний характер исследования. Применение различных методов на разных уровнях анализа позволяет достичь поставленных целей и решить основные задачи диссертационного исследования, обеспечивая синергетический эффект. В частности, обоснование авторских концепций достигается следующим образом. Понятие *«нормативной турбулентности»* вводится и обосновывается с помощью системного подхода, сравнительно-правового метода и метода правового прогнозирования. Концепция *трансформации «вторичных» норм в «первичные»* (субстантивизация процедурных гарантий) в цифровой среде обосновывается с применением функционального и аксиологического подходов. Авторское определение *«цифровых следов»* формулируется на основе синтеза формально-юридического анализа, системного подхода, технико-правового анализа и социо-психологического метода. Понятие *«правовой технологии обеспечения защиты персональных данных»* разрабатывается с использованием системного и функционального подходов. Обоснование *невозможности распространения режима персональных данных на сведения о юридических лицах* опирается на формально-юридический анализ (теория правосубъектности), аксиологический и функциональный подходы.

Соответственно, избранная методология не только обеспечивает научную обоснованность, достоверность и новизну полученных результатов, но и позволяет провести комплексное международно-правовое исследование защиты личной информации (персональных данных) в глобальном и национальном информационном пространстве и выработать эффективные предложения по совершенствованию правового регулирования в данной сфере.

*Таким образом,* проведенное исследование теоретических и методологических основ международно-правовой защиты личной информации позволило сформулировать следующие обобщающие выводы, определяющие концептуальные рамки диссертации.

В ходе исследования прослежена эволюция международно-правовой доктрины неприкосновенности частной жизни, зафиксировавшая фундаментальную трансформацию от пассивной концепции «права быть оставленным в покое» к активному принципу информационного самоопределения. В условиях глобальной цифровизации, характеризующейся формированием «цифровых досье» и рисками алгоритмического профилирования, происходит становление формирование защиты персональных данных как самостоятельного международно-правового института, конкретизирующего фундаментальное право на неприкосновенность частной жизни.

*Установлено,* что в современном международном праве (Конвенция 108+, GDPR) утвердилось универсальное, технологически нейтральное определение персональных данных, основанное на критерии идентифицируемости

физического лица, что позволяет распространить правовую охрану на широкий спектр сведений, включая цифровые идентификаторы и поведенческие данные.

*Установлено* формирование комплексной, но фрагментированной многоуровневой системы источников международно-правового регулирования. Данная система эволюционировала от универсальных норм о приватности (МПГПП) к специализированным региональным режимам. Особо выделяется роль GDPR, который, обладая выраженным экстерриториальным эффектом, фактически определяет глобальные стандарты комплаенса. Нормативная основа регулирования составляют общепризнанные принципы обработки персональных данных: законность, справедливость, прозрачность, целевое ограничение, минимизация данных, точность, целостность и конфиденциальность, а также императив подотчетности контролера (оператора).

Сравнительно-правовой анализ продемонстрировал, что, несмотря на глобальную конвергенцию дефиниций, национальные регуляторные модели (ЕС, США, КНР) существенно фрагментарны. Различия обусловлены подходами к балансированию прав субъекта данных, интересов частного сектора и императивов государственной безопасности, что порождает коллизии юрисдикций и осложняет трансграничные потоки персональных данных. Анализ правового режима Республики Казахстан показал имплементацию базовых международных стандартов, однако выявил существенные пробелы, в частности, институциональный дефицит (отсутствие независимого специализированного надзорного органа по защите персональных данных) и недостаточную реализацию современных прав субъектов.

Ввиду динамизма объекта исследования, обусловленного глобальной цифровой трансформацией, обоснована необходимость применения комплексной методологии, основанной на диалектическом методе и междисциплинарном подходе. Диалектический метод позволил выявить внутренние противоречия, определяющие развитие международно-правового регулирования: конфликт между трансграничным характером информационных потоков и территориальным характером юрисдикции, а также разрыв между темпами технологических инноваций и инерционностью правотворческих процессов («нормативная турбулентность»). Применение технико-правового анализа обеспечивает учет нормативности, встроенной в технологическую архитектуру.

Сформулированные теоретико-методологические положения создают необходимую основу для последующего анализа правового обеспечения защиты персональных данных в международном и национальном информационном пространстве, что является предметом второго раздела диссертации.

# 2 МЕЖДУНАРОДНО-ПРАВОВОЙ И НАЦИОНАЛЬНЫЙ РЕЖИМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

## 2.1 Международно-правовой статус субъектов отношений по защите персональных данных

В современных условиях глобальной цифровизации и международного обмена данными вопрос защиты персональных данных затрагивает широкий круг субъектов - от физических и юридических лиц до государственных органов и международных организаций. Традиционно под «персональными данными» понимается информация, относящаяся к идентифицированному или идентифицируемому физическому лицу [153, с. 2-25; 154, с. 1873; 155, с. 494]. Соответственно, классическим главным носителем права на защиту таких данных выступает именно физическое лицо - субъект, чья неприкосновенность частной жизни охраняются международным правом (ст.12 ВДПЧ 1948 г. [47], ст. 17 МПГПП 1966 г. [48]) и национальным законодательством. Однако в условиях интенсивного развития информационно-коммуникационных технологий и появления новых видов данных, представляющих ценность, все более актуальным встает вопрос: нуждаются ли в особой правовой охране данные, относящиеся не только к физическим лицам, но и к юридическим лицам? Далее рассмотрены категории субъектов права на защиту персональных данных - физические лица, юридические лица, государство и организации, а также их основные права и обязанности в данной сфере.

**Физические лица как субъекты права на защиту персональных данных.** Физические лица являются субъектами права на защиту персональных данных. Именно им посвящены базовые международно-правовые нормы о неприкосновенности частной жизни. В европейской традиции защита персональных данных возникла как развитие права на частную жизнь, и сегодня закреплена, например, в Общем регламенте ЕС о защите персональных данных (GDPR). GDPR прямо указывает, что его правила применяются к данным только физических лиц: «Настоящий Регламент не распространяется на обработку персональных данных, которые касаются юридических лиц…» [4]. Аналогично, законодательство Республики Казахстан [66] определяет персональные данные как («…сведения, относящиеся к определенному или определяемому…») об определенном физическом лице (субъекте персональных данных). Таким образом, во всех этих актах закрепляется приоритет прав субъекта персональных данных: личная информация неотделима от конкретного лица и охраняется прежде всего в его интересах.

Права физических лиц в области персональных данных многообразны и закреплены как в международных актах, так и в национальных законах. К основным правомочиям субъекта таких относятся: право на информированность (знать, какие данные, кем и с какой целью собираются), право на доступ к своим данным, на их исправление, обновление, а в предусмотренных случаях - и уничтожение (право на забвение). Кроме того,

субъект персональных данных вправе требовать от контролеров (операторов) и обработчиков соблюдения принципов законности, минимизации данных и конфиденциальности при обработке его персональных данных. Эти принципы закреплены, например, в GDPR и имплементированы в законодательства многих стран, включая РК. Государства обязуются создать механизмы, позволяющие человеку защищать свои персональные данные: уполномоченные органы (например, в ЕС - независимые надзорные органы по защите персональных данных, в РК - подразделения при министерствах, отвечающие за контроль в сфере персональных данных), судебную защиту, административные процедуры обжалования нарушений.

Обязанности физических лиц в сфере персональных данных носят ограниченный характер, но закреплены прямо - «Субъект обязан представлять свои персональные данные в случаях, установленных законами Республики Казахстан.» (п. 2 ст. 24 ЗРК «О персональных данных и их защите»), а отзыв согласия не допускается, если это противоречит закону или при наличии неисполненных обязательств. Вместе с тем, требование соблюдения неприкосновенности частной жизни и запрет злоупотребления правом обеспечиваются смежными нормами - общими положениями гражданского права и уголовной ответственностью за незаконный сбор или распространение сведений о частной жизни и неправомерный доступ к электронным информационным ресурсам ограниченного доступа. В случае, когда физическое лицо само выступает оператором (например, индивидуальный предприниматель, собирающий персональные данные клиентов), на него распространяются общие обязанности операторов - обеспечивать законность и безопасность обработки. Таким образом, роль физического лица в системе защиты персональных данных двояка: с одной стороны, оно является основным субъектом защиты (субъектом персональных данных), с другой - участником правоотношений, который при определенных обстоятельствах может нести ответственность (например, за незаконное распространение персональных данных или нарушение тайны переписки, что предусмотрено уголовным и административным законодательством РК).

**Юридические лица и персональные данные организаций.** Традиционно европейское право защиты персональных данных адресовано физическим лицам. В доктрине действительно обсуждается частичное распространение отдельных гарантий на информацию, относящуюся к юридическим лицам, но это не ведет к признанию «персональных данных юридических лиц» как самостоятельной категории: для них речь идет лишь об ограниченной и опосредованной защите вне основных положений GDPR [156, с. 41; 157, с. 32]. Вместе с тем допускается частичная защита определенных интересов юридических лиц (конфиденциальность, справедливость обработки и т. п.). Под этой категорией условно понимают совокупность сведений, позволяющих идентифицировать конкретную организацию и имеющих для нее конфиденциальный характер (например, внутренние документы организации, информация о структуре собственности, коммерческие планы, данные об операциях и контрагентах и т. п.). В классическом праве концепция персональных данных ограничена

информацией о частных лицах - на том основании, что только человеку присущи право на личную жизнь и особая психологическая связь с собственными данными. Как отмечается в литературе, большинство ученых полагает невозможным распространение режима персональных данных на организации, указывая, в частности, на отсутствие у юридического лица «психологического» отношения к своим «личным» сведениям и на необходимость разграничения юридических лиц и физических с точки зрения обеспечения неприкосновенности личности [156, с. 42; 157, с. 32]. Действительно, право на неприкосновенность частной жизни исторически направлено на защиту человеческого достоинства физического лица, тогда как юридическое лицо является искусственной правовой конструкцией, лишенной неотъемлемых атрибутов индивида (таких как сознание и эмоции). Кроме того, данные о юридических лицах (например, название, регистрационный номер, адрес) во многом носят открытый характер - предприятия необходимо регистрировать, публиковать и раскрывать определенную информацию в реестрах и т. д., что формально противоречит режиму защиты персональных данных.

Тем не менее, в современных условиях не представляется возможным полностью отказаться от идеи правовой охраны конфиденциальной информации юридических лиц. Ряд исследователей указывают на принцип равенства физических и юридических лиц как субъектов частного права и на взаимозависимость их интересов, из чего следует, что эволюция законодательства может пойти по пути сближения правовых режимов защиты информации [156, с. 40-42; 158]. В частности, Рамочная программа АТЭС по защите конфиденциальности (2004 г.) направлена на обеспечение баланса между свободным трансграничным потоком данных и защитой персональных данных [91, с. 3-4; 159, с. 42-46], а Основные положения ОЭСР, регулирующие защиту неприкосновенности частной жизни и международные обмены персональными данными (1980 г.) [160, с. 3-4] легли в основу многих национальных законов о приватности (защите персональных данных). Поскольку с деятельностью организации неразрывно связаны имущественные и неимущественные блага и права физических лиц (таких как акционеры, работники и клиенты), то вред, причиненный в результате нарушения безопасности данных организации (например, неправомерного распространения персональных данных или разглашения коммерческой тайны), в конечном счете причиняется именно этим физическим лицам. Как отмечается в исследовании, определенные сведения о юридическом лице требуют защиты конфиденциальности не в меньшей степени, чем персональные данные физических лиц, и поэтому могут потребовать аналогичной правовой защиты [157, с. 28, 32]. В качестве примера возможно привести инциденты, связанные с неправомерным разглашением данных. Когда неуполномоченные лица осуществляют разглашение коммерческой тайны организации или персональных данных ее клиентов, последствиями становятся причинение вреда деловой репутации, материальный ущерб (убытки) и утрата конкурентного преимущества. По своей правовой природе, неправомерное распространение (разглашение) конфиденциальных данных юридического лица сопоставимо с нарушением права на неприкосновенность частной жизни для

физического лица. В обоих случаях причиняется вред, однако для юридического лица он выражается преимущественно в материальном ущербе (убытках) и вреде деловой репутации, тогда как для физического лица - также и в моральном вреде.

**Применимость критерия идентифицируемости к юридическим лицам.** Для обоснования концепции «персональных данных юридических лиц», исследователи обращаются к критерию идентификации. Если под персональными понимаются данные, позволяющие установить личность, то у юридического лица также есть своя идентичность - наименование, реквизиты, уникальные атрибуты и проч. В указанной научной работе отмечается, что определенные сведения о юридическом лице являются «идентифицирующими свойствами» этого субъекта [161, с. 44, 48]. Например, регистрационный номер компании, номер лицензии, адрес веб-сайта - все это данные, однозначно связывающие информацию с конкретной организацией. В этом смысле они функционально подобны персональным данным физических лиц (как ФИО, ИИН и т. п.). Однако существующие нормы прямо не устанавливают, что такие сведения юридического лица охраняются аналогично персональным данных физических лиц. Более того, публичный характер ключевой идентифицирующей информации об организациях (наименование организации, БИН в РК, местонахождение и проч.) противоречит режиму ограниченного доступа, присущему персональным данным. Поэтому сторонники новой концепции делают акцент не на общедоступных сведениях (реквизитах), а на конфиденциальной информации - тех сведениях, которые связаны с конкретным юридическим лицом, но обычно не подлежат разглашению без соответствующей санкции и неправомерное распространение которых способно причинить вред (включая материальный ущерб или вред деловой репутации) этому юридическому лицу. Например, внутренняя документация, база клиентов, сведения о финансовых показателях до их официального раскрытия - все это прямо не подпадает под традиционные категории тайны (не всегда составляет именно коммерческую тайну в узком смысле), но имеет для организации чувствительную природу.

**Потенциальный вред и уязвимость юридических лиц как основание для защиты информации.** Существенным аргументом в пользу защиты данных организаций является их способность нести убытки, то есть потенциальная уязвимость к негативным последствиям неправомерного разглашения информации. Если признать, что раскрытие определенных сведений об организации приводит к ущербу (репутационному, материальному) для нее, то возникает вопрос - достаточно ли действующих правовых механизмов для возмещения этого ущерба и предотвращения подобных ситуаций? В настоящее время подобные случаи регулируются нормами о коммерческой тайне, недобросовестной конкуренции, гражданско-правовой ответственностью за убытки и т. д. Например, если конкурент незаконно получил и разгласил секретные сведения о бизнес-плане организации, то последняя может требовать возмещения убытков. Однако режим персональных данных мог бы предложить превентивные меры защиты, аналогичные тем, что существуют для физических лиц: специальные требования к хранению и обработке таких сведений, контроль

со стороны уполномоченных органов, юридическая ответственность за неправомерное распространение (разглашение) данных, возникающая независимо от наличия или условий договорных обязательств между сторонами и пр. Пока же вопрос остается дискуссионным - как отмечается, единого мнения о том, следует ли считать данные юридических лиц «персональными» и охранять их по той же модели, еще не выработано [161, с. 45]. Тем не менее, тенденции цифровой эпохи подталкивают к переосмыслению классических подходов.

**Двойственный статус государства и обязанности организаций по защите персональных данных.** Государственные органы выступают в сфере защиты персональных данных в двух функциях. Во-первых, как гаранты и регуляторы выполнения международно-правовых и национальных норм о защите персональных данных. Государство - основной субъект международного права - принимает на себя обязательства по соблюдению права на неприкосновенность частной жизни, внедряет соответствующее законодательство, учреждает надзорные органы. Например, государства - участники Конвенции Совета Европы № 108 от 1981 г., модернизированной Протоколом 2018 г. [14; 162]) - обязаны внутри страны имплементировать необходимые меры, обеспечивающие соблюдение базовых принципов обработки персональных данных. В Республике Казахстан функция контроля возложена на уполномоченный орган - Министерство искусственного интеллекта и цифрового развития РК (ранее - МЦРИАП). Профильный надзор осуществляет Комитет по информационной безопасности, однако в юрисдикции Международного финансового центра «Астана» (МФЦА) действует отдельный режим с самостоятельным регулятором - Комиссар по защите персональных данных [163, с. 5, 23; 164, с. 3]. Органы власти издают подзаконные акты, разъяснения, проводят проверки операторов, рассматривают обращения физических лиц о нарушении их прав на защиту персональных данных. Одновременно государство само является крупнейшим оператором, осуществляющим обработку персональных данных - в регистрах населения, налоговых и таможенных базах, системах безопасности и иных государственных информационных ресурсах. Во-вторых, государство само является крупнейшим оператором, осуществляющим обработку персональных данных в государственных регистрах населения, налоговых и таможенных базах, системах общественной безопасности и иных информационных ресурсах. Следовательно, второй правовой статус государства - это статус собственника и (или) оператора персональных данных, на которого в полной мере распространяются требования по обеспечению законности и безопасности их обработки. Государственные органы обязаны принимать необходимые меры по защите персональных данных (включая обеспечение их конфиденциальности и предотвращение несанкционированного доступа) наравне с негосударственными организациями. Более того, к ним предъявляются повышенные требования, поскольку обработка персональных данных осуществляется в рамках реализации властных полномочий и оказания государственных услуг.

Государство также выполняет «балансирующую» (регулятивную) роль, обеспечивая баланс интересов личности, общества и частного сектора в вопросах

информационной безопасности. В источниках права отмечается относительный характер права на защиту персональных данных и необходимость обеспечения баланса между этим правом, правом на свободу выражения мнения и информации и иными законными интересами (преамб. 4, 47, 153 GDPR [4]; п. 1 ст. 52 Хартии ЕС об основных правах [165]). При установлении требований к защите данных принципиально обеспечить баланс интересов: меры должны быть соразмерны и разумны, чтобы, с одной стороны, не создавать чрезмерных препятствий развитию рынка и инноваций, а с другой - не оставлять без защиты права субъектов данных. В этой системе отношений участвуют и сами государства, преследующие свои публичные интересы (национальная безопасность, общественный порядок). Современное законодательство о защите персональных данных, в частности GDPR, представляет собой сложную систему компромиссов, где права субъектов персональных данных могут быть ограничены в целях соблюдения общественного интереса и права на свободу выражения мнения и информации, а обязанность контролеров (операторов) по защите данных уравновешивается признанием их права осуществлять обработку при наличии законного интереса. В итоге круг субъектов в сфере защиты персональных данных включает: 1) физических лиц - носителей охраняемых прав; 2) организации (компании) - операторов информации, несущих обязанности и отстаивающих свои интересы в свободе экономической деятельности; 3) государство - законодателя, арбитра и одновременно заинтересованное лицо, требующее данные для управленческих целей. Как верно отмечает Э. В. Талапина, примирить столь разных участников и их интересы сложно, но крайне важно для эффективности правового регулирования [166, с. 7; 167, с. 31].

**Организации (коммерческие, в том числе публичные компании или эмитенты, ценные бумаги которых включены в официальный список (прошли листинг) фондовой биржи, и некоммерческие)** в контексте защиты персональных данных обычно выступают как операторы (контролеры) персональных данных физических лиц. Особую роль играют информационные посредники (провайдеры), поскольку они обладают технической возможностью воздействовать на информационный обмен. В мировой практике сложилось три основных подхода к их ответственности за действия пользователей: полная ответственность, условная ответственность (например, в ЕС) и иммунитет (преимущественно в США) [5, с. 18-21]. Именно на них возлагается основной объем обязанностей по соблюдению законодательства о защите персональных данных. В соответствии с принципами, заложенными в международных нормах и национальных законах, организации должны: собирать и обрабатывать только те данные, которые необходимы для конкретной законной цели (принцип минимизации); получать согласие субъекта персональных данных или иное законное основание на обработку; обеспечивать точность данных и актуализацию; принимать меры для сохранности данных и предотвращения несанкционированного доступа; не передавать данные третьим лицам без оснований и т. д. Эти обязательства в совокупности часто называют цифровым комплаенсом, то есть соблюдением организациями требований

информационного законодательства. Невыполнение обязанностей влечет юридическую ответственность: административные штрафы, санкции вплоть до приостановления деятельности (например, ст. 83 GDPR предусматривает штрафы до 20 млн. евро или 4 % мирового годового оборота компании за грубые нарушения [4]). Такой строгий режим стимулирует организации внедрять у себя политики конфиденциальности, проводить обучение персонала, улучшать систему кибербезопасности - фактически создавать внутрикорпоративную культуру защиты персональных данных.

Важно отметить, что меры цифрового комплаенса и кибербезопасности, принимаемые организациями, защищают не только персональные данные клиентов или сотрудников, но и ценную информацию о самих организациях. Практика показывает, что кибератаки на организации нацелены как на кражу персональных данных, так и на хищение коммерческой информации (ноу-хау, маркетинговых планов, финансовых записей и проч.). Поэтому требование закона о защищенности информационных систем в равной мере работает на благо как частной жизни физических лиц, так и корпоративной безопасности. Например, в ЕС действует Директива NIS2 (Директива (ЕС) 2022/2555 от 14 декабря 2022 г. о мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза [168]), которая обязывает широкий круг критически важных секторов и важных организаций (транспорт, энергетика, здравоохранение, цифровые сервисы и др.) внедрять повышенные меры кибербезопасности и регулярно отчитываться об инцидентах [169, с. 8, 10]. Цель - защитить именно критическую информационную инфраструктуру, которая часто находится в руках частных организаций, от киберугроз, ведь сбой на таких объектах угрожает общественным интересам. В Казахстане существует Закон «Об информатизации» [98]), вводящий обязанности для владельцев объектов такой инфраструктуры по защите своих систем и данных. Таким образом, смыкаются два аспекта: защита персональных данных и общая информационная безопасность организаций. Если на ранних этапах развития законодательства о защите персональных данных субъект предпринимательства воспринимался преимущественно как источник рисков для прав и свобод физических лиц (субъектов персональных данных), то в настоящее время он сам все чаще признается потерпевшей стороной в результате кибератак, нуждающейся в защите своих информационных активов.

**Существующие правовые механизмы охраны данных организаций.** Хотя юридические лица формально не наделены «правом на персональные данные», их важная информация уже защищается законом в иных формах. В Республике Казахстан охраняются несколько категорий сведений о юридических лицах, имеющих конфиденциальный характер: коммерческая тайна, служебная тайна, банковская тайна, налоговая тайна и др. Эти режимы создают правовую основу для неприкосновенности значимой для организации информации.

Коммерческая тайна - согласно Гражданскому кодексу РК, это сведения, имеющие «…действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее

конфиденциальности.». Иными словами, сюда относятся сведения, составляющие коммерческую тайну (секреты производства (ноу-хау), бизнес-планы, техническая документация, сведения о контрагентах) - то есть информация, которую организация сохраняет в режиме конфиденциальности для обеспечения конкурентного преимущества. Если информация отвечает признакам коммерческой тайны (наличие ценности, отсутствие свободного доступа к ней, принятие мер к охране ее конфиденциальности), то ее неправомерное получение или разглашение влечет установленную законом ответственность: виновное лицо обязано возместить убытки, а в предусмотренных случаях наступает и уголовная ответственность за незаконные получение, разглашение или использование сведений, составляющих коммерческую тайну (ст. 223 УК РК). Аналогичные положения действуют и в международном масштабе - например, ст. 39 Соглашения по торговым аспектам прав интеллектуальной собственности Всемирной торговой организации (ТРИПС) [170] обязывает страны защищать нераскрытую информацию, позволяющую вести конкурентную деятельность. В США понятие «коммерческая тайна» (в английской версии: «*trade secret*») определяется очень широко - как «любая финансовая, деловая, научно-техническая, экономическая или инженерная информация… если владелец принимает разумные меры к ее секретности, и она имеет самостоятельную ценность от непубличности» [171]. Эта широкая формулировка, данная в законе США о коммерческой тайне (Economic Espionage Act, 18 U.S. Code § 1839) [172], охватывает практически все виды данных предприятий при условии, что они не общедоступны. Таким образом, через институт коммерческой тайны уже обеспечивается охрана существенной части сведений, относящихся к юридическим лицам, прежде всего, в сфере предпринимательства и инноваций.

Служебная тайна в законодательстве РК - это информация ограниченного доступа внутри организации или ведомства, распространение которой нежелательно для самого субъекта. Понятие служебной тайны обычно связывается с государственными органами (например, внутренние документы государственных органов, служебная переписка и проч.), однако может применяться и в корпоративном секторе (например, внутренняя политика компании, содержание совещаний, иные рабочие материалы не для публичного распространения). Гражданский кодекс ставит служебную тайну в один ряд с коммерческой, предоставляя ей аналогичную защиту. Нарушение служебной тайны работниками может рассматриваться как дисциплинарный проступок или даже как разглашение коммерческих сведений, если информация ценна для конкурентов.

Банковская тайна охраняется специальным законодательством о банках и банковской деятельности. В РК Закон «О банках и банковской деятельности» [107] запрещает разглашение сведений о счетах и вкладах клиентов банка без их согласия либо специального разрешения (например, по запросу правоохранительных органов). Под защитой находится информация как о физических, так и о юридических лицах - клиентах банка. Например, операции по счету компании, остатки средств, банковская корреспонденция - все это

составляет банковскую тайну. Участник финансового рынка обязан обеспечивать защиту охраняемой законом тайны (банковской, коммерческой, тайны предоставления микрокредита и иной). Нарушение этого требования влечет применение уполномоченным органом мер надзорного реагирования, вплоть до отзыва лицензии. Аналогичные нормы существуют практически во всех странах, поскольку доверие к банковской системе строится на сохранении конфиденциальности финансовых данных клиентов.

В соответствии со ст. 30 Налогового кодекса РК [173] любые сведения о налогоплательщике, полученные налоговыми органами, составляют налоговую тайну и не подлежат разглашению, за исключением прямо предусмотренного Кодексом перечня (например, суммы уплаченных налогов и платежей, суммы возврата НДС, сведения о задолженности и мерах ответственности и др.). Следовательно, финансовая и хозяйственная информация, представляемая организацией в налоговые органы (налоговые декларации, бухгалтерская отчетность, данные о доходах и расходах), охраняется как налоговая тайна, если иное не установлено законом (обязанность публикации, межведомственный обмен, запрос суда или правоохранительных органов). Налоговые органы и иные лица, имеющие доступ к сведениям, составляющим налоговую тайну, не вправе их раскрывать. Режим налоговой тайны установлен ст. 30 НК РК: тайной является любая информация о налогоплательщике, полученная налоговым органом, за исключением перечисленных в Кодексе открытых сведений. За разглашение предусмотрена административная ответственность по ст. 473 КоАП РК; в отдельных случаях возможно привлечение к уголовной ответственности (ст. 223 УК РК). Таким образом, значительный массив передаваемой в налоговые органы информации об организациях защищается законом, хотя и в разных правовых режимах (налоговая, коммерческая, банковская тайна).

Кроме указанных, в Казахстане и других странах действуют режимы служебной тайны (для госслужащих и работников отдельных отраслей), адвокатской тайны (охрана информации, доверенной юридическим консультантам), тайны связи (конфиденциальность переписки, переговоров, распространяющаяся и на организации). К последнему важно добавить: секретность коммуникаций юридических лиц также признается правом. Например, в Европейском союзе Директива 2002/58/ЕС (о конфиденциальности и электронных средствах связи) (2002 г.) [174] распространяет режим тайны связи на юридических лиц наряду с физическими, гарантируя конфиденциальность электронных сообщений организаций. То есть переписка компании и служебные переговоры охраняются режимом тайны связи (в том числе для юридических лиц), но в праве ЕС эта защита сформулирована как охрана их законных интересов, а не как право на частную жизнь.

Таким образом, на национальном и международном уровнях уже существует массив норм, охраняющих данные, связанные с юридическими лицами. Однако они разрозненны, фрагментарны и не образуют целостного правового института, подобного институту защиты персональных данных физических лиц. Возникает вопрос: предоставляет ли практический смысл

введение специального статуса «персональных данных юридического лица»? С одной стороны, признание такового могло бы заполнить пробелы - например, защитить репутационно значимую информацию, которая не подпадает под критерии коммерческой тайны. Ведь известно, что закон защищает деловую репутацию организаций - юридическое лицо вправе требовать опровержения порочащих сведений и возмещения ущерба [175]. В этом смысле сведения, идентифицирующие юридическое лицо и носящие негативный характер (например, отзывы, рейтинги), затрагивают нематериальное благо - деловую репутацию - и, соответственно, подлежат защите, установленной законодательством.

**Применимость принципов GDPR и национального законодательства к «персонифицируемым» организациям.** Хотя сфера действия GDPR распространяется на персональные данные физических лиц и не распространяется на сведения о юридических лицах, отдельные его принципы и механизмы обеспечения соответствия (комплаенс) оказывают косвенное влияние на обработку данных организаций. Так, принципы ограничения цели и минимизации данных (пп. «b», «c» п. 1 ст. 5 GDPR) предполагают сбор только необходимого объема информации; принцип подотчетности (п. 2 ст. 5 и ст. 24) обязывает документировать соответствие; а требование безопасности обработки (ст. 32) обуславливает необходимость внедрения технических и организационных мер, которые на практике также укрепляют защиту и иных массивов данных, включая коммерческую тайну. В ряде случаев организации назначают уполномоченное лицо по защите персональных данных (ст. 37), выстраивая единый «контур» управления данными. Иными словами, соблюдение норм о персональных данных часто повышает общую культуру управления информацией, хотя сами правила GDPR не предназначены для прямой защиты данных юридических лиц.

На национальном уровне наблюдается тенденция сближения регуляторных подходов. Например, положения о локализации данных сначала появились применительно к персональным данным физических лиц (требование хранить персональные данные внутри страны (п. 2 ст. 12 ЗРК «О персональных данных и их защите»)), а затем аналогичный подход применяется к определенным категориям данных о деятельности организаций (например, требование локально хранить бухгалтерскую информацию, государственные электронные базы данных (ст. 42 ЗРК «Об информатизации») и т. д.). Локализация возникает из Закона «О персональных данных и их защите» - если бухгалтерская информация содержит персональные данные (персональные данные сотрудников, контрагентов-физических лиц и т. п.), то хранение таких персональных данных должно осуществляться «…в базе, находящейся на территории Республики Казахстан.» (п. 2 ст. 12).

Из-за территориальных правил GDPR (ст. 3) организации, зарегистрированные в РК, которые предлагают товары/услуги лицам в ЕС или отслеживают их поведение в ЕС, подпадают под требования GDPR и вынуждены привести в соответствие свои процессы защиты персональных данных. Аналогично, обрабатывая данные иностранных физических лиц, организации в

РК могут попасть под юрисдикцию соответствующих зарубежных законов (включая GDPR - при соблюдении критериев ст. 3).

Несмотря на отсутствие общего режима «персональных данных юридических лиц», отдельные принципы обращения с данными (минимизация, ограничение цели, конфиденциальность, подотчетность) могут использоваться как ориентиры при работе с информацией об организациях. При этом право на доступ и право на исправление сведений для юридических лиц уже реализованы фрагментарно - через установленные процедуры в государственных реестрах, кредитных бюро и посредством обращений в государственные органы, но универсального права, сопоставимого с правом субъекта персональных данных на доступ (ст. 15 GDPR), не существует. Идеи о применении модели согласия к распространению конфиденциальных сведений о юридических лицах требуют тщательной проработки, чтобы не вступать в противоречие с установленной законодательством обязанностью по раскрытию информации. Представляется более целесообразным развивать существующие правовые режимы (коммерческая, банковская и налоговая тайна) и секторные процедуры исправления неточных сведений [176; 177].

*Таким образом,* по итогам анализа правового статуса субъектов в сфере защиты персональных данных возможно сформулировать следующие выводы.

В современном международном праве (GDPR, Конвенция 108+) и национальных правопорядках субъектом права на защиту персональных данных признается исключительно физическое лицо. Данная позиция основана на аксиоме о том, что право на информационное самоопределение является неотъемлемым атрибутом человеческого достоинства и неприкосновенности частной жизни, не присущим юридическим лицам.

Юридические лица не обладают статусом субъектов персональных данных. Несмотря на доктринальные дискуссии, распространение соответствующего правового режима на организации не нашло нормативного закрепления. Защита их законных интересов в отношении конфиденциальной информации обеспечивается посредством специализированных правовых институтов (коммерческая, банковская тайна, тайна связи).

Государственные органы и организации (коммерческие, в том числе публичные компании или эмитенты, ценные бумаги которых включены в официальный список (прошли листинг) фондовой биржи, и некоммерческие) организации выступают в качестве операторов (контролеров) персональных данных, неся бремя обеспечения цифрового комплаенса. Имплементация принципов защиты персональных данных (подотчетность, целостность и конфиденциальность) способствует сближению стандартов информационной безопасности, косвенно усиливая защиту информационных активов организаций, однако не ведет к уравниванию правового статуса физических и юридических лиц.

Определив международно-правовой статус субъектов отношений по защите персональных данных, перейдем к анализу правовых средств, формирующих этот режим. В подразделе 2.2 рассматриваются международно-правовые инструменты и проблемные аспекты защиты персональных данных.

## 2.2 Международно-правовые инструменты и проблемные аспекты защиты персональных данных

**Правовые механизмы регулирования обработки персональных данных.** Современное международное право выработало ряд правовых инструментов для регулирования обработки персональных данных. К ключевым механизмам относятся правовые основания обработки персональных данных, процедуры оценки рисков (включая оценку воздействия на защиту персональных данных), а также принцип подотчетности. В первую очередь, законность обработки обеспечивается наличием правовых оснований - условий, при которых сбор и обработка персональных данных допускаются.

В GDPR перечень оснований установлен п. 1 ст. 6: согласие, исполнение договора, юридическая обязанность, жизненно важные интересы, выполнение задачи в общественных интересах, осуществление публичных полномочий, а также законные интересы контролера при соблюдении баланса с правами субъекта. Для отдельных «особых категорий» действует ст. 9, в т. ч. обработка в общественных интересах в сфере здравоохранения (например, эпиднадзор) при гарантиях защиты прав. Вопросы правоохранительной деятельности в ЕС регулируются не GDPR, а Директивой 2016/680 (2016 г.) (в английской версии: *Law Enforcement Directive - LED*) [178]. В Республике Казахстан сбор и обработка персональных данных осуществляются с согласия субъекта (п. 1 ст. 7 ЗРК «О персональных данных и их защите»), за исключением случаев, перечисленных в ст. 9 данного Закона (в частности, при оказании государственных услуг, осуществлении статистической или законной журналистской деятельности). Наличие надлежащего основания служит балансом между правом на частную жизнь и потребностями государства и бизнеса в обработке данных. В финансовом секторе Казахстана действует специализированный центр обмена данными по платежным транзакциям с признаками мошенничества (антифрод-центр Национального Банка Республики Казахстан [179]), обеспечивающий межведомственное взаимодействие организаций финансового рынка, операторов связи и правоохранительных органов при обработке сведений, включая обезличенные персональные данные. Правила центра предусматривают возврат средств на основании уведомления органа уголовного преследования, санкционированного прокурором. Вместе с тем в грифе согласования Генеральная прокуратура Республики Казахстан не указана, что потенциально указывает на институциональный пробел и требует оценки с точки зрения достаточности гарантий прав и свобод личности.

Помимо законности обработки через правовое основание, важным правовым инструментом защиты персональных данных является предварительная оценка воздействия на защиту персональных данных (далее - «оценка»). В ЕС процедура прямо закреплена: оценка проводится до начала обработки, когда предполагаемая обработка способна повлечь высокий риск для прав и свобод субъектов. Типичные признаки включают: 1) систематическую и обширную оценку личных аспектов (включая составление профилей); 2) крупномасштабную обработку особых категорий данных;

3) систематическое наблюдение за общественно доступными территориями в крупном масштабе; при сохранении высокого остаточного риска предусмотрена предварительная консультация с надзорным органом. Оценка включает описание операций обработки, анализ необходимости и соразмерности, выявление рисков и определение мер по их снижению. Данный превентивный механизм стал частью международной практики и постепенно интегрируется в национальные режимы вне ЕС. В Республике Казахстан специального требования об обязательной оценке воздействия законом не установлено. Вместе с тем с 2024 года введены процедурные правила уведомления уполномоченного органа о нарушении безопасности персональных данных в течение одного рабочего дня, а также механизм оповещения субъектов через инфраструктуру «электронного правительства», что усиливает риск-ориентированность надзора.

**Превентивные меры и защита персональных данных на этапе проектирования и по умолчанию.** На принципиальном уровне GDPR закрепляет принципы защиты персональных данных на этапе проектирования и по умолчанию (в английской версии: «*data protection by design and by default*»). Контролер должен проектировать процессы и системы так, чтобы по умолчанию обрабатывались лишь необходимые персональные данные и их доступ был ограничен целям обработки (ст. 25). На уровне реализации это подкрепляется обязанностью обеспечивать безопасность обработки с учетом риска (ст. 32), что включает, в числе прочего, шифрование персональных данных, управление доступом, регулярное тестирование и оценку эффективности мер безопасности, журналирование и план реагирования на инциденты. Закон РК об информатизации [98] требует, чтобы персональные данные хранились в базе данных, расположенной на территории РК (локализация), а также возлагает на собственника (и/или оператора) обязанность принимать меры по защите персональных данных по правилам, утвержденным правительством. С 2024 года действуют правила уведомления субъектов о нарушениях безопасности, а также установлен срок в один рабочий день для уведомления уполномоченного органа о факте нарушения. Дополнительно в РК действуют нормы взаимодействия с исследователями по информационной безопасности, создающие формализованный канал сообщений об уязвимостях и сроки их обработки, что усиливает превентивный характер мер безопасности [180]. В актуальной статистике отмечается ценность проактивных мер: по отчету IBM «Cost of a Data Breach Report 2025» [181] среднемировой размер ущерба от нарушения безопасности персональных в 2025 году составил 4,44 млн. долл. США (-9 % к 2024 г.), при этом организации без надлежащего управления ИИ чаще сталкивались с инцидентами и большими затратами.

**Принцип подотчетности.** Пункт 2 статьи 5 GDPR возлагает на контролера не только обязанность соблюдать принципы обработки, но и обязанность доказывать такое соблюдение. Практическая реализация включает поддержание надлежащей документации и процедур комплаенса: реестр операций обработки (ст. 30 GDPR), политики и регламенты, протоколы обучений, результаты аудитов/оценок, фиксацию согласий и пр. [182]. Этот массив доказательств предназначен для представления надзорному органу или суду и дополняется

общим режимом ответственности, включая административные штрафы (ст. 83 GDPR). Надзорные органы по защите персональных данных ожидают от организаций проактивного и проверяемого соблюдения требований, с подотчетностью, встроенной в проектирование и функционирование процессов.

В условиях широкого использования частной модерации контента и принятия автоматизированных решений особенно важно обеспечить прозрачность и проверяемость оснований для принятия соответствующих мер. Принятые решения должны сопровождаться раскрытием примененных критериев и обоснования, допускать возможность независимой проверки (аудита) и основываться на заранее установленных, прозрачных и доступных правилах (в том числе при использовании систем ИИ - обеспечивать объяснимость принятия решений [183, с. 399]). Такая модель обеспечивает соблюдение принципов законности, прозрачности, подотчетности, позволяет распределить обязанности между государством и онлайн-платформами, преобразуя модерацию в процесс, основания которого являются проверяемыми и который подлежит внешнему аудиту.

Показательно, что в деле Delfi AS v. Estonia ЕСПЧ признал допустимым возложение на владельцев интернет-ресурса ответственности за очевидно противоправные пользовательские высказывания и фактически ожидал от оператора превентивных и оперативных мер контроля (включая регистрацию пользователей, предварительную модерацию и ускоренный последующий обзор), оценив такое вмешательство как «обоснованное и соразмерное» ограничение свободы выражения по ст. 10 Конвенции ЕКПЧ [184]. Вместе с тем Март Суси обоснованно критикует данный подход за опору на общие правовые положения и перенос стандартов «традиционной печати» в сетевую (онлайн) среду, что снижает требование предсказуемости правового регулирования и создает неопределенность границ ответственности посредников [185, с. 298-301].

В РК уполномоченным органом в сфере персональных данных является Министерство искусственного интеллекта и цифрового развития РК (ранее - МЦРИАП). Его надзорные и контрольные полномочия закреплены законом и подзаконными актами, которые в 2023-2024 годах также ввели проверочные листы и процедуры уведомления о нарушениях безопасности [186]. Правоприменительная практика свидетельствует об учащении случаев привлечения к административной ответственности (в частности, по ст. 79 КоАП РК). Зафиксированы случаи наложения административных взысканий в виде штрафа в размере 100 МРП за факты неправомерного распространения персональных данных (включая дела, получившие общественный резонанс в 2024 г.), при этом о применении мер взыскания к ряду юридических лиц сообщалось и в 2021 году [187]. В целом принцип подотчетности представляет собой системный механизм контроля, интегрирующий иные элементы: наличие законных оснований обработки, оценку рисков, применение организационно-технических мер безопасности и способность контролера (оператора) продемонстрировать надлежащее управление рисками и соблюдение прав субъектов [188, с. 8-12; 189, с. 14-28].

**Проблемные аспекты и вызовы в сфере защиты персональных данных.** Несмотря на наличие развитого инструментария правового регулирования, на практике сохраняются существенные проблемные аспекты, требующие совершенствования правовых норм и подходов. Рассмотрим основные из них: 1) поручение обработки персональных данных и связанные с этим трансграничные передачи (аутсорсинг); 2) деятельность электронных торговых площадок; 3) цифровая идентификация (e-ID) и ее влияние на приватность; 4) роль цифровых следов.

**Поручение обработки персональных данных**. В условиях глобализации бизнес-процессов организации часто привлекают сторонние организации для обработки персональных данных - от облачных сервисов хранения до сторонних колл-центров и маркетинговых агентств. Такая передача функций может повышать эффективность, однако порождает юридические вопросы распределения ответственности и контроля. Согласно общей норме (в том числе закрепленной в ст. 28 GDPR и аналогичных правилах), если оператор поручает обработку персональных данных внешнему лицу (обработчику), то он обязан обеспечить, чтобы тот соблюдал все требования защиты этих данных, обычно через заключение соглашения об обработке персональных данных. Контролер (оператор) должен тщательно выбирать обработчика, предоставляющего достаточные гарантии принятия соответствующих технических и организационных мер для обеспечения безопасности обработки, и несет ответственность перед субъектом персональных данных за действия этого обработчика. Например, в России оператор вправе: поручить обработку иному лицу; лицо, обрабатывающее персональные данные по поручению оператора, не обязано получать отдельное согласие; оператор несет ответственность за его действия (чч. 4-5 ст. 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» [190]). Основание обработки (согласие либо иное из ч. 1 ст. 6) должно быть у оператора. По Закону РК «О персональных данных и их защите» общий принцип - сбор и обработка осуществляется собственником/оператором и третьим лицом с согласием субъекта, если не применяется исключение (п. 1 ст. 7; ст. 9). Согласие должно прямо указывать, допускается ли передача третьим лицам и/или за пределы РК (пп. 4), 5) п. 4 ст. 8). Договор между оператором и обработчиком (аутсорсером) должен предусматривать обязательство соблюдения конфиденциальности, применение надлежащих мер безопасности и осуществление обработки персональных данных только на основании документированных поручений оператора. Проблема возникает, когда персональные данные передаются за пределы национальной юрисдикции, т. е. трансгранично.

Риск повышается при передаче персональных данных за пределы юрисдикции, где уровень правовой защиты иной. В ЕС глава V GDPR требует либо решения об надлежащем уровне защиты (ст. 45), либо надлежащих гарантий (ст. 46), либо исключений (ст. 49). В ЕС эти правила строго соблюдаются и контролируются надзорными органами по защите персональных данных. Показателен прецедент с компанией Meta (Facebook). В 2023 году ирландский надзорный орган по защите персональных данных на основании

обязательного решения Европейского комитета по защите данных оштрафовал компанию Meta на 1,2 млрд. евро за систематическую трансграничную передачу персональных данных субъектов данных из ЕС в США в отсутствие надлежащих гарантий [191]. Компании было предписано приостановить передачу персональных данных и привести процессы в соответствие с главой V GDPR (требования к трансграничным передачам). Этот случай отметил, что поручение обработки или трансграничная передача персональных данных в юрисдикцию, не обеспечивающую адекватный уровень защиты (в данном случае - передача персональных данных субъектов данных из ЕС в США), может повлечь крайне серьезные правовые последствия для контролера (оператора) данных.

В Казахстане действуют собственные ограничения. Закон РК «О персональных данных и их защите» (ст. 16) допускает трансграничную передачу только при обеспечении защиты персональных данных иностранным государством. Если такой защиты нет, то возможны исключения: наличие согласия субъекта или случаи, предусмотренные международным договором, ратифицированным РК (пп. 1), 2) п. 3 ст. 16). Отдельно действует требование локализации хранения: персональные данные должны храниться в базах данных, размещенных на территории РК. С 2024 года введены правила уведомления субъектов о нарушениях безопасности персональных данных и срок один рабочий день для уведомления уполномоченного органа. Однако на практике контроль за трансграничными потоками данных остается сложной задачей. Многие субъекты предпринимательства используют облачные сервисы глобальных провайдеров, в результате чего персональные данные могут подвергаться трансграничной передаче в различные юрисдикции в режиме реального времени. Необходимость соблюдения национальных требований (вроде регистрации баз данных, уведомления регулятора) при этом нередко игнорируется. В итоге одним из уязвимых мест становится ответственность подрядчиков. Как отмечают специалисты, уязвимости в защите часто находятся не у самой компании-оператора, а у ее партнеров и поставщиков [192, с. 13, 27, 30]. Факты, получившие общественный резонанс, подтверждают этот тезис. Нарушения безопасности персональных данных зачастую являются следствием нарушения режима безопасности именно сторонних (внешних) информационных систем. Законодательство РК реализует меры по реагированию на вызовы: вводятся институты сертификации подрядчиков, стандартные пункты договоров, требования уведомлять заказчика о субподрядчиках. Тем не менее, риск «размывания» ответственности при договоре поручения обработки (аутсорсинге) остается проблемной зоной. Субъекту персональных данных зачастую затруднительно определить, кто именно несет ответственность за обработку его персональных данных, если в этом процессе участвуют несколько контролеров (операторов) и обработчиков (включая суб-обработчиков), находящихся в разных юрисдикциях. Для усиления защиты требуются более четкие механизмы трансграничного сотрудничества между надзорными органами и единые стандарты для обработчиков, что на глобальном уровне пока не достигнуто в полной мере.

**Международно-правовая ответственность государств за международно-противоправные деяния в сфере трансграничной обработки персональных данных.** В продолжение ранее изложенного анализа возникает необходимость рассмотреть, при каких условиях трансграничный инцидент, затрагивающий персональные данные, может квалифицироваться как международно-противоправное деяние государства. В общем виде проблема сводится к двум элементам. Во-первых, должно иметь место нарушение международно-правового обязательства (например, вмешательство в право на неприкосновенность частной жизни). Во-вторых, это деяние должно быть присвоено определенному государству. Сложность атрибуции в киберпространстве свидетельствует о необходимости международного правового регулирования глобальных информационных процессов. В доктрине обосновывается целесообразность «создания международного органа (организации) при ООН в целях правового урегулирования вопросов управления Интернетом» [3, с. 11].

Нарушения безопасности персональных данных, имеющие трансграничный характер, или неправомерный трансграничный сбор персональных данных способны повлечь нарушение норм международного права (в частности, обязательств в области прав человека) и потому при определенных обстоятельствах могут представлять собой международно-противоправные деяния. Однако для возложения ответственности необходимо установить присвоение этого деяния государству. Правила («механизм») присвоения как раз и отвечают на вопрос о том, когда поведение конкретных лиц или образований рассматривается в международном праве как деяние государства.

Правила присвоения поведения государству кодифицированы в Главе II Проекта статей об ответственности государств за международно-противоправные деяния [18], и ключевую роль для рассматриваемой темы составляют положения ст. 5, 6, 8.

Согласно ст. 5, поведение лица или образования, не являющихся органом государства, но уполномоченных правом этого государства осуществлять элементы государственной власти, рассматривается как деяние этого государства, если данное лицо или образование действовали в таком качестве. Иными словами, государство не может уклониться от ответственности, ссылаясь на то, что определенные действия совершил частный субъект, если этому субъекту были делегированы элементы государственной власти. Применительно к сфере персональных данных это означает, что если, к примеру, государственный орган Казахстана заключил договор с частной организацией на эксплуатацию системы, связанной с обработкой персональных данных субъектов (предположим, управление национальной базой данных или эксплуатация средств перехвата электронных коммуникаций), то действия этой организации при выполнении указанных функций рассматриваются в международном праве как действия самого государства. Таким образом, нарушение безопасности персональных данных или иная неправомерная их обработка, совершенные лицом (или образованием), которому государством

было делегировано осуществление элементов государственной власти, могут повлечь международную ответственность этого государства.

Статья 6 охватывает ситуацию, когда орган одного государства «помещается в распоряжение» другого и, действуя в осуществление элементов государственной власти этого другого государства, считается его органом. В таком случае поведение «предоставленного» органа присваивается принимающему государству. Простое сотрудничество или выполнение указаний без «помещения в распоряжение» подлежат оценке по критериям ст. 8. Если орган иностранного государства «помещен в распоряжение» Республики Казахстан и осуществляет полномочия государственной власти (например, при администрировании государственной базы данных), то его международно-противоправное деяние будет присваиваться РК (ст. 6 Проекта статей КМП ООН); если же такое «помещение в распоряжение» отсутствует, а поведение осуществляется лицом или группой лиц под руководством или контролем государства, то оценка присвоения проводится по критериям ст. 8 Проекта статей КМП ООН.

Статья 8 Проекта статей об ответственности государств регулирует присвоение действий частных лиц. Поведение лица или группы лиц присваивается государству, если они фактически действовали по его указаниям, под его руководством либо под его «эффективным контролем». Это принципиально важно для оценки квазигосударственных структур и ИКТ-инцидентов. Если будет доказано, что «независимая» группа действовала по прямым указаниям органов государства либо под их «эффективным контролем» над конкретной операцией, то ее поведение присваивается государству. Само по себе финансирование, обучение или общее покровительство являются недостаточными (для присвоения поведения). Данный строгий критерий «эффективного контроля» сформулирован и подтвержден в практике Международного суда ООН (дела Никарагуа против США, 1986 г.; Босния и Герцеговина против Сербии, 2007 г.).

Для полноты обзора следует сопоставить указанный подход международного права с ключевыми моделями регулирования персональных данных в различных юрисдикциях. В ЕС действует всеобъемлющий механизм защиты данных (GDPR), который устанавливает строгие требования к обработке персональных данных, включая трансграничную передачу. GDPR основан на признании права на защиту данных фундаментальным правом и распространяется экстерриториально на компании за пределами ЕС, если они обрабатывают данные субъектов, находящихся в ЕС. Тем самым в ЕС создана модель, где за трансграничные нарушения прежде всего несут ответственность частные операторы (контролеры) данных, привлекаемые к ответственности наднациональными или национальными надзорными органами, а государства-члены обязаны обеспечивать применение единых правил.

В Китайской Народной Республике, напротив, реализована модель «цифрового суверенитета», закрепленная в Законе КНР «О защите личной информации» 2021 года. Законодательство КНР делает акцент на государственном контроле за потоками данных: введены строгие ограничения на

передачу персональных данных за рубеж, требование локализации важных данных и механизм государственной оценки безопасности при трансграничной передаче. Таким образом, в КНР защита данных рассматривается сквозь призму национальной безопасности, и нарушения режима персональных данных могут повлечь серьезные санкции, при этом государство играет активную регулятивную роль (например, через Администрацию киберпространства КНР).

США пока придерживаются секторального подхода: отсутствует единый федеральный закон, сопоставимый с GDPR, вместо этого действует совокупность отраслевых актов (таких как HIPAA, COPPA, GLBA и др.) и нормативов отдельных штатов. В результате американская модель фрагментирована: трансграничная защита данных обеспечивается через механизмы передачи (например, предшествовавшие договоренности с ЕС, такие как Соглашение о защите конфиденциальности («Privacy Shield»)) и правоприменение со стороны регулирующих органов (в частности, Федеральной торговой комиссии) по отношению к корпорациям. Государство несет ответственность непосредственно за несоблюдение своих собственных международных обязательств (в том числе вытекающих из международных договоров о киберпреступности), однако отсутствие единого всеобъемлющего правового режима в данной сфере создает пробелы в регулировании трансграничных нарушений безопасности персональных данных.

Наконец, Рамочные программы АТЭС и ОЭСР представляют собой «мягкое право», ориентированное на регуляторную совместимость (гармонизацию подходов). АТЭС разработало Систему трансграничных правил защиты конфиденциальности, основанную на добровольной сертификации компаний, а ОЭСР предлагает Руководящие принципы. Эти инструменты не создают юридически обязывающих норм, но способствуют выработке совместимых стандартов и доверия между государствами.

В отличие от подхода Проекта статей об ответственности государств за международно-противоправные деяния, ориентированного на ответственность государства за правонарушение, модели ЕС, КНР, США и АТЭС/ОЭСР фокусируются преимущественно на оценке и снижении рисков и ответственности частных субъектов (контролеров/операторов). Тем не менее, все они учитывают роль государства как гаранта соблюдения правил: либо через надзор и наказание нарушителей (ЕС, КНР, отчасти США), либо через координацию принципов (ОЭСР/АТЭС). Сравнительный обзор указывает на отсутствие единого глобального режима защиты персональных данных, из-за чего в случае серьезных трансграничных инцидентов неизбежно встает вопрос об обращении к универсальным нормам международного права - таким, как институт ответственности государств.

Таким образом, применение норм международного публичного права об ответственности государств и обязательства должной осмотрительности формирует публично-правовой механизм (контур) обеспечения кибербезопасности, дополняющий частноправовые механизмы. Укрепление международно-правового сотрудничества и выработка подходов на основе консенсуса к вопросам присвоения поведения в связи с кибер-инцидентами

являются необходимыми условиями обеспечения (реализации) международно-правовой ответственности в глобальном информационном пространстве.

**Персональные данные на электронных торговых площадках (цифровых торговых платформах, выступающих в роли информационных посредников и обеспечивающих ИКТ-инфраструктуру для заключения и исполнения сделок между продавцами и покупателями), правовые проблемы сохранения конфиденциальности.** Развитие онлайн-платформ и электронных торговых площадок (пп. 58) ст. 1 ЗРК «О регулировании торговой деятельности») [193] создало новые вызовы в сфере защиты персональных данных. Электронные торговые площадки (мирового уровня как Amazon, eBay, Alibaba, AliExpress и проч., а также региональные аналоги) накапливают и обрабатывают значительное количество персональных данных пользователей: профили покупателей и продавцов, истории поиска и заказов, платежная информация, отзывы и проч. С одной стороны, оператор платформы выступает контролером (оператором) этих данных и должен соблюдать все требования закона о защите персональных данных. С другой стороны, многие персональные данные передаются сторонним продавцам, которые реализуют товары через платформу. То есть происходит своеобразное совместное использование персональных данных между множеством участников экосистемы [194; 195; 196].

Возникает вопрос: кто и в каких пределах вправе использовать эту информацию, и как обеспечивается согласие субъектов? Проблемной является практика, когда данные покупателей могут использоваться не только для исполнения конкретного заказа, но и для последующей прямой рекламы, иными продавцами или партнерами ЭТП, без явного на то согласия клиента. Например, покупатель, зарегистрировавшийся на ЭТП, может начать получать рекламные рассылки от десятков продавцов, которым ЭТП передала его контактные данные - налицо риск нарушения принципа целевого использования данных. GDPR требует в таких случаях либо раздельного сбора согласий (на передачу данных третьим лицам в маркетинговых целях), либо как минимум предоставления механизма простого отказа. Электронные торговые площадки обязаны прозрачно информировать пользователей, какие их данные и кому передаются. На практике же условия пользовательских соглашений часто сформулированы расплывчато, и средний потребитель не осознает, на что именно он соглашается.

Еще одна правовая проблема - обеспечение безопасности данных на ЭТП. Наиболее масштабные нарушения безопасности персональных данных за последние годы были связаны с информационными системами (базами данных), обеспечивающими предоставление услуг в электронной форме. Так, неправомерный доступ к резервной базе данных сети гостиниц Marriott привел к компрометации сведений до 500 млн. гостей (имена, контакты, номера паспортов, банковские карты) [197]. Кибер-атака длилась несколько лет до обнаружения, что указывает на трудности своевременного мониторинга в больших системах. Еще более масштабным был инцидент с Yahoo!, в результате которого неуполномоченные лица получили неправомерный доступ к персональным данным, связанным с 3 млрд. учетных записей - наиболее

масштабное нарушение безопасности персональных данных в истории на сегодняшний день. [198]. Эти примеры из международной практики значимы и для электронных торговых площадок, поскольку последние, по сути, оперируют аналогичными объемами разнородной информации о пользователях. Кроме внешних угроз информационной безопасности, существует риск внутренних злоупотреблений. Сотрудники ЭТП или недобросовестные продавцы могут незаконно использовать данные покупателей (например, анализировать ценовую информацию о конкурентах, используя личные данные клиентов конкурентных продавцов). Правовое регулирование деятельности электронных торговых площадок в настоящее время не содержит специализированных норм в области защиты персональных данных, помимо общих требований законодательства. Тем не менее, возникла тенденция к введению дополнительных обязанностей для крупных платформ. В ЕС усилены обязанности крупных онлайн-платформ двумя законодательными актами: Регламент (ЕС) 2022/2065 о цифровых услугах [199] и Регламент (ЕС) 2022/1925 о цифровых рынках [200]. Первый требует повышенной прозрачности рекламы и работы систем рекомендаций, запрещает адресную рекламу детям и использование чувствительных данных для персонализированной рекламы; для очень крупных платформ предусмотрена возможность выбора рекомендаций без учета профиля пользователей. Второй устанавливает запреты и обязанности для платформ, занимающих системообразующее положение на рынке, в том числе запрещает объединять персональные данные из разных сервисов без согласия и требует обеспечивать пользователю реальную альтернативу без персонализации.

В Казахстане [193; 201] и ряде стран СНГ [202; 203; 204; 205] специальное регулирование деятельности ЭТП и онлайн-платформ уже принято (*в РФ вступает в силу 01.10.2026 г.*) и продолжает развиваться, что свидетельствует о переходе от этапа обсуждения к их практической имплементации. На практике ЭТП остаются зоной повышенного риска нарушений безопасности персональных данных - любая уязвимость способна затронуть права миллионов (а в крупнейших экосистемах - свыше миллиарда [206]) пользователей, а сложные цепочки подрядчиков и распределенная инфраструктура затрудняют расследование инцидентов и установление ответственности.

**Цифровая идентификация (e-ID).** В последние годы государства и компании все активнее внедряют системы электронной (дистанционной) идентификации физических лиц, такие как цифровые удостоверения личности (включая сервисы цифровых документов), электронные паспорта, ID-карты и мобильные идентификаторы. Цифровая идентичность призвана облегчить получение услуг - как государственных (через порталы электронного правительства), так и коммерческих (электронные банковские услуги, дистанционная подписка договоров и т. п.). Однако распространение систем электронной идентификации актуализирует вопрос правовой защиты персональных данных в этих системах. Электронное удостоверение обычно привязано к обширному набору персональных данных: ФИО, дата и место рождения, ИИН или аналогичные номера, биометрические параметры (фото, отпечатки пальцев), а также к цифровому следу действий владельца (история

авторизаций, транзакций, запросов в реестры). Уязвимость в системе цифровой идентификации может привести к катастрофическим последствиям - от неправомерного распространения персональных данных до подделки данных личности для совершения преступлений [207, с. 20; 208, с. 77].

Проблемные аспекты двоякие: во-первых, правовая незащищенность инфраструктуры электронной идентификации от технических сбоев и нарушения безопасности персональных данных; во-вторых, опасность чрезмерной концентрации данных о физических лицах в одной системе. Известны случаи, когда централизованные (единые) базы персональных данных становились объектом неправомерного доступа или иных противоправных посягательств. Например, в 2018 году в Индии произошел скандал вокруг системы Aadhaar [209] - национальной системы биометрической идентификации. Журналисты выяснили, что персональные данные 1,1 млрд. индийцев, хранящиеся в этой системе, возможно было получить в сети всего за 8 долл. США из-за недостатков в защите базы данных. Это вызвало волну критики и пересмотр правовых режимов доступа к системе Aadhaar [210].

В ЕС действует Регламент об электронной идентификации, аутентификации и доверительных услугах (Регламент (ЕС) 910/2014 - eIDAS [211]), устанавливающий требования к доверенным электронным идентификационным схемам, включая меры безопасности и криптографической защиты. Однако даже в развитых юрисдикциях время от времени случаются технические сбои государственных информационных систем. В Эстонии государство вынуждено было приостановить электронные сертификаты сотен тысяч ID-карт из-за уязвимости, что временно нарушало работу цифровой идентификации и сервисов [212].

В 2025 году веб-портал «электронного правительства» РК (eGov.kz) был периодически недоступен из-за технических неполадок, приводящих к недоступности получения цифровых услуг [213]. Подобные инциденты (включая технические сбои в функционировании систем) не обязательно связаны с неправомерным распространением данных, но актуализируют проблему обеспечения правовой и технической надежности и устойчивости инфраструктуры электронной идентификации. Если лицо полностью зависит от сервиса цифровых документов, то сбой в функционировании соответствующей информационной системы (ее недоступность) лишает его возможности подтвердить свою личность и воспользоваться услугами, что существенно ограничивает реализацию его прав и законных интересов. С учетом рисков нарушения безопасности электронных идентификаторов регулирование должно: 1) предусматривать альтернативные способы идентификации на случай недоступности основного сервиса электронной идентификации; 2) возлагать на собственников и операторов обязанность обеспечивать устойчивость и бесперебойность сервисов (резервирование, отказоустойчивость, восстановление); 4) устанавливать усиленную правовую ответственность за неправомерные операции с электронной подписью и иными идентификаторами, а также обязанность немедленно уведомлять уполномоченный орган и субъектов при возникших инцидентах. В Казахстане часть этих элементов уже реализована:

действует простая электронная подпись как альтернативный механизм идентификации (ст. 20-1 Закона «Об информатизации»); установлены требования к резервированию и защите объектов информатизации (в т. ч. ст. 42); с 2024 года введены правила уведомления субъектов и срок 1 рабочий день для уведомления уполномоченного органа; с 13 марта 2025 года введены штрафы за использование ЭЦП другого лица (ч. 6 ст. 640 КоАП РК); действует программа взаимодействия с исследователями в сфере информационной безопасности для государственных информационных систем. В то же время остаются законодательные пробелы. Отсутствует прямо установленная обязанность проводить оценку воздействия на защиту персональных данных для обработок высокого риска. Отсутствуют единые процедуры резервной идентификации на случай отказов основных средств. Унифицированные требования к сертификации/аудиту подрядчиков в частном секторе развиты недостаточно. Механизмы организованного раскрытия уязвимостей пока ограниченно охватывают коммерческие платформы.

Дополнительная сложность - это необходимость защиты биометрических данных, которые широко используются в электронной идентификации (сканы лица, сетчатки, голосовые образцы). Биометрические данные обладают уникальностью и высокой степенью неизменности. Вследствие этого, нарушение их безопасности (включая неправомерное распространение) носит необратимый характер, поскольку в отличие от иных аутентификационных данных (например, пароля), субъект персональных данных не может их заменить. Законы многих стран (включая Казахстан) относят биометрические данные к категории чувствительных персональных данных, требуя для их обработки повышенных гарантий (прямого согласия, специальной охраны). Тем не менее, на практике обеспечение конфиденциальности биометрии достигается с трудом - любой сбой может раскрыть эти данные. В ряде стран произошли кражи биометрических данных [214] из баз данных банков и визовых центров, что заставило регуляторов пересмотреть требования к хранению таких данных (например, обязательное шифрование на уровне аппаратных модулей, раздельное хранение биометрических шаблонов и личных сведений и т. д.). Таким образом, электронная (дистанционная) идентификация повышает доступность услуг, но актуализирует правовые вопросы, связанные с необходимостью гарантировать защиту персональных данных и неприкосновенность частной жизни субъекта в цифровой среде. Требуются комплексные подходы [215, с. 3, 5-8], сочетающие технические стандарты кибербезопасности [216, с. 21-53; 217, с. 13-15] и юридические гарантии, включая международное сотрудничество в этой сфере [218], поскольку операторы угроз могут действовать в трансграничном масштабе, осуществляя кибератаки на национальные системы электронной идентификации вне зависимости от их местонахождения.

**Значение цифровых следов в управлении рисками.** Важным элементом современных правовых технологий защиты данных становятся цифровые следы: разнообразные записи и журналы событий (лог-файлы), автоматически фиксирующие операции с персональными данными. Речь идет не о данных как таковых, а о метаданных процессов: кто и когда получил доступ к информации,

какие действия выполнил (просмотр, копирование, изменение), с какого устройства и IP-адреса и т. д. Надлежащий сбор и анализ журналов аудита (логов событий) позволяют решить две задачи: во-первых, способствовать обеспечению подотчетности и прозрачности обработки, а во-вторых, своевременно обнаруживать инциденты безопасности (включая утечки персональных данных) или несанкционированный доступ к данным. Многие нормативные акты прямо или косвенно требуют ведения таких журналов. Например, государственные информационные системы Казахстана обязаны регистрировать все обращения к охраняемым персональным данным и хранить эти журналы в течение установленного срока [97; 219; 220].

В корпоративных политиках информационной безопасности журналирование операций с персональными данными стало стандартом. Информационные системы управления данных осуществляют ведение журналов (лог-файлов), а системы предотвращения неправомерного распространения данных фиксируют попытки неправомерной передачи конфиденциальной информации. Цифровой след выступает своего рода «черным ящиком» (в английской версии: «*black box»* [221]) системы защиты данных - в случае неправомерного распространения или нарушения он позволяет ретроспективно выяснить, что произошло. Кроме того, накопленная статистика обращений к данным помогает управлять рисками проактивно. Так, в ходе анализа журналов событий могут быть выявлены факты, когда работник систематически осуществляет копирование баз, содержащих персональные данные клиентов, на внешние накопители информации. Это служит индикатором риска для уполномоченного подразделения (службы) информационной безопасности и позволяет принять превентивные меры по недопущению неправомерного распространения данных.

В научной литературе отмечается возрастание роли цифровых следов как фактора безопасного обращения с персональными данными в сфере ИКТ [1, с. 82; 222, с. 194-198; 223, с. 166]. Исследователи предлагают развивать специальные правовые режимы работы с цифровыми следами: стандартизировать требования к их формату, обеспечивать их неизменность (например, с помощью блокчейн-технологий или электронных подписей в журналах (лог-файлах)), а также урегулировать порядок доступа к ним для целей комплаенса и расследования инцидентов. В ранее приведенной статье М. С. Бисалиева и К. Н. Шакирова введено авторское определение цифровых следов и предложен алгоритм выявления способов посягательств на персональные данные с помощью анализа таких следов, включая типичные фазы компьютерных атак и действий нарушителя. В частности, исследователи выходят с инициативой принятия международного или по крайней мере регионального акта, устанавливающего стандарты использования специальных познаний при обнаружении несанкционированного доступа к персональных данным, включая перехват данных в интернете. Возможно предположить, что такой закон закрепил бы единый подход к фиксированию и анализу цифровых следов во взаимодействии разных юрисдикций. С точки зрения управления рисками в организациях, цифровые следы интегрируются в программу защиты

как средство мониторинга и аудита. Надзорные органы все чаще проверяют ведение оператором (контролером) надлежащих журналов событий (лог-файлов), поскольку это является частью реализации принципа подотчетности. В случае инцидента информационной безопасности наличие детализированных журналов событий (аудиторских следов) может рассматриваться как смягчающее обстоятельство, поскольку это свидетельствует о принятии собственником и (или) оператором надлежащих мер по защите персональных данных и способствует оперативному уведомлению субъектов персональных данных и уполномоченного органа о масштабах инцидента. Таким образом, журналы аудита (лог-файлы событий) выступают в качестве инструмента в правовой системе защиты персональных данных, позволяющего осуществлять мониторинг соблюдения установленных правил и реагировать на инциденты (отклонения).

**Инциденты в сфере защиты персональных данных и необходимость совершенствования правового регулирования.** Рассмотренные проблемные аспекты не являются теоретическими - их значимость подтверждается фактами неправомерного распространения персональных данных и нарушений, которые получили огласку в последние годы. Обращение к таким примерам международной и национальной практики позволяет выявить уязвимые места действующих режимов и стимулировать реформы.

В глобальном масштабе число нарушений безопасности персональных данных продолжает расти значительными темпами. Уже упоминалось неправомерное распространение данных 3 млрд. пользователей Yahoo! (2013-2016 гг.), ставшая рекордной. В последующем десятилетии масштабные компрометации случались практически ежегодно: так, в 2017 году произошло нарушение безопасности персональных данных в кредитном бюро Equifax (США), затронувшая личные сведения примерно 147 млн. человек (почти каждый второй взрослый американец); в 2018 году - 500 млн. записей гостей сети гостиниц Marriott; в 2019 году - серия нарушений безопасности у технологий онлайн-платформ (например, данные 533 млн. пользователей Facebook оказались выложены в открытый доступ в 2021 году вследствие автоматического сбора данных (парсинга) и недостатков защиты программных интерфейсов приложений (в английской версии: *Application Programming Interface - API* [224]). Статистика неутешительна - по данным Центра ресурсов по краже личных данных (ITRC), в США в 2024 году зафиксировано 2 850 нарушений (всего 3 158 инцидентов). Число уведомлений, направленных пострадавшим субъектам персональных данных, выросло на 211 % в результате нескольких масштабных нарушений. 2024 год - почти рекордный, но уступает 2023-му на 44 события [225]. Это свидетельствует о том, что существующие меры защиты зачастую оказываются недостаточными перед лицом все более изощренных атак. Для правовой системы такой вызов означает необходимость постоянного обновления стандартов безопасности и ужесточения ответственности за их несоблюдение, чтобы побудить компании инвестировать в защиту. Практика GDPR в ЕС уже демонстрирует высокие штрафы: помимо рекордного штрафа для Meta (2023 г.) за незаконную передачу данных, крупные санкции налагались на Google

(50 млн. евро штрафа во Франции в 2019 году за непрозрачность обработки и недостаток оснований для персонализированной рекламы) и Amazon (746 млн. евро штрафа в Люксембурге в 2021 году за нарушения порядка получения согласия на cookie-файлы). Эти случаи относятся к нарушениям комплаенс-режима, когда компании не применяли установленные правила обработки. С одной стороны, миллиардные штрафы привлекают внимание и служат серьезным стимулом к изменению бизнес-практик. С другой стороны, они подчеркивают проблемные моменты их правового регулирования: например, кейс Amazon выявил неясности в трактовке требований к согласию на обработку онлайн-идентификаторов, что требует разъяснений на уровне ЕС.

В Республике Казахстан последние годы также отмечены инцидентами, свидетельствующими о необходимости повышения эффективности правового регулирования защиты персональных данных. Наиболее масштабным стало нарушение безопасности персональных данных, затронувшее 16 млн. субъектов в Республике Казахстан, произошедшее в июне 2025 года - беспрецедентный по масштабу инцидент, затронувший практически все население страны [226]. В анонимных Telegram-каналах была распространена база данных, содержащая персональные данные физических лиц: ФИО, даты рождения, ИИН, абонентские номера телефонов (мобильные, рабочие, домашние), адреса и иные сведения. Данный инцидент выявил ряд проблем. Во-первых, отсутствие надлежащего контроля за дальнейшим оборотом персональных данных, ранее полученных в результате нарушений. Если персональные данные, скомпрометированные в результате предшествующих нарушений безопасности, продолжают незаконно распространяться и остаются доступными неопределенному кругу лиц (продолжают использоваться), то это свидетельствует о неэффективности существующих механизмов реализации права субъектов на уничтожение (стирание) своих персональных данных (включая «право на забвение»). Во-вторых, стало очевидно, что субъектам персональных данных необходимо предоставлять инструменты самозащиты (такие как проверки через NomadGuard [227]) и повышать их информированность. В-третьих, инцидент актуализировал вопрос об ответственности должностных лиц государственных органов за необеспечение надлежащей защиты персональных данных. Из данной ситуации следует вывод о том, что если источником нарушения безопасности значительной части этих данных являются уязвимости в государственных электронных информационных ресурсах (базы данных), то это указывает на необходимость принятия соответствующих организационных мер и совершенствования системы защиты персональных данных в государственном секторе.

Другие инциденты также свидетельствуют о наличии системных недостатков (уязвимостей). В марте 2024 года Государственной технической службой (ГТС) было выявлено нарушение безопасности персональных данных, затронувшее более 2 млн. клиентов одной из микрофинансовых организаций. [16]. Вероятно, уязвимость была связана с недостаточной защищенностью внешней информационной системы, посредством которой оформлялись договоры займа (микрокредиты). Этот пример вновь показывает риск при

привлечении сторонних «финтех-платформ» к обработке чувствительных данных. Еще один компонент - технические сбои государственных информационных систем. Периодическая недоступность веб-портала «электронного правительства» (eGov.kz) затрудняет получение услуг. Нормативные акты уже предусматривают, что при техническом сбое информационной системы срок рассмотрения электронного запроса услугодателем продлевается на время устранения неполадки, однако это правило относится к сроку органа, а не к срокам заявителя [228]. Для последнего следует предусмотреть (и/или шире применять) компенсационные регламенты - автоматическое продление/восстановление пользовательских сроков при документированном сбое и единый порядок фиксации инцидента (логирование, уведомление). Пока восстановление пропущенного срока для заявителя решается по общим правилам как «уважительная причина» (ст. 92 АППК РК [229]).

Все перечисленные вызовы, такие как поручение обработки персональных данных (аутсорсинг), функционирование электронных торговых площадок, распространение систем электронной идентификации и нарушения безопасности персональных данных, свидетельствуют о необходимости постоянной адаптации правового режима защиты персональных данных к динамичным технологическим и организационным изменениям. Международные и национальные механизмы уже сформировали прочную основу (принципы, процедуры, институты ответственности), однако правоприменительная практика выявляет недостатки, требующие дальнейшего совершенствования. Необходимо дальнейшее сближение подходов на глобальном уровне: например, гармонизация правил для трансграничных обработок (возможно, через универсальные соглашения или присоединение большего числа стран к Конвенции 108+ Совета Европы). Требуются специальные правила для новых сфер - тех же ЭТП и цифровой идентичности - которые бы учли их особенности. В научной доктрине предлагается разрабатывать единую концепцию правовых инструментов защиты персональных данных, объединяющую лучшие практики разных дисциплин. Междисциплинарный подход (правовой, технологический, этический) позволит выработать более эффективные решения. В конечном счете, цель всех усилий - использовать личную информацию так, чтобы права человека были надежно защищены, а информационное пространство оставалось безопасной и доверительной средой для всех участников.

*Таким образом,* по итогам анализа правовых инструментов и проблемных аспектов защиты персональных данных возможно сформулировать следующие выводы.

Современное международно-правовое регулирование обработки персональных данных характеризуется переходом к риск-ориентированному подходу и превентивным механизмам обеспечения комплаенса. Ключевыми инструментами выступают принципы подотчетности, защиты персональных данных на этапе проектирования и по умолчанию, а также процедура оценки воздействия на защиту персональных данных. Принцип подотчетности

модифицирует модель регуляторного надзора, возлагая на оператора (контролера) бремя доказывания соблюдения им установленных норм.

Эффективность правового инструментария снижается под воздействием глобальных технологических вызовов. К существенным проблемным аспектам относятся: сложности в разграничении ответственности в сложных цепочках обработки персональных данных (в частности, между операторами (контролерами) и обработчиками), а также коллизии юрисдикций при трансграничной передаче персональных данных. Это существенно затрудняет экстерриториальное правоприменение и контроль за соблюдением императивных норм, включая требования о локализации данных.

В международно-правовом аспекте установлено, что трансграничные нарушения в сфере обработки персональных данных при наличии критериев атрибуции (делегирование публичных функций, эффективный контроль) могут квалифицироваться как международно-противоправные деяния государства (согласно Проекту статей КМП ООН). Это актуализирует обязанность государств по проявлению должной осмотрительности для предотвращения трансграничного вреда и укреплению механизмов международного сотрудничества.

Деятельность онлайн-платформ, электронных торговых площадок и внедрение систем цифровой идентификации (e-ID) порождают системные риски, связанные с концентрацией данных и уязвимостью централизованной инфраструктуры. Это требует внедрения специализированных правовых режимов (по аналогии с DSA/DMA в ЕС) и повышенных гарантий безопасности, включая защиту биометрических данных и обеспечение устойчивости сервисов.

Анализ правоприменительной практики и масштабных инцидентов нарушения безопасности данных (включая инциденты в Республике Казахстан в 2024-2025 гг.) свидетельствует о наличии пробелов в национальном регулировании, в частности, отсутствии обязательной процедуры оценки воздействия на защиту персональных данных для высокорисковых обработок и недостаточной эффективности механизмов контроля за третьими лицами (обработчиками).

Отметим, что стремительное развитие технологий порождает новые вызовы правовому регулированию. В подразделе 2.3 анализируются стратегические проблемы - влияние технологий искусственного интеллекта и явления «нормативной турбулентности» на правовой режим персональных данных.

## 2.3 Стратегические вызовы для правового режима защиты персональных данных: искусственный интеллект и «нормативная турбулентность»

В данном подразделе проводится международно-правовой анализ стратегических вызовов, связанных с ИИ и защитой персональных данных, включая сравнительный обзор подходов ЕС, Китая и Казахстана, концепцию «самонормативности» (в английской версии: «*self-normativity*»**)** цифровых участников, а также трансформацию соотношения первичных и вторичных норм

(в контексте теории Г. Л. А. Харта [130, с. 79-123]) под влиянием цифровизации. В цифровой среде наблюдается изменение иерархии норм: предписания, носившие вспомогательный характер (например, принципы прозрачности и подотчетности), приобретают фундаментальное (материальное) значение и становятся обязательными условиями законности обработки данных (субстантивизация процедурных гарантий). Отдельное внимание уделено новейшим инициативам Казахстана по регулированию ИИ и оценке правовых рисков, вытекающих из опережающего внедрения ИИ. В заключение обосновывается необходимость международно-правовой координации и гибкости нормативных инструментов, а также включения этико-правовых ориентиров в цифровую политику для преодоления «нормативной турбулентности». Указанные выводы логически подводят к разработке критериев эффективности правового регулирования и практических мер по достижению этой эффективности, что составляет предмет раздела 3.

Современное международное право сталкивается с беспрецедентной «нормативной турбулентностью» в цифровой сфере. Как справедливо отмечается в современной доктрине, доверие к автоматизированным решениям в сфере информатизации по существу не учитывает критерий нормативной справедливости, в отличие от судьи, способного в исключительных ситуациях отказаться от применения несправедливой нормы. Искусственный интеллект по своей конструкции исходит из презумпции корректности позитивного правила и выступает, образно говоря, крайним позитивистом (*по состоянию на 2025 год, по мнению автора диссертационного исследования*) [230, с. 234]. Это порождает несогласованность между логикой защиты прав человека и машинным правоприменением, пока системы не обретают способность к самостоятельному неприменению несправедливых правил. В научной литературе предлагается отказаться от акцента на «машинной этике» как самоцели - заложенные в алгоритм моральные правила сами по себе не обеспечивают гарантий правомерного функционирования сложных систем [231, с. 390]. Вместо этого обосновывается развитие «инженерии безопасности ИИ», ориентированной на проверяемую безопасность и соответствие правовым требованиям, включая режимы изоляции, независимый аудит и сертификацию систем. Именно такой подход к верификации и «коллективному аудиту» систем разделяет главный ученый по ИИ компании Meta, лауреат премии Тьюринга Ян Лекун, продвигающий «открытые платформы» (в английской версии: «*open-source*» [232]), подобные «большим языковым моделям» Meta AI 2 (в английской версии: *Large Language Model Meta AI, версия 2* [233]). По его мнению, опасность заключается не столько в самой технологии, сколько в ее монополизации. Концентрация власти у ограниченного числа субъектов, контролирующих закрытые, частные системы, представляет собой значительно более серьезную угрозу глобальной безопасности и демократическим институтам, чем риски, связанные с «открытыми релизами» и публичной проверяемостью [234]. Однако этот тезис об «открытых релизах» (программное обеспечение с открытым кодом) как главном инструменте обеспечения безопасности является предметом фундаментальных разногласий. Прямо оппонируя данному подходу, другой

лауреат премии Тьюринга, Йошуа Бенжио, приравнивает риски неконтролируемого ИИ к экзистенциальным угрозам, сопоставимым с катастрофическими [235] и призывает к повышенному регулированию мощнейших моделей (включая ограничения на «открытые релизы»), о чем свидетельствуют его публичные заявления и международный научный доклад под его председательством [236]. С этой точки зрения открытое распространение наиболее мощных систем следует рассматривать не как решение, а как фактор возможной эскалации угроз, что обосновывает необходимость более повышенных регуляторных мер и многосторонних механизмов надзора. При этом существующие подходы к оценке и сертификации на текущем этапе остаются недостаточно зрелыми для надежного предотвращения катастрофических рисков. Вместе с тем сам Международный научный доклад по безопасности ИИ носит информационно-аналитический характер и не формулирует конкретных политических рекомендаций [237, с. 184-190]. Приведенный выше вывод представляет собой научно обоснованную интерпретацию выявленных рисков и пробелов в методиках. Позицию о «потере контроля» как о реальной угрозе разделяет и третий лауреат премии Тьюринга из этой группы, Джеффри Хинтон. По его мнению, фундаментальная уязвимость заключается в том, что системы могут начать «автономно писать собственный компьютерный код для модификации самих себя» и, обладая непревзойденными способностями к манипуляции, «выйти из-под контроля» человека. Проводя прямую параллель с разработкой ядерного оружия и деятельностью Р. Оппенгеймера, Дж. Хинтон призывает к международному договору о запрете автономных боевых систем о запрете автономных боевых систем (в английской версии: *«world treaty to ban the use of military robots»*) [238].

Стремительное развитие ИИ и глобальных цифровых платформ создает эти самые разрывы между технологической реальностью и способностью государств вырабатывать устойчивые правовые нормы [239, с. 24-27; 240, с. 47-48; 241, с. 12; 242, с. 4]. Возникают ситуации, когда технические стандарты и корпоративные правила фактически подменяют собой государственное (публично-правовое) регулирование, а национальные регуляторные режимы вступают в сложное взаимодействие и даже в коллизию друг с другом. Следует отметить, что в США отсутствует единый закон о защите персональных данных - действует совокупность отраслевых норм и множество регуляторов [53]. Попытка ЕС и США сблизить стандарты через механизм «Щит конфиденциальности ЕС-США» была аннулирована Судом ЕС в решении Schrems II (июль 2020 г.) [243]. В июле 2023 года появилась новая Рамочная программа ЕС-США по защите данных, однако указанные события демонстрируют фрагментацию нормативных подходов и указывают на необходимость дальнейшей гармонизации на международном уровне.

Показательно, что при отсутствии единого федерального законодательного акта в США формируется подход к регулированию инвазивных идентификационных технологий на уровне штатов: в ряде штатов (начиная с Висконсина (2005 г.) и Калифорнии (2007 г.), а также Арканзаса, Невады, Северной Дакоты, Миссури и Оклахомы) приняты запреты на принудительную

имплантацию микрочипов как посягательство на «телесную неприкосновенность» (в английской версии: *«bodily integrity»*) и как действие, выходящее за пределы допустимых в рамках трудовых отношений [244, с. 249-251]. Одновременно статистический анализ поисковых трендов по темам «чипирование человека» (в английской версии: *«human chipping»*) и «дополненные люди» (в английской версии: *«augmented humans»*) показывает их долговременную взаимосвязь (коинтеграцию), что указывает на устойчивую регуляторную значимость данной проблематики для цифровой политики.

Для преодоления эффекта «нормативной турбулентности» необходимо внедрять технологически нейтральные подходы к регулированию и механизмы опережающего реагирования. Законодателю необходимо осуществлять постоянный мониторинг развития новых цифровых технологий, оперативно адаптировать правовые нормы и укреплять международное сотрудничество в данной сфере, с целью обеспечения адекватности правового регулирования темпам технологических инноваций [245, с. 103-104]. В этой связи показателен и межгосударственный консенсус. Согласно Тяньцзиньской декларации ШОС от 1 сентября 2025 года, государства признают равное право на развитие ИИ и берут курс на совместное предотвращение рисков, направленное на устойчивое повышение безопасности, прозрачности и справедливости его применения во благо человечества [246, с. 16].

Возникают пробелы и коллизии в правовом регулировании, обусловленные отставанием процесса правотворчества от высоких темпов технологических инноваций. В этих условиях особое значение приобретает «мягкое право» - совокупность юридически не обязательных норм, рекомендаций и принципов, разрабатываемых международными организациями и иными участниками международных отношений. Мягкое право обеспечивает гибкость и оперативность реагирования на технологические вызовы: принципы и руководства согласовываются быстрее, чем договоры или законы, и их легче обновить по мере развития технологий. Тем самым мягкое право создает временные ориентиры для участников цифровых отношений, снижая неопределенность и способствуя преодолению разрыва между темпами инноваций (технического прогресса) и законодательного процесса. В условиях нормативной турбулентности мягкое право играет стабилизирующую роль, выступая временным этико-правовым ориентиром. Одним из первых и наиболее влиятельных примеров такого подхода стала Окинавская Хартия глобального информационного общества (2000 г.) [6]. Принятая в период становления глобальной сети, когда многие правовые режимы еще не были сформированы, Хартия определила базовые ценности и направления для международного сотрудничества. Задолго до появления детализированных режимов, таких как GDPR, в Хартии было отмечено внимание на необходимости баланса между свободным потоком информации и защитой фундаментальных прав, включая приватность. Этот документ продемонстрировал, как политические декларации могут задавать вектор для последующего нормотворчества в условиях высокой неопределенности.

**Ключевые механизмы мягкого права в сфере ИИ и защиты персональных данных.** В сфере ИИ и управления данными на глобальном уровне сформирован ряд знаковых актов мягкого права. ОЭСР еще в 1980 году приняла Основные положения, регулирующие защиту неприкосновенности частной жизни и международные обмены персональными данными (пересмотрены в 2013 г.) - первый международный свод принципов приватности [160, с. 3]. Этот документ оказал огромное влияние на национальное законодательство: с момента его принятия базовые принципы легли в основу законов о защите данных во многих странах. В 2019 году ОЭСР утвердила Рекомендацию по искусственному интеллекту, одобренную изначально 42, а по состоянию на август 2025 года - 48 странами [247, с. 3]. В них закреплены ключевые требования к ИИ-системам: технологии должны уважать права человека и демократические ценности, обеспечивать прозрачность, безопасность, подотчетность и служить инклюзивному устойчивому развитию [248, с. 12]. Одновременно государствам рекомендовано инвестировать в исследования ИИ, формировать инклюзивную экосистему, развивать человеческий капитал и международную координацию.

ЮНЕСКО в ноябре 2021 года приняла всеобщую Рекомендацию по этике ИИ - первый глобальный стандарт этических принципов для новых технологий [249, с. 5]. Документ провозглашает ряд фундаментальных ценностей: уважение прав человека, инклюзивность, устойчивое развитие, справедливость общества и переводит их в конкретные принципы (пропорциональность, безопасность, конфиденциальность, человеческий контроль и др.), сопровождая их детальными мерами реализации по сферам политики [249, с. 14-38]. Рекомендация ЮНЕСКО по этике искусственного интеллекта, не создавая юридически обязательных норм, стала первым глобальным стандартом в этой сфере [250, с. 18-19]. В ноябре 2021 года документ единогласно поддержали все 193 государства, входившие на тот момент в ЮНЕСКО. На текущий момент уже 194 государства-члена, включая вновь присоединившиеся в 2023 году США, руководствуются этим документом, и многие из них активно его внедряют. Республика Казахстан, как государство-член ЮНЕСКО, участвует в профессиональном диалоге и практическом сотрудничестве по вопросам этики ИИ в контексте рекомендации ЮНЕСКО 2021 года, включая обсуждение ее практической значимости для страны и возможности применения методики «оценки готовности» к этичному использованию ИИ [251; 252].

К числу значимых актов мягкого права относится также документ, известный как Мадридская резолюция (в английской версии: *International Standards on the Protection of Personal Data and* Privacy, 2009 г.) - согласованный набор международных стандартов защиты персональных данных и частной жизни, принятый на 31-й Международной конференции комиссаров по защите данных [253, с. 1, 3]. В данной Резолюции были закреплены основные принципы (прозрачность, ограничение цели, пропорциональность, подотчетность и др.), и она служила ориентиром для государств при разработке национальных правовых режимов и для организаций при формировании корпоративных политик.

Всемирный экономический форум (ВЭФ) - влиятельная негосударственная площадка, которая разрабатывает добровольные стандарты и руководства для цифровой сферы. ВЭФ продвигает концепцию «ответственного управления данными» (в английской версии: «*data stewardship»*) и модели «доверительных» структур для обмена данными (например, модели доверительного хранения данных). Форум предлагает решения и подходы для повышения доверия (например, подходы этичного использования данных, акцентирующие прозрачность, справедливость и конфиденциальность [254, с. 3]) и формирует добровольные принципы для ИИ (включая корпоративные кодексы этики), побуждая бизнес к саморегулированию до введения государственных норм. Такие подходы мягкого права фактически создают стандарты поведения и дорожную карту для отрасли.

Региональным примером мягкого регулирования является Система трансграничных правил конфиденциальности АТЭС (в английской версии: *APEC Cross Border Privacy Rules System - CBPR*), одобренная в 2011 году в рамках Азиатско-Тихоокеанского экономического сотрудничества [93, с. 1-3]. Она представляет собой добровольную программу сертификации на соответствие принципам АТЭС по конфиденциальности и безопасности данных. Механизм построен на принципе подотчетности: присоединившиеся организации обязуются выполнять утвержденные правила, их практики проверяются аккредитованными аудиторами, а соблюдение требований контролируется национальными надзорными органами. Хотя документ не является международным договором, он фактически обеспечивает взаимное признание стандартов приватности организаций разных юрисдикций и облегчает трансграничный поток данных.

Инструменты мягкого права нередко преобразуются в положения, имеющие обязательную силу. Международные принципы и руководства часто кодифицируются в национальных законах. Классический пример - Основные положения ОЭСР 1980 года, которые повлияли на законодательство ЕС (Директива 95/46/ЕС, затем GDPR) и многих других стран, установив базовый набор требований к обработке данных. Те положения, что изначально были добровольными - прозрачность, ограничение цели, ответственность, со временем превратились в обязательные юридические требования и условия законности обработки персональных данных. В цифровую эпоху мы видим, как рекомендации становятся нормами - если принципы открытости и подотчетности, прежде были факультативными, то теперь провозглашаются обязательными условиями законности обработки данных.

В сфере ИИ влияние мягкого права также существенно. Принципы ОЭСР по ИИ послужили ориентиром при разработке политики ЕС. Еще до принятия законодательства ЕС выпустил добровольные руководства по этичному ИИ (2019 г.), во многом основанные на тех же ценностях. Эти идеи легли в основу проекта Регламента ЕС об ИИ [255], который преобразовал многие ранее добровольные требования (например, оценка рисков, обеспеченность человеком контроля) в юридические обязанности. В США, напротив, пока сохраняется «мягкий» подход: государство выпускает рекомендательные стандарты

(например, Руководство NIST AI 100-1 по управлению рисками ИИ [256, с. 2, 42]), а многое отдано саморегулированию. Лишь в 2023 году федеральные власти инициировали шаги к правовому контролю ИИ, но параллельно были оформлены и механизмы мягкого права. Так, в 2023 году крупные организации публично взяли на себя добровольные обязательства по содействию разработке безопасному и этичному ИИ [257]. Подобные соглашения, сохраняя рекомендательный характер, фактически формируют основу для последующего нормативного закрепления. Другие страны также делают ставку на гибкие нормы: например, Япония ограничивается выпуском рекомендаций вместо закона о ИИ [258]. Такой подход позволяет оперативно обновлять рекомендации и вовлекать бизнес в выработку правил, прежде чем закрепить их на законодательном уровне.

Для Республики Казахстан механизмы мягкого права могут служить временными стандартами на этапе, предшествующем принятию всеобъемлющих нормативных актов об ИИ и данных. Это предполагает, во-первых, интеграцию международных принципов - закрепление на уровне государственной стратегии (политики) базовых ориентиров ответственного ИИ и управления данными по образцу документов ОЭСР и ЮНЕСКО для целей правоприменения. Во-вторых, разработку совместно с частным сектором отраслевых кодексов практики и руководств по использованию ИИ в отдельных секторах, построенных на лучших международных практиках и принципах мягкого права. В-третьих, внедрение процедур предварительной оценки воздействия ИИ-систем на интересы и законные ожидания субъектов персональных данных, а также стимулирование добровольной сертификации алгоритмов по признанным критериям надежности и этичности.

Таким образом, мягкое право выступает гибким регулятором, позволяя оперативно отвечать на вызовы ИИ и данных и смягчать эффект нормативной турбулентности. Со временем многие элементы мягкого права интегрируются в юридические обязательства как на национальном уровне, так и через международные соглашения, превращаясь в юридически обязательные стандарты. Для Казахстана опора на мягкое право позволяет ускоренно заимствовать лучший мировой опыт - адаптация глобальных принципов и добровольных стандартов как временных ориентиров позволит сформировать гибкий правовой режим. Такой подход позволит обеспечить баланс между стимулированием инноваций и защитой прав человека, создаст предпосылки для эффективного законодательства, способного преодолеть современную «нормативную турбулентность».

**Регулирование ИИ и персональных данных в ЕС, Китае и Казахстане: сравнительный анализ.** Одним из ключевых различий в регулировании персональных данных и ИИ между юрисдикциями является требование проводить оценки воздействия на защиту персональных данных. В ЕС данный механизм закреплен в Общем регламенте ЕС о защите персональных данных (ст. 35 GDPR) и обязателен в случаях, когда планируемая обработка персональных данных сопряжена с высоким риском для прав и свобод субъектов (например, массовое слежение, составление профилей, обработка специальных

категорий данных). Формулировки GDPR относительно обязательности оценки воздействия на защиту персональных данных достаточно общие - оценка нужна при использовании новых технологий и иных операциях, создающих «высокий риск» для субъектов. Для конкретизации Европейский комитет по защите данных разработал рекомендации с перечнем случаев, когда данная оценка необходима [259, с. 3-5].

В Китае аналогичный инструмент введен сравнительно недавно в рамках Закона КНР «О защите персональной информации» (в английской версии: *Personal Information Protection Law - PIPL*). Статья 55 Закона КНР [59] требует проводить оценку влияния на защиту персональной информации (в английской версии: *Personal Information Protection Impact Assessment - PIPIA*) в более широком спектре ситуаций, чем GDPR. Прямо предусмотрено, что такая оценка обязательна при обработке чувствительных персональных данных, использовании данных для автоматизированного принятия решений, передаче данных третьим лицам или за границу и иных операциях, существенно затрагивающих права и интересы лиц. Иными словами, законодательство КНР устанавливает своего рода презумпцию риска при обработке персональных данных. Практически любая значимая операция (особенно с участием чувствительных данных или трансграничная) требует предварительной оценки и принятия мер по минимизации рисков. Это заметное отличие от подхода ЕС, где критерии более гибкие - в Китае же законодатель более детально регламентировал случаи проведения оценки влияния на защиту персональной информации, что фактически обязывает компании гораздо чаще проводить такие оценки. Таким образом, в КНР прослеживается более (основанный на принципе предосторожности) и государственно-управляемый подход к управлению потенциальными цифровыми рисками, тогда как в ЕС - делегированный риск-ориентированный подход, оставляющий организациям определенное усмотрение в оценке существенности риска.

В Казахстане требование проведения оценки воздействия на защиту персональных данных пока выражено слабее. Закон РК «О персональных данных и их защите» не содержит прямого аналога ст. 35 GDPR, фокусируясь главным образом на принципах законности обработки, согласии субъекта и т. п. Однако под влиянием глобальных стандартов Казахстан в последние годы усиливает регулирование персональных данных, постепенно приближая его к моделям ЕС. Так, с 2020 года внесены изменения, обязующие назначать ответственных за защиту данных (аналог уполномоченного лица по защите персональных данных) (ст. 25 ЗРК «О персональных данных и их защите»), уведомлять уполномоченный орган о нарушениях безопасности персональных данных [260] и применять меры защиты [97] при обработке ограниченно-доступных данных. В проекте нового «Цифрового кодекса» РК [261] и сопутствующих законодательных актах рассматривается возможность внедрения оценок воздействия на данные для обработки высокого риска по примеру оценки воздействия на защиту персональных данных. Кроме того, разрабатываемое специальное законодательство об ИИ [262] также предусматривает оценку и классификацию рисков, что будет рассмотрено более подробно ниже. В целом, в

Республике Казахстан признается, что внедрение передовых технологий требует предварительного анализа рисков, однако соответствующие нормативные механизмы находятся в стадии формирования [263].

**Классификация и презумпция рисков при использовании технологий ИИ.** В сфере прямого регулирования технологий ИИ наиболее системный подход предложен в ЕС. Европейский союз в 2024 году принял первый всеобъемлющий акт об ИИ - «Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года, устанавливающий гармонизированные правила в отношении искусственного интеллекта» (Регламент ЕС об ИИ), выстроенный по принципу «регулирования, основанного на уровне риска» [255]. Данный закон вводит категории ИИ-систем по уровням риска (недопустимый, высокий, ограниченный, минимальный) и устанавливает дифференцированные требования: от запрета наиболее опасных применений (например, социальный скоринг, массовая биометрическая идентификация в реальном времени) до строгих требований для «высокорискованных» систем (сертификация, отчетность, прозрачность). По сути, в ЕС закреплена презумпция высокой опасности отдельных видов ИИ - законодатель заранее определяет сферы (образование, здравоохранение, правосудие и др.), где использование ИИ изначально считается рискованным и требует повышенного контроля. Такой подход, основанный на принципе предосторожности, отражает европейские ценности защиты прав человека и приверженность этическим принципам при развитии ИИ.

Китай следует иной парадигме, основанной на государственных приоритетах и контроле за стратегически важными технологиями. Вместо формальной трехуровневой градации рисков, как в ЕС, Китай применяет сочетание «негативного списка» [264] и разрешительного надзора [265; 266; 267]. Регуляторы заранее обозначают нежелательные или подлежащие особому контролю применения ИИ - например, генеративный ИИ должен соответствовать требованиям по недопустимости запрещенного контента и пройти проверку безопасности перед запуском для широкой публики. В 2022-2024 годах в КНР были введены ряд адресных нормативных актов: правила использования алгоритмов рекомендаций [267], меры по управлению «глубокими фейками» [265], временные положения по генеративному ИИ [266]. Все они подчинены логике обеспечения национальной безопасности и социальной стабильности. Так, для алгоритмов, влияющих на общественное мнение, введена обязательная регистрация и аудит, а некоторые технологии (как распознавание лиц в реальном времени) фактически запрещены либо ограничены испытаниями. Подход КНР возможно охарактеризовать как презумпцию управляемости рисков государством. Риски ИИ признаются, но смягчаются через прямое государственное вмешательство - лицензирование, модерацию контента, требования локализации данных и проч. Вместо предоставления организациям права самим оценивать риски, государство само определяет, какие технологии допустимы, а какие нет, исходя из национальных интересов. В целом, в КНР обеспечивается баланс между инновациями и безопасностью преимущественно через модель государственного управления

рисками, в то время как в ЕС делается акцент на нормативном установлении гарантий и ответственности разработчиков.

В Республике Казахстан, юрисдикция которой в рассматриваемой сфере относительно невелика, внимательно изучаются оба подхода при формировании национальной политики. В 2024 году Правительством РК принята «Концепция развития искусственного интеллекта на 2024-2029 годы» [268], основанная на учете международного опыта и направленная на создание экосистемы ИИ и условий для инноваций. Опираясь на эту Концепцию, в 2025 году был разработан первый проект Закона РК «Об искусственном интеллекте», который прошел слушания мажилиса [269]. Государственный курс на комплексную цифровую трансформацию и повсеместное внедрение технологий искусственного интеллекта закреплен на высшем уровне в Послании Президента Республики Казахстан Касым-Жомарта Токаева от 8 сентября 2025 года «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» [11], в котором определена задача повсеместного применения ИИ в экономике и системе государственного управления. Среди обозначенных мер - создание отдельного ведомства по вопросам искусственного интеллекта и цифрового развития; придание городу Алатау специального статуса как пилотной цифровой территории. Хотя законопроект «не копирует зарубежные модели», в нем явно воспринимается идея классификации ИИ-систем по уровням риска - предлагается разделение на минимальный, средний и высокий риск с соответствующей дифференциацией регулирования. Таким образом, Казахстан во многом следует европейскому принципу предосторожности в отношении наиболее рискованных ИИ. С другой стороны, законодатели РК отмечают, что новый закон не должен замедлять развитие технологии, а напротив - сопровождать его, создавая понятные условия для инвесторов. Политика Республики Казахстан направлена на стимулирование разработок в сфере ИИ посредством предотвращения излишних регуляторных барьеров, но в рамках соблюдения базовых правовых требований. Это во многом отсылка к опыту прошлых лет (например, неконтролируемое развитие майнинга криптовалют [270, с. 337] из-за отсутствия регулирования, приведшее затем к строгим мерам [271; 272]). В проекте закона об ИИ упор сделан на гибкое регулирование с опорой на саморегулирование индустрии. В 2024 году Правительство учредило Комитет искусственного интеллекта и развития инноваций в структуре МЦРИАП (ныне Министерство искусственного интеллекта и цифрового развития РК). С 18 сентября 2025 года Комитет, функционируя в системе Министерства искусственного интеллекта и цифрового развития, осуществляет разработку методик оценки рисков ИИ-систем и подготовку (пилотирование) процедур сертификации алгоритмов. Иными словами, Казахстан пытается занять промежуточную позицию между строгим регулированием ЕС и прагматичным контролем Китая, учитывая собственные ограниченные возможности надзора: принять основные принципы этичного и безопасного ИИ; запретить наиболее опасные практики, но предоставить бизнесу пространство для инноваций в рамках «регуляторных песочниц» и пилотных проектов. Последнее проявляется, например, в намерении создать Национальную платформу ИИ [273] для

апробации решений и специализированный научно-образовательный центр Alem.ai [274] в Астане, что фактически будет служить тестовой средой для ИИ-инициатив без риска для широкой публики. В то же время контроль за соблюдением минимальных требований (например, защита персональных данных, недопустимость дискриминации алгоритмов) останется за государственными органами. Таким образом, правовые режимы ЕС, КНР и Казахстана отражают признание наличия серьезных рисков в сфере ИИ и персональных данных, однако подходы к их регулированию различаются: от детального нормативного контроля и презумпции высокого риска (ЕС, отчасти КНР) до комбинирования «гибкого» регулирования и саморегуляции при участии государства (Казахстан).

*Таким образом,* по итогам анализа стратегических вызовов, связанных с искусственным интеллектом и нормативной турбулентностью, возможно сформулировать следующие выводы.

Стремительное развитие технологий искусственного интеллекта (ИИ) порождает нормативную турбулентность, характеризующуюся отставанием международно-правового регулирования от технологических реалий, фрагментацией глобальной регуляторной среды и возникновением системных рисков для защиты персональных данных. Дискуссия о потенциальных экзистенциальных угрозах ИИ актуализирует необходимость выработки новых регуляторных парадигм и международно-правовых механизмов контроля (включая инициативы по заключению международных договоров).

В условиях правовой неопределенности значительно возрастает регуляторная роль инструментов «мягкого права» (акты ОЭСР, ЮНЕСКО). Данные акты выполняют функцию гибкого этико-правового ориентира, способствуя гармонизации национальных подходов и формируя основу для последующей кодификации в юридически обязательные нормы.

Сравнительно-правовой анализ демонстрирует фрагментацию национальных подходов к регулированию (в частности, риск-ориентированный подход ЕС и государственно-ориентированная модель КНР). Несмотря на различия, общей тенденцией является имплементация процедур оценки воздействия на защиту персональных данных (*DPIA* в ЕС; *PIPIA* в КНР) как ключевого механизма управления рисками.

Республика Казахстан формирует национальный правовой режим регулирования ИИ, ориентированный на адаптацию международных стандартов риск-ориентированного подхода при сохранении регуляторной гибкости. Преодоление «нормативной турбулентности» и обеспечение устойчивости информационной безопасности и информатизации требует углубления международно-правового сотрудничества в целях выработки универсальных, технологически нейтральных стандартов.

Проанализировав стратегические вызовы для правового режима защиты персональных данных (включая искусственный интеллект и «нормативную турбулентность»), необходимо перейти к рассмотрению особенностей их в национальной правовой системе (подраздел 2.4).

## 2.4 Судебная практика в Республике Казахстан и пробелы правоприменения в сфере защиты персональных данных

**Конституционные и нормативно-правовые основы защиты персональных данных.** Право на защиту личной информации в Республике Казахстан закреплено в конституционных нормах о неприкосновенности частной жизни, личной и семейной тайне, защиту своей чести и достоинства (ст. 18 Конституции РК), что соответствует международным источникам права в области прав человека (например, ст. 12 ВДПЧ). Указанные тенденции институционально закреплены, в том числе, в Будапештской конвенции о компьютерных преступлениях 2001 г., что позволяет использовать их как ориентир для устранения пробелов национального правоприменения. Для реализации этих конституционных гарантий выстроена национальная нормативная база. Ключевым уголовно-правовым актом является Уголовный кодекс Республики Казахстан (УК РК), содержащий специальные составы преступлений в сфере информатизации, связи и персональных данных. В частности, глава 7 УК РК предусматривает ответственность за правонарушения в сфере информатизации и связи (ст. 205-213). Например, ст. 147 УК РК устанавливает ответственность за незаконный сбор или распространение сведений о частной жизни (личная и семейная тайна). Наказание варьируется от штрафов и работ до лишения свободы (вплоть до 3 лет по ч. 2 и до 5 лет по ч. 3). Дополнительную уголовную ответственность несут должностные лица. В частности, за злоупотребление должностными полномочиями, повлекшее разглашение персональных данных, предусмотрена ответственность по ст. 361 УК РК. Процессуальный порядок доказывания и рассмотрения таких дел регламентируются Уголовно-процессуальным кодексом РК (УПК РК). В нем, в частности, прямо указано, что электронные документы могут выступать доказательствами в уголовном процессе при условии соответствия общим критериям относимости, допустимости и достоверности (п. 15) ст. 7; ст. 120, 125 УПК РК). Кроме того, гражданско-правовые аспекты - возмещение вреда, причиненного преступлением - регулируются Гражданским кодексом РК (ст. 917 ГК РК). В сфере же профилактики и регулирования оборота данных действуют ранее приведенные Закон РК «О персональных данных и их защите» от 21 мая 2013 года № 94-V, устанавливающий принципы сбора, обработки и защиты персональных данных, а также Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V, закрепляющий режим конфиденциальности информации и меры по ее защите. Анализ сведений, содержащихся в Банке судебных актов Республики Казахстан, свидетельствует о наличии значительного объема правоприменительной практики в рассматриваемой сфере. Так, за период с 2011-2023 гг., поисковый запрос «персональные данные» в базе данных по гражданским делам выявил 2 189 судебных актов (дел) [7, с. 14], из обстоятельств (фабулы) которых усматриваются факты нарушения либо признаки нарушения Законодательства РК «О персональных данных и их защите». Кроме того, обстоятельства ряда дел указывают на наличие признаков деяний, квалифицируемых как уголовные

правонарушения. Эти наблюдения находят прямое подтверждение в диссертационном исследовании Р. Б. Джилкишиева, где представлен детальный анализ современного состояния уголовных правонарушений в сфере информатизации (киберпреступности), основанный на актуальных статистических данных за 2021-2025 гг. В данном анализе отмечен стремительный рост (в 3,7 раза) количества таких противоправных деяний, преобладание в их структуре интернет-мошенничества и низкий уровень раскрываемости [37, с. 15-21].

**Виды уголовных правонарушений, совершаемых с неправомерным использованием персональных данных.** Анализ судебной практики Республики Казахстан показывает, что наиболее распространенными преступными посягательствами на личную информацию являются хищения имущества и мошенничества, совершаемые с применением информационных технологий. В зависимости от способа лица привлекаются к ответственности либо по ст. 190 УК РК (мошенничество), либо по ст. 188 УК РК (кража), иногда по совокупности указанных норм. Характерный пример - оформление микрокредитов электронным способом или микрокредитов на имя потерпевших без их ведома, с последующим хищением полученных денежных средств или товаров. Судебные решения квалифицируют такие деяния преимущественно как мошенничество, совершенное с использованием информационных систем (п. 4) ч. 2 ст. 190 УК РК), поскольку лица путем обмана завладевают чужими денежными средствами. Лица применяют разнообразные способы: от направления ссылок на подложные интернет-ресурсы и смс-кодов до предложения потерпевшему улучшить кредитную историю через фиктивные сделки. Нередко потерпевшие сами, введенные в заблуждение, добровольно сообщают преступникам свои персональные данные, после чего на их имя оформляются кредиты. Так, например, в Северо-Казахстанской области была выявлена схема, где лицо, представившись представителем организации, сфотографировал гражданку под предлогом вручения приза. Впоследствии эта фотография и чужой номер телефона были использованы для дистанционного заключения договора микрокредита на ее имя. Данное дело показало, что минимальной информации (фотография и ИИН) оказалось достаточным для оформления кредита, а потерпевшая узнала о задолженности лишь от судебного исполнителя. Подобные случаи не единичны - по данным правоохранительных органов, только по фактам мошенничества, совершенного путем обмана или злоупотребления доверием пользователя информационной системы, ежегодно возбуждается множество дел, значительная часть которых связана с несанкционированным использованием персональных данных.

Отдельную опасность представляют преступления, совершаемые лицами, имеющими законный доступ к базам данных. В судебной практике имеются примеры рассмотрения уголовных дел, материалы которых подтверждают указанное обстоятельство. Показательным является анализ одного из уголовных дел (в ноябре 2022 г.), включавшего 112 эпизодов противоправной деятельности с причинением имущественного вреда (ущерба) на сумму около 300 млн. тенге [7, с. 14]. Материалы данного дела свидетельствуют о ключевой роли

работников банка (менеджеров) в организации и совершении уголовных правонарушений (преступных схем). Данное обстоятельство указывает на актуальность проблемы неправомерного использования персональных данных работниками организаций финансового сектора при исполнении ими своих служебных обязанностей. Если такие действия совершаются должностным лицом с использованием служебного положения, то суды квалифицируют их как мошенничество при отягчающем признаке должностного положения (п. 2) ч. 3 ст. 190 УК РК) либо как злоупотребление должностными полномочиями (ст. 361, 362 УК РК) при ущербе правам физических лиц. Например, неправомерное получение сотрудником органа внутренних дел конфиденциальных сведений из ведомственных информационных систем квалифицируется как превышение власти или должностных полномочий и одновременно незаконное распространение персональных данных, что является нарушением конституционных прав на неприкосновенность частной жизни. В подобных случаях судебные органы отмечают общественную опасность незаконного распространения данных из государственных информационных систем, ведь такие действия дискредитируют институты государственной власти.

Лица порой сочетают различные формы хищений. Имеют место случаи, когда после заключения договора кредита электронным способом на имя потерпевшего совершается хищение приобретенного имущества. Так, лица могут оформить микрокредиты электронным способом на дорогостоящий товар (например, смартфон) и затем совершить хищение указанного имущества, не передавая его лицу, на имя которого был заключен договор (займа). Судебная квалификация подобных деяний включает совокупность преступлений: помимо мошенничества (ст. 190 УК РК) в части получения кредита обманным путем, виновные лица дополнительно осуждаются за кражу имущества (ст. 188 УК РК). Таким образом, совокупность деяний может образовывать составы нескольких уголовных правонарушений, что ставит вопрос о наличии множественности уголовных правонарушений.

**Неоднократность и совокупность уголовных правонарушений (эпизодов), совершенных в сфере информатизации и связи.** В делах об уголовных правонарушениях, связанных с незаконным оборотом персональных данных, часто возникает вопрос о квалификации множественности деяний: образуют ли они продолжаемое правонарушение (как однотипные действия) или совокупность уголовных правонарушений. Законодательство РК и разъяснения, содержащиеся в нормативных постановлениях Верховного Суда определяют порядок для таких ситуаций. Согласно нормативному постановлению Верховного Суда РК № 11 от 25.12.2006 г. «О квалификации неоднократности и совокупности уголовных правонарушений» [275], если статья Особенной части Уголовного кодекса РК предусматривает неоднократность в качестве квалифицирующего признака, то несколько тождественных деяний, совершенных одним лицом, должны квалифицироваться по одной статье с указанием этого признака. Иными словами, несколько тождественных деяний (например, серия мошенничеств, совершенных одним способом) образуют

неоднократное уголовное правонарушение, квалифицируемое по одной статье (части статьи) Уголовного кодекса. Это препятствует необоснованному расширению объема обвинения и назначению наказания по совокупности уголовных правонарушений. В частности, в случаях неоднократного оформления микрокредитов в отношении нескольких потерпевших одним лицом, суды квалифицируют содеянное как неоднократное мошенничество, без отдельной квалификации каждого деяния (эпизода). В случае совершения разнородных деяний, например, мошенничества, совершенного путем обмана или злоупотребления доверием пользователя информационной системы, и сопряженной с ним кражи имущества - они образуют реальную совокупность уголовных правонарушений и подлежат самостоятельной квалификации по каждой соответствующей статье Особенной части Уголовного кодекса РК. В соответствии с разъяснениями Верховного Суда РК, важными критериями для разграничения (неоднократности и совокупности) являются однородность деяний и наличие единого умысла. При рассмотрении данной категории дел суды устанавливают, образуют ли все деяния единое продолжаемое уголовное правонарушение или самостоятельные уголовные правонарушения, поскольку от этого зависит квалификация содеянного по признаку неоднократности либо по совокупности уголовных правонарушений. В результате формируется более единообразная судебная практика назначения наказаний за неоднократное совершение мошенничеств в сфере информатизации - в соответствии с принципами справедливости и соразмерности наказания, назначаемого лицу, признанному виновным.

**Допустимость и достоверность доказательств, закрепленных на электронных носителях информации.** Рост числа уголовных правонарушений в сфере информатизации и связи ставит перед судами сложные задачи по оценке доказательств. Специфика сведений в электронной форме (в отличие от иных вещественных доказательств) требует от правоприменительных органов применения новых подходов (методик) к доказыванию, имеющих значение для дела. В первую очередь, суды осуществляют проверку соблюдения процессуального порядка собирания сведений в электронной форме. Согласно разъяснениям Верховного Суда РК, доказательства, полученные в установленном законом порядке, подлежат оценке на предмет их относимости, допустимости и достоверности в соответствии с Уголовно-процессуальным кодексом РК. На практике это означает, что при изъятии электронных носителей информации или осмотре сведений, содержащихся на них, должны соблюдаться требования уголовно-процессуального закона: участие понятых, санкционирование следственных действий, составление протоколов соответствующих следственных действий. Нарушение установленного законом порядка сбора и закрепления доказательств влечет их признание недопустимыми.

В качестве доказательств по делам об уголовных правонарушениях в сфере информатизации и связи используются сведения в электронной форме и электронные носители информации. Суды Республики Казахстан принимают в качестве доказательств протоколы осмотра электронных документов (в том

числе снимки экрана переписок из информационных систем обмена мгновенными сообщениями), сведения о телефонных соединениях, выписки по банковским счетам, сведения, содержащиеся в кредитных историях, информацию об операциях (транзакциях) в информационных системах и иные сведения, полученные в электронной форме (ст. 120-122 УПК РК; ч. 2. ст. 65 ГПК РК; п. 1. ст. 7 ЗРК «Об электронном документе и электронной цифровой подписи»; ст. 50 ЗРК «О банках и банковской деятельности в Республике Казахстан»; пп. 2) п. 3 Приказа и. о. Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171 «Об утверждении правил оказания услуг связи» [276]). В этой связи правовая сущность такого документа заключается в представлении информации в электронно-цифровой форме на носителе, подлинность которого удостоверена законодательно закрепленными цифровыми способами идентификации [277, с. 14].

При этом каждое такое доказательство подлежит надлежащей оценке. Например, снимки экрана признаются допустимыми доказательствами лишь при подтверждении их достоверности - как правило, посредством назначения судебной компьютерно-технической экспертизы или путем исследования иных доказательств, подтверждающих их происхождение и подлинность (например, показаниями свидетелей). Финансовые документы в электронной форме (электронные документы) признаются допустимыми доказательствами при условии подтверждения их достоверности (например, удостоверения электронной цифровой подписью) либо их истребования в установленном процессуальном порядке. В судебной практике сформированы подходы к оценке сведений в электронной форме. Суды путем привлечения специалистов устанавливают, не подвергались ли такие сведения модификации (несанкционированному изменению), устанавливают лицо, создавшее или отправившее сообщение, а также обстоятельства (включая время и источник) создания снимков экрана.

Особое значение приобретает судебная экспертиза электронных носителей информации и информационных систем. По делам об уголовных правонарушениях в сфере информатизации и связи назначаются судебные компьютерно-технические экспертизы, целью которых является восстановление хронологии событий, установление фактов доступа к учетным записям, идентификация устройств или программных средств, использованных обвиняемыми. Заключения эксперта часто имеет существенное значение для дела, например, при установлении IP-адреса, с которого осуществлялся неправомерный доступ, или при установлении принадлежности электронного кошелька. Верховный Суд РК в нормативном постановлении № 16 от 26.11.2004 г. «О судебной экспертизе по уголовным делам» [278] указал на обязанность судов оценивать заключение эксперта на предмет его обоснованности и соответствия методикам проведения экспертизы. Если сторона защиты заявляет ходатайство (приводит доводы) об оспаривании заключения эксперта (ссылаясь, к примеру, на необоснованность выводов, нарушение методик исследований либо недостаточную квалификацию

эксперта), то суд оценивает эти доводы. При наличии оснований, предусмотренных ст. 287 УПК РК (в частности, если выводы вызывают сомнение или заключение недостаточно обоснованно), суд вправе назначить повторную или дополнительную экспертизу.

В целом судебная практика в Республике Казахстан сформирована следующим образом: с одной стороны, суды принимают в качестве доказательств сведения, полученные с использованием научно-технических средств (включая заключения экспертов), с другой - такие доказательства не имеют заранее установленной силы и подлежат оценке наравне с иными доказательствами в их совокупности. Разъяснения, содержащиеся в нормативном постановлении Верховного Суда РК № 4 от 20.04.2006 г. «О некоторых вопросах оценки доказательств по уголовным делам» [279], также ориентируют суды на необходимость оценки доказательств в их совокупности по внутреннему убеждению, при этом никакие доказательства не имеют заранее установленной силы. Это имеет существенное значение ввиду возможности фальсификации сведений в электронной форме или их искажения (утраты) вследствие сбоев в работе информационных систем (технических сбоев). Суд не признает достаточными электронные документы и данные, содержащиеся на электронных носителях, если они не подтверждены совокупностью иных доказательств либо вызывают сомнения в их достоверности (подлинности). При таких обстоятельствах указанные доказательства не могут быть положены в основу обвинительного приговора без проведения дополнительных процессуальных действий, направленных на установление их относимости, допустимости и достоверности. В силу принципа оценки доказательств в их совокупности, при котором никакие доказательства не имеют заранее установленной силы (ст. 125 УПК РК), один снимок с экрана, чья достоверность не установлена или оспаривается, не может образовывать достаточную совокупность доказательств для постановления обвинительного приговора без его надлежащей процессуальной проверки и подкрепления иными относимыми и допустимыми доказательствами по делу.

Судебная практика по гражданским и уголовным делам, предметом рассмотрения которых выступает оспаривание сделок, совершенных в электронной форме (или в форме электронного документа), демонстрирует порядок оценки судами доказательств, закрепленных на электронных носителях информации. Так, при рассмотрении упомянутого уголовного дела по факту мошенничества, выразившегося в оформлении договора микрокредита в отношении жительницы г. Петропавловска, суд подверг детальному исследованию сведения в электронной форме (электронные следы), относящиеся к процедуре заключения указанной сделки. Было установлено, что для дистанционной идентификации субъекта (клиента) был применен одноразовый пароль, направленный на абонентский номер, не принадлежавший потерпевшей. Микрофинансовая организация не произвела надлежащую проверку принадлежности указанного абонентского номера и расценила ввод пароля как волеизъявление потерпевшей на заключение договора. Суд указал, что направление одноразового пароля на абонентский номер, не принадлежащий

стороне договора (потерпевшей), и последующий его ввод неуполномоченным лицом не могут свидетельствовать о выражении воли самой потерпевшей (истца) на совершение сделки (заключение договора). Кроме того, видеозапись, предположительно фиксирующая процедуру биометрической аутентификации, в ходе которой обвиняемый кратковременно зафиксировал лицо потерпевшей, была признана недопустимым доказательством волеизъявления. Установленные нарушения порядка проведения идентификации личности исключили возможность признания достоверными доказательствами согласия на совершение сделки как самого видеоизображения (без аудиофиксации), так и извлеченного из него статичного изображения (фото-снимка) [280].

Данный судебный акт свидетельствует о том, что суды осуществляют оценку новых цифровых методов идентификации личности с позиций их соответствия требованиям закона. При установлении факта нарушения установленного порядка идентификации, любые сведения (видео-, фотоизображения, электронные документы), полученные в ходе такой процедуры, могут быть признаны недопустимыми доказательствами. В силу ст. 112 УПК РК, они считаются полученными с нарушением закона и, следовательно, лишенными юридической силы. Таким образом, судебная практика в Республике Казахстан формирует критерии оценки допустимости доказательств, представленных в электронной форме (на электронных носителях). Для использования их в доказывании требуется не только техническое представление самих сведений, но и обеспечение соблюдения процессуального порядка их получения и закрепления, позволяющего проверить их достоверность.

**Обеспечение прав потерпевшего и возмещение вреда, причиненного уголовным правонарушением.** Обеспечение восстановления нарушенных прав потерпевшего является одной из задач уголовного судопроизводства по делам об уголовных правонарушениях, связанных с незаконным использованием персональных данных. Уголовно-процессуальным кодексом РК предусмотрено право потерпевшего предъявить гражданский иск в ходе производства по уголовному делу для возмещения имущественного и (или) морального вреда, причиненного ему непосредственно уголовным правонарушением. Нормативное постановление Верховного Суда РК № 1 от 20.06.2005 г. «О рассмотрении гражданского иска в уголовном процессе» [281] разъясняет порядок разрешения гражданского иска в ходе производства по уголовному делу. Правоприменительная практика свидетельствует, что по уголовным делам о мошенничестве (ст. 190 УК РК), совершенном с неправомерным использованием персональных данных, в качестве гражданских истцов (ст. 71 УПК РК) нередко признаются финансовые организации (банки или микрофинансовые организации), которым в результате совершения уголовного правонарушения был причинен непосредственный имущественный вред (вследствие выдачи займа (микрокредита) с использованием данных иного лица). При рассмотрении дела по существу суды удовлетворяют подобные гражданские иски, взыскивая с осужденных сумму причиненного имущественного вреда (ущерба) в полном объеме. В случае совершения

уголовного правонарушения группой лиц (в соучастии), обязанность по возмещению вреда, как правило, возлагается на всех соучастников солидарно, в соответствии с положениями ст. 932 Гражданского кодекса РК (об ответственности за совместно причиненный вред). При постановлении приговора и удовлетворении гражданского иска, суд устанавливает срок для добровольного исполнения приговора в части взыскания ущерба. По истечении этого срока, в случае неисполнения решения осужденным добровольно, приговор в данной части обращается к принудительному исполнению в порядке, предусмотренном законодательством Республики Казахстан об исполнительном производстве и статусе судебных исполнителей.

Особенностью правоприменительной практики в Республике Казахстан по данной категории уголовных дел является то, что исковые требования о возмещении морального вреда (ст. 167 УПК РК) удовлетворяются, как правило, лишь частично, а определяемые судом размеры компенсации являются незначительными. Поскольку объектом посягательства при совершении данных уголовных правонарушений (например, мошенничества) выступают преимущественно имущественные права (хищение денежных средств, приобретение права на имущество путем обмана при оформлении займов), и само деяние не сопряжено с причинением вреда жизни или здоровью потерпевшего, либо иным посягательством на его личные неимущественные блага и права (как того требует ст. 951 ГК РК), суды, руководствуясь нормами ГК РК, зачастую отказывают в удовлетворении исковых требований о компенсации морального вреда, мотивируя решение тем, что были нарушены исключительно имущественные права гражданского истца. Само по себе деяние, выразившееся в противоправном оформлении договора займа (кредита) на имя потерпевшего, расценивается судами преимущественно как посягательство на имущественные права [282]. Таким образом, установление факта мошеннического оформления кредита не влечет автоматического удовлетворения требований о компенсации морального вреда, поскольку данное правонарушение напрямую не посягает на личные неимущественные блага и права потерпевшего (такие как жизнь, здоровье, честь, достоинство, неприкосновенность частной жизни), нарушение которых является основным основанием для взыскания такой компенсации.

Данная правоприменительная позиция является предметом дискуссий в правовой доктрине. Ряд правоведов указывает, что уголовные правонарушения в сфере информатизации, связанные с неправомерным обращением с персональными данными, причиняют потерпевшим не только имущественный вред, но и моральный вред (нравственные страдания), выражающийся в испытываемых переживаниях, нарушении чувства безопасности и причинении вреда репутации [283, с. 831]. Вместе с тем, на сегодняшний день законодательные акты Республики Казахстан прямо не относят подобные ситуации к случаям (исключениям, предусмотренным законодательными актами), допускающим компенсацию морального вреда при нарушении имущественных прав (п. 4 ст. 951 ГК РК). В связи с этим, правоприменительная (судебная) практика исходит из буквального толкования и применения

указанной нормы материального права. Представляется возможным дальнейшее совершенствование законодательства в данной части в целях обеспечения более полной защиты прав и законных интересов личностей, потерпевших от противоправных посягательств, связанных с неправомерным использованием их персональных данных.

**Проблемные вопросы правоприменительной практики и пробелы законодательного регулирования.** Несмотря на деятельность судов и органов, осуществляющих уголовное преследование, правоприменительная практика свидетельствует о наличии ряда пробелов в законодательстве и сложностей, возникающих при применении норм, регулирующих сферу персональных данных и их защиты. Во-первых, наблюдается опережающее развитие способов и средств совершения уголовных правонарушений (преступных схем) по сравнению с разработкой и внедрением эффективных мер противодействия. Субъекты преступлений активно используют современные ИКТ-технологии: системы дистанционного банкинга (мобильные приложения), платформы, обеспечивающие анонимность пользователей, и инструменты оборота цифровых активов (криптовалюты). Это обстоятельство существенно затрудняет проведение негласных следственных действий и иных оперативно-розыскных мероприятий, направленных на установление причастных лиц, отслеживание (финансовый мониторинг) финансовых потоков и, как следствие, изобличение виновных в совершении противоправных деяний. Денежные средства и иное имущество, полученные преступным путем, все чаще легализуются (выводятся) посредством электронных средств платежа (в том числе электронных кошельков) или иностранных платежных сервисов, находящихся вне юрисдикции Республики Казахстан. Уголовным кодексом РК (ст. 48 УК РК) предусмотрена принудительная мера уголовно-правового воздействия в виде конфискации имущества, то есть принудительного безвозмездного изъятия и обращения в собственность государства имущества, добытого преступным путем либо приобретенного на средства, добытые преступным путем. Однако правоприменительная практика свидетельствует, что применение данной меры нередко затруднено или невозможно. Органом, ведущим уголовный процесс, не выявляются либо не доказывается преступное происхождение активов, подлежащих конфискации. В таких случаях, согласно судебной практике, конфискация не назначается, даже если санкция статьи предусматривает ее в качестве обязательной меры. Кроме того, к моменту вынесения приговора такое имущество может фактически отсутствовать у осужденного (ввиду его сокрытия, отчуждения третьим лицам либо легализации (отмывания) в соответствии с ст. 218 УК РК), что делает невозможным его фактическое исполнение. Вследствие этого, конфискация имущества не во всех случаях достигает своей цели по предупреждению совершения новых уголовных правонарушений (превентивной функции), что снижает общую эффективность применяемых мер уголовно-правового воздействия. Представляется необходимой разработка процессуальных механизмов оперативного наложения ареста на цифровые активы и приостановления (блокировки) операций (транзакций) с ними, которые в настоящее время находятся на стадии формирования (разработки).

Во-вторых, уязвимость процедур дистанционной идентификации личности. Анализ судебной практики свидетельствует, что существующие механизмы идентификации (через СМС-коды, биометрическую аутентификацию, одноразовые пароли) в ряде случаев не обеспечивают надлежащей защиты от неправомерного доступа к информации со стороны посторонних лиц. Ненадлежащее исполнение финансовыми организациями (как субъектами финансового мониторинга) обязанностей по надлежащей проверке клиентов, установленных законодательством Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ), создает условия для совершения уголовных правонарушений (в частности, мошенничества или легализации (отмывания) доходов, полученных преступным путем).

Требуется дальнейшее совершенствование систем идентификации и аутентификации. Это предполагает внедрение более строгих мер в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ). В частности, необходимо усиление процедур надлежащей проверки клиента [284, с. 14-15] (реализующих международный стандарт «знай своего клиента» (в английской версии: *Know Your Customer - KYC*)) и текущего мониторинга деловых отношений и операций [285, с. 21-22] (включая «знай свою транзакцию» (в английской версии: *Know Your Transaction - KYT)*), а также применение усиленных методов двухфакторной, многофакторной аутентификации и биометрической идентификации, устойчивой к фальсификации. Суды в судебных актах устанавливают, что ненадлежащее исполнение финансовыми организациями обязанностей по надлежащей проверке клиента являлось одним из условий, способствовавших совершению уголовного правонарушения. Данные обстоятельства, выявляемые в ходе судебного разбирательства, служат сигналом для уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций о необходимости совершенствования нормативных правовых актов, ужесточающих требования к процедурам идентификации и верификации заемщиков (клиентов).

В-третьих, значительная часть уголовных правонарушений приобретает транснациональный характер. Материалы уголовных дел содержат эпизоды, свидетельствующие об участии транснациональных организованных групп (или преступных сообществ) и совершении преступных деяний с территории иностранных государств (например, информационные ресурсы, используемые в преступных целях (в частности, для совершения мошенничества), расположены на ресурсах, находящихся за пределами Республики Казахстан, а абонентские номера зарегистрированы на лиц иностранных государств). Указанные обстоятельства препятствуют установлению всех соучастников уголовного правонарушения и их привлечению к уголовной ответственности. Решение данной проблемы видится в активизации международного сотрудничества в сфере уголовного судопроизводства. Как ранее указывалось в настоящей работе, Казахстан уже ратифицировал ряд конвенций ООН о борьбе с транснациональной организованной преступностью [286] и находится в

процессе присоединения к Будапештской конвенции о компьютерных преступлениях [287]. Однако на практике исполнение запросов (поручений) об оказании правовой помощи (по Главе 60 УПК РК), запросов о выдаче (экстрадиции) лиц (по Главе 61 УПК РК), совершивших уголовные правонарушения в сфере информатизации и связи (по Главе 7 УК РК), а также проведение совместных следственных действий осуществляются недостаточно оперативно. Судьи нередко сталкиваются с необходимостью проведения главного судебного разбирательства в отсутствие подсудимого (выступающего организатором уголовного правонарушения), который находится вне пределов Республики Казахстан и уклоняется от явки в суд (п. 2) ч. 2 ст. 335 УПК РК). Это, безусловно, является не пробелом национального законодательства Республики Казахстан (в частности, уголовно-процессуального), а проблемой практической реализации механизмов международного сотрудничества в сфере уголовного судопроизводства. Для преодоления данной проблемы требуются унификация национального законодательства и выработка механизмов взаимного признания (обеспечения допустимости) электронных доказательств (документов на электронных носителях и иной информации в электронной форме) в рамках международного сотрудничества в сфере уголовного судопроизводства. Например, признание протоколов осмотра сведений в электронной форме, полученных за рубежом, или упрощение процедуры передачи сведений в электронной форме между государствами. В нормативных постановлениях Верховного Суда РК отмечается необходимость учитывать международные договоры и практику при расследовании уголовных правонарушений в сфере информатизации и связи - в частности, применять положения о взаимной правовой помощи, предусмотренные соответствующими конвенциями [288; 289].

Наконец, одним из существенных факторов, влияющих на уровень правонарушений в сфере защиты персональных данных, является недостаточная осведомленность населения об угрозах информационной безопасности. Суды в описательной части приговоров иногда упоминают, что потерпевшие проявили небрежность, сообщив посторонним свои конфиденциальные сведения, либо воспользовались сомнительными предложениями, размещенными на интернет-ресурсах. Такая неосмотрительность потерпевших не освобождает лиц, совершивших уголовное правонарушение, от ответственности, но указывает на необходимость повышения цифровой грамотности общества. Государство и общество должны усилить информирование населения о распространенных способах совершения мошенничества, правилах соблюдения информационной безопасности и защите персональных данных. Повышение цифровой грамотности общества прямо влияет на снижение числа потерпевших, что, в свою очередь, способствует профилактике правонарушений.

*Таким образом,* по итогам анализа судебной практики Республики Казахстан и пробелов правоприменения в сфере персональных данных возможно сформулировать следующие выводы.

Судебная практика Республики Казахстан демонстрирует адаптацию системы уголовного судопроизводства к правонарушениям, связанным с

неправомерным использованием персональных данных, квалифицируемым преимущественно как мошенничество с использованием информационно-коммуникационных технологий. Судами выработаны строгие критерии допустимости электронных доказательств, акцентирующие необходимость неукоснительного соблюдения процессуального порядка их собирания и обязательность экспертной верификации для подтверждения достоверности.

Анализ правоприменительной практики выявляет системные уязвимости, в частности, несовершенство процедур дистанционной идентификации (аутентификации) личности (допускающих неправомерный доступ посторонних лиц к информации или управлению счетами) и ненадлежащее исполнение субъектами финансового мониторинга обязанностей по надлежащей проверке клиентов и мониторингу операций, установленных законодательством Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ). Указанные обстоятельства создают условия, способствующие совершению уголовных правонарушений (в частности, мошенничества и легализации доходов, полученных преступным путем), а также препятствуют органам, ведущим уголовный процесс, в обнаружении, наложении ареста (ст. 161 УПК РК) и последующей конфискации (ст. 48 УК РК) цифровых активов, являющихся доходами, полученными преступным путем, либо орудиями (средствами) совершения уголовного правонарушения.

Существенным пробелом материального права является ограничение компенсации морального вреда. Трактовка данных деяний преимущественно как посягательств на имущественные права диссонирует с международно-правовой доктриной защиты приватности как фундаментального неимущественного блага и требует совершенствования законодательства.

Транснациональный характер киберпреступности требует интенсификации международно-правового сотрудничества в сфере уголовного судопроизводства, включая гармонизацию стандартов допустимости электронных доказательств и повышение оперативности механизмов взаимной правовой помощи.

*Таким образом,* проведенный анализ правового обеспечения защиты персональных данных в международном и национальном информационном пространстве позволяет сформулировать следующие обобщающие выводы:

В ходе исследования определен субъектный состав правоотношений. Подтверждено, что в современном международном праве (GDPR, Конвенция 108+) и национальных правопорядках субъектом права на защиту персональных данных признается исключительно физическое лицо. Данная позиция основана на аксиоме о неразрывной связи информационного самоопределения с человеческим достоинством. Юридические лица не обладают аналогичным статусом; защита их информационных активов обеспечивается посредством специализированных институтов (коммерческая тайна и др.). Государственные органы и частные организации выступают в качестве операторов (контролеров), неся основное бремя обеспечения цифрового комплаенса.

Установлено, что современное международно-правовое регулирование характеризуется фундаментальным сдвигом к риск-ориентированному подходу и превентивным механизмам. Ключевыми инструментами обеспечения комплаенса выступают принципы подотчетности, защиты персональных данных на этапе проектирования и по умолчанию, а также процедура оценки воздействия на защиту персональных данных. Принцип подотчетности трансформирует модель надзора, возлагая на оператора (контролера) бремя доказывания соблюдения норм.

Выявлены факторы, снижающие эффективность правового инструментария. К ним относятся коллизии юрисдикций при трансграничных передачах, затрудняющие экстерриториальное правоприменение, и размывание ответственности в сложных цепочках обработки персональных данных. Применение норм международного публичного права об ответственности государств и обязательства должной осмотрительности формирует публично-правовой механизм (контур) обеспечения кибербезопасности, дополняющий частноправовые механизмы. Деятельность глобальных цифровых платформ и внедрение систем цифровой (дистанционной) идентификации (e-ID) порождают системные риски, связанные с концентрацией персональных данных и уязвимостью централизованной инфраструктуры, что требует внедрения специализированных правовых режимов.

Стремительное развитие технологий искусственного интеллекта определяет состояние «нормативной турбулентности», характеризующееся фрагментацией глобальной регуляторной среды и отставанием правотворчества. В условиях правовой неопределенности особенно возрастает регулятивное значение инструментов «мягкого права». Сравнительно-правовой анализ демонстрирует фрагментацию национальных регуляторных моделей ИИ (ЕС, КНР), при этом общей тенденцией является имплементация риск-ориентированного подхода.

Анализ судебной практики РК демонстрирует адаптацию системы уголовного судопроизводства к правонарушениям в сфере персональных данных, квалифицируемым преимущественно как мошенничество. Судами выработаны строгие критерии допустимости электронных доказательств. Вместе с тем выявлены системные пробелы национального регулирования: отсутствие обязательной процедуры оценки воздействия на защиту персональных данных, недостаточная эффективность контроля за обработчиками персональных данных, а также ограничение компенсации морального вреда, что противоречит с международно-правовой доктриной защиты неприкосновенности частной жизни как фундаментального неимущественного блага. Транснациональный характер киберпреступности требует интенсификации международно-правового сотрудничества.

Сформулированные выводы о состоянии правового регулирования и выявленных системных рисках создают необходимую основу для разработки критериев эффективности правового регулирования защиты персональных данных и методов повышения этой эффективности, что является предметом третьего раздела диссертации.

# 3 ЭФФЕКТИВНОСТЬ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И НАПРАВЛЕНИЯ ЕГО СОВЕРШЕНСТВОВАНИЯ

## 3.1 Понятие, условия и критерии эффективности правового регулирования защиты персональных данных

**Понятие эффективности правового регулирования защиты персональных данных.** Эффективность правового регулирования защиты персональных данных представляет собой степень полноты и согласованности правовых норм и механизмов, обеспечивающих реализацию фундаментального права на неприкосновенность частной жизни и права на защиту персональных данных [290, с. 14]. Иными словами, данное понятие отражает степень, с которой существующее законодательство и правоприменительная практика фактически обеспечивают защиту персональных данных. Высокая степень эффективности правового регулирования предполагает, что правовая система четко устанавливает правила обработки персональных данных, соответствует применимым международным стандартам, обеспечена эффективными механизмами правоприменения (включая средства правовой защиты и механизмы ответственности) и способна адаптироваться к технологическим изменениям. Низкая эффективность правового регулирования, напротив, характеризуется наличием пробелов и коллизий в правовых нормах и недостаточностью правоприменительной практики, что (как следствие) создает или порождает риски для прав субъектов персональных данных.

В условиях стремительной цифровизации и трансграничной передачи персональных данных эффективность правового регулирования приобретает особое методологическое значение. Системный подход требует целостности: все элементы (от принципов сбора персональных данных до судебной защиты) должны образовывать согласованную систему, исключая пробелы и коллизии. Функциональный подход фокусируется на том, выполняет ли право свою защитную функцию - предотвращать нарушения и обеспечивать баланс интересов. Аксиологический (ценностный) подход обращает внимание, отражает ли регулирование фундаментальные ценности (права и свободы личности, справедливость, доверие). Социо-психологический подход учитывает восприятие обществом - уровень правосознания, доверие общества к цифровым услугам и готовность участников правоотношений соблюдать установленные нормы в сфере защиты персональных данных. Эффективное правовое регулирование защиты персональных данных должно удовлетворять всем этим критериям: быть целостным (системным), исполнимым, ценностно обоснованным и вызывать доверие в обществе.

**Условия обеспечения эффективности правового регулирования защиты персональных данных.** Для достижения высокой эффективности правового регулирования необходимы определенные условия.

Во-первых, совершенство нормотворчества: законы должны содержательно охватывать все ключевые аспекты защиты персональных данных, быть

непротиворечивыми и понятными. В Казахстане отмечалась проблема громоздкости и нестабильности законодательства в сфере информатизации [291] - преодоление этого требует кодификации и устранения дублирующих или конфликтующих норм.

Во-вторых, институциональные гарантии. Эффективная защита персональных данных предполагает наличие уполномоченного и институционально независимого органа по защите персональных данных с правом проведения проверок, выдачи предписаний, наложения штрафов и рассмотрения жалоб, включая ситуации с зарубежными обработчиками персональных данных. В Казахстане эти функции осуществляет Комитет по информационной безопасности в структуре Министерства искусственного интеллекта и цифрового развития РК (ранее - МЦРИАП), который принимает обращения субъектов и проводит государственный контроль в пределах национальной юрисдикции. Региональные договоренности [292] в рамках СНГ и ШОС обеспечивают, главным образом, взаимную правовую помощь между органами (обмен запросами и информацией), но не создают координированного порядка трансграничного рассмотрения жалоб по образцу Европейского союза. Следовательно, единый механизм «единого окна» для трансграничных дел в настоящее время отсутствует - такие обращения решаются по нормам национального права, через международные запросы и договорные процедуры сотрудничества. Встроенность Комитета в исполнительную власть и ограниченные санкционные инструменты не обеспечивают сопоставимого уровня независимости и правоприменения, а прокурорский надзор носит общий характер и не заменяет специализированного контроля. Показательным индикатором эффективности межведомственной координации в финансовом секторе выступает функционирование «антифрод-центра» Национального Банка Республики Казахстан [179]. В оценку деятельности целесообразно включать сроки реагирования (блокировка/разблокировка), долю обоснованных возвратов по уведомлениям, санкционированным прокурором, и прозрачность оснований включения/исключения в соответствующие базы. Эти метрики позволяют оценить соотношение между эффективностью мер по противодействию мошенничеству и уровнем фактического обеспечения гарантий прав субъектов данных. Для гармонизации с лучшими практиками необходимы нормативные гарантии институциональной автономии (статус, бюджет, кадровое обеспечение), расширение надзорных и корректирующих полномочий, процессуальная регламентация порядка рассмотрения жалоб и обязательная публичная отчетность.

В-третьих, ресурсное и технологическое обеспечение: достаточное финансирование и экспертиза для реализации требований (например, проведение аудитов, экспертиз). Наконец, уровень правовой культуры и осведомленности участников правоотношений - операторы (контролеры), собственники, и субъекты персональных данных - предполагает осознание ими значимости защиты персональных данных, в противном случае даже наиболее совершенные правовые нормы останутся декларативными (или не найдут практического применения). Все эти условия взаимосвязаны.

Для методологической ясности следует разграничить, что «условия обеспечения эффективности» правового регулирования защиты персональных данных представляют собой исходные предпосылки (целостность законодательства, институциональные гарантии, надлежащая ресурсообеспеченность и т. д.), необходимые для достижения эффективного правоприменения, тогда как «критерии эффективности» - это конкретные индикаторы (метрики) для оценки достигнутого уровня эффективности (например, наличие конкретных правовых механизмов и процедур, степень соответствия международным стандартам и пр.).

**Критерии эффективности правового регулирования.** Для оценки и повышения эффективности правового регулирования автор предлагает систему конкретных критериев. Эти критерии отражают ключевые требования к правовому регулированию защиты персональных данных и охватывают весь жизненный цикл обработки персональных данных - от сбора и определения целей до трансграничной передачи и судебной защиты. Далее приводится обоснованный перечень таких критериев эффективности.

**1. Целевое назначение и законность обработки.** Эффективность правового регулирования предполагает: нормативное закрепление принципа ограничения цели и процедуры теста на совместимость целей; исчерпывающий перечень законных оснований; проверяемость выбора основания и фиксацию целей/оснований в реестрах операций обработки. В ЕС «определенных, явных и законных целей», законные основания и тест совместимости закреплены прямо (пп. «b» п. 1 ст. 5, ст. 6; тест совместимости - п. 4 ст. 6 GDPR). В РК принцип целевого ограничения установлен (ст. 7 ЗРК «О персональных данных и их защите»), однако за пределами согласия альтернативные основания предусмотрены фрагментарно и через отсылку к иным законам, что снижает юридическую определенность и стимулирует практику «формального согласия». Для повышения эффективности правового регулирования необходимы: законодательное закрепление закрытого перечня оснований (договор, закон, жизненно важные интересы, публичный интерес/властные полномочия, законный интерес с балансировочным тестом), формализация теста совместимости [293], обязательное ведение реестров операций с персональными данными с указанием целей и оснований, а также методические критерии недопустимости навязанного согласия. В РК для персональных данных ограниченного доступа подзаконные акты [97] прямо требуют устанавливать цели обработки.

**2. Минимизация данных.** Критерием эффективности является наличие императивной нормы, требующей, чтобы объем собираемых и обрабатываемых персональных данных был строго необходим и достаточен для заявленной цели (минимизация данных), а также требующей документальной фиксации этого обоснования для целей контроля (проверки). В ЕС это прямо закреплено: данные должны быть «адекватны, релевантны и ограничены необходимым» (пп. «c» п. 1 ст. 5 GDPR, а выбор полей и объема подчинен цели и тестам совместимости (риска). Международные стандарты ОЭСР поддерживают этот подход через «принцип качества данных» (актуальность, соразмерность,

отсутствие избыточности) [290, с. 28-29]. В Казахстане явного термина «минимизация» в законе нет, но подзаконные Правила сбора и обработки персональных данных обязывают ограничивать сбор «…перечнем персональных данных, необходимого и достаточного для выполнения осуществляемых задач…» и формально утверждать такой перечень [294]. Это представляет собой шаг к сближению с GDPR, однако его практический эффект зависит от эффективности контроля (надзора) и правоприменения.

**3. Оценка воздействия на защиту персональных данных и риск-ориентированность.** Критерием эффективности правового регулирования является наличие императивной (обязательной) процедуры оценки воздействия на защиту персональных данных и имплементация риск-ориентированного подхода на всех этапах обработки. В ЕС это закреплено напрямую: ст. 35 GDPR, ст. 36 (предварительная консультация), а также ст. 24, 25, 32 (обязанности контролера, защита персональных данных на этапе проектирования и по умолчанию, безопасность обработки). Оценка проводится при «вероятности высокого риска» и документирует риски, меры их снижения и остаточный риск; при сохранении высокого риска контролер обращается за консультацией к надзорному органу. В Республике Казахстан действующий закон не содержит императивной процедуры оценки воздействия на защиту персональных данных. При этом с 2024 года введены правила уведомления об инцидентах безопасности в течение 1 рабочего дня, а также усилены контрольные полномочия уполномоченного органа. Для перехода к превентивной модели целесообразно: 1) ввести обязательную оценку воздействия на защиту персональных данных для высокорисковых операций (биометрия, масштабный мониторинг, уязвимые группы) с типовыми критериями; 2) закрепить тест совместимости целей и его связь с оценкой воздействия на защиту персональных данных; 3) обязать вести реестры операций с фиксацией целей, правовых оснований, рисков и мер, заверенные уполномоченным лицом по защите персональных данных; 4) предусмотреть предварительную консультацию с уполномоченным органом по защите персональных данных при остаточном высоком риске; 5) установить ответственность за непроведение оценки и непредставление документации по запросу надзорного органа. В ЕС сильной стороной выступают проактивность и проверяемость (оценка воздействия на защиту персональных данных и надзор); в РК - намечаемые институты управления рисками (в т. ч. через реформы 2024-2025 гг. и закона об ИИ (проект)), однако без их системного закрепления соответствующие механизмы защиты не получают должного нормативного развития и носят фрагментарный характер.

**4. Прозрачность и верифицируемость согласия субъекта персональных данных.** Поскольку согласие субъекта персональных данных является одним из ключевых правовых оснований обработки персональных данных, то система защиты должна обеспечивать его осознанность и проверяемость. Прозрачность означает, что субъект персональных данных получает исчерпывающую информацию об объемах и целях обработки персональных данных, а также о том, кто и каким образом их использует. Верифицируемость подразумевает, что факт и содержание данного согласия могут быть доказаны (например, посредством

хранения соответствующего электронного журнала или документа волеизъявления). Эффективное правовое регулирование требует соблюдения строгих требований к получению согласия и возлагает на оператора (контролера) обязанность продемонстрировать (доказать) наличие юридически действительного согласия. Так, ст. 7 GDPR прямо предписывает: «если обработка основана на согласии, то контролер должен быть способен продемонстрировать, что субъект дал согласие». В GDPR дополнительно содержатся строгие требования к форме получения согласия и реализации права на его отзыв. В частности, в преамбуле 32 отмечено, что согласие должно выражаться «четким утвердительным действием», быть добровольным, конкретным, информированным и однозначным. Если запрос осуществляется электронно, то он должен быть «ясным, четким и не препятствовать использованию сервиса». Регламент ЕС (GDPR) гарантирует субъекту персональных данных возможность отозвать согласие в любой момент. Такие нормы стимулируют организации внедрять системы управления согласием, фиксировать время и содержание волеизъявления пользователя. Аналогичные принципы закреплены в международных руководящих документах. Так, Основные положения ОЭСР 1980 г. содержат принцип открытости, требующий прозрачности при обработке личных данных [160, с. 7]. На Всемирном экономическом форуме отмечают идею «цифрового достоинства» (в английской версии: *«digital dignity»*) - то есть уважительного отношения к пользователю предполагающего понятные механизмы информирования и контроля над персональными данными [295, с. 6, 28; 296, с. 5-11].

В Казахстане информированное согласие предусмотрено законом и конкретизировано подзаконно: форма согласия должна включать, как минимум, сведения об операторе, о субъекте, сроке действия и перечне передаваемых данных (изменения 2022 г. к требованиям к форме согласия [297]; Правила сбора и обработки персональных данных - 2020 г. [294]). Это повышает проверяемость содержания согласия. Проблема правоприменения в РК: в отличие от ЕС, в РК нет прямой императивной обязанности вести детальные журналы/реестры согласий субъекта персональных данных и предъявлять их надзорному органу; на практике часто ограничиваются отметкой («галочкой»), что ослабляет доказуемость добровольности (конкретности) в споре. Тем не менее для эффективной защиты возможно предложить дополнительные меры. Например, введение реестра выданных согласий, доступного самим субъектам персональных данных, или требование дополнительного подтверждения (например, двухфакторного) при особо чувствительных персональных данных. В ЕС такие практики поощряются принципом подотчетности: контролер обязан в любой момент доказать законность обработки персональных данных и сохранять архив выданных согласий.

Сравнительный анализ конкретных практик ЕС и Казахстана в данном аспекте указывает также на следующие факторы:

- Преимущества ЕС. Четкие критерии действительности согласия (волеизъявление должно быть добровольным, конкретным, информированным и однозначным); гарантированная возможность отзыва согласия; строгая

ответственность контролера за документирование и доказательство наличия согласия.

- Недостаток ЕС. Обилие формальных требований к пользовательским соглашениям приводит к «усталости согласия» субъектов (пользователи привыкают автоматически нажимать «принимаю» и могут игнорировать условия).

- Преимущества Казахстана. Более простые и гибкие процедуры для субъектов предпринимательства (отсутствие чрезмерно детального регулирования формы согласия), что упрощает взаимодействие.

- Недостаток Казахстана. Такая простота снижает защиту прав субъектов: согласие часто получается формально и неосознанно, а в случае спора трудно доказать, нарушил ли оператор (контролер) заявленные условия.

Повышение эффективности законодательства Казахстана требует имплементации ключевых принципов (положений) GDPR в национальное право: например, закрепления обязанности предоставлять субъекту четкое и понятное уведомление (информацию) о целях, правовых основаниях и объемах (категориях) обработки и обязанности контролера (оператора) хранить доказательства полученного согласия (записи или журналы (лог-файлы)) в течение установленного срока. Это повысило бы прозрачность отношений с субъектами персональных данных и укрепило бы доверие общества к системам обработки персональных данных.

**5. Ведение журналов (логирование) операций обработки персональных данных и учет обращений субъектов.** Ведение журналов (логирование) и аудит операций с персональными данными - один из ключевых элементов принципа подотчетности. Журналирование изменений и запросов позволяет обеспечить отслеживаемость действий (кто, когда и каким образом проводил работу с данными) и повышает доверие субъектов в том, что их обращения будут обработаны должным образом. В соответствии с принципом подотчетности GDPR контролер не только обязан следовать основным принципам обработки, но и доказывать свое соблюдение. Это означает, что организациям следует вести подробные реестры операций с данными. В частности, согласно ст. 30 GDPR, контролер (и где нужно - его представитель) ведет реестр операций обработки персональных данных. Обязанность ведения таких реестров является общей, однако организации с числом сотрудников менее 250 человек освобождаются от данной обязанности, за тем исключением, когда осуществляемая ими обработка: может создать риск для прав и свобод субъектов данных; носит не разовый (а систематический) характер; касается специальных категорий персональных данных (ст. 9 GDPR) или персональных данных, относящихся к уголовным судимостям и правонарушениям (ст. 10 GDPR).

Международные стандарты безопасности (например, ISO/IEC 27001:2022 [217]) также отмечают важность аудитов - неизменяемого журнала событий для целей безопасности и контроля. В них прямо рекомендуется фиксировать ключевые события (доступ к персональным данным, изменения в системе и т. п.) и защищать журналы (лог-файлы) от изменений. Таким образом, требования

журналирования встроены в международную практику обеспечения информационной безопасности.

В Казахстане формальная обязанность вести журналы обращений субъектов пока не закреплена для большинства операторов. Вместе с тем государственные и электронные сервисы (веб-портал «электронного правительства») часто снабжены встроенным аудитом. Например, разработаны функции, где через личный кабинет субъект персональных данных может узнать, кем запрашивались его данные в конкретных реестрах. Так, последнее изменение законодательства ввело обязанность уведомлять субъекта персональных данных о том, кем был запрошен доступ к его персональным данным в системе электронного правительства [298]. Это значит, что в рамках государственных услуг уже заложен частичный механизм прозрачности запросов.

**6. Регулирование трансграничной передачи персональных данных.** В Международных стандартах отмечается, что при защите личной персональных данных важно учитывать не только внутренние правила, но и условия передачи персональных данных за рубеж. С точки зрения международного права Концепция «свободный обмен данными с доверием» (в английской версии: *Data Free Flow with Trust - DFFT*) призвана обеспечить баланс между свободой передачи информации и сохранением высокого уровня приватности [299, с. 3-5]. В Принципах ОЭСР отмечается ответственность контролера: он отвечает за защиту персональных данных независимо от места их хранения и обработки. [160, с. 8]. При этом ОЭСР не рекомендует без веских оснований ограничивать трансграничные потоки персональных данных: передача персональных данных может ограничиваться лишь при отсутствии надлежащего уровня защиты на стороне получателя или в иных предусмотренных законом случаях. В ЕС трансграничные передачи персональных данных строго регулируются положениями GDPR. Передача персональных данных в страны без признанного надлежащего («адекватного») уровня защиты запрещена (при этом законодательство допускает исключения, например, на основании согласия субъекта или для защиты жизненно важных интересов) [300]. Передачи возможны либо на основании решения ЕК об надлежащем уровне гарантий (страна обеспечивает «европейский» уровень безопасности), либо при наличии специальных гарантий - стандартных договорных условий, обязательных корпоративных правил (в английской версии: *Binding Corporate Rules - BCR*) или других надежных механизмов. Такая система позволяет контролировать трансграничную передачу персональных данных и обеспечивать экстерриториальную защиту персональных данных субъектов (физических лиц). Однако строгие требования GDPR усложняют трансграничный обмен данными. Например, после решения Schrems II [301] передачи данных в США стали проблематичными для бизнеса.

В Казахстане трансграничная передача персональных данных длительное время регулировалась в минимальной степени. Формально страна позиционировалась как с наиболее свободным режимом передач (что упрощало интеграцию в глобальные сервисы), но на практике Закон РК «О персональных данных и их защите» 2013 г. лишь устанавливал общее условие - передача

разрешена при условии защиты данных страной-получателем, без четкого списка «безопасных» юрисдикций. Между тем мировые тенденции локализации стимулируют усиление требований - именно поэтому в проекте Цифрового Кодекса РК (ст. 74, 77) операторы обязаны уведомлять субъектов о намерении передавать персональные данные за рубеж [302]. Проект предусматривает дополнительные меры для трансграничной обработки данных; конкретные механизмы (перечни стран, посредники и т. п.) в официальных источниках пока (по состоянию на август 2025 года) не были закреплены. Для Республики Казахстан важно обеспечить баланс между процессами международной интеграции и защитой персональных данных субъектов (физических лиц). Таким образом, эффективное регулирование трансграничной передачи персональных данных становится ключевым критерием эффективности системы защиты персональных данных, и в Республике Казахстан данный механизм находится в стадии формирования, с учетом подходов ЕС и ОЭСР.

**7. Судебная оценка электронных доказательств по делам о нарушении прав субъектов персональных данных.** Эффективность судебной защиты напрямую влияет на общую эффективность системы защиты персональных данных: субъект персональных данных должен иметь реальную возможность доказать факт неправомерной обработки его персональных данных и получить эффективные средства правовой защиты (включая возмещение вреда (ущерба) и обеспечение привлечения виновных лиц к установленной законом ответственности). В сфере информатизации ключевые доказательства электронные: журналы событий, записи в базах, переписки, метаданные и проч. Законодательство должно четко устанавливать, принимаются ли судом такие доказательства и на каких условиях. Иначе могут возникать произвольные решения (одни суды принимают снимки с экрана чата, другие - нет). При проверке электронных доказательств важны три условия: подтверждение источника данных, их целостность (например, через хеш-функции или электронную подпись [303]) и соблюдение процессуальных норм при сборе. Внедряются стандарты фиксации электронных доказательств: применение электронной подписи, проставление метки времени, нотариальное обеспечение доказательств (например, осмотр веб-страниц) и т. п. Без соответствующих процессуальных норм суду затруднительно провести надлежащую оценку электронным доказательствам (таким как выписки по банковским счетам, данные переписки в мессенджерах, журналы событий информационной системы (логи-файлы)) и принять обоснованное решение.

Регламент (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года «об электронной идентификации и доверительных услугах для электронных транзакций на внутреннем рынке и об отмене Директивы 1999/93/ЕС» (в английской версии: *electronic Identification, Authentication and Trust Services - eIDAS*) гарантирует, что электронные подписи и отметки времени имеют юридическую силу и допускаются в качестве доказательств [304, с. 1-2]. Многие страны ввели в процессуальное право понятие «электронный документ» как особого вида доказательство. Например, файлы журналов событий признаются доказательством при условии их заверения экспертом или

подписания ключом системы. Работает и трансграничный механизм сбора электронных доказательств (на основе Конвенции о киберпреступности и регламента ЕС об электронных доказательствах [305; 306, с. 21-24]). В ЕС суды изначально доверяют цифровым доказательствам благодаря общим стандартам (ЭЦП, доверенным сервисам), хотя остаются проблемы обеспечения цепочки хранения и защиты их от фальсификаций.

В РК есть базовые достижения - ГПК РК (ч. 6 ст. 100) признает электронные документы (или их копии с ЭЦП) письменными доказательствами. С 2021 года введены нормы об электронном судопроизводстве (ст. 133-1, 133-2), позволяющие предоставлять материалы в электронной форме. То есть технически возможна работа с электронными документами. Проблема заключается в верификация содержимого. Если документ подписан ЭЦП, то претензий мало. Однако многие электронные доказательства (например, данные переписки в мессенджере WhatsApp, снимки экрана (скриншоты), видеозаписи с камер наблюдения) не заверены электронной подписью. Для подтверждения достоверности электронных доказательств (или в случае их оспаривания) суд вправе назначить судебную экспертизу (а также оценивает представленное нотариальное обеспечение доказательств), от полноты и обоснованности заключения которой во многих случаях зависит исход дела.

Для повышения эффективности защиты персональных данных необходимо закрепить понятие «электронного доказательства» во всех процессуальных кодексах и установить четкие критерии его допустимости. Например, разрешить данные журнала (лог-файла) как доказательство, если оператор системы заверил его ЭЦП или независимый аудитор подтвердил целостность. Проект Цифрового кодекса РК уже затрагивает электронный документооборот (пп. 4) п. 2. ст. 7) и объявляет право субъектов цифровых данных на судебную защиту цифровых прав (п. 4 ст. 11), а также предполагает унификацию подходов с учетом трансграничности (ст. 77). Это свидетельствует об осознании проблемы на уровне государственной политики. К преимуществам правовой системы РК относится развитие электронного судопроизводства: суды активно переходят на цифровой формат и принимают электронные доказательства. Недостатком является отсутствие специализированных механизмов поддержки физических лиц в этом процессе. Субъект персональных данных, пострадавший в результате нарушения, зачастую не имеет самостоятельной возможности обеспечить надлежащее заверение журналов событий или системных журналов оператора для целей доказывания. Так, субъект персональных данных не имеет прямого доступа к аудиторским журналам (лог-файлам) системы оператора (предполагаемого нарушителя) и не может подтвердить факт нарушения без истребования указанных сведений в судебном порядке. Из этого вытекает смежная задача - обязать операторов данных вести и по запросу суда предоставлять журналы регистрации. В конечном счете, критерий судебной проверяемости объединяет все предыдущие. Если в законе надежно прописаны законные цели: минимизация данных, прозрачность и прочие принципы, цифровые следы их соблюдения сохранятся, то суд будет в состоянии защитить права пострадавшего.

Таким образом, критерии эффективности защиты персональных данных представляют собой взаимосвязанную систему, отражающую системный подход. Они охватывают весь цикл обработки данных - от сбора до судебной защиты. Законность и минимизация задают основу системы, оценки воздействия на защиту персональных данных и прозрачность обеспечивают процесс, а контроль трансграничных потоков персональных данных и судебная защита связывают систему с внешней средой. Все элементы взаимодополняют друг друга, а отсутствие любого (например, непрозрачность согласий) снижает эффективность системы.

С функциональной точки зрения каждый критерий выполняет конкретную защитную функцию: законность целей предотвращает произвольное вмешательство в частную жизнь; минимизация снижает риски злоупотреблений, оценка воздействия на защиту персональных данных минимизирует вред; прозрачность и информированность дают субъекту контроль над персональными данными; журналирование обеспечивает подотчетность, трансграничный контроль сохраняет суверенитет; судебная проверяемость восстанавливает нарушенные права. Все вместе эти меры обеспечивают эффективное правовое регулирование, защищая права субъектов и выполняя основную функцию системы - защиту прав и свобод личности.

Аксиологический подход демонстрирует ценностную основу критериев: законность целей связана с верховенством права; минимизация - с достоинством личности; оценка воздействия на защиту персональных данных - с безопасностью; прозрачность согласий - с автономией и свободой выбора; журналирование - с ответственностью и доверием; контроль трансграничных потоков - с суверенитетом; судебная проверяемость - со справедливостью. В итоге, система этих критериев ориентирована на защиту прав и свобод личности, а не на формальные процедуры.

Социально-психологический аспект проявляется в доверии общества: соблюдение принципов законности, минимизации данных и прозрачности обработки повышает его, поскольку субъекты персональных данных ощущают контроль над ними и испытывают меньшую обеспокоенность в связи с использованием технологий. Напротив, неинформированные или «навязанные» согласия подрывают доверие и вызывают обеспокоенность. Применение риск-ориентированного подхода свидетельствует об ориентации на противодействие актуальным угрозам и способствует внедрению новых технологий. Надлежащее регулирование трансграничной передачи персональных данных укрепляет режим их безопасности, поскольку субъекты персональных данных осведомлены, что их данные не будут передаваться на территорию иностранных государств без надлежащих правовых оснований и гарантий. Доступность средств судебной защиты в случае инцидентов (нарушений) безопасности персональных данных способствует укреплению доверия к правовой системе. Совершенствование правового регулирования с акцентом на эффективном обеспечении прав субъектов и принципа прозрачности могло бы способствовать повышению доверия общества, улучшая социально-психологический климат и повышая законность соответствующих правовых норм в обществе.

**Международные стандарты и национальные инициативы.** В международных стандартах определяется содержательная основа критериев эффективности защиты персональных данных. В GDPR кодифицированы ключевые начала: законность и ограничение целей, минимизацию и прозрачность, условия действительного согласия, подотчетность (включая оценку воздействия на защиту персональных данных и защиту персональных данных на этапе проектирования и по умолчанию), целостность и конфиденциальность, правила трансграничных передач и судебную защиту.

В свою очередь, в руководящих принципах ОЭСР закреплены восемь базовых принципов - ограничение сбора, «качество данных», определенность целей и ограничение использования, безопасность, открытость, участие субъекта и подотчетности - и дополняют их риск-ориентированным управлением приватностью, а также акцентом на международной совместимости и кооперации надзорных органов. Обсуждение ВЭФ/ООН содержания «цифрового доверия» (в английской версии: *«digital trust»*) усиливает ту же логику: прозрачность, участие пользователя, подотчетность, общие стандарты безопасности и принципо-ориентированное, технологически нейтральное регулирование [295, с. 4; 296, с. 6, 15; 307, с. 16-32; 308]. В этом смысле предложенные критерии не являются абстрактными: они отражают признанные международные стандарты и охватывают механизмы их практической реализации (такие как модели доверия, проведение оценок, надзор, многостороннее участие).

Инициативы РК движутся в направлении этой повестки, но находятся на стадии институционального оформления. Послание Президента РК [11], «Цифровой Казахстан» [68] и материалы к проекту Цифрового кодекса [261] фиксируют потребность в систематизации цифровых прав, ограничении сбора чувствительных персональных данных, алгоритмических экспертизах и «регуляторных песочницах», а также в унификации правил трансграничных передач персональных данных с ориентацией на надлежащий уровень гарантий защиты и международное сотрудничество. Одновременно усиливаются требования к обеспечению безопасности в государственном секторе; развиваются институты электронного правосудия и инструменты обеспечения прозрачности для общества, в то время как санкционные и надзорные механизмы в частном секторе пока применяются сравнительно умеренно. Для достижения сопоставимого с ЕС/ОЭСР уровня эффективности правового регулирования требуются: императивное (обязательное) закрепление процедуры оценки воздействия на защиту персональных данных для тех операций обработки, которые представляют (создают) высокий риск для прав и свобод физических лиц; формализованная подотчетность (реестры операций, журналирование и проверяемость согласий); ясные процедуры и критерии трансграничных передач персональных данных; а также институциональные гарантии независимого надзора и международной правоприменительной кооперации. Такая «конфигурация» позволит преобразовать декларативное следование стандартам в устойчивую практику защиты прав и свобод личности в цифровой среде.

*Таким образом,* по итогам анализа понятия, условий и критериев эффективности правового регулирования защиты персональных данных возможно сформулировать следующие выводы.

Эффективность правового регулирования защиты персональных данных представляет собой комплексную международно-правовую категорию, требующую применения комбинированного методологического подхода (системного, функционального, аксиологического). Эффективность определяется степенью полноты и согласованности правовых механизмов, гарантирующих реализацию фундаментального права на неприкосновенность частной жизни и права на защиту персональных данных в условиях глобальной цифровизации и обеспечивающих общественное доверие.

Для достижения высокой эффективности правового регулирования ключевыми условиями выступают институциональные гарантии, в частности, наличие независимого и ресурсно-обеспеченного надзорного органа по защите персональных данных, а также стабильность, целостность и технологическая нейтральность нормативной базы.

Обоснована система критериев оценки эффективности правовых режимов защиты персональных данных, основанная на степени имплементации общепризнанных международных стандартов (GDPR, Принципы ОЭСР). К фундаментальным критериям относятся: соблюдение принципов законности, справедливости, прозрачности и ограничения цели обработки; минимизация данных; обязательность (наличие императивной процедуры) оценки воздействия на защиту персональных данных для операций, связанных с высоким риском для прав и свобод физических лиц; эффективная реализация принципа подотчетности (включая документальное подтверждение (верифицируемость) согласия и ведение реестров операций обработки); наличие действенных (эффективных) механизмов регулирования трансграничной передачи персональных данных и наличие (закрепление) четких процессуальных критериев судебной оценки (допустимости) электронных доказательств.

Сравнительно-правовой анализ показывает, что законодательство Республики Казахстан в сфере защиты персональных данных находится в процессе активной гармонизации с рассматриваемыми (передовыми) международными стандартами. Для достижения полного соответствия этим стандартам и обеспечения условий для свободной (надлежащей) трансграничной передачи персональных данных (включая возможное получение решения об «адекватности»), требуется императивное (обязательное) законодательное закрепление процедуры оценки воздействия на защиту персональных данных, а также укрепление (или обеспечение фактической) институциональной независимости уполномоченного органа по защите персональных данных.

Определив критерии эффективности правового регулирования защиты персональных данных, перейдем к рассмотрению направлений повышения этой эффективности (подраздел 3.2).

### 3.2 Направления совершенствования правового регулирования защиты персональных данных

В данном подразделе представлен план предполагаемых мероприятий Республики Казахстан по повышению эффективности защиты субъектов персональных данных и юридических лиц, основанный на передовых международных практиках и учете национальных особенностей. Цель - сформировать целостную систему управления с согласованным комплексом организационных, правовых и технологических мер. В данную систему входят: 1) введение института независимого надзорного органа по защите персональных данных; 2) развитие кадрового потенциала и внедрение института уполномоченного лица по защите персональных данных в специальных секторах; 3) ведение реестров операций и инвентаризацию массивов персональных данных; 4) проведение оценки воздействия обработки на защиту персональных данных; 5) применение типовых договоров между оператором и обработчиком (включая соглашения об уровне оказания услуг) с закреплением мер безопасности и распределением ответственности; 6) проведение регулярных правовых и технических проверок (аудита); 7) внедрение индивидуализированной (субъектно-ориентированной) защиты данных; 8) использование цифровых следов и журналов событий как инструмента подотчетности.

**Проект институциональной модели независимого надзорного органа по защите персональных данных.** С учетом национального контекста целесообразно предусмотреть орган специализированного надзора в сфере защиты персональных данных и алгоритмических рисков. Возможны три конструктивных решения: 1) полностью независимый орган вне системы министерств с гарантиями несменяемости руководителя на фиксированный срок и самостоятельной сметой; 2) квази-независимое агентство при Администрации Президента либо при одной из палат Парламента - с высоким статусом и меньшей административной инерцией; 3) реформирование и усиление существующего звена (например, профильного комитета при Министерстве искусственного интеллекта и цифрового развития РК) путем закрепления функциональной автономии, отдельной бюджетной строки и процедурной независимости при принятии предписаний (см. ст. 51-52 GDPR) [4; 14; 309, с. 3]. Подпункт 6-1) п. 1 ст. 27-1 Закона РК «О персональных данных и их защите» уже предусматривает создание консультативного совета по вопросам персональных данных и их защиты.

В качестве базовой модели предлагается независимый государственный орган вне системы министерств со следующими нормативными положениями. Правовой статус: исключительная компетенция в области персональных данных и алгоритмических рисков; запрет на получение указаний по конкретным делам от любых органов исполнительной власти; процессуальная самостоятельность. Руководство и структура: руководитель назначается на 5-7 лет без немедленного повторного срока; основания досрочного прекращения исчерпывающие (вступивший в силу обвинительный приговор, грубое дисциплинарное

нарушение, устойчивый конфликт интересов). Решения о крупных санкциях и методических актах утверждаются коллегиальным органом (3 или 5 членов). Финансирование и независимость - отдельная бюджетная программа с правом целевых внебюджетных поступлений в ограниченном объеме (сертификация/регистрация - не более установленного процента от годового финансирования); собственная смета, кадровая служба и система закупок.

Полномочия независимого надзорного органа: 1) инспекции (плановые/внеплановые) с правом доступа к помещениям и системам, истребования документов и журналов (лог-файлов), проведения опросов и экспертиз; 2) составление предписаний об устранении нарушений и приостановлении (ограничении) обработки, включая эксплуатацию высокорисковых ИИ-систем; 3) санкционные меры с прогрессивной шкалой, привязанной к обороту крупных операторов; 4) ведение реестра оценки воздействия на защиту персональных данных и реестра высокорисковых ИИ-систем, утверждение перечня «высокого риска»; 5) требование независимого внешнего аудита алгоритмов для операторов, превышающих пороговые критерии масштаба/риска (см. Закон ЕС о цифровых услугах [199], ст. 34 - оценка системных рисков; ст. 37 - независимый аудит; Регламент ЕС об ИИ [255] - эффективные расширенные и корректирующие полномочия надзора, включая доступ к данным/документации/исходному коду); 6) утверждение кодексов практики, типовых договоров и стандартных оговорок для трансграничной передачи; 7) методическое сопровождение операторов (разъяснения по согласию, минимизации, срокам хранения, прозрачности). Пороговые критерии обязательного внешнего аудита устанавливаются регулятором (масштаб аудитории, доля рынка, категории (объем) чувствительных данных и иные объективные факторы).

Процедурные гарантии и судебная защита: обязательный прием и рассмотрение жалоб субъектов персональных данных; уведомление оператора о начале производства и сроках; мотивированность решений и их опубликование в обезличенном виде; право регулятора на иск/вступление в процесс в защиту неопределенного круга лиц; судебное обжалование актов регулятора в сокращенные сроки (например, в течение 30 дней со дня получения) с обеспечительными мерами; ежегодный публичный отчет с детальной статистикой (см. ст. 59 GDPR [4]); срок рассмотрения жалоб - до 60 дней.

Взаимоотношения с государственными органами строятся на функциональном разграничении. С Министерством искусственного интеллекта и цифрового развития РК осуществляется разделением функций: министерство формирует политику и развитие цифровой экосистемы, регулятор осуществляет контроль и правоприменение; закрепляется запрет ведомственных указаний регулятору по индивидуальным делам [310]. С прокуратурой заключается меморандум о недопущении дублирующих проверок: прокуратура осуществляет общий надзор за законностью, регулятор осуществляет специализированный технически-правовой надзор; предусмотрены обмен материалами, координация внеплановых проверок и единые стандарты реагирования [311]. С правоохранительными органами и финансовым мониторингом

взаимодействие осуществляется через формализацию запросов данных на основе мотивированных оснований с фиксацией правовых целей обработки; регулятор проводит аудит законности и соразмерности запросов, включая чувствительные категории данных (при необходимости - судебное разрешение и отчетность).

Этапы внедрения (переходные положения): преобразование действующего консультативного совета при Министерстве искусственного интеллекта и цифрового развития РК в экспертный комитет при регуляторе; инвентаризация подзаконных актов и реестров; утверждение методик оценок воздействия на защиту персональных данных и аудита алгоритмов; обучение кадров (алгоритмический аудит, информационная безопасность, кибербезопасность и проч.); «комплаенс-каникулы» на 6-9 месяцев для добросовестных (по принципу справедливости) операторов при выполнении дорожной карты.

Ключевые правовые вызовы и меры смягчения: 1) независимость и бюджетный контроль - закрепление отдельной бюджетной программы и запрет целевых поручений по делам; 2) разграничение с прокуратурой - прямой запрет дублирующих проверок, приоритетность материала ведущего органа, совместные стандарты отбора дел; 3) доступ к данным (исходному коду) при охраняемых тайнах - процедура пропорционального доступа (минимально достаточный объем, протоколирование, судебное разрешение для особо чувствительных случаев); 4) совместимость санкций с КоАП РК - отдельная глава с расширенным набором мер и процессуальными гарантиями; 5) трансграничные потоки данных - утверждение стандартных договорных оговорок и критериев эквивалентности режимов; 6) кадровая емкость - целевое финансирование на экспертов по аудиту ИИ, создание реестра внешних аттестованных аудиторов; 7) единая доказательная база - обязательные журналы операторов, стандарты верификации и воспроизводимости результатов аудита. Предлагаемая архитектура согласуется с лучшими практиками ЕС по независимости органом по защите данных (ст. 51-52 GDPR [4]), системной оценке и внешнему аудиту алгоритмических рисков (ст. 34, 37 Закона ЕС о цифровых услугах [199]) и «эффективным полномочиям» надзора в отношении высокорисковых ИИ-систем [255], а также с национальным правовым регулированием в сфере защиты персональных данных и с ролью органов прокуратуры по общему надзору за законностью. Дополнительно предполагается использовать цифровые следы как инструмент контроля и подотчетности операторов при обработке персональной информации.

**2. Развитие кадрового потенциала и внедрение института уполномоченного лица по защите персональных данных в ключевых секторах.** Стратегически значимой мерой выступает развитие кадрового потенциала посредством разработки и внедрения междисциплинарных программ подготовки по направлению «технологическая политика и государственное управление», «цифровое право», ориентированных на специалистов, сочетающих инженерные, правовые и управленческие компетенции. Подобные программы уже успешно реализуются в ведущих мировых научно-образовательных центрах, таких как: Массачусетский технологический институт

[312], Колумбийский университет [313], Стэнфордский университет [314], Гарвардский университет [315], Парижский институт политических исследований [316], Делфтский технический университет [317], Университетский колледж Лондона [318], Университет Цинхуа [319], Университет Китайской академии наук [320], Московский государственный юридический университет имени О. Е. Кутафина [321; 322; 323; 324], Национальный исследовательский университет «Высшая школа экономики» [325; 326], Московский государственный университет имени М. В. Ломоносова [327] и др. Подготовленные таким образом специалисты призваны преобразовывать технические риски в юридически проверяемые требования и критерии и применять их при разработке, внедрении и экспертизе правовых норм.

Одним из ключевых шагов в этом направлении является внедрение функции уполномоченного лица по защите персональных данных в государственных учреждениях и финансовых организациях. Зарубежный опыт, прежде всего ЕС, показывает, что назначение уполномоченного лица по защите персональных данных в государственных органах и компаниях, обрабатывающих большие объемы особо чувствительной информации, значительно укрепляет систему защиты. В европейском законодательстве должность уполномоченного лица по защите персональных данных обязательна для многих государственных органов и крупных организациях с соответствующими категориями данных. В законодательстве РК нет «европейской» обязанности назначать полноценного уполномоченного лица по защите персональных данных, однако юридические лица обязаны назначать лицо, ответственное за организацию обработки персональных данных (ст. 25 Закона РК «О персональных данных и их защите»). В специальном режиме МФЦА действует ближе к модели ЕС. Правила защиты данных МФЦА [163] предусматривают обязательное назначение уполномоченного лица по защите персональных данных для органов МФЦА и для контролеров/обработчиков, систематически выполняющих высокорисковые обработки, а также вводят ежегодную оценку и оценку воздействия на защиту персональных данных для высокорисковых операций (разд. 10-1-10-5). Это означает, что «пробел» касается прежде всего общего режима РК, тогда как в МФЦА соответствующие требования уже закреплены.

Для государственных органов и финансовых институтов (банков, страховых организаций, платежных систем и проч.) назначение уполномоченного лица по защите персональных данных позволит более единообразно применять национальные и международные стандарты при обработке персональных данных. Уполномоченное лицо по защите персональных данных должно обладать независимостью и достаточными полномочиями: правом проводить проверки, вносить рекомендации по изменению процедур обработки, приостанавливать операции, не соответствующие нормам закона, и т. д. Закрепление такого статуса на законодательном уровне повысит институциональную устойчивость системы защиты персональных данных. Иностранный опыт подтверждает, что наличие уполномоченного лица по защите персональных данных институционализирует ответственность контролеров

(операторов) за соблюдение требований и служит встроенным механизмом постоянного мониторинга соответствия законодательству. Таким образом, внедрение института ответственного по защите персональных данных является фундаментальным шагом к созданию надежной системы защиты данных в стране.

**3. Ведение реестров операций и инвентаризация персональных данных.** Международные стандарты в области защиты персональных данных (например, GDPR) требуют от организаций ведения подробных записей обо всех операциях с персональными данными. Так, ст. 30 GDPR предписывает контролерам и обработчикам фиксировать «цели обработки», категории обрабатываемых данных, категории получателей (включая третьи страны), сроки уничтожения и описание мер безопасности. Наличие такого реестра операций создает основу для внутреннего и внешнего контроля соответствия требованиям законодательства. В частности, централизованный реестр обработки упрощает проверку и аудит - регулятор по запросу получает доступ к полному описанию процессов обработки и использованным мерам защиты.

Важным дополнением к учету операций является «инвентаризация данных» (в английской версии: «*data mapping»*). Это систематический процесс выявления всех персональных данных в организации и путей их движения между информационными системами, а также учет внешних передач. Результатом инвентаризации становится «карта данных» - наглядная схема, где указаны категории персональных данных, их места хранения, ответственные лица и внешние получатели. Для проведения инвентаризации обычно рекомендуют следующий подход:

- выявление бизнес-процессов и информационной системы персональных данных: определить все ключевые процессы, в рамках которых обрабатываются персональные данные, и соответствующие информационные системы. Это гарантирует, что не будет упущена ни одна система с персональными данными;
- описание состава и категорий персональных данных: для каждой системы перечислить, какие именно персональные данные в ней обрабатываются (например, ФИО, ИИН, медицинская информация и пр.), отнести их к обычным или специальным категориям и указать цель обработки;
- идентификация субъектов и объемов: зафиксировать, чьи персональные данные хранятся (сотрудники, клиенты, контрагенты и т. д.) и примерный объем (число записей), что важно для оценки уровня защиты;
- маршруты передачи: отследить, как персональные данные перемещаются внутри организации и передаются третьим лицам (включая трансграничные передачи), чтобы знать все точки обмена. Меры защиты и доступ: задокументировать, какие технические и организационные меры применяются в каждой системе (шифрование, авторизация, резервные копии и т. п.), и кто имеет доступ к данным. В частности, следует указать права доступа (роли или группы пользователей, имеющие доступ к системе с персональными данными) и методы аутентификации;

- сроки хранения: определить регламентированные сроки удаления или обезличивания данных в каждой системе.

Все эти сведения фиксируются в едином реестре и регулярно актуализируются. Сформированный по итогам инвентаризации реестр используется для дальнейших задач - например, для оценки уровня защищенности каждой системы и обоснования выбора мер защиты. Как отмечается экспертами, правильно составленная карта данных повышает прозрачность: сотрудники и менеджеры видят, какие данные, где обрабатываются и кто за них отвечает. Кроме того, такая «карта» облегчает доступ к нужной информации при внешних проверках.

Инвентаризация и реестры обработки существенно повышают эффективность управления персональными данными. Во-первых, они создают дисциплинирующий эффект: каждый акт сбора, просмотра, изменения или передачи персональных данных фиксируется, а значит, сотрудники осознают повышенную ответственность за свои действия. Во-вторых, наличие подробных записей облегчает внешние проверки - органы надзора могут оперативно получить отчетность по всем операциям. Наличие полного и актуального реестра процессов обработки персональных данных также является существенным, поскольку это упрощает оценку рисков, связанных с такой обработкой. Это позволяет выявить (спрогнозировать) потенциальные источники (уязвимости) нарушений безопасности персональных данных и своевременно принять надлежащие меры по усилению режима защиты. Как указывают зарубежные источники, такой подход «помогает отслеживать потоки данных» и «обеспечивает ведение детальных записей о процессах обработки».

На сегодняшний день Закон РК «О персональных данных и их защите» не предусматривает обязанности вести детальный реестр всех операций обработки персональных данных. Это затрудняет доказуемость соблюдения принципов законности, целевого ограничения и соразмерности (минимизации) при проверках, а также усложняет прослеживаемость ответственности в случае инцидентов. С учетом быстрого развития электронных сервисов и трансграничного обмена данными внедрение практик инвентаризации и учета обработок представляется особенно актуальным. В специальном режиме МФЦА установлено более строгое регулирование: контролеры обязаны вести записи операций обработки и уведомлять Комиссара по защите персональных данных; обработчики персональных данных обязаны обеспечивать выполнение требований по договору, предоставлять информацию и содействовать проверкам (разд. 16-2, 19 Регламента защиты персональных данных МФЦА [163, с. 17-19, 21], п. 4.1-4.2 Правил защиты данных МФЦА [164, с. 6-8]).

**4. Проведение оценки воздействия обработки на защиту персональных данных.** Оценка воздействия на защиту персональных данных - это проактивный анализ рисков, являющийся неотъемлемой частью современной модели управления персональными данными. Предлагается ввести процедуру оценки воздействия на защиту персональных данных для новых процессов и систем, используя стандартизированные шаблоны. Международная практика (особенно ст. 35 GDPR) предписывает проводить оценки воздействия на защиту

персональных данных перед началом любой обработки, которая может нести высокий риск для прав субъектов персональных данных. Оценка предусматривает системный анализ планируемых операций с персональными данными, выявление потенциальных уязвимостей и негативных последствий для конфиденциальности, а также разработку мер по снижению этих рисков. В рамках предлагаемой «дорожной карты» планируется разработать типовые формы и методики проведения оценки, адаптированные к законодательству Казахстана и специфике локальных отраслей.

Единый шаблон оценки воздействия на защиту персональных данных упростит внедрение этой практики в казахстанских организациях. В шаблоне могут быть собраны вопросы о законности и целях обработки данных, объеме и чувствительности данных, мерах безопасности (шифрование, псевдонимизация и др.), вероятности инцидентов и плане реагирования. Заполнение шаблона до запуска проекта позволяет выявить риски на ранней стадии и внедрить соответствующие меры защиты. Результаты оценки направляются на рассмотрение уполномоченному лицу по защите персональных данных (если предусмотрено) или руководству для принятия решения: продолжать проект, скорректировать его или ввести дополнительные гарантии. Хотя оценка воздействия на защиту персональных данных - новшество для Казахстана, этот инструмент соответствует системному превентивному подходу к защите персональных данных. Опыт ЕС показывает, что внедрение оценки не только сокращает число инцидентов, но и формирует культуру осознанного обращения с данными, поскольку организации начинают рассматривать защиту данных как постоянный процесс управления рисками. Таким образом, внедрение оценки (с едиными шаблонами и рекомендациями регулятора) является важным шагом в создании эффективной системы защиты персональных данных, дополняя требования закона практическими механизмами.

**5. Применение типовых договоров между оператором и обработчиком (включая соглашения об уровне оказания услуг) с закреплением мер безопасности и распределением ответственности.** Многочисленные нарушения безопасности персональных данных происходят не только по вине самих операторов (контролеров), но и при передаче данных третьим лицам (включая обработчиков). В цифровой экономике распространено привлечение сторонних сервисов, облачных провайдеров и аутсорсинговых компаний для обработки персональных данных. В этих случаях важным становится надежное договорное регулирование отношений между владельцем данных (контролером) и обработчиком (третьей стороной). Так, европейское законодательство (ст. 28 GDPR) строго требует наличия договора при привлечении обработчика и установления его конкретных обязанностей по защите данных.

В Казахстане Закон «О персональных данных и их защите» оперирует терминами «собственник», «оператор» и «третье лицо», при этом третьи лица обязаны соблюдать те же требования, что и оператор. Однако специальных стандартов типовых соглашений на обработку персональных данных законом не установлено. Из-за этого многие передачи персональных данных (например, при аутсорсинге ИТ-услуг или маркетинге) осуществляются на основании общих

гражданско-правовых договоров, где не прописаны детальные меры защиты информации. Такой подход порождает правовую неопределенность: затрудняется распределение ответственности в случае нарушения безопасности персональных данных; создается неясность в отношении обязательств по уведомлению о нарушениях; отсутствуют достаточные гарантии обеспечения надлежащего уровня защиты при обработке этих данных.

Для повышения эффективности защиты персональных данных целесообразно разработать и внедрить типовые соглашения об уровне оказания услуг между контролерами (операторами) и обработчиками. Такое соглашение должно включать четко определенные цель и объем поручаемой обработки данных, а также запрет на использование персональной информации в иных целях. Необходимо закрепить требования к сохранности и конфиденциальности данных: конкретные организационно-технические меры, соответствующие стандартам информационной безопасности. В соглашении также следует определить порядок мониторинга соблюдения установленных условий обработки (например, право собственника базы персональных данных или оператора проводить аудиты или получать отчеты) и обязательства по уведомлению о выявленных нарушениях безопасности персональных данных.

Наличие типового соглашения обеспечит единообразие практики: операторы и их контрагенты будут действовать в ясном правовом поле, что повысит предсказуемость и эффективность мер защиты. Такое соглашение укрепляет принцип подотчетности: оператор (собственник) персональных данных при передаче их третьей стороне не снимает с себя ответственность, а, напротив, контролирует выполнение требований их защиты на договорной основе. Представляется целесообразным, чтобы уполномоченный государственный орган (например, Министерство искусственного интеллекта и цифрового развития РК) разработал рекомендованные образцы таких договоров или минимальные обязательные условия. Это позволит снизить регуляторную фрагментацию и обеспечить соответствие практики РК международным стандартам, что особенно важно для трансграничных потоков данных.

**6. Проведение регулярных правовых и технических проверок (аудит).** Регулярный правовой и технический аудит необходим для повышения эффективности защиты персональных данных. Внутренний аудит может проводить служба информационной безопасности или комплаенс-подразделение (с участием уполномоченного лица по защите персональных данных) и заключается в периодической проверке соответствия текущих практик требованиям законодательства. Мероприятия проводятся на предмет актуальности политик информационной безопасности, обработки, наличия у субъектов данных согласий или иных правовых оснований, соблюдения принципов минимизации и ограниченных сроков хранения, реализации мер защиты (шифрование, резервное копирование, контроль доступа) и ведения надлежащей документации [328; 329; 330; 331; 332; 333]. Такие проверки помогают выявлять несоответствия и устранять их. Обнаруженные пробелы устраняются через корректировку процессов, дополнительное обучение сотрудников и обновление документов. Международная сеть аудиторских и

консалтинговых фирм ПрайсуотерхаусКуперс (PwC) рекомендует при этом разработать план внутреннего аудита и регулярно оценивать его [334], а также документально фиксировать получение согласий субъектов на обработку.

Параллельно внешние аудиты обеспечивают независимую оценку защищенности системы. Международная практика включает добровольную сертификацию (например, стандарта ISO/IEC 27701:2022 для систем управления конфиденциальной информацией, расширяющего ISO/IEC 27001:2019 мерами по управлению конфиденциальностью) [217, с. 11, 13]. Соответствие ISO/IEC 27701:2022 демонстрирует внедрение структурированного управления конфиденциальностью в организации [335, с. 24]. Такая сертификация укрепляет доверие партнеров и подтверждает, что компания системно выполняет требования по защите данных. Кроме того, внешние эксперты могут обнаруживать уязвимости, которые остались незамеченными при внутренних проверках, что повышает надежность системы защиты.

В Казахстане законодательными изменениями от декабря 2023 года был усилен государственный контроль в сфере персональных данных. МЦРИАП (в настоящее время - Министерство искусственного интеллекта и цифрового развития РК) было наделено полномочиями проводить внеплановые проверки организаций на предмет соблюдения закона о персональных данных (ст. 27-2, 27-3 ЗРК «О персональных данных и их защите»). По результатам таких проверок выдаются предписания и могут применяться санкции за выявленные нарушения (ст. 79 КоАП РК). В новых условиях игнорирование требований законодательства становится особенно рискованным, а проактивный аудит позволяет выявлять и устранять несоответствия до начала проверки уполномоченным органом.

Для повышения эффективности рекомендуется разработать методические рекомендации и отраслевые стандарты аудита соответствия Закону РК «О персональных данных и их защите». Например, возможно предусмотреть обязательную ежегодную техническую экспертизу для крупных государственных информационных систем и регламентированные правовые аудиты для частного сектора. Результаты таких проверок могут быть доведены до сведения уполномоченного органа или акционеров, что создает дополнительный стимул к устранению выявленных нарушений. В целом аудит как элемент системы управления защитой персональных данных обеспечивает обратную связь: он измеряет эффективность мер безопасности, выявляет пробелы и учитывает новые угрозы, способствуя непрерывному совершенствованию практик защиты.

**7. Внедрение индивидуализированной (субъектно-ориентированной) защиты персональных данных.** Персонализированная защита персональных данных - концепция настройки мер защиты с учетом контекста обработки, категории данных и уязвимости субъекта. Предложенный исследователями, этот подход смещает акцент с универсальных мер, рассчитанных на «среднего» пользователя, на систему гибких мер, учитывающих уникальные риски и потребности личности при неизменности базовых прав и гарантий [336, с. 577-592]. Иными словами, уровень и режим защиты информации

адаптируются к особенностям конкретного субъекта, контексту обработки и его персональным рискам.

Законодательство о персональных данных предполагает общие стандарты защиты для всех, за исключением отдельных случаев (например, биометрических или специальных категорий данных). Концепция «персонализированной защиты» призвана расширить права субъектов персональных данных - предоставить им активную роль в управлении своими данными и инструменты для индивидуальной настройки параметров конфиденциальности. К примеру, посредством электронных сервисов субъект персональных данных сможет управлять параметрами доступа к своим данным и выбирать режим конфиденциальности - от строгого до более гибкого, допускающего передачу данных для конкретных целей [337]. Выбранные субъектом параметры конфиденциальности должны имплементироваться оператором (контролером) посредством применения адекватных технических и организационных мер (например, применение усиленного шифрования, установление сокращенных сроков хранения) и влечь соответствующие правовые последствия (в частности, необходимость получения дополнительного согласия при обработке в целях, выходящих за пределы установленных параметров).

Правовой аспект персонализированной защиты предполагает адресную оценку и минимизацию рисков для прав и свобод конкретного физического лица (субъекта персональных данных). Если обработка персональных данных представляет высокую угрозу правам определенного субъекта (учитывая его состояние здоровья, социальное положение и т. п.), то закон мог бы предусматривать дополнительные гарантии: более строгие условия для операторов, дополнительные проверки при сборе и использовании данных и т. д. Таким образом, защита становится не фиксированной, а динамичной, «настроенной» под потребности и риски конкретного субъекта.

Концепция персонализированной защиты также соответствует международному тренду человеко-ориентированного подхода в цифровом праве и идеям о суверенитете личных данных [308; 296, с. 4; 338; 247; 339].

Для Казахстана эта концепция реализована в создании «личных кабинетов» на веб-портале «электронного правительства», где субъект видит запросы на доступ к его данным и управляет дальнейшими разрешениями. Это повышает прозрачность и доверие к системе. Кроме того, применение принципов минимизации данных и строгого контроля доступа служит дополнительной технической и организационной мерой защиты от негативных последствий ошибок персонала и технических сбоев. При наличии таких заранее определенных ограничений обработки негативные последствия непреднамеренных нарушений безопасности персональных данных будут минимизированы. Интеграция концепции «персонализированной защиты» (субъектно-ориентированного подхода) в национальную стратегию и законодательство ознаменовала бы принципиально (концептуально) новый этап правового регулирования защиты персональных данных - переход к гибкой,

адаптивной модели регулирования, учитывающей разнообразие контекстов обработки и волеизъявление (выбор) субъектов персональных данных.

**8. Применение цифровых следов и журналов событий как инструмента подотчетности.** Любая операция с персональными данными оставляет цифровой след - автоматическую запись в системном журнале о том, кто, когда и какие действия совершил с этими данными [340, с. 170, 175; 341, с. 1, 4]. При надлежащем применении, цифровые следы (лог-файлы) становятся действенным механизмом для обеспечения соответствия установленным требованиям, подотчетности и возможности проведения аудиторских проверок. Надлежащим образом сконфигурированные системы ведения журналов и мониторинга позволяют в любой момент восстановить сведения об операциях по обработке персональных данных. Все это позволяет постоянно контролировать соблюдение установленных процедур.

Современные исследования подтверждают ключевую роль цифровых следов в обеспечении безопасности персональных данных [1; 342, с. 14; 343, с. 20-26; 344, с. 301-304]. Их применение в рамках модели управления данными означает неизбежность контроля - все операции фиксируются и могут быть проверены на соответствие требованиям. Это повышает уровень ответственности сотрудников и контрагентов и снижает риск преднамеренного неправомерного доступа к данным (злоупотребления полномочиями доступа). В случае нарушений безопасности персональных данных, таких как несанкционированный доступ или несанкционированное раскрытие (распространение) данных, цифровые (электронные) следы способствуют оперативному установлению причин нарушения и выявлению ответственных лиц, что является существенным для привлечения их к ответственности и минимизации негативных последствий.

Таким образом, цифровые следы институционализируют принцип подотчетности и обеспечивают проверяемость действий оператора в юридически значимой форме. Цифровые следы также обеспечивают подотчетность операторов перед субъектами данных и регуляторами. При обращении физического лица с жалобой или запросом оператор может предоставить журналы событий, подтверждающие, какие действия выполнялись с его данными, кому и на каком основании они передавались. Такая прозрачность облегчает разрешение споров и укрепляет доверие, обеспечивая фактическую (а не только декларативную) подотчетность оператора (контролера). На нормативном уровне существуют требования ведения и хранения журналов (лог-файлов) в течение установленного срока и регламентировать порядок их предоставления по запросу уполномоченных органов или самого субъекта данных [97; 298; 345; 346].

Технически важно надежно защищать сами журналы от несанкционированного изменения, например, с помощью методов хеширования, цифровых меток времени или блокчейн-технологий. Необходимо обеспечивать полную отслеживаемость операций обработки персональных данных. Реализация этого принципа превращает абстрактные требования закона в проверяемые события, а соблюдение режима защиты - в объективно

контролируемое обстоятельство. Таким образом, цифровые следы служат связующим звеном между правовым регулированием и фактическим поведением участников обработки данных, повышая эффективность комплаенс-механизмов.

**Обеспечение устойчивости правового режима защиты персональных данных к нормативной фрагментации, человеческим ошибкам и техническим сбоям.** Предлагаемые меры укрепляют защиту данных и повышают устойчивость правового режима к ключевым вызовам. Данные меры позволяют преодолевать нормативную фрагментацию: при сочетании международных стандартов и национальных особенностей модель в Казахстане должна оставаться работоспособной даже при расхождениях норм. Единая система регулирования, основанная на принципах подотчетности, прозрачности, риск-ориентированном подходе и «защите персональных данных на этапе проектирования и по умолчанию», позволяет компенсировать пробелы в законодательстве. Введение уполномоченного лица по защите персональных данных и утверждение внутренних процедур соблюдения требований обеспечивает надлежащую организацию обработки независимо от юрисдикции поставщиков услуг. Реестры операций обработки и соглашения об уровне оказания услуг компенсируют недостающие элементы регулирования (при том если конкретное правило не закреплено в законе, то его можно формализовать во внутренних политиках и договорах). Такая модель сохраняет преемственность с международными подходами, снижает уязвимость к расхождению норм и способствует соответствию критерию надлежащему уровню гарантий (эквивалентности уровня защиты) ЕС, упрощая трансграничное взаимодействие.

Многоуровневый контроль (включая деятельность уполномоченного лица по защите персональных данных, проведение внутреннего аудита и анализ журналов аудита (лог-файлов) способствует предупреждению и выявлению ошибок и неправомерных действий со стороны персонала. Регистрация операций и журналирование фиксируют неверные действия (например, ошибочную рассылку или удаление данных) и позволяют оперативно их исправить, а умышленные нарушения становятся рискованными из-за неизбежности обнаружения. Обучение сотрудников и их участие в оценке воздействия на защиту персональных данных и других процедурах соблюдения требований защиты персональных данных повышают уровень ответственности и бдительности. Разграничение доступа, основанное на принципе «необходимости знания» (в английской версии: *«need-to-know»*), ограничивает последствия ошибок (инцидентов), поскольку система не допускает доступа к персональным данным в объеме, превышающем предоставленные полномочия (служебную необходимость).

Для управления техническими рисками применяются регулярные технические проверки, которые выявляют уязвимости до их эксплуатации. Планы оценки воздействия на защиту персональных данных и планы реагирования на инциденты обеспечивают готовность к техническим сбоям: резервное копирование и аварийное восстановление встроены в систему управления рисками. Журналы событий (лог-файлы) позволяют оперативно установить характер инцидента (технического сбоя) и затронутые им

персональные данные, что способствует скорейшему устранению его последствий. Централизованный реестр может служить системой раннего оповещения, сигнализируя ответственному и администратору безопасности о массовом несанкционированном доступе. Взаимосвязанные элементы функционируют как единая система защиты с принципом резервирования: при недостаточной эффективности (или сбое) одного уровня задействуется другой.

Гибкость модели обеспечивается возможностью точечной корректировки без перестройки всей системы. При появлении новых угроз или изменении международных требований достаточно обновить шаблон оценки воздействия для новой категории риска либо дополнить соглашение об уровне оказания услуг новыми типами данных и гарантий. Таким образом, многоуровневая и адаптивная архитектура правового регулирования повышает его надежность (устойчивость) и отвечает ключевому критерию эффективности - способности правового режима сохранять свою действенность в условиях изменчивой технологической и нормативной среды.

*Таким образом,* по итогам анализа методов повышения эффективности защиты персональных данных могут возможно сформулировать следующие выводы.

Достижение высокой эффективности правового регулирования требует имплементации системного подхода, основанного на синергии правовых, организационных и технических мер, обеспечивающего устойчивость правового режима к нормативной фрагментации и технологическим рискам. Переход к риск-ориентированному управлению и практическая реализация принципа подотчетности являются стратегическими приоритетами.

Ключевыми направлениями повышения эффективности правового регулирования и обеспечения комплаенса выступают: нормативное закрепление обязательных процедур оценки воздействия на защиту персональных данных для высокорисковых операций; ведение детализированных реестров операций и инвентаризация персональных данных; стандартизация договорных отношений между операторами (контролерами), собственниками и обработчиками; проведение регулярных независимых аудитов. Внедрение концепции персонализированной (субъектно-ориентированной) защиты персональных данных усиливает контроль со стороны субъекта.

Фундаментальным условием эффективности национального правового режима является институциональная реформа. Обоснована необходимость учреждения в РК независимого надзорного органа по защите персональных данных, функционально автономного от исполнительной власти, наделенного расширенными надзорными и корректирующими полномочиями (включая аудит алгоритмов), а также закрепления статуса уполномоченных лиц по защите персональных данных в ключевых секторах.

Рассмотрев направления совершенствования правового регулирования защиты персональных данных, перейдем к анализу концепции «правовой технологии обеспечения защиты персональных данных» как механизма имплементации международных стандартов (подраздел 3.3).

### 3.3 «Правовая технология обеспечения защиты персональных данных» как механизм имплементации международных стандартов

**Феномен «нормативной турбулентности» при регулировании технологий ИИ.** Стремительное развитие технологий обуславливает появление не только новых объектов защиты, но и новых регуляторных вызовов. Ярким примером являются сферы применения технологий искусственного интеллекта (ИИ) и технологий обработки больших данных. Государства сталкиваются с феноменом «нормативной турбулентности» - состоянием права, при котором нормативная система не успевает за технологическими прорывами, реагируя на них поспешно и точечно [347, с. 12, 17; 348, с. 1862-1864]. Как отмечалось во введении диссертационного исследования, фрагментация правовых подходов различных стран (правоцентричного подхода ЕС до государственно-ориентированной модели КНР) приводит к ускоренной, но несистемной выработке норм в ответ на изменения, что порождает атмосферу правовой неопределенности [349, с. 11-13; 350, с. 108-112]. Нормотворческие процессы приобретают «турбулентный» характер: законодатели, стремясь предотвратить риски новых технологий, принимают законы «на ходу», часто без достаточной концептуальной проработки и согласованности с уже существующей нормативной базой. Системный подход требует признать, что право в цифровой сфере переживает этап трансформации, где первичные нормы (права, обязанности) и вторичные нормы (правила принятия, применения законов) находятся под давлением необходимости быстрых изменений.

В условиях описанной нормативной турбулентности традиционные методы правового регулирования, основанные на статичных предписаниях, демонстрируют недостаточную эффективность. Для обеспечения действенной имплементации международных стандартов (в частности, Конвенции 108+, GDPR) и достижения «адекватного уровня защиты» требуется переход к системному, риск-ориентированному управлению процессами обработки данных. В целях концептуализации данного подхода в настоящем исследовании вводится понятие «правовая технология обеспечения защиты персональных данных». Под данной категорией понимается интегрированная совокупность правовых, организационных и технических средств и процедур, направленных на реализацию прав субъектов персональных данных. Ключевыми элементами данной технологии выступают: 1) проведение оценки воздействия на защиту персональных данных; 2) реализация принципа подотчетности (включая ведение реестров операций и инвентаризацию массивов персональных данных); 3) имплементация принципа защиты данных на этапе проектирования и по умолчанию. Эта модель выступает необходимым механизмом адаптации национального правопорядка к вызовам цифровой эпохи, смещая акцент с реактивного нормотворчества на проактивное управление рисками и обеспечивая необходимую регуляторную совместимость.

Одним из проявлений «нормативной турбулентности» является смещение центров нормотворчества. Появляются ситуации, когда частные субъекты и технические эксперты фактически устанавливают правила поведения раньше

или вместо государственных органов [120, с. 591-592; 351, с. 37-38; 352, с. 3-7]. Пример - глобальные ИТ-корпорации и онлайн-платформы, которые вводят собственные стандарты обработки данных, алгоритмов модерации контента, этические кодексы для ИИ и т. д. [353, с. 1631-1647; 354, с. 541-557]. Такие нормы самонормативности часто действуют экстерриториально и существенно влияют на права пользователей, иногда опережая или даже подменяя публичное регулирование [353, с. 1662-1666; 352, с. 3-13]. Так, политика конфиденциальности глобальной онлайн-платформы фактически определяет порядок обработки персональных данных миллионов субъектов, опережая развитие соответствующего национального законодательства. Это ставит вопрос о соотношении публичного и частного начал в регулировании киберпространства. Функционально такие частные нормы заполняют регуляторный вакуум (пробелы в праве) в тех сферах, где государства не успели сформировать надлежащие правила, однако эти нормы лишены демократической легитимности (как с аксиологической, так и с формально-юридической точки зрения), поскольку не основаны на демократически принятом решении. В результате возникают коллизии и конфликты юрисдикций: национальные законы разных стран (например, требования локализации, запреты на обработку определенных данных) могут противоречить друг другу или стандартам, установленным глобальными компаниями [355, с. 727-734; 356, с. 236].

Для преодоления хаотичности и разночтений государствами все активнее применяются гибкие инструменты регулирования, призванные совместить ускоренную выработку правил с экспертизой и испытанием новых подходов. Один из таких инструментов - «регуляторные песочницы» [357, с. 584-600; 358, с. 31-45]. Режим «регуляторной песочницы» позволяет на ограниченной основе (для определенных участников, в рамках пилотного проекта) отступить от строгих требований закона и протестировать инновационные технологии под надзором регулятора [357, с. 642; 358, с. 45, 78]. За время эксперимента выявляются риски и эффективность новых правил, после чего возможна корректировка законодательства. Концепция «регуляторных песочниц» изначально возникла в финансовой сфере (финтех), но быстро была распространена на сферы ИИ, больших данных, медицинских технологий и др. [359, с. 362; 360, с. 273]. Для Казахстана идея регуляторных песочниц не нова - страна уже вводила режимы пилотного регулирования в финтех-секторе через Международный финансовый центр «Астана» (МФЦА) [361, с. 55, 62, 64, 79]. В 2023-2024 годах обсуждалось применение подобного подхода и в сфере ИИ, позволяя организациям с инновационными продуктами работать в контролируемых условиях, где регулятор рассчитывает получить эмпирические данные для дальнейшего нормотворчества [359, с. 367; 360, с. 284]. Таким образом, «регуляторные песочницы» снижают «нормативную турбулентность» - вместо поспешного введения запретов технология сначала изучается в тестовом режиме, что отвечает принципу разумной достаточности регулирования (функциональный подход).

Аналогичным образом развиваются отраслевые кодексы и стандарты как элементы мягкого права. В условиях, когда принятие международных договоров или национальных законов отстает, заинтересованные стороны разрабатывают добровольные нормы поведения [362, с. 292-298; 363, с. 10-14]. Примером являются этические кодексы в сфере ИИ (например, принципы ИИ ОЭСР [247, с. 4], этические руководства ЮНЕСКО по ИИ [249, с. 17-23; 250]), корпоративные декларации о защите данных, технические стандарты безопасности. В ЕС механизмы мягкого права и саморегулирования поощряются наряду со строгими нормами: GDPR предусматривает возможность утверждения кодексов [364, с. 241] поведения отраслей (ст. 40), разработки сертификаций (ст. 42) [365, с. 9-10; 366, с. 246-249] для подтверждения надлежащей обработки данных. Европейская комиссия инициировала Кодекс практики по дезинформации и обсуждает аналогичные договоренности в отношении генеративного ИИ, где компании добровольно принимают на себя повышенные обязательства по прозрачности систем ИИ, маркировке ИИ-контента и пр. [367, с. 15; 368, с. 4-5]. Достоинство мягкого права - гибкость и оперативность. Такие акты могут быть приняты быстрее закона и обновляться по мере развития технологий. Недостаток - их необязательность: без механизмов контроля и санкций соблюдение кодексов зависит лишь от доброй воли участников. Тем не менее комбинация строгого регулирования и саморегулирования все чаще рассматривается как оптимальная модель в высокотехнологичных отраслях, требующая постоянного диалога государства, бизнеса и общества (социо-психологический аспект взаимодействия и доверия между ними) [364, с. 235-238; 365, с. 12; 366, с. 246-256].

В целях практической реализации, изложенных в подразделе 2.3 принципов мягкого права, представляется целесообразным в Республике Казахстан закрепить их на уровне стратегических актов и отраслевых кодексов практики, предусматривающих добровольную оценку воздействия ИИ-систем на права и свободы личности, сертификационные критерии надежности алгоритмов и совместимость корпоративных политик с трансграничными механизмами уровня АТЭС (в английской версии: *APEC Cross Border Privacy Rules System*). Такие ориентиры могут действовать как временные стандарты до принятия детализированных норм, а также использоваться в режиме «регуляторных песочниц» для пилотирования решений под надзором регулятора. Это позволит согласовать технико-правовые меры со сравнительно-правовыми подходами, изложенными в подразделе 2.3, и снизить эффекты «нормативной турбулентности» без избыточной регуляторной нагрузки.

Рассмотрим, как феномен «нормативной турбулентности» отражается в подходах ключевых юрисдикций - ЕС, Китая и Казахстана к регулированию ИИ и данных.

ЕС демонстрирует стремление к системности и опережающему регулированию на основе ценностей. В 2024 году в ЕС приняли первый всеобъемлющий акта об ИИ - Регламент ЕС об ИИ [255]. Данный источник права устанавливает принцип регулирования, основанного на уровне риска: все ИИ-системы разделяются на четыре категории риска (недопустимый, высокий,

ограниченный, минимальный), для каждой предусмотрены дифференцированные требования. Однако имеются мнения, которые критикуют этот подход, указывая, что данные категории риска были определены не на основе достаточных эмпирических данных, а стали результатом политического компромисса, что делает их в значительной степени произвольными [369, с. 692; 370, с. 12]. Наиболее опасные применения ИИ (например, социальный скоринг, массовое распознавание биометрии в режиме реального времени) подлежат прямому запрету (ст. 5 Регламента ЕС об ИИ [256]). Однако, как отмечает исследователь, эти запреты не являются абсолютными и содержат существенные пробелы, такие как широкие исключения для использования биометрии правоохранительными органами или (в проекте) ограничение запрета на социальный скоринг только госорганами. Ключевая критика исследователя заключается в том, что Регламент ЕС об ИИ ошибочно рассматривает эти четыре запрещенные категории (включая подсознательные техники и эксплуатацию уязвимостей) по отдельности, в то время как их главная угроза - это их взаимосвязанность и возможность комбинации для манипулирования человеческим мышлением и поведением [371, с. 8, 12, 13].

Системы высокого риска (например, ИИ в сфере образования, здравоохранения, правосудия) должны проходить обязательную сертификацию, обеспечивать прозрачность, иметь систему управления данными и человеческого контроля. Одновременно следует учитывать, что риск-ориентированное регулирование само по себе не обеспечивает ни эффективной компенсации вреда, ни оптимальных превентивных стимулов; его необходимо дополнять деликтно-правовыми механизмами ответственности. При этом наличие человеческого надзора не устраняет риски неправомерного переноса ответственности: правоприменитель должен требовать институционального надзора за алгоритмами, обоснования их включения в процесс принятия решений и подтверждения возможности их эффективного контроля [372, с. 1, 8, 11]. В праве ЕС функции компенсации вреда в цифровую эпоху возложены на обновленную Директиву об ответственности за дефектную продукцию - Директиву (ЕС) 2024/2853 от 23.10.2024 [373] (вступила в силу 08.12.2024; применяется к продуктам, размещенным на рынке после 09.12.2026). Она прямо относит к «продуктам» программное обеспечение и ИИ-системы и вводит раскрытие доказательств (ст. 9) и опровержимые презумпции дефектности и причинной связи (ст. 10). Предложенная Комиссией в 2022 году Проект Директивы об ответственности за ИИ [374] (в английской версии: *AI Liability Directive, COM(2022)496*) была включена в перечень к отзыву в Программе работы Европейской комиссии на 2025 год, после чего ее отзыв подтвержден в 11 февраля 2025 года [375, с. 3]. На этом фоне, при поэтапном применении Регламента ЕС об ИИ (вступил в силу 01.08.2024; запреты - с 02.02.2025), на уровне ЕС отсутствует единый горизонтальный инструмент для виновной (внедоговорной деликтной) ответственности за вред, причиненный ИИ вне режима дефектной продукции. Вопросы решаются по Директиве об ответственности за дефектную продукцию и нормам национального деликтного права государств-членов, что чревато фрагментацией.

Информационные системы с более низким уровнем риска регулируются менее строго (достаточно соблюдения базовых требований по информированию субъекта и обеспечению возможности отказа от обработки), а системы с низким (минимальным) риском не подвергаются специальному регулированию. Такой превентивно-ориентированный подход отражает европейские ценности - приоритет прав человека и безопасности над коммерческой выгодой, этические ориентиры при внедрении технологий. Фактически закрепляется презумпция потенциальной опасности отдельных видов ИИ - законодатель заранее перечисляет сферы и случаи, где применение ИИ изначально считается чувствительным и требует особого контроля [363, с. 10]. Этот подход соответствует принципу предосторожности и нацелен на предотвращение вреда до его возникновения. Помимо Регламента ЕС об ИИ, в ЕС действует развитый массив смежного регулирования: Директива (ЕС) 2022/2555 о мерах по обеспечению высокого уровня кибербезопасности на территории Союза (NIS2), Регламент (ЕС) 2018/1807 о свободном потоке неперсональных данных [376], а также Проект Регламента о конфиденциальности в электронных коммуникациях (COM/2017/010 [377]) (был отозван 11 февраля 2025 года в связи с отсутствием реальных перспектив достижения согласованной позиции между со-законодателями; кроме того, проект утратил актуальность ввиду существенных изменений в технологической среде и появления нового законодательства, регулирующего соответствующие отношения [375, с. 3]). В совокупности эти акты формируют систему, дополняющую Общий регламент ЕС о защите персональных данных (GDPR), и адаптируют регулирование к новым технологиям [378, с. 18].

Таким образом, в ЕС происходит формирование целостной регуляторной экосистемы, что, однако, сопровождается значительной сложностью и объемностью (масштабностью) правового регулирования. Ключевыми компонентами предложенной «правовой технологии обеспечения защиты персональных данных», обеспечивающими ее эффективность на практике, выступают инструменты, реализующие принципы подотчетности и проактивного управления рисками. Отдельно следует отметить институт оценки воздействия на защиту персональных данных. ЕС одним из первых внедрил требование проводить оценки воздействия на защиту персональных данных для новых проектов, связанных с рисками для приватности (ст. 35 GDPR). Оценка стала обязательной при планировании операций, потенциально опасных для прав субъектов (составление профилей, обработка специальных категорий данных, наблюдение за общественными местами и т. п.). Формулировки GDPR достаточно общие (оценка нужна при наличии высокого риска), однако разъяснения Европейского комитета по защите данных дают примеры, когда оценка требуется. Этот механизм - яркий пример реализации принципа подотчетности: контролер (оператор) персональных данных самостоятельно проводит оценку и документирует риски, а надзорный орган вправе проверить обоснованность его выводов. В контексте нормативной турбулентности оценка представляет собой гибкую само-нормотворческую меру: частный субъект (компания) фактически сам прописывает для себя нормы (меры по

нейтрализации выявленных рисков), исходя из общих положений требований закона. Так сочетаются публичное предписание (обязанность провести оценку) и элемент саморегуляции (содержание оценки зависит от специфики проекта). Методологически такой подход сочетает системный анализ (оценка всех аспектов риска) с функциональной направленностью (минимизация вреда субъектам данных).

В КНР применяется иной подход, при котором основной упор делается на государственный контроль и приоритет общественной безопасности. Нормативная база КНР в последние годы стремительно расширяется путем издания отраслевых регуляций и административных мер - своего рода точечных «надстроек» над базовыми законами. Если в ЕС создается (принимается) единый горизонтальный акт (Регламент ЕС об ИИ), то в КНР применяется комплекс специализированных (секторальных) нормативных актов: введены нормы об алгоритмах рекомендаций (2022 г.), о глубоко-фейковых медиа (2022 г.), временные положения о генеративном ИИ (2023 г.) и др. [379, с. 3, 6; 380, с. 6-8; 381, с. 207]. Все они подчинены логике обеспечения национальной безопасности и социальной стабильности [380, с. 4; 382, с. 15]. Надзорные органы КНР заранее определяют нежелательные применения ИИ и вводят строгие условия для их допуска. Например, генеративные модели (чат-боты, способные создавать тексты/изображения) обязаны пройти процедуру безопасности и модерирования перед запуском широкому кругу пользователей. Алгоритмы, влияющие на общественное мнение (новостные ленты, рекомендации в онлайн-платформах), подлежат обязательной регистрации и аудиту; некоторые технологии (в частности, системы распознавания лиц в режиме реального времени) фактически запрещены к коммерческому использованию либо допустимы лишь в рамках пилотных зон с особым разрешением [382, с. 10; 267; 383]. Такой подход возможно охарактеризовать как презумпцию управляемости рисков государством: государственные органы не ожидают, что частные организации сами адекватно оценят и минимизируют риски, а берут эту функцию на себя, устанавливая детальные запреты и разрешительные процедуры. Вместо признания за организациями свободы инноваций под ответственность (как в ЕС), в КНР упор делается на лицензировании, модерации контента, локализации данных и иных инструментах прямого государственного влияния [384, с. 10, 13]. Аксиологически модель КНР уделяет первоочередное внимание на коллективные ценности - общественную безопасность, порядок - над индивидуалистическими правами, что отражается и в нормативных актах. Возможно сказать, что Китай демонстрирует представляет собой управленческую стратегию снижения «нормативной турбулентности»: государственный регулятор активно вмешивается с целью недопущения (предотвращения) ситуаций, способных вызвать резкую негативную общественную реакцию вследствие бесконтрольного внедрения ИИ. Однако такая строгая регламентация сама по себе создает фрагментарность: множество отдельных актов трудно встроить в единую систему, возможны пробелы между ними или устаревание норм из-за быстрого прогресса. Подход, применяемый в КНР, имеет свои преимущества и недостатки: с одной стороны,

он обеспечивает строгий контроль над обработкой персональных данных в интересах национальной безопасности, но с другой - предполагает более существенные ограничения права на защиту персональных данных (а также препятствует инновационной деятельности организаций) в сравнении с моделью ЕС. Это следует учитывать при адаптации элементов модели КНР в других юрисдикциях.

При формировании национальной цифровой политики в Республике Казахстан (государстве, не обладающем сопоставимыми ресурсами и влиянием), тем не менее прослеживается стремление учесть обе эти модели. В РК развитие ИИ официально признано одним из стратегических приоритетов: в 2024 году была утверждена Концепция развития искусственного интеллекта на 2024-2029 гг. [268; 385, с. 68], а в 2025 году подготовлен первый проект Закона РК «Об искусственном интеллекте» [262]. Данный законопроект, как отмечается, «не копирует зарубежные модели», однако явно воспринял ключевые идеи европейского подхода. При этом еще в 2021 году в отечественной юридической литературе отмечалась необходимость выработки единых согласованных подходов к месту ИИ в системе права и закрепления на международном и национальном уровнях основных принципов распределения ответственности между участниками разработки и использования ИИ [386, с. 67, 71]. В проекте предлагается классификация ИИ-систем по трем уровням риска - минимальному, среднему и высокому - с соответствующей дифференциацией регулирования. То есть РК во многом следует европейскому принципу предосторожности в отношении высокорискованных систем, презумпции недопустимости отдельных ИИ-продуктов. Однако в контексте здравоохранения, как заключается в работе, для Казахстана актуальным является дополнить Кодекс «О здоровье народа и системе здравоохранения», чтобы четко определить ответственность за врачебные ошибки при использовании медицинского оборудования на базе ИИ [387, с. 159]. С другой стороны, казахстанские разработчики концепции ИИ осознают и необходимость стимулировать инновации - в официальных разъяснениях отмечается, что новое регулирование не должно замедлять развитие технологии, а напротив - сопровождать его, создавая понятные основания для инвесторов и разработчиков. Планируется внедрение механизмов регуляторных песочниц [388, с. 202] для тестирования ИИ-решений, упрощение процедур для проектов низкого риска, активное сотрудничество государства с бизнесом и научным сообществом при выработке стандартов (элементы саморегулирования). Такой подход возможно охарактеризовать как комбинированный: Казахстан стремится соединить гибкость и самонормативность (через «регуляторные песочницы», стандарты, диалоги с частными субъектами) с базовыми обязательными требованиями (через закон об ИИ, поправки в закон о персональных данных и их защите). В терминах методологии, налицо попытка системного баланса между разными моделями: от контроля и презумпции риска (как в ЕС, отчасти КНР) до стимулирования инноваций и доверительного регулирования (через мягкое право, как в элементах англо-американского подхода).

Проведенный сравнительно-правовой анализ подходов ЕС, КНР и Казахстана свидетельствует, что в условиях «нормативной турбулентности» и стратегических вызовов, связанных с развитием ИИ, эффективная защита персональных данных не может быть достигнута исключительно путем принятия горизонтального законодательства или секторальных норм. Необходима системная институционализация описанной «правовой технологии обеспечения защиты персональных данных». Интеграция риск-ориентированного подхода, механизмов подотчетности и принципа защиты данных на этапе проектирования в единую методологическую цепочку позволит национальным правопорядкам обеспечить необходимый уровень регуляторной совместимости и эффективно имплементировать международные стандарты в условиях глобальной цифровой трансформации.

Важной частью преодоления «нормативной турбулентности» является гармонизация терминологии и принципов. Казахстан, интегрируясь в мировое информационное пространство, учитывает стандарты, заложенные в Конвенции Совета Европы 108+ и связанных документах, хотя формально не является участником этой Конвенции [389, с. 2, 17]. Принципы законности, пропорциональности, уважения прав человека при обработке персональных данных признаются в качестве ориентиров национальной политики (аксиологический аспект). В то же время Казахстан стремится адаптировать зарубежный опыт к своим реалиям (социо-психологический аспект): учитывается уровень цифровой грамотности населения, состояние кибербезопасности инфраструктуры, готовность субъектов предпринимательства соблюдать новые правила [390, с. 78; 391, с. 120]. Например, требование о проведении оценки воздействия на защиту персональных данных для высокорисковой обработки, отсутствующее в действующем законодательстве, в настоящее время активно обсуждается в профессиональных и экспертных кругах (в том числе в контексте разработки нового «Цифрового кодекса» РК). Это свидетельствует об осознании необходимости имплементации данного механизма, особенно с учетом роста услуг на основе ИИ, однако процесс его нормативного закрепления требует времени для подготовки субъектов предпринимательства и предварительной выработки методических рекомендаций совместно с экспертным сообществом.

Таким образом, учет явления «нормативной турбулентности» требует от национальных правовых систем гибкости, скорости и открытости к международному опыту. Резюмируя, возможно отметить несколько ключевых подходов, выработанных мировым сообществом для смягчения нормативной турбулентности: оперативная выработка и принятие норм на основе риск-ориентации (пример ЕС), строгое государственное регулирование стратегических технологий (пример КНР), гибкие режимы и саморегулирование («регуляторные песочницы», кодексы, характерные для англо-саксонской модели), а также международная координация (обмен лучшими практиками, выработка глобальных этических принципов ИИ на площадках ООН, ВЭФ, G20 и пр.). Для Республики Казахстан представляется оптимальным следующий (комбинированный) подход: сочетание базовых строгих правил (в отношении

высокорисковых операций (систем)) с возможностью гибкого регулирования и «мягкого права». Это обеспечит одновременно и правовую определенность, и пространство для инновационного развития, что соответствует функциональной задаче права - эффективно решать социально-экономические проблемы, сохраняя фундаментальные ценности.

**Специфика правовой системы Казахстана: нормативные пробелы, правоприменение и потенциал мягкого права**. Завершающий подраздел данного диссертационного исследования - анализ особенностей национальной юрисдикции Казахстана в контексте защиты персональных данных. В Республике Казахстан, где провозглашен курс на цифровизацию, формируется собственная модель регулирования, опирающаяся на международные стандарты и одновременно учитывающая национальный контекст (внутренние особенности). Конституция РК гарантирует неприкосновенность частной жизни, личной и семейной тайны (ст. 18) как одно из основных прав человека, находясь в системной связи с универсальными нормами (ст. 12 ВДПЧ). Для реализации этих положений создана многоуровневая национальная законодательная база: действует специальный Закон «О персональных данных и их защите», устанавливающий принципы и требования к обработке данных; Закон «Об информатизации», закрепляющий общий режим защиты информации и обязанности владельцев информационных систем; Уголовный кодекс РК содержит ряд составов преступлений, предусматривающих ответственность за незаконный сбор, распространение персональных данных и нарушение законодательства об их защите (в частности, ст. 147 УК РК - «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите», в том числе квалифицируемый состав, связанный с использованием служебного положения (ч. 3 ст. 147 УК РК). В УПК РК сведения в электронной форме (на электронных носителях информации) и электронные документы признаются доказательствами (ст. 120, 121 УПК РК) при условии установления их достоверности и соблюдения процессуального порядка их получения и фиксации. Данный правовой режим дополняют нормы гражданского законодательства (в частности, институты возмещения вреда и защиты деловой репутации), а также законодательство в сфере информатизации. На первый взгляд, нормативная база РК довольно широка и охватывает ключевые аспекты. Однако углубленный анализ выявляет ряд пробелов и трудностей правоприменения, которые снижают эффективность техно-правовой защиты на практике [391, с. 116, 120; 392, с. 2].

**Нормативные пробелы и направления совершенствования правового регулирования.** Во-первых, для законодательства Республики Казахстан в сфере защиты персональных данных длительное время было характерно отставание от современных международных тенденций. Закон о персональных данных и их защите 2013 года в исходной редакции ориентировался на устоявшиеся к тому времени международные подходы (законность, согласие субъекта, конфиденциальность и т. п.), но не содержал многих современных механизмов, появившихся позже в GDPR и других актах. К примеру, не были прямо предусмотрены оценки воздействия на защиту персональных данных,

права на переносимость персональных данных, подробная регламентация трансграничных передач персональных данных, институт уполномоченного органа по защите персональных данных имел ограниченные функции. Лишь в 2020-2021 гг. в национальное законодательство были внесены существенные изменения, приблизившие его к модели регулирования ЕС: были введены нормы об обязательном назначении оператором (собственником и/или оператором) лица, ответственного за организацию обработки персональных данных (аналог уполномоченного лица по защите персональных данных), о необходимости уведомления уполномоченного органа в сфере защиты персональных данных и субъектов персональных данных в случае нарушения безопасности персональных данных, а также о принятии мер по защите персональных данных ограниченного доступа (т. е. фактически по обеспечению информационной безопасности). Эти нововведения повысили уровень подотчетности операторов (контролеров), собственников персональных данных и внедрили принцип профилактики нарушений. Тем не менее, некоторых важных элементов до сих пор нет. Так, пока не закреплена на законодательном уровне обязанность проведения оценки воздействия на защиту персональных данных при начале высокорисковой обработки данных - хотя как обсуждалось выше, вопрос о внедрении такого инструмента вынесен на повестку при разработке «Цифрового кодекса». Отсутствуют нормативно закрепленные процедуры оценки и сертификации информационных систем на соответствие требованиям в области защиты персональных данных (в отличие от требований информационной безопасности, которые регулируются национальными стандартами (СТ РК/ГОСТ) и техническими регламентами). Отсутствует отдельный закон или раздел закона, посвященный вопросам искусственного интеллекта - соответствующий законопроект еще находится в стадии рассмотрения. В сфере защиты персональных данных несовершеннолетних, а также специальных категорий персональных данных (таких как биометрические и генетические данные) также имеются пробелы в правовом регулировании либо применяется общий режим обработки без учета особого характера этих данных. Такие пробелы создают риски как для субъектов персональных данных (их права могут быть недостаточно защищены), так и для операторов (неясность требований затрудняет соблюдение закона). Устранение этих пробелов является актуальной задачей, работа над которой уже ведется (в рамках разработки Цифрового кодекса и сопутствующих ему нормативных правовых актов).

Во-вторых, необходима адаптация правовых определений и принципов к новой реальности. Например, понятие «согласие субъекта» в казахстанском законе все еще трактуется довольно традиционно (как письменное или равнозначное ему электронное согласие на обработку определенных данных) - тогда как в эпоху технологий обработки больших данных этот механизм не всегда эффективно защищает субъекта персональных данных [391, с. 116]. Методологически следует применить аксиологический подход: переосмыслить ценность согласия и усилить акцент на других принципах (подотчетность, законность целей, минимизация), чтобы не перегружать субъекта обязанностью постоянно давать формальные согласия, которые теряют

свою осознанность с сфере информатизации. Следующий пример - трансграничная передача персональных данных - Закон о персональных данных и их защите (ст. 16) устанавливает, что персональные данные могут передаваться за рубеж при обеспечении иностранным государством надлежащим уровнем гарантий защиты. Однако отсутствует надлежащий механизм признания таких государств или выдачи разрешений на передачу, нет перечня «адекватных юрисдикций» (как это делает Европейская комиссия). Это создает пробел в правовом регулировании, затрудняющий деятельность международных компаний (транснациональных корпораций) в Республике Казахстан. В перспективе целесообразно разработать критерии и порядок трансграничной передачи (возможно, через двусторонние соглашения или на основе присоединения к Конвенции 108+).

**Вопросы правоприменения и судебная практика.** Наличие эффективного законодательства является лишь частью решения. Не менее важна эффективность правоприменительной практики (то, как эти нормы реализуются). Казахстанская судебная и административная практика в сфере персональных данных находится в стадии становления. В судебной практике Республики Казахстан отмечается относительно небольшое количество дел, непосредственно связанных с применением Закона РК «О персональных данных и их защите» или ст. 18 Конституции РК. Зачастую деяния, связанные с незаконным использованием (оборотом) персональных данных, квалифицируются в рамках общеуголовных составов преступлений: мошенничество (ст. 190 УК РК), совершенное с использованием персональных данных, хищение денежных средств посредством неправомерного доступа к банковским счетам (информационным системам), вымогательство (ст. 194 УК РК) под угрозой распространения конфиденциальных сведений и т. п. Такие деяния квалифицируются по статьям УК РК о мошенничестве (ст. 190) или краже (ст. 188), а не по ст. 147 («Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите») или ст. 211 («Неправомерное распространение электронных информационных ресурсов ограниченного доступа»). Это обусловлено тем, что непосредственным объектом посягательства по ст. 147 и ст. 211 являются конституционные права (на частную жизнь) и установленный порядок обращения с персональными данными или ресурсами ограниченного доступа. В рассматриваемых же случаях основное посягательство направлено непосредственно против собственности (Глава 6 УК РК), а нарушение прав по ст. 147 (Глава 3 УК РК) или ст. 211 (Глава 7 УК РК) выступает лишь способом совершения хищения и полностью охватывается составами ст. 188 или ст. 190. В результате создается ситуация, что ответственность за посягательства на личную информацию наступает, но опосредованно, через другие составы. Это затрудняет формирование единообразной судебной практики именно по делам, связанным с нарушениями в сфере защиты персональных данных. Данный пробел частично восполняется разъяснениями Верховного Суда РК, содержащимися в обзорах судебной практики и нормативных постановлениях, в которых указывается на порядок квалификации преступлений в сфере

информационно-коммуникационных технологий и на необходимость отграничения смежных составов, в частности, при оценке множественности эпизодов неправомерного завладения данными (как продолжаемого преступления либо их совокупности) [275; 393; 394].

Отдельная сложность - доказательства в сфере информационно-коммуникационных технологий. Для привлечения к ответственности за неправомерную обработку персональных данных необходимо надлежащим образом процессуально закрепить (зафиксировать) обстоятельства такой обработки, что нередко требует производства выемки электронных носителей, исследования журналов аудита (лог файлов), осмотра и фиксации снимков экрана (скриншотов) переписки, данных о действиях (событиях) в информационных системах и т. д. В процессуальном законодательстве РК закреплен правовой статус электронных доказательств, однако к их достоверности и процессуальному закреплению предъявляются строгие требования. Суды при рассмотрении дел тщательно проверяют, не подверглись ли электронные данные изменениям, кем и когда сделаны снимки с экрана, возможно ли достоверно установить автора электронного сообщения. Нарушения установленного процессуального порядка получения (сбора) электронных доказательств (например, производство осмотра компьютерной техники без участия понятых, несанкционированное судом (следственным судьей) получение информации у поставщика услуг (провайдера)) могут привести к признанию таких доказательств недопустимыми. Таким образом, электронные (цифровые) следы должны быть не только обнаружены, но и надлежащим образом процессуально закреплены, что предъявляет повышенные требования к квалификации (компетенции) лиц, осуществляющих досудебное расследование, и судей (социо-психологический фактор - уровень подготовки человеческого элемента правоприменения). Постепенно накапливается опыт судебной оценки электронных доказательств: например, суды принимают распечатки переписки из мессенджеров, данные об IP-адресах, результаты компьютерных экспертиз. В одном из дел, получивших общественный резонанс, о мошенническом оформлении договора займа (кредита) электронным способом суд детально исследовал электронные доказательства («цифровые следы») и на основании совокупности исследованных доказательств вынес обвинительный приговор. Эта практика формирует подходы к оценке допустимости электронных (цифровых) доказательств: суды требуют подкреплять сведения в электронной форме иными (в том числе традиционными) доказательствами (исследованными в совокупности) или заключениями экспертов, избегая вынесения решения исключительно на основании данных, полученных в электронной форме. Также суды критически оценивают новые методы аутентификации - например, отмечают риски, связанные с дистанционной биометрической идентификацией субъектов (клиентов), указывая, что технический сбой или неправомерный доступ (злоупотребление) в данных системах могут повлечь совершение противоправных деяний (включая совершения мошенничества) [395]. Следовательно, правоприменительная практика постепенно адаптируется к условиям цифровой трансформации,

однако требует дальнейшего совершенствования, в том числе на нормативном уровне (посредством детальной процессуальной регламентации порядка работы с электронными доказательствами и укрепления международного сотрудничества (взаимной правовой помощи) по вопросам получения (сбора) электронных доказательств, находящихся в иностранных юрисдикциях и т. д. [87; 396]).

**Роль мягкого права и саморегулирования.** Ввиду того, что законодательство не всегда успевает своевременно реагировать на все вызовы, в Республике Казахстан начали задействовать механизмы «мягкого права» для поддержки правоприменительной практики. Так, уполномоченные органы (например, Министерство искусственного интеллекта и цифрового развития РК, прежде - МЦРИАП) издают методические рекомендации для организаций по защите персональных данных, памятки о кибер-гигиене - данные документы носят рекомендательный характер, однако способствуют повышению уровня осведомленности (компетенции) соответствующих субъектов. Разрабатываются национальные стандарты в сфере информационной безопасности и защиты персональных данных (часть из которых в настоящее время носит добровольный (рекомендательный) характер). Отраслевые ассоциации (в финансовом секторе, телекоммуникациях) принимают кодексы практики, где закрепляют повышенные обязательства своих членов по защите данных клиентов. Например, в рамках отраслевого саморегулирования (или кодексов профессиональной этики) участники финансового рынка принимают на себя обязательства не допускать раскрытия сведений, составляющих охраняемую законом тайну (в частности, банковскую тайну, тайну предоставления микрокредита), за исключением случаев, прямо предусмотренных законодательными актами РК - проявляя тем самым саморегуляцию сверх требований закона [397, с. 6; 398, с. 3, 7; 399, с. 3, 4, 9, 12]. В ИТ-секторе Казахстана, особенно среди организаций, осуществляющих международное сотрудничество (или работающих на международном рынке), получает распространение сертификация по международным стандартам (в частности, ISO/IEC 27001 в области менеджмента информационной безопасности и ISO/IEC 27701 в области менеджмента информации о конфиденциальности (PIMS) и пр.), что представляет собой добровольную имплементацию повышенных требований (стандартов) в данной сфере [400; 97]. Государство стимулирует повышение стандартов защиты данных: в частности, в рамках (государственных) закупок заказчики вправе устанавливать требование о наличии у потенциальных поставщиков (подрядчиков) соответствующих (профильных) сертификатов (например, ISO/IEC 27001) на основании Правил осуществления государственных закупок [401]. Кроме того, государственные органы организовывают и поддерживают конкурсы и образовательные программы в сфере кибербезопасности, что способствует совершенствованию корпоративных практик в области защиты персональных данных [402; 403; 404]. Данный подход, направленный на повышение культуры обработки персональных данных посредством механизмов «мягкого права», соответствует аксиологическому и социально-психологическому подходам: вместо применения исключительно мер

ответственности к нарушителям, акцент делается на стимулировании добросовестного поведения (по принципу справедливости) и формировании ценности защиты персональных данных в обществе и в предпринимательской среде.

Значительный потенциал кроется в механизме юридической подотчетности как части корпоративного саморегулирования. В дополнение к уже нормативно закрепленным обязанностям (в частности, назначение лица, ответственного за организацию обработки персональных данных, и уведомление уполномоченного органа о нарушениях безопасности персональных данных), уполномоченные органы рекомендуют операторам (контролерам), собственникам внедрять внутренние политики в области защиты персональных данных (в рамках организационно-технических мер), проводить обучение персонала и осуществлять оценку рисков для прав и свобод физических лиц при разработке новых продуктов. Хотя применение этих мер пока не носит строго обязательного характера в соответствии с законодательством, приведение внутренних процессов в соответствие с лучшими (передовыми) практиками может рассматриваться в качестве смягчающего обстоятельства (фактора) при проведении проверок уполномоченным органом и в случае возникновения инцидентов безопасности персональных данных. Более того, закрепляемые в стратегических документах принципы «цифровое по замыслу» и «защита персональных данных на этапе проектирования и по умолчанию» ориентируют организации и государственные органы на интеграцию защиты персональных данных уже на ранних этапах цифровых проектов. В данном случае проявляется методология системного и функционального подходов: защита персональных данных должна быть интегрирована во все элементы («процессы») управления информацией и выполнять превентивную функцию, а не носить реактивный характер.

Необходимо также отметить важность международного сотрудничества для Республики Казахстан в устранении пробелов в национальном законодательстве. Республика активно участвует в глобальных инициативах: поддерживает резолюции ООН по праву на неприкосновенность частной жизни в цифровую эпоху, обменивается опытом с европейскими и азиатскими партнерами, изучает возможность присоединения к Конвенции 108+. Уже сейчас Казахстан применяет некоторые положения Конвенции 108+ фактически, как отмечалось (например, принцип совместимости трансграничных потоков персональных данных с «адекватными» гарантиями). Казахстан укрепляет международное сотрудничество в сфере защиты персональных данных, в том числе посредством участия в диалогах с европейскими надзорными органами и заключения профильных соглашений на уровне регуляторов (например, заключенный в 2025 году Меморандум о сотрудничестве в сфере защиты персональных данных между соответствующими органами МФЦА и Глобальным рынком Абу-Даби (Abu Dhabi Global Market) [405]), а также в рамках более широких соглашений между ЕС и РК.

*Таким образом,* по итогам анализа компонентов технико-правовой защиты персональных данных в сфере информатизации возможно сформулировать следующие выводы.

Феномен «нормативной турбулентности», обусловленный стремительным развитием технологий искусственного интеллекта, характеризуется отставанием международно-правового регулирования, фрагментацией глобальных подходов и усилением «самонормативности» (фактического нормотворчества) частных цифровых платформ. Это порождает коллизии юрисдикций и снижает уровень правовой определенности.

Ключевыми механизмами адаптации права к технологическим вызовам выступают гибкие регуляторные инструменты: риск-ориентированный подход (модель ЕС), экспериментальные правовые режимы («регуляторные песочницы») и инструменты «мягкого права» (стандарты, кодексы поведения, этики). Они позволяют оперативно реагировать на риски и тестировать инновации до их кодификации в обязательные нормы.

Сравнительно-правовой анализ регуляторных моделей ЕС, КНР и Казахстана демонстрирует глобальную тенденцию к имплементации риск-ориентированного подхода в регулировании ИИ. Несмотря на расхождения акцентов (приоритет прав человека в ЕС, государственная безопасность в КНР), Республика Казахстан формирует гибридную модель, интегрируя элементы риск-ориентированного подхода при сохранении регуляторной гибкости.

Анализ национальной правовой системы Казахстана выявляет существенные нормативные пробелы (в частности, отсутствие обязательной процедуры оценки воздействия на защиту персональных данных, недостаточная регламентация трансграничных передач) и сложности правоприменения. Наблюдается недостаточная эффективность уголовно-правовой защиты приватности (поглощение специальных составов общеуголовными) и процессуальные трудности при сборе и оценке электронных доказательств, что требует системного совершенствования законодательства и унификации судебной практики.

*Таким образом,* проведенное исследование эффективности правового регулирования защиты персональных данных, направлений его повышения и адаптации к стратегическим вызовам позволяет сформулировать следующие обобщающие выводы.

*Обосновано* определение эффективности правового регулирования защиты персональных данных как комплексной международно-правовой категории. Оценка эффективности правового регулирования требует применения комбинированного методологического подхода (системного, функционального, аксиологического), учитывающего степень полноты и согласованности правовых механизмов, гарантирующих реализацию фундаментального права на неприкосновенность частной жизни и права на защиту персональных данных в условиях глобальной цифровизации и «нормативной турбулентности». Установлено, что ключевыми условиями достижения высокой эффективности правового регулирования выступают институциональные гарантии, в частности,

наличие независимого надзорного органа по защите персональных данных, а также стабильность и технологическая нейтральность нормативной базы.

*Разработана* и обоснована система критериев оценки эффективности правовых режимов защиты персональных данных, основанная на степени имплементации общепризнанных международных стандартов (GDPR, Принципы ОЭСР). К фундаментальным критериям отнесены: законность и целевое ограничение обработки; минимизация данных; обязательность оценки воздействия на защиту персональных данных для высокорисковых операций; реализация принципа подотчетности, включая верифицируемость согласия и журналирование; наличие эффективных механизмов регулирования трансграничных передач персональных данных и стандартизация судебной оценки электронных доказательств. Сравнительный анализ подтвердил, что для достижения соответствия международным стандартам и обеспечения трансграничной совместимости правовому режиму Республики Казахстан особенно необходимо законодательное закрепление обязательной процедуры оценки воздействия на защиту персональных данных.

*Обосновано,* что повышение эффективности правового регулирования требует имплементации системного подхода, основанного на синергии правовых, организационных и технических мер и обеспечивающего переход к риск-ориентированному управлению (в сфере обработки персональных данных). Этот подход реализуется через внедрение ключевых институтов (механизмов) подотчетности, к основным из которых отнесены: нормативное закрепление процедуры оценки воздействия на защиту персональных данных; ведение реестров операций обработки и инвентаризация массивов персональных данных; стандартизация договорных отношений между контролерами (операторами) и обработчиками и проведение регулярных независимых аудитов.

*Обоснована* необходимость фундаментальной институциональной реформы как условия эффективности национального правового режима. Предложена модель создания в РК независимого надзорного органа по защите персональных данных, функционально автономного от исполнительной власти, наделенного расширенными надзорными функциями и корректирующими полномочиями (включая аудит алгоритмов ИИ), а также закрепления статуса уполномоченных лиц по защите персональных данных в ключевых секторах.

*Установлено,* что феномен «нормативной турбулентности», обусловленный развитием технологий ИИ, требует внедрения гибких регуляторных инструментов (экспериментальные правовые режимы, инструменты «мягкого права») для адаптации права к технологическим вызовам.

*Обосновано,* что в международно-правовом аспекте деяния (или поведение), связанные с трансграничной обработкой персональных данных и нарушающие международно-правовые обязательства, при наличии оснований для их присвоения государству, квалифицируются как международно-противоправные деяния этого государства. Это актуализирует обязательство государств по проявлению должной осмотрительности для предотвращения трансграничного вреда и необходимость углубления международно-правовой координации в целях выработки универсальных стандартов.

# ЗАКЛЮЧЕНИЕ

Проведенное комплексное международно-правовое диссертационное исследование теоретических и практических аспектов защиты личной информации в глобальном и национальном информационном пространстве позволило достичь поставленной цели и сформулировать следующие **основные выводы**:

*Установлена* фундаментальная трансформация международно-правовой доктрины защиты неприкосновенности частной жизни, эволюционировавшей от пассивной негативной концепции «права быть оставленным в покое» к активному позитивному праву (принципу) на информационное самоопределение. *На основе анализа* эволюции универсальных и региональных международно-правовых инструментов (от Международного пакта о гражданских и политических правах до Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. и Регламента (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС) и практики международных юрисдикционных органов (ЕСПЧ, Суд ЕС) *доказано,* что в условиях глобальной цифровизации, характеризующейся формированием «цифровых досье» и рисками алгоритмического профилирования, происходит становление защиты персональных данных как самостоятельного международно-правового института, конкретизирующего фундаментальное право на неприкосновенность частной жизни (ст. 17 МПГПП, ст. 8 ЕКПЧ).

*Введено и концептуализировано* понятие «нормативной турбулентности» как характеристики современного международно-правового регулирования в глобальном информационном пространстве (Положение 1, выносимое на защиту). *Обосновано,* что стремительное развитие технологий искусственного интеллекта (ИИ) является ключевым фактором турбулентности. Установлено, что данный феномен проявляется в фрагментации глобальной регуляторной среды, возникновении коллизий национальных режимов и усилении фактического нормотворчества частных акторов («самонормативности»).

*Разработана* концепция трансформации «вторичных» (процедурных) норм в «первичные» (субстантивные) как условие реализации фундаментальных прав человека в глобальном информационном пространстве (Положение 2, выносимое на защиту). *На основе функционального анализа* требований современных международно-правовых стандартов в контексте применения алгоритмических систем (от Международного пакта о гражданских и политических правах до Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. и Регламента (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС) и

практики международных юрисдикционных органов (ЕСПЧ, Суд ЕС) *доказано,* что в условиях глобальной цифровизации, характеризующейся формированием «цифровых досье» и рисками алгоритмического профилирования, происходит становление защиты персональных данных как самостоятельного международно-правового института, конкретизирующего фундаментальное право на неприкосновенность частной жизни.

*Разработано* авторское определение «цифровых следов» с учетом их трансграничной природы и международно-правового значения (Положение 3, выносимое на защиту). *Обоснована* двойственная международно-правовая природа цифровых следов: как объекта правовой охраны (элемент персональных данных) и как транснационального средства доказывания, требующего гармонизации процессуальных стандартов.

*Определен* субъектный состав правоотношений в сфере защиты персональных данных. Аргументирована невозможность распространения международно-правового режима персональных данных на сведения о юридических лицах (Положение 4, выносимое на защиту). *На основе анализа* универсальных и региональных международно-правовых инструментов и доктрины международного права прав человека *доказано,* что субъектом данного права является исключительно физическое лицо, поскольку право на информационное самоопределение неразрывно связано с человеческим достоинством и не присуще юридическим лицам.

*Сформулировано* понятие «правовой технологии обеспечения защиты персональных данных» как механизма имплементации международных обязательств (Положение 5, выносимое на защиту). *Предложена* оригинальная концепция правовой технологии как интегрированной совокупности правовых, организационных и технических средств и процедур (проведение оценки воздействия на защиту персональных данных, ведение реестров операций и инвентаризацию массивов персональных данных, защита персональных данных на этапе проектирования). Посредством системного и функционального анализа требований международных актов (в частности, критериев «адекватности уровня защиты» по Регламенту (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС и принципа подотчетности) *доказано,* что данная модель выступает необходимым инструментом для эффективной имплементации международных стандартов в национальный правопорядок, обеспечивая регуляторную совместимость и достижение «адекватного уровня защиты».

*Систематизирован* анализ международно-правового регулирования в сфере защиты персональных данных. *Выявлено* формирование комплексной, но фрагментированной многоуровневой системы. Определена определяющая роль Регламента (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС, который, обладая выраженным экстерриториальным эффектом («Брюссельский эффект»), фактически задает глобальные стандарты комплаенса. *Обобщены*

общепризнанные принципы обработки данных, составляющие нормативные основы регулирования.

*Обосновано* применение норм международного публичного права об ответственности государств (Проект статей КМП ООН) к трансграничным инцидентам в сфере обработки персональных данных. Установлено, что такие инциденты при наличии критериев атрибуции (присвоения) (в частности, осуществление делегированных элементов государственной власти (ст. 5) или наличие «эффективного контроля» (ст. 8) могут квалифицироваться как международно-противоправные деяния государства. Это актуализирует обязательство государств по проявлению должной осмотрительности для предотвращения трансграничного вреда.

*Выявлены* системные пробелы национального регулирования Республики Казахстан: институциональный дефицит (отсутствие независимого специализированного надзорного органа по защите персональных данных); отсутствие обязательной (императивной) процедуры по оценке воздействия на защиту персональных данных; недостаточное (неполное) нормативное закрепление современных прав субъектов. *Предложена* модель фундаментальной институциональной реформы в сфере защиты персональных данных в Республике Казахстан. *Обоснована* необходимость создания независимого надзорного органа по защите персональных данных, институционально и функционально автономного от исполнительной власти, наделенного достаточными надзорными и корректирующими полномочиями (включая полномочия по аудиту алгоритмических систем ИИ), а также нормативного закрепления правового статуса уполномоченных лиц по защите персональных данных.

*Разработан* комплекс практических рекомендаций по совершенствованию правового регулирования, включающий предложения по модернизации национального законодательства (внедрение обязательной оценки воздействия на защиту персональных данных, ведения реестра операций обработки персональных данных, закрепление принципов защиты персональных данных на этапе проектирования и по умолчанию, расширение прав субъектов персональных данных) и меры в сфере международно-правового сотрудничества. *Обоснована* необходимость присоединения Республики Казахстан к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. и разработки межведомственного порядка атрибуции и реагирования на трансграничные инциденты на основе норм об ответственности государств.

**Оценка полноты решений поставленных задач.** Задачи, поставленные в диссертационном исследовании для достижения цели комплексного международно-правового анализа защиты личной информации в глобальном и национальном информационном пространстве, решены в полном объеме. В рамках теоретико-методологического блока (Раздел 1) раскрыто понятие личной информации как объекта международно-правовой защиты, проанализированы источники и принципы регулирования, обоснована

комплексная методология исследования. В разделе 2 определен международно-правовой статус субъектов отношений по защите персональных данных, исследованы международно-правовые инструменты и проблемные аспекты защиты персональных данных, проанализированы стратегические вызовы для правового режима (включая искусственный интеллект и «нормативную турбулентность»), а также проанализирована судебная практика в РК и пробелы правоприменения. В разделе 3 сформулированы понятие и критерии эффективности правового регулирования, разработаны направления его совершенствования, охарактеризованы технико-правовые компоненты защиты. На основе проведенного анализа обоснованы конкретные предложения по совершенствованию законодательства РК и его гармонизации с передовыми международными стандартами. Таким образом, все поставленные задачи выполнены, а полученные результаты образуют целостное научное исследование.

В заключении диссертационного исследования предлагаются следующие **практические рекомендации** по совершенствованию правового регулирования защиты персональных данных:

*Рекомендовать* Парламенту Республики Казахстан совместно с Правительством Республики Казахстан инициировать разработку комплексного проекта Закона о внесении изменений и дополнений в законодательные акты Республики Казахстан по вопросам защиты персональных данных и цифровых технологий. В рамках данного законопроекта предлагается предусмотреть проведение институциональной реформы путем внесения изменений в Закон РК от 21 мая 2013 года N 94-V «О персональных данных и их защите». В частности, рекомендуется дополнить Закон новой Главой «Статус и полномочия независимого уполномоченного органа по защите персональных данных». В статьях данной главы должны быть закреплены правовой статус уполномоченного органа как государственного органа, не входящего в структуру центральных исполнительных органов и обладающего функциональной, организационной и финансовой автономией, а также определен порядок назначения его руководителя на фиксированный срок с гарантиями несменяемости и исчерпывающим перечнем оснований для досрочного прекращения полномочий. Кроме того, необходимо наделить Уполномоченный орган исключительной компетенцией в сфере защиты персональных данных и надзора за рисками алгоритмических систем, а также расширенными надзорными и корректирующими полномочиями, включая проведение аудита алгоритмов и наложение административных взысканий.

*Рекомендуется* также предусмотреть имплементацию риск-ориентированного подхода и принципа подотчетности путем внесения соответствующих изменений в Закон РК от 21 мая 2013 года N 94-V «О персональных данных и их защите». Предлагается дополнить Закон новой статьей (например, статья 25-1) «Оценка воздействия на защиту персональных данных», устанавливающей обязанность оператора проводить документированную оценку воздействия до начала операций обработки, представляющих высокий риск для прав и свобод субъектов (включая обработку

биометрических данных, масштабное профилирование, внедрение систем ИИ). Одновременно *рекомендуется* дополнить Закон новой статьей (например, статья 25-2) «Подотчетность и ведение реестров операций обработки персональных данных», в которой закрепляется принцип подотчетности, обязывающий оператора документально подтверждать соответствие обработки требованиям законодательства, а также устанавливается обязанность ведения детализированных реестров операций обработки. Кроме того, *рекомендуется* ввести новую статью (например, статья 25-3) «Защита персональных данных на этапе проектирования и по умолчанию», закрепляющую обязанность оператора внедрять соответствующие технические и организационные меры на самых ранних стадиях проектирования операций обработки. Помимо этого, *предлагается* внести изменения в статью 1 Закона, дополнив ее определениями «псевдонимизация» и «профилирование», а также изложив определение «согласие» в новой редакции, соответствующей международным стандартам (добровольное, конкретное, информированное, однозначное). Одновременно *рекомендуется* внести изменения в статью 24 Закона, дополнив перечень прав субъектов правом на переносимость персональных данных и правом на возражение против решений, основанных исключительно на автоматизированной обработке (включая профилирование).

*Рекомендуется* Правительству Республики Казахстан, Министерству иностранных дел Республики Казахстан, Генеральной прокуратуре Республики Казахстан и Министерству искусственного интеллекта и цифрового развития Республики Казахстан принять комплексные меры в сфере международно-правового сотрудничества. В частности, в целях обеспечения трансграничной совместимости правовых режимов и достижения признания «адекватного уровня защиты», необходимо обеспечить успешное завершение процесса присоединения Республики Казахстан к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) с изменениями, внесенными Протоколом CETS № 223 от 10.10.2018 г. Достижение этой цели требует приоритетной реализации необходимых правовых и институциональных реформ, направленных на приведение национального правового режима в полное соответствие с требованиями Конвенции (в том числе через обеспечение фактической независимости уполномоченного надзорного органа по защите персональных данных и имплементацию риск-ориентированного подхода).

*Рекомендуется* Правительству Республики Казахстан совместно с Министерством искусственного интеллекта и цифрового развития Республики Казахстан при разработке проекта Цифрового кодекса РК обеспечить включение в него специализированного раздела, посвященного регулированию искусственного интеллекта (ИИ) и основанного на риск-ориентированном подходе. Предлагается включить в проект Кодекса нормы, устанавливающие классификацию систем ИИ по уровням риска (неприемлемый, высокий, ограниченный и минимальный). При этом необходимо запретить оборот и эксплуатацию систем ИИ неприемлемого риска (в частности, предназначенных для социальной классификации, использующих методы подсознательного

воздействия или осуществляющих дистанционную биометрическую идентификацию в режиме реального времени в общедоступных местах, за исключением случаев, прямо установленных законом). Для систем ИИ высокого риска (используемых в критической инфраструктуре, здравоохранении, правосудии и государственном управлении) *рекомендуется* нормативно закрепить императивные требования, включая наличие системы управления рисками на протяжении всего жизненного цикла, обеспечение качества и репрезентативности наборов данных, минимизацию алгоритмической предвзятости, ведение технической документации и автоматическое журналирование событий, а также обеспечение прозрачности функционирования, возможности человеческого надзора и кибербезопасности. Кроме того, необходимо установить, что до ввода в эксплуатацию системы ИИ высокого риска подлежат обязательной процедуре оценки соответствия и проведению оценки воздействия на права и свободы физических лиц.

**Оценка научного уровня выполненной работы в сравнении с лучшими достижениями в данной области.** Научный уровень диссертационного исследования соответствует передовым разработкам (подходам) современной международно-правовой доктрины в сфере регулирования глобального информационного пространства и защиты прав человека в цифровую эпоху. Исследование соответствует актуальной глобальной повестке дискуссий, посвященных вызовам, обусловленным применением технологий искусственного интеллекта, фрагментации глобальной регуляторной среды и проблеме адаптации права к технологическим изменениям. Автором предложена концептуализация феномена «нормативной турбулентности». Данное понятие формирует новый аналитический подход для анализа системных разрывов в международном регулировании, дополняя существующие в доктрине теории (например, «Брюссельский эффект»). Научную ценность представляет применение доктрины международно-правовой ответственности государств (Проект статей КМП ООН) к анализу трансграничных инцидентов с персональными данными. Такой подход соответствует передовым исследованиям, направленным на комплексный анализ (осмысление) правового регулирования сферы информатизации (киберпространства), и позволяет преодолеть разрыв (дуализм) между публично-правовыми нормами в сфере кибербезопасности и специальным регулированием защиты персональных данных. В прикладном аспекте работа восполняет пробел в сравнительно-правовой литературе, предлагая детальный анализ правового режима Республики Казахстан в сопоставлении с ведущими мировыми моделями (ЕС, США, КНР). Разработанные предложения по институциональной реформе и имплементации риск-ориентированного подхода основаны на анализе передовых международных практик и представляют собой значимый вклад в развитие национальной правовой системы. Таким образом, диссертационное исследование отвечает актуальным вызовам в сфере международно-правовых аспектах защиты личной информации в глобальном и национальном информационном пространстве и представляет весомый вклад в развитии науки международного права.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1 Бисалиев М. С., Шакиров К. Н. Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет // Вестник Евразийского национального университета имени Л. Н. Гумилёва. Серия: Право. – 2023. – Т. 142. – № 1. – С. 81–98.

2 Wachter S., Mittelstadt B., Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation // International Data Privacy Law. – 2017. – Vol. 7, No. 2. – pp. 76–99.

3 Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. ... д-ра юрид. наук : 12.00.14 / Т. А. Полякова ; ГОУВПО «Российская правовая академия». – М., 2008. – 39 с.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс] // Official Journal of the European Union. – 2016. – L 119. – pp. 1–88. – URL: https://data.europa.eu/eli/reg/2016/679/oj (дата обращения: 18.02.2025).

5 Наумов В. Б. Право и Интернет: очерки теории и практики. – М. : Книжный дом «Университет», 2002. – 432 с.

6 Okinawa Charter on Global Information Society [Электронный ресурс] // Ministry of Foreign Affairs of Japan. – URL: https://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf (дата обращения: 09.09.2025).

7 Bissaliyev M. S., Susi M., Shakirov, K. Convergence between and among the Chinese, the EU and Kazakhstan Approaches towards Personal Data Protection against the AI in the Digital Sphere // Chinese Journal of International Law. – 2025. – Vol. 24, No. 2. – Article ID jmaf011. – pp. 1–32.

8 Копылов В. А. Информационное право : учебник. – 2-е изд., перераб. и доп. – М. : Юристъ, 2003. – 512 с.

9 Организационно-правовое обеспечение информационной безопасности : учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов [и др.] ; под ред. А. А. Стрельцова. – М. : Издательский центр «Академия», 2008. – 256 с.

10 Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы [Электронный ресурс] : Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P2300000269 (дата обращения: 18.02.2025).

11 Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» от 8 сентября 2025 года [Электронный ресурс] // Официальный сайт Президента Республики Казахстан.

– URL: https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-kazahstan-v-epohu-iskusstvennogo-intellekta-aktualnye-zadachi-i-ih-resheniya-cherez-cifrovuyu-transformaciyu-885145 (дата обращения: 09.09.2025).

12 О мерах по дальнейшему совершенствованию системы государственного управления [Электронный ресурс] : Указ Президента Республики Казахстан от 18 сентября 2025 года // Официальный сайт Президента Республики Казахстан. – URL: https://akorda.kz/ru/o-merah-po-dalneyshemu-sovershenstvovaniyu-sistemy-gosudarstvennogo-upravleniya-1883846 (дата обращения: 23.09.2025).

13 Глава государства принял участие в саммите «Центральная Азия – США» [Электронный ресурс] // Официальный сайт Президента Республики Казахстан. – 2025. – URL: https://akorda.kz/ru/glava-gosudarstva-prinyal-uchastie-v-sammite-centralnaya-aziya-ssha-7104132 (дата обращения: 08.11.2025).

14 Convention 108+: Convention for the Protection of Individuals with regard to the Processing of Personal Data [Электронный ресурс] // Council of Europe. – URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (дата обращения: 17.09.2025).

15 Масштабная база данных «Жители Казахстана 2024» утекла в сеть – ЦАРКА [Электронный ресурс] // Международное информационное агентство «Казинформ». – 2025. – URL: https://www.inform.kz/ru/masshtabnaya-baza-dannih-zhiteli-kazahstana-2024-utekla-vset-tsarka-d5840c (дата обращения: 18.06.2025).

16 Об утечке персональных данных граждан Республики Казахстан в микрофинансовой организации «zaimer.kz» [Электронный ресурс] // Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. – 2024. – URL: https://www.gov.kz/memleket/entities/mdai/press/news/details/722908?lang=ru (дата обращения: 19.02.2025).

17 Brownlie I. System of the Law of Nations: State Responsibility. Part I. – New York : Oxford University Press, 1983. – 320 p.

18 Responsibility of States for Internationally Wrongful Acts [Электронный ресурс] / International Law Commission. – 2001. – 15 p. – URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (дата обращения: 25.03.2025).

19 Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries [Электронный ресурс] / International Law Commission. – 2001. – 114 p. – URL: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (дата обращения: 25.03.2025).

20 Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : 2nd ed. – Cambridge : Cambridge University Press, 2017. – 638 p.

21 Crawford, J. The ILC’s Articles on Responsibility of States for Internationally Wrongful Acts: A Retrospect // American Journal of International Law. – 2002. – Vol. 96, No. 4. – pp. 874–890.

22 Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. – 1890. – Vol. 4, No. 5. – pp. 193–220.

23 Westin A. F. Privacy and Freedom. – New York : Atheneum, 1967. – 558 p.

24 Solove D. J. The Digital Person: Technology and Privacy in the Information Age. – New York : NYU Press, 2004. – 283 p. – (GWU Law School Public Law Research Paper No. 2017-5; GWU Legal Studies Research Paper No. 2017-5). – URL: https://ssrn.com/abstract=2899131 (дата обращения: 18.02.2025).

25 Сман А. Права человека и гражданина в Республике Казахстан: учебное пособие. – Нур-Султан: Туран-Астана, 2019. – 143 с.

26 Жетписов С. К. Право на неприкосновенность частной жизни и его судебная защита в Республике Казахстан [Текст] : дис. ... канд. юрид. наук : 12.00.11 / С. К. Жетписов ; Университет имени Д. А. Кунаева. – Алматы, 2007. – 146 с.

27 Жетписов С. К. Комплексный межотраслевой институт тайны: обзор международного законодательства // Наука, новые технологии и инновации Кыргызстана. – 2018. – № 6. – С. 112–116.

28 Жексембаева Н. Е. Қазақстан Республикасын цифрландыру жағдайында адамның ақпараттық құқықтары [Текст] : дис. ... философия докторы (PhD) : 6D030100 – Құқықтану / Н. Е. Жексембаева ; әл-Фараби атындағы Қазақ ұлттық университеті. – Алматы, 2024. – 154 с.

29 Татаринов Д. В. Правовые основы защиты права на неприкосновенность частной жизни в глобальных коммуникационных сетях // Правовые основы борьбы с правонарушениями в глобальных коммуникационных сетях : монография / под общ. ред. Д. В. Татаринова, Т. К. Ерджанова, Л. Ф. Татариновой, Д. В. Голобурда. – Алматы : Қазақ университеті, 2014. – С. 145–161. – 344 с.

30 Tatarinova L., Erdzhanov T., Tatarinova D. Conceptual Problems of Developing a Mechanism to Protect the Right to Privacy in Global Communications Networks // Middle-East Journal of Scientific Research. – 2013. – Vol. 15, No. 7. – P. 937–943.

31 Ерджанов Т. К. Актуальные вопросы правового регулирования деятельности в глобальных информационно-коммуникационных сетях // Правовые основы борьбы с правонарушениями в глобальных коммуникационных сетях : монография / под общ. ред. Д. В. Татаринова, Т. К. Ерджанова, Л. Ф. Татариновой, Д. В. Голобурда. – Алматы : Қазақ университеті, 2014. – С. 259–308. – 344 с.

32 Шакенов, М. А. Правовое регулирование информационного пространства [Текст] : дис. ... канд. юрид. наук : 12.00.01 / М. А. Шакенов ; Казахский гуманитарно-юридический университет. – Астана, 2009. – 148 с.

33 Ерджанов Т. К., Танекова М. О. Правовые аспекты защиты чести и достоинства от посягательств в социальных сетях // Государственное управление и государственная служба. – 2016. – № 1. – С. 132–141.

34 Ерджанов Т. К., Голобурда Д. В. К вопросу о «праве на анонимность» в Интернете // Вестник КазНУ. Серия международные отношения и международное право. – 2016. – № 2 (74). – С. 84–89.

35 Татаринова Л. Ф. Проблемные аспекты защиты чести и достоинства от посягательства в глобальных коммуникационных сетях // Актуальные проблемы гуманитарных и естественных наук. – 2013. – № 3. – С. 205–209.

36 Габдыжамалов Н. М. Информационная безопасность в рамках интеграционных процессов: политологический анализ [Текст] : дис. ... канд. полит. наук : 23.00.02 / Н. М. Габдыжамалов ; Академия государственного управления при Президенте Республики Казахстан. – Астана, 2010. – 183 с.

37 Джилкишиев Р. Б. Расследование преступлений в сфере информационных технологий [Текст] : 8D12301 – Правоохранительная деятельность : диссертация на соискание степени доктора философии (PhD) / Р. Б. Джилкишиев ; Костанайская академия Министерства внутренних дел Республики Казахстан им. Ш. Кабылбаева. – Костанай, 2025. – 186 с. – На правах рукописи.

38 Alan Westin’s Legacy of Privacy and Freedom [Электронный ресурс] // IAPP. – URL: https://iapp.org/news/a/alan-westins-legacy-of-privacy-and-freedom/ (дата обращения: 16.02.2025).

39 Federal Constitutional Court of Germany. Judgment of the First Senate of 15 December 1983, Case No. 1 BvR 209/83 et al. (Census Act Ruling), in Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 65, 1 [Электронный ресурс] // Bundesverfassungsgericht. – URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html (дата обращения: 28.02.2025).

40 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [Электронный ресурс] : [done at Strasbourg, 28.01.1981] // Council of Europe. – URL: https://rm.coe.int/1680078b37 (дата обращения: 11.03.2025).

41 Susi M. Human rights in the digital domain – the idea of non-coherence theory // In: Human Rights, Digital Society and the Law / ed. M. Susi. – Routledge, 2019. – pp. 3–11. – 412 p.

42 Orwell G. Nineteen Eighty-Four. – London : Penguin Group (UK), 2008. – 352 p.

43 Kafka F. The Trial. – London : Penguin Random House (UK), 2024. – 208 p.

44 Foucault M. Discipline and Punish: The Birth of the Prison / M. Foucault ; transl. from the French by A. Sheridan. – 2nd Vintage Books ed. – New York : Vintage Books, 1995. – 333 p.

45 Haggerty K. D., Ericson R. V. The Surveillant Assemblage // The British Journal of Sociology. – 2000. – Vol. 51, No. 4. – pp. 605–622.

46 Zuboff S. The Age of Surveillance Capitalism // In: Social Theory Re-Wired: New Connections to Classical and Contemporary Perspectives / eds. W. Longhofer, D. Winchester. – 3rd ed. – London; New York: Routledge, 2023. – pp. 203–213. – 514 p.

47 Всеобщая декларация прав человека: принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года [Электронный ресурс] // Организация Объединенных Наций. – URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 18.02.2025).

48 Международный пакт о гражданских и политических правах: принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года [Электронный ресурс] // Организация Объединенных Наций. – URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 18.02.2025).

49 Европейская конвенция о защите прав человека и основных свобод (ETS № 5) : [заключена в г. Риме 04.11.1950] (с изм. и доп. от 01.06.2010) [Электронный ресурс] // Совет Европы. – URL: https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols (дата обращения: 18.02.2025).

50 Judgment of the Grand Chamber in the case of Rotaru v. Romania (Application no. 28341/95), 4 May 2000 [Электронный ресурс] // HUDOC: European Court of Human Rights. – URL: https://hudoc.echr.coe.int/eng?i=001-58586 (дата обращения: 18.02.2025).

51 Judgment of the Grand Chamber in the case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04), 4 December 2008 [Электронный ресурс] // HUDOC: European Court of Human Rights. – URL: https://hudoc.echr.coe.int/eng?i=001-90051 (дата обращения: 21.02.2025).

52 Хартия Европейского союза об основных правах (2012/C 326/02) [Электронный ресурс] // Official Journal of the European Union. – 2012. – pp. 391–407. – URL: https://data.europa.eu/eli/treaty/char_2012/oj (дата обращения: 18.02.2025).

53 Data protection laws in the United States [Электронный ресурс] // DLA Piper Intelligence. – URL: https://dlapiperdataprotection.com/index.html?t=law&c=US (дата обращения: 22.02.2025).

54 Summary of the HIPAA Privacy Rule [Электронный ресурс] // U.S. Department of Health and Human Services. – URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (дата обращения: 25.02.2025).

55 Gramm-Leach-Bliley Act [Электронный ресурс] : Public Law No. 106-102 (Nov. 12, 1999) // Congress.gov. – URL: https://www.congress.gov/bill/106th-congress/senate-bill/900 (дата обращения: 19.02.2025).

56 California Consumer Privacy Act of 2018 [Электронный ресурс] : Cal. Civ. Code §§ 1798.100-1798.199.100 // California Legislative Information. – URL:

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (дата обращения: 19.02.2025).

57 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) [Электронный ресурс] / E. McCallister, T. Grance, K. Scarfone. – Gaithersburg : National Institute of Standards and Technology, 2010. – 59 p. – (NIST Special Publication ; 800-122). – URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf (дата обращения: 25.08.2025).

58 California Privacy Protection Agency Announces 2025 Increases for CCPA Fines and Penalties [Электронный ресурс] // California Privacy Protection Agency. – 2024. – URL: https://cppa.ca.gov/announcements/2024/20241217.html (дата обращения: 25.08.2025).

59 Personal Information Protection Law of the People's Republic of China [Электронный ресурс] : [adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on August 20, 2021] // The National People's Congress of the People's Republic of China. – URL: https://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (дата обращения: 25.08.2025).

60 Cybersecurity Law of the People's Republic of China [Электронный ресурс] : [adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress on November 7, 2016] // The Central People's Government of the People's Republic of China. – URL: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата обращения: 25.02.2025).

61 Data Security Law of the People's Republic of China [Электронный ресурс] : [adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress on June 10, 2021] // The Central People's Government of the People's Republic of China. – URL: https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm (дата обращения: 25.02.2025).

62 Конституция Республики Казахстан : [принята на республиканском референдуме 30 августа 1995 года (с изменениями и дополнениями по состоянию на 01.01.2023 г.) [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K950001000_ (дата обращения: 25.02.2025).

63 Сейтхожина Г. Право на прайвеси [Электронный ресурс] / Г. Сейтхожина // ZAKON.KZ. – 2011. – URL: https://online.zakon.kz/Document/?doc_id=31069351 (дата обращения: 25.02.2025).

64 Иванова Ж. Б., Татаринова Л. Ф. Проблемы корреляции права на информацию и права на неприкосновенность частной жизни в сети интернет // Eurasian Scientific Journal of Law. – 2023. – №. 3 (4). – С. 32-39.

65 Миндрова Е. А. Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества: автореф. дис. … канд. юрид. наук: 12.00.14. – М., 2007. – 31 с.

66 О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 года № 94-V (с изменениями и дополнениями по состоянию на 08.01.2025 г.) [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 25.02.2025).

67 Письмо Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 6 мая 2024 года № ЖТ-2023-03797512 [Электронный ресурс] // ZAKON.KZ. – URL: https://online.zakon.kz/Document/?doc_id=34375785 (дата обращения: 25.08.2025).

68 Об утверждении Государственной программы "Цифровой Казахстан" [Электронный ресурс] : Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827 (с изменениями и дополнениями по состоянию на 17.05.2022 г.) (утратило силу) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P1700000827 (дата обращения: 25.02.2025).

69 Egov.kz : электронное правительство Республики Казахстан [Электронный ресурс]. – URL: https://egov.kz/cms/ru (дата обращения: 25.02.2025).

70 eQurylys.kz : Единая цифровая платформа строительства [Электронный ресурс]. – URL: https://equrylys.kz/ru/about (дата обращения: 25.02.2025).

71 Kezekte.kz : сервис постановки в очередь на жилище [Электронный ресурс]. – URL: https://hf.kezekte.kz/ru/hf/info/help (дата обращения: 25.02.2025).

72 Bissaliyev M. S., Shakirov K. N. Personal data of legal entities as a potential special object of legal protection in cyberspace // Scientific and Legal Journal “Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan.” – 2023. – Vol. 2, No. 73. – pp. 42–52.

73 Жетписов С. К., Алибаева Г. А., Дубовицкая О. Б. Цифрландыру дәуіріндегі дербес деректерді қорғау: конституциялық-құқықтық аспект // Вестник Института законодательства и правовой информации Республики Казахстан. – 2023. – №. 3 (74). – С. 68-76.

74 Дәрібай А. Утечка данных 16 миллионов казахстанцев: возбуждено уголовное дело [Электронный ресурс] / А. Дәрібай // Tengrinews.kz. – 2025. – URL: https://tengrinews.kz/kazakhstan_news/utechka-dannyih-16-millionov-kazahstantsev-vozbujdeno-573411/ (дата обращения: 18.07.2025).

75 О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий [Электронный ресурс] : Закон Республики Казахстан от 25 июня 2020 года № 347-VI ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2000000347 (дата обращения: 11.08.2025).

76 О мерах по реализации Указа Президента Республики Казахстан от 17 июня 2019 года № 24 «О мерах по дальнейшему совершенствованию системы

государственного управления Республики Казахстан» [Электронный ресурс] : Постановление Правительства Республики Казахстан от 12 июля 2019 года № 501 (с изменениями и дополнениями по состоянию на 01.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P1900000501 (дата обращения: 11.08.2025).

77 Akhmetova S. B., Tursynkulova D. A., Ibrayev N. S. Powers of the Personal Data Protection Authority in Europe and Kazakhstan: comparative analysis, recommendations for improving the activities of the Kazakhstani Personal Data Protection Authority // Bulletin of the L. N. Gumilyov Eurasian National University. Law Series. – 2024. – Vol. 148. – No. 3. – pp. 201-214.

78 Greenleaf G., Kaldani, T. Data privacy laws in Central Asia: between ex-SSR and 'Belt & Road' // International Data Privacy Law. – 2025. – Vol. 15, No. 1. – pp. 67–90.

79 Data Protection Authority and you [Электронный ресурс] // European Data Protection Board. – URL: https://edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en (дата обращения: 11.03.2025).

80 Review of the Kazakhstan Commission on Access to Information [Электронный ресурс] / OECD. – Paris : OECD Publishing, 2020. – 53 p. – URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/03/review-of-the-kazakhstan-commission-on-access-to-information_7bd3e08f/3a8d6a0e-en.pdf (дата обращения: 11.03.2025).

81 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [Электронный ресурс] / European Data Protection Board, European Data Protection Supervisor. – [Brussels], 2021. – 23 p. – URL: https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf (дата обращения: 11.03.2025).

82 EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination [Электронный-ресурс] // European Data Protection Board. – 2021. – URL: https://www.edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en (дата обращения: 11.03.2025).

83 Бисалиев М. С., Шакиров К. Н. Характеристика источников международного права в сфере кибербезопасности // Вестник Карагандинского университета. Серия «Право». – 2021. – № 3(103). – С. 15–27.

84 Collins A. A Recipe for Success? Assessing the EU's actorness and effectiveness in the data protection domain [Электронный ресурс] / A. Collins. – Brussels : Centre for European Policy Studies, 2023. – 101 p. – (CEPS In-Depth Analysis). – URL: https://cdn.ceps.eu/wp-content/uploads/2023/04/CEPS-2023-09-In-depth-analysis_EU-Data-Protection.pdf (дата обращения: 25.08.2025).

85 eCommerce Week 2022 Outcome Report: Data and Digitalization for Development [Электронный ресурс] / UNCTAD. – [Geneva], 2022. – 84 p. – URL: https://unctad.org/system/files/information-document/eWeek-2022-Outcome-Report-FINAL.eng_.pdf (дата обращения: 25.08.2025).

86 Convention on Cybercrime (ETS No. 185) [Электронный ресурс] : [done at Budapest, 23.11.2001] // Council of Europe. – URL: https://rm.coe.int/1680081561 (дата обращения: 11.03.2025).

87 Kazakhstan invited to join the Convention on Cybercrime [Электронный ресурс] // Council of Europe. – 2023. – URL: https://www.coe.int/en/web/cybercrime/-/kazakhstan-invited-to-join-the-convention-on-cybercrime (дата обращения: 11.03.2025).

88 Octopus Project: Authorities of Kazakhstan coordinate on the next steps to complete accession to the Convention on Cybercrime [Электронный ресурс] // Council of Europe. – 2024. – URL: https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-of-kazakhstan-coordinate-on-the-next-steps-to-complete-accession-to-the-convention-on-cybercrime (дата обращения: 11.03.2025).

89 Kazakhstan's Participation in OCTOPUS 2025 Strengthens OSCE-Supported International Efforts to Combat Cybercrime [Электронный ресурс] // OSCE. – 2025. – URL: https://www.osce.org/programme-office-in-astana/593222 (дата обращения: 11.03.2025).

90 О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий [Электронный ресурс] : Закон Республики Казахстан от 9 декабря 2019 года № 277-VI ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1900000277 (дата обращения: 25.08.2025).

91 APEC Privacy Framework [Электронный ресурс] / APEC. – 2004. – 23 p. – (2004/AMM/014rev1). – URL: https://www.apec.org/docs/default-source/press/newsrelease/2004/04_amm_014rev1.pdf (дата обращения: 11.09.2025).

92 APEC Privacy Framework [Электронный ресурс] / APEC. – 2015. – URL: https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (дата обращения: 25.08.2025).

93 APEC Cross-border Privacy Enforcement Arrangement [Электронный ресурс] // APEC. – URL: https://www.apec.org/docs/default-source/groups/ecsg/cbpr/cpea-2019.pdf?sfvrsn=f1643e20_1 (дата обращения: 25.08.2025).

94 Kuner C., Bygrave, L. A., Docksey, C. (eds.) The EU General Data Protection Regulation (GDPR): A Commentary. – Oxford: Oxford University Press, 2020. – 1488 p.

95 De Terwangne C. Principles relating to processing of personal data // In: The EU General Data Protection Regulation (GDPR): A Commentary / eds. C. Kuner, L.

A. Bygrave, C. Docksey. – Oxford: Oxford University Press, 2020. – pp. 309–320. – 1488 p.

96 Docksey C. Article 24 Responsibility of the controller // In: The EU General Data Protection Regulation (GDPR): A Commentary / eds. C. Kuner, L. A. Bygrave, C. Docksey. – Oxford: Oxford University Press, 2020. – pp. 555–570. – 1488 p.

97 Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных [Электронный ресурс] : Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 12 июня 2023 года № 179/НҚ (с изменениями дополнениями на 08.01.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2300032810 (дата обращения: 19.08.2025).

98 Об информатизации : Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК (с изменениями и дополнениями по состоянию на 08.01.2025 г.) [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 11.03.2025).

99 Гражданский кодекс Республики Казахстан [Электронный ресурс] : Кодекс Республики Казахстан от 27 декабря 1994 года № 268-XIII (с изменениями и дополнениями по состоянию на 10.06.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K940001000_ (дата обращения: 11.03.2025).

100 Уголовный кодекс Республики Казахстан [Электронный ресурс] : Кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК (с изменениями и дополнениями по состоянию на 07.03.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 11.03.2025).

101 Кодекс Республики Казахстан об административных правонарушениях [Электронный ресурс] : Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗРК (с изменениями и дополнениями по состоянию на 01.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K1400000235 (дата обращения: 12.07.2025).

102 Уголовно-процессуальный кодекс Республики Казахстан [Электронный ресурс] : Кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК (с изменениями и дополнениями по состоянию на 07.03.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения: 11.03.2025).

103 Об утверждении Концепции кибербезопасности («Киберщит Казахстана») [Электронный ресурс] : Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями по состоянию на 17.03.2023 г.) // Информационно-правовая система нормативных

правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 11.03.2025).

104 Персональные данные в Республике Казахстан: проблемы обеспечения конфиденциальности в условиях цифровизации / Е. Е. Ерболатов [и др.] // Вестник Инновационного Евразийского университета. – 2020. – № 3. – С. 49–58.

105 Ерболатов, Е. Е., Жетписов, С. К., Бексултанов, А. С. Конфиденциальность персональных данных в условиях применения цифровых технологий // Ученые труды Алматинской академии МВД РК. – 2023. – № 3. – С. 25–33.

106 Бачило И. Л. Информационное право : учебник для вузов / И. Л. Бачило. – 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 419 с.

107 О банках и банковской деятельности в Республике Казахстан [Электронный ресурс] : Закон Республики Казахстан от 31 августа 1995 года № 2444 (с изменениями и дополнениями по состоянию на 16.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z950002444_ (дата обращения: 19.08.2025).

108 О здоровье народа и системе здравоохранения [Электронный ресурс] : Кодекс Республики Казахстан от 7 июля 2020 года № 360-VI ЗРК (с изменениями и дополнениями по состоянию на 16.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K2000000360 (дата обращения: 25.08.2025).

109 О доступе к информации [Электронный ресурс] : Закон Республики Казахстан от 16 ноября 2015 года № 401-V ЗРК (с изменениями и дополнениями по состоянию на 16.03.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1500000401 (дата обращения: 26.08.2025).

110 Обработка персональных данных в Казахстане [Электронный ресурс] // TAdviser. – URL: https://www.tadviser.ru/index.php/Статья:Обработка_персональных_данных_в_Казахстане (дата обращения: 18.08.2025).

111 Susi M. The Internet Balancing Formula // In: The Non-coherence Theory of Digital Human Rights. – Cambridge: Cambridge University Press, 2024. – pp. 249–266. – 338 p.

112 Керимов Д. А. Методология права: Предмет, функции, проблемы философии права. М.: Аванта+, 2000. – 560 с.

113 Internet of Things [Электронный ресурс] // Merriam-Webster Dictionary. – URL: https://www.merriam-webster.com/dictionary/Internet%20of%20Things (дата обращения: 18.08.2025).

114 Quantum Computing [Электронный ресурс] // Merriam-Webster Dictionary. – URL: https://www.merriam-webster.com/dictionary/quantum%20computing (дата обращения: 18.08.2025).

115 Hegel G. W. F. Georg Wilhelm Friedrich Hegel: The Science of Logic. – Cambridge: Cambridge University Press, 2010. – 866 p.

116 Энгельс Ф. Анти-Дюринг. Переворот в науке, произведённый господином Евгением Дюрингом. – М. : Политиздат, 1988. – 482 с.

117 Венгеров А. В. Теория государства и права : учеб. для юрид. вузов / А. В. Венгеров. – 3-е изд., испр. и доп. – М. : Омега-Л, 2006. – 608 с.

118 Степин В.С. Теоретическое знание. М.: Прогресс-Традиция, 2000. – 744 с.

119 Лазарев В. В. Интегративное восприятие права //Юридическая наука: история и современность. – 2017. – №. 2. – С. 20–29.

120 Reidenberg J. R. Lex Informatica: The Formulation of Information Policy Rules Through Technology // Texas Law Review. – 1997. – Vol. 76. – P. 553–594.

121 Lessig L. Code: Version 2.0. – New York: Basic Books, 2006. – 410 p.

122 Brignull H. Dark patterns: Deception vs. Honesty in UI Design [Электронный ресурс] // A List Apart. – 2011. – Issue 338. – URL: https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/ (дата обращения: 18.08.2025).

123 Cavoukian A. Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices [Электронный ресурс]. – 2011. – URL: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (дата обращения: 18.08.2025).

124 Kingsbury B., Krisch N., Stewart R. B. The Emergence of Global Administrative Law // Law and Contemporary Problems. – 2005. – Vol. 68, No. 3–4. – P. 15–61.

125 Krisch N., Kingsbury B. Introduction: Global Governance and Global Administrative Law in the International Legal Order // European Journal of International Law. – 2006. – Vol. 17, No. 1. – P. 1–13.

126 Benvenisti E. The Law of Global Governance. – Leiden (Netherlands) : Brill | Nijhoff, 2014. – 331 p. – (The Pocket Books of The Hague Academy of International Law ; vol. 24).

127 Pauwelyn J. Informal International Lawmaking: Framing the Concept and Research Questions // In: Informal International Lawmaking / eds. J. Pauwelyn, R. Wessel, J. Wouters. – Oxford : Oxford University Press, 2012. – pp. 13–34. – 580 p.

128 Katz M. L., Shapiro C. Network Externalities, Competition, and Compatibility // The American Economic Review. – 1985. – Vol. 75, No. 3. – P. 424–440.

129 Khan L. M. Amazon’s Antitrust Paradox // Yale Law Journal. – 2017. – Vol. 126. – P. 710–805.

130 Hart H. L. A. The Concept of Law. – Oxford: OUP Oxford, 2012. – 333 p.

131 Bradford A. The Brussels effect: How the European Union Rules the World. – Oxford University Press, 2020. – 404 p.

132 Давид Р. Основные правовые системы современности / пер. с фр., вступ. ст. В. А. Туманова. – М. : Прогресс, 1988. – 496 с.

133 Vienna Convention on the Law of Treaties, 1969 : [Convention : done at Vienna on 23 May 1969] // United Nations, Treaty Series [Электронный ресурс]. – URL: https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf (дата обращения: 18.08.2025).

134 Case of Tyrer v. The United Kingdom : Judgment of the European Court of Human Rights, 25 April 1978 (Application no. 5856/72) [Электронный ресурс]. – Strasbourg, 1978. – URL: https://hudoc.echr.coe.int/fre?i=001-57587 (дата обращения: 18.08.2025).

135 North Sea Continental Shelf, Judgment [Электронный ресурс] // I.C.J. Reports. – 1969. – P. 3. – URL: https://www.icj-cij.org/sites/default/files/case-related/52/052-19690220-JUD-01-00-EN.pdf (дата обращения: 18.08.2025).

136 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) : Merits, Judgment [Электронный ресурс] // I.C.J. Reports. – 1986. – P. 14. – URL: https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (дата обращения: 18.08.2025).

137 Bissaliyev M. S., Shakirov K. N. Ensuring Safety and Protection of Personal Data on the Internet: Issues of Selection of Optimal Research Methodology // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. – 2024. – Vol. 78, No. 3. – pp. 42–54.

138 Michaels R. The Functional Method of Comparative Law // The Oxford Handbook of Comparative Law. – 2006. – Vol. 2. – pp. 345–389.

139 Полдников Д. Ю. Функциональный метод сравнительной истории права в Европе // Вестник Московского университета. Серия 11. Право. – 2017. – № 4. – С. 47–56.

140 Нерсесянц В. С. Философия права. Учебник для вузов. М. : Норма, 2005. – 656 с.

141 Dziedziak W. Axiological Basis for the Application of Law – a Perspective of the Equitable law // Studia Iuridica Lublinensia. – 2015. – Vol. 24, No. 2. – pp. 49–71.

142 Lang P. P. Legal axiology in the information society // Proceedings of the II International Scientific Conference “Global Challenges and Prospects of Modern Economic Development”. European Proceedings of Social and Behavioural Sciences. – 2020. – Vol. 79. – pp. 778–783.

143 Banakar R., Travers M. Law, Sociology and Method // In: Theory and Method in Socio-Legal Research / eds. R. Banakar, M. Travers. – London: Bloomsbury Publishing, 2005. – pp. 1–31. – (Oñati International Series in Law and Society). – 392 p.

144 Acquisti A., Brandimarte L., Loewenstein G. Privacy and Human Behavior in the Age of Information // Science. – 2015. – Vol. 347, No. 6221. – pp. 509–514.

145 Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon // Computers & Security. – 2017. – Vol. 64. – pp. 122–134.

146 Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information [Электронный ресурс] / B. Auxier [et al.]. – Washington, D.C. : Pew Research Center, November 2019. – URL: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf (дата обращения: 11.03.2025).

147 Fundamental Rights Report 2020 [Электронный ресурс] / European Union Agency for Fundamental Rights. – [Vienna] : FRA, 2020. – URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-report-2020_en.pdf (дата обращения: 11.03.2025).

148 Special Eurobarometer 487a: The General Data Protection Regulation [Электронный ресурс] / European Commission. – Brussels, 2019. – URL: https://europa.eu/eurobarometer/surveys/detail/2225 (дата обращения: 11.03.2025).

149 Алматбаева Ж. Как казахстанцы относятся к защите своих персональных данных [Электронный ресурс] / Ж. Алматбаева // The Pulse. – 2021. – URL: https://thepulse.kz/show?slug=kak-kazahstancy-otnosyatsya-k-zashite-svoih-personal-nyh-dannyh&category=business (дата обращения: 18.08.2025).

150 Thaler R. H., Sunstein C. R. Nudge: Improving Decisions About Health, Wealth, and Happiness. – New Haven; London: Yale University Press, 2008. – 293 p.

151 Black J. The emergence of risk-based regulation and the new public risk management in the United Kingdom // Public Law. – 2005. – P. 510–546.

152 Dunn P.; de Gregorio G. Risk-based regulation in European digital constitutionalism [Электронный ресурс] // The Digital Constitutionalist. – 21 Apr. 2022. – URL: https://digi-con.org/risk-based-regulation-in-european-digital-constitutionalism/ (дата обращения: 18.08.2025).

153 Bygrave L. A. Data Protection Law: Approaching its Rationale, Logic and Limits. – The Hague; New York: Kluwer Law International, 2002. – 448 p.

154 Schwartz P. M., Solove D. J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information // New York University Law Review. – 2011. – Vol. 86, No. 6. – pp. 1814–1894.

155 Voss W. G. Cross-Border Data Flows, the GDPR, and Data Governance // Washington International Law Journal. – 2020. – Vol. 29, No. 3. – pp. 485–532.

156 Van der Sloot B. Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system // Computer Law & Security Review. – 2015. – Vol. 31, No. 1. – pp. 26–45.

157 Erdos D. Dead ringers? Legal persons and the deceased in European data protection law // Computer Law & Security Review. – 2021. – Vol. 40. – Article ID 105495. – pp. 1–34.

158 New Federal Act on Data Protection (nFADP) [Электронный ресурс] // SME Portal of SECO. – URL: https://www.kmu.admin.ch/kmu/en/home/facts-and-

trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html (дата обращения: 18.08.2025).

159 Cooper E. R., Raul A. C., Rockwell S. P. APEC Overview // In: The Privacy, Data Protection and Cybersecurity Law Review / ed. A. C. Raul. – London: Law Business Research Limited, 2021. – pp. 41–53.

160 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [Электронный ресурс] : [adopted on 23 September 1980; as amended on 11 July 2013] / OECD. – URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (дата обращения: 20.08.2025).

161 Bissaliyev M. S., Shakirov K. N. Personal Data of Legal Entities as a Potential Special Object of Legal Protection in Cyberspace // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. – 2023. – Vol. 73, No. 2. – pp. 42–52.

162 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 223) [Электронный ресурс] : [done at Strasbourg, 10.X.2018] // Council of Europe. – URL: https://rm.coe.int/16808ac918 (дата обращения: 26.08.2025).

163 AIFC Data Protection Regulations [Электронный ресурс] : AIFC Regulations No. 10 of 2017 (with amendments as of April 1, 2025). – Astana, 2017. – 40 p. – URL: https://aifc.kz/wp-content/uploads/2024/06/aifc-data-protection-regulations-2025-1.pdf (дата обращения: 26.08.2025).

164 AIFC Data Protection Rules [Электронный ресурс] : AIFC Rules No. 1 of 2018 (with amendments as of April 1, 2025). – Astana, 2018. – 16 p. – URL: https://aifc.kz/wp-content/uploads/2024/06/aifc-data-protection-rules-2025-2.pdf (дата обращения: 28.08.2025).

165 Charter of Fundamental Rights of the European Union (2012/C 326/02) [Электронный ресурс] // Official Journal of the European Union. – 2012. – C 326. – pp. 391–407. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2012/326/02 (дата обращения: 18.08.2025).

166 Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. – 2018. – № 2 (254). – С. 5–17.

167 Талапина Э. В. Право на защиту персональных данных с позиций публичного права // Конституционное и муниципальное право. – 2022. – № 10. – С. 29–32.

168 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [Электронный ресурс] // Official Journal of the European Union. – 2022. – L 333. – pp. 80–152. – URL: https://data.europa.eu/eli/dir/2022/2555/oj (дата обращения: 18.08.2025).

169 Vandezande N. Cybersecurity in the EU: How the NIS2-Directive Stacks Up Against Its Predecessor // Computer Law & Security Review. – 2024. – Vol. 52. – Article ID 105890. – pp. 1–10.

170 Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС) [Электронный ресурс] : [заключено в г. Марракеше 15.04.1994] // WIPO Lex. – URL: https://wipolex.wipo.int/ru/text/379915 (дата обращения: 19.08.2025).

171 Criminal Resource Manual 1127. 18 U.S.C. § 1831 Element Three – The Information Was a Trade Secret [Электронный ресурс] // Criminal Resource Manual / U.S. Department of Justice. – URL: https://www.justice.gov/archives/jm/criminal-resource-manual-1127-18-usc-1831-element-three-information-was-trade-secret (дата обращения: 19.08.2025).

172 18 U.S. Code § 1839 – Definitions [Электронный ресурс] // Legal Information Institute, Cornell Law School. – URL: https://www.law.cornell.edu/uscode/text/18/1839 (дата обращения: 19.08.2025).

173 О налогах и других обязательных платежах в бюджет (Налоговый кодекс) [Электронный ресурс] : Кодекс Республики Казахстан от 25 декабря 2017 года № 120-VI ЗРК (с изменениями и дополнениями по состоянию на 18.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K1700000120 (дата обращения: 19.08.2025).

174 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Электронный ресурс] // Official Journal of the European Union. – 2002. – L 201. – pp. 37–47. – URL: https://data.europa.eu/eli/dir/2002/58/oj (дата обращения: 19.08.2025).

175 О применении в судебной практике законодательства о защите чести, достоинства и деловой репутации физических и юридических лиц [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 18 декабря 1992 г. № 6 (с изменениями и дополнениями по состоянию на 28.11.2024 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P92000006S_ (дата обращения: 19.08.2025).

176 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [Электронный ресурс] // Official Journal of the European Union. – 2016. – L 157. – pp. 1–18. – URL: https://data.europa.eu/eli/dir/2016/943/oj (дата обращения: 19.08.2025).

177 Registrar of Companies: rules and powers [Электронный ресурс] // GOV.UK. – 2024. – URL: https://www.gov.uk/government/publications/company-registrars-rules-and-powers/company-registrars-rules-and-powers (дата обращения: 19.08.2025).

178 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [Электронный ресурс] // Official Journal of the European Union. – 2016. – L 119. – pp. 89–131. – URL: https://data.europa.eu/eli/dir/2016/680/oj (дата обращения: 27.08.2025).

179 Об утверждении Правил организации деятельности центра обмена данными по платежным транзакциям с признаками мошенничества (антифрод-центр Национального Банка Республики Казахстан) [Электронный ресурс] : постановление Правления Национального банка Республики Казахстан от 25 августа 2025 года № 54 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2500036742 (дата обращения: 18.09.2025).

180 Об утверждении Правил функционирования программы взаимодействия с исследователями информационной безопасности [Электронный ресурс] : Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 апреля 2024 года № 185/НҚ// Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2400034211 (дата обращения: 27.08.2025).

181 Cost of a Data Breach Report 2025: The AI Oversight Gap [Электронный ресурс] / IBM. – 2025. – URL: https://www.ibm.com/reports/data-breach (дата обращения: 19.08.2025).

182 Accountability principle [Электронный ресурс] // Information Commissioner's Office. – URL: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/accountability-principle/ (дата обращения: 19.08.2025).

183 Explainable AI to Mitigate the Lack of Transparency and Legitimacy in Internet Moderation / T. P. Ferraz [et al.] // Estudos Avançados. – 2024. – Vol. 38, No. 111. – P. 381–405.

184 Judgment of the Grand Chamber in the case of Delfi AS v. Estonia (Application no. 64569/09), 16 June 2015 [Электронный ресурс] // HUDOC: European Court of Human Rights. – URL: https://hudoc.echr.coe.int/fre?i=001-155105 (дата обращения: 31.08.2025).

185 Susi M. Delfi AS v. Estonia // American Journal of International Law. – 2014. – Vol. 108, No. 2. – pp. 295–302.

186 Об утверждении проверочного листа за соблюдением законодательства Республики Казахстан о персональных данных и их защите в отношении собственников и (или) операторов, а также третьих лиц [Электронный ресурс] : Совместный приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 19 марта 2024 года

№ 149/НҚ и Заместителя Премьер-Министра - Министра национальной экономики Республики Казахстан от 19 марта 2024 года № 12 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2400034179 (дата обращения: 27.08.2025).

187 Ишекенова, Б. Две крупных компании оштрафовали за нарушения при защите персональных данных [Электронный ресурс] / Б. Ишекенова // LSM.kz. – 2024. – URL: https://lsm.kz/dve-nackompanii-oshtrafovali-za-narusheniya-v-zashite-personal-nyh-dannyh (дата обращения: 19.08.2025).

188 Opinion 3/2010 on the principle of accountability (WP 173) [Электронный ресурс] / Article 29 Data Protection Working Party. – [Brussels], 2010. – 19 p. – URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (дата обращения: 19.08.2025).

189 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0) [Электронный ресурс] / European Data Protection Board. – [Brussels], 2020. – 31 p. – URL: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (дата обращения: 19.08.2025).

190 О персональных данных [Электронный ресурс] : Федеральный закон от 27.07.2006 № 152-ФЗ (с изменениями и дополнениями по состоянию на 24.06.2025 г.) // КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 27.08.2025).

191 1.2 billion euro fine for Facebook as a result of EDPB binding decision [Электронный ресурс] // European Data Protection Board. – 2023. – URL: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (дата обращения: 19.08.2025).

192 ENISA Threat Landscape for Supply Chain Attacks [Электронный ресурс] / European Union Agency for Cybersecurity (ENISA). – [Athens], 2021. – 57 p. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-supply-chain-attacks (дата обращения: 19.08.2025).

193 О регулировании торговой деятельности [Электронный ресурс] : Закон Республики Казахстан от 12 апреля 2004 года № 544 (с изменениями и дополнениями по состоянию на 20.07.2025 г.) // Әділет : Информационно-правовая система нормативных правовых актов Республики Казахстан. – URL: https://adilet.zan.kz/rus/docs/Z040000544_ (дата обращения: 19.08.2025).

194 Amazon.com Privacy Notice [Электронный ресурс] // Amazon. – URL: https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (дата обращения: 19.08.2025).

195 Privacy Policy for Customers [Электронный ресурс] // Shopify. – URL: https://www.shopify.com/legal/privacy/customers (дата обращения: 19.08.2025).

196 Что означает графа «Услуги по обработке данных» в счёт-фактуре от Магазина на Kaspi.kz? [Электронный ресурс] // Kaspi Гид для партнёров. – 2022.

– URL: https://guide.kaspi.kz/partner/ru/shop/returns/q2295 (дата обращения: 19.08.2025).

197 Marriott security breach exposed data of up to 500M guests [Электронный ресурс] // AP News. – 2018. – URL: https://apnews.com/article/d496fce7a77347d6aa058470d38a69bc (дата обращения: 19.08.2025).

198 Chin K. Biggest Data Breaches in US History (Updated 2025) [Электронный ресурс] / K. Chin // UpGuard. – 2025. – URL: https://www.upguard.com/blog/biggest-data-breaches-us (дата обращения: 19.08.2025).

199 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [Электронный ресурс] // Official Journal of the European Union. – 2022. – L 277. – pp. 1–102. – URL: https://data.europa.eu/eli/reg/2022/2065/oj (дата обращения: 19.08.2025).

200 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [Электронный ресурс] // Official Journal of the European Union. – 2022. – L 265. – pp. 1–66. – URL: https://data.europa.eu/eli/reg/2022/1925/oj (дата обращения: 19.08.2025).

201 Об онлайн-платформах и онлайн-рекламе [Электронный ресурс] : Закон Республики Казахстан от 10 июля 2023 года № 18-VIII ЗРК (с изменениями и дополнениями по состоянию на 18.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2300000018 (дата обращения: 27.08.2025).

202 Об отдельных вопросах регулирования платформенной экономики в Российской Федерации [Электронный ресурс] : Федеральный закон от 31.07.2025 № 289-ФЗ // КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_511088/ (дата обращения: 27.08.2025).

203 Onlayn-platforma va veb-saytlar foydalanuvchilarining huquqlarini himoya qilish to'g'risida [Электронный ресурс] : [проект]. – URL: https://regulation.gov.uz/oz/d/6294 (дата обращения: 27.08.2025).

204 В Азербайджане ужесточены правила онлайн-рекламы [Электронный ресурс] // 1news.az. – 2025. – URL: https://1news.az/news/20250422012057697-V-Azerbaidzhane-uzhestocheny-pravila-onlain-reklamy (дата обращения: 27.08.2025).

205 Об изменении Закона Республики Беларусь «О государственном регулировании торговли и общественного питания» [Электронный ресурс] : Закон Республики Беларусь от 7 марта 2024 г. № 358-З // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=12551&p0=H12400358 (дата обращения: 27.08.2025).

206 Alibaba Group Announces March Quarter and Full Fiscal Year 2022 Results [Электронный ресурс] / Alibaba Group Holding Limited. – 2022. – // U.S. Securities and Exchange Commission (EDGAR). – URL: https://www.sec.gov/Archives/edgar/data/1577552/000110465922065269/tm2217018d1_ex99-1.htm (дата обращения: 31.08.2025).

207 Егорова, М. А. Проблема цифровой идентификации личности в Российской Федерации и Европейском Союзе // Вестник университета имени О. Е. Кутафина. – 2022. – № 1 (89). – С. 17–29.

208 World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank. [Электронный ресурс] // The World Bank. – URL: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf (дата обращения: 19.08.2025).

209 Unique Identification Authority of India [Электронный ресурс]. – URL: https://uidai.gov.in/en/ (дата обращения: 19.08.2025).

210 Initial analysis of the Indian Supreme Court decision on Aadhaar [Электронный ресурс] // Privacy International. – URL: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar (дата обращения: 19.08.2025).

211 eIDAS Regulation [Электронный ресурс] // European Commission. – URL: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (дата обращения: 19.08.2025).

212 Estonia resolves its ID-card crisis [Электронный ресурс] // RIA. – 2017. – URL: https://ria.ee/en/news/estonia-resolves-its-id-card-crisis (дата обращения: 19.08.2025).

213 В работе eGov.kz и сайтов госорганов произошёл сбой из-за технических неполадок [Электронный ресурс] // Казахстан телеграф. – 2025. – URL: https://www.kt.kz/rus/incidents/v_rabote_egov_kz_i_saytov_gosorganov_proizoshel_sboy_iz-za_1377973509.html (дата обращения: 19.08.2025).

214 Taylor J. Major breach found in biometrics system used by banks, UK police and defence firms [Электронный ресурс] / J. Taylor // The Guardian. – 2019. – URL: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (дата обращения: 19.08.2025).

215 Principles on Identification for Sustainable Development: Toward the Digital Age [Электронный ресурс] / The World Bank. – Washington, DC, 2017. – 32 p. – URL: https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf (дата обращения: 19.08.2025).

216 Digital Identity Guidelines [Электронный ресурс] / D. Temoshok [et al.]. – Gaithersburg : National Institute of Standards and Technology, 2025. – 86 p. – (NIST Special Publication; 800-63-4). – URL:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf (дата обращения: 19.08.2025).

217 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements [Электронный ресурс] // ISO. – URL: https://www.iso.org/standard/27001 (дата обращения: 19.08.2025).

218 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [Электронный ресурс] // Official Journal of the European Union. – 2022. – L 333. – pp. 80–152. – URL: https://data.europa.eu/eli/dir/2022/2555/oj (дата обращения: 19.08.2025).

219 Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности [Электронный ресурс] : Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями по состоянию на 13.05.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P1600000832 (дата обращения: 19.08.2025).

220 Об утверждении Правил проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности [Электронный ресурс] : Приказ и. о. Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ (с изменениями и дополнениями по состоянию на 19.08.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1800016756 (дата обращения: 19.08.2025).

221 Black box [Электронный ресурс] // Merriam-Webster Dictionary. – URL: https://www.merriam-webster.com/dictionary/black%20box (дата обращения: 19.08.2025).

222 Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2 (89). – С. 193–202.

223 Мочалов А. Н. Цифровые следы человека и неприкосновенность частной жизни // Антиномии. – 2024. – Т. 24, № 4. – С. 164–189.

224 Application programming interface [Электронный ресурс] // Merriam-Webster Dictionary. – URL: https://www.merriam-webster.com/dictionary/application%20programming%20interface (дата обращения: 19.08.2025).

225 ITRC 2024 Annual Data Breach Report [Электронный ресурс] // Identity Theft Resource Center. – 2025. – URL:

https://www.idtheftcenter.org/publication/2024-data-breach-report/ (дата обращения: 19.08.2025).

226 Сыздыкбаев А. «Утечка данных 16 миллионов казахстанцев»: Минцифры сделало заявление [Электронный ресурс] / А. Сыздыкбаев // Tengrinews.kz. – 2025. – URL: https://tengrinews.kz/kazakhstan_news/utechka-dannyih-16-millionov-kazahstantsev-mintsifryi-573113/ (дата обращения: 19.08.2025).

227 Nomad Guard : Кибербезопасность и защита от DDoS-атак [Электронный ресурс]. – URL: https://nomadguard.kz/ (дата обращения: 19.08.2025).

228 Об утверждении Правил оказания государственных услуг в сфере предпринимательства и признании утратившими силу некоторых приказов Министра национальной экономики Республики Казахстан [Электронный ресурс] : Приказ Министра национальной экономики Республики Казахстан от 11 июня 2021 года № 59 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2100023051 (дата обращения: 27.08.2025).

229 Административный процедурно-процессуальный кодекс Республики Казахстан [Электронный ресурс] : Кодекс Республики Казахстан от 29 июня 2020 года № 350-VI // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/K2000000350 (дата обращения: 31.08.2025).

230 Susi M. Automated Systems and Artificial Intelligence // In: The Non-Coherence Theory of Digital Human Rights. – Cambridge: Cambridge University Press, 2024. – pp. 232–245. – 338 p.

231 Yampolskiy R. V. Artificial Intelligence Safety Engineering: Why Machine Ethics Is a Wrong Approach // In: Philosophy and Theory of Artificial Intelligence / ed. V. C. Müller. – Springer, 2013. – pp. 389–396. – 418 p.

232 Open-source [Электронный ресурс] // Merriam-Webster Dictionary. – URL: https://www.merriam-webster.com/dictionary/open-source (дата обращения: 19.08.2025).

233 Large language model [Электронный ресурс] // Merriam-Webster Dictionary. – URL: https://www.merriam-webster.com/dictionary/large%20language%20models (дата обращения: 19.08.2025).

234 Transcript for Yann LeCun: Meta AI, Open Source, Limits of LLMs, AGI & the Future of AI | Lex Fridman Podcast #416 of March 8, 2024 [Электронный ресурс] // Lex Fridman Podcast. – URL: https://lexfridman.com/yann-lecun-3-transcript/ (дата обращения: 19.08.2025).

235 Bengio Y. AI and Catastrophic Risk [Электронный ресурс] // Journal of Democracy. – September 2023. – URL: https://www.journalofdemocracy.org/ai-and-catastrophic-risk/ (дата обращения: 19.08.2025).

236 AI Extinction Statement Press Release [Электронный ресурс] // Center for AI Safety. – 2023. – URL: https://safe.ai/work/press-release-ai-risk (дата обращения: 19.08.2025).

237 International AI Safety Report [Электронный ресурс] / Y. Bengio [et al.]. – London: Department for Science, Innovation and Technology (DSIT), 2025. – (DSIT 2025/001). – URL: https://assets.publishing.service.gov.uk/media/679a0c48a77d250007d313ee/International_AI_Safety_Report_2025_accessible_f.pdf (дата обращения: 21.08.2025).

238 Pelley S. “Godfather of Artificial Intelligence” Geoffrey Hinton on the promise, risks of advanced AI [Электронный ресурс] / S. Pelley // CBS News. – 2024. – URL: https://www.cbsnews.com/news/geoffrey-hinton-ai-dangers-60-minutes-transcript/ (дата обращения: 21.08.2025).

239 Marchant G. E. The Growing Gap Between Emerging Technologies and the Law // In: The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem / eds. G. E. Marchant, B. R. Allenby, J. R. Herkert. – Dordrecht: Springer, 2011. – pp. 19–33. – 212 p.

240 Rejeski D. Public Policy on the Technological Frontier // In: The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem / eds. G. E. Marchant, B. R. Allenby, J. R. Herkert. – Dordrecht: Springer Netherlands, 2011. – pp. 47–59.

241 Interim Report: Governing AI for Humanity [Электронный ресурс] / United Nations. – [New York], 2023. – 35 p. – URL: https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf (дата обращения: 21.08.2025).

242 Digital Enablers of the Global Economy [Электронный ресурс] / OECD. – Paris : OECD Publishing, 2022. – URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/digital-enablers-of-the-global-economy_e4fb65ba/f0a7baaf-en.pdf (дата обращения: 19.08.2025).

243 The CJEU judgment in the Schrems II case [Электронный ресурс] : At a Glance / European Parliament. – [Brussels], 2020. – 2 p. – URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf (дата обращения: 23.08.2025).

244 Bissaliyev M. S., Shakirov K. N., Baimagambetova Z. M. Legal Aspects of Human Microchipping: US Experience and Prospects for Kazakhstan // The journal "KHABARSHI – VESTNIK" of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan. – 2024. – No. 1(83). – pp. 249–255.

245 Sarewitz D. Anticipatory Governance of Emerging Technologies // In: The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem / eds. G. E. Marchant, B. R. Allenby, J. R. Herkert. – Dordrecht: Springer Netherlands, 2011. – pp. 95–105. – 212 p.

246 Тяньцзиньская декларация Совета глав государств-членов Шанхайской организации сотрудничества [Электронный ресурс] : [принята 1 сентября 2025

г.]. – URL: https://rus.sectsco.org/images/07e9/09/01/1958599.pdf (дата обращения: 09.09.2025).

247 Recommendation of the Council on Artificial Intelligence [Электронный ресурс] : [adopted on 22 May 2019 ; as amended on 03 May 2024] / OECD. – URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (дата обращения: 17.09.2025).

248 Futures of Global AI Governance: Co-Creating an Approach for Transforming Economies and Societies [Электронный ресурс] / OECD. – Paris: OECD Publishing, 2024. – 82 p. – URL: https://www.oecd.org/content/dam/oecd/en/about/programmes/strategic-foresight/GSG%20Background%20Note_GSG(2024)1en.pdf (дата обращения: 17.09.2025).

249 Recommendation on the Ethics of Artificial Intelligence [Электронный ресурс] / UNESCO. – 2022. – 43 p. – (SHS/BIO/PI/2021/1). – URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата обращения: 17.09.2025).

250 Recommendation on the Ethics of Artificial Intelligence: Conditions for the Implementation in Germany [Электронный ресурс] / German Commission for UNESCO. – URL: https://www.unesco.de/assets/dokumente/Deutsche_UNESCO-Kommission/02_Publikationen/Publikation_UNESCO_Recommendation_on_the_Ethics_of_Artificial_Intelligence.pdf (дата обращения: 21.08.2025).

251 UNESCO emphasizes importance of AI Ethics in Kazakhstan [Электронный ресурс] // UNESCO. – 2023. – URL: https://www.unesco.org/en/articles/unesco-emphasizes-importance-ai-ethics-kazakhstan (дата обращения: 11.09.2025).

252 Казахстан и ЮНЕСКО обсудили сотрудничество в области этики искусственного интеллекта [Электронный ресурс] // Министерство иностранных дел Республики Казахстан. – 2025. – URL: https://www.gov.kz/memleket/entities/mfa/press/region-news/details/25302 (дата обращения: 17.09.2025).

253 International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution [Электронный ресурс] / International Conference of Data Protection and Privacy Commissioners. – [Madrid], 2009. – 36 p. – URL: https://edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_en.pdf (дата обращения: 17.09.2025).

254 Good Data: Sharing Data and Fostering Public Trust and Willingness [Электронный ресурс] : White Paper / World Economic Forum. – [Geneva], 2021. – 31 p. – URL: https://www3.weforum.org/docs/WEF_Good_Data_Sharing_Data_and_Fostering_2021.pdf (дата обращения: 17.09.2025).

255 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU)

2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [Электронный ресурс] // Official Journal of the European Union. – 2024. – L 2024/1689. – URL: https://data.europa.eu/eli/reg/2024/1689/oj (дата обращения: 19.08.2025).

256 Artificial Intelligence Risk Management Framework (AI RMF 1.0) [Электронный ресурс] / National Institute of Standards and Technology. – Gaithersburg: NIST, 2023. – 48 p. – (NIST AI 100-1). – URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (дата обращения: 17.09.2025).

257 Voluntary AI Commitments [Электронный ресурс] // The White House. – [Washington], 2023. – 3 p. – URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/09/Voluntary-AI-Commitments-September-2023.pdf (дата обращения: 17.09.2025).

258 Guidelines for AI Business Operators (Version 1.0) Compiled [Электронный ресурс] // Ministry of Economy, Trade and Industry. – 2024. – URL: https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html (дата обращения: 17.09.2025).

259 Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725) [Электронный ресурс] : [adopted on 10 July 2019] / European Data Protection Board. – [Brussels], 2019. – 7 p. – URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendation_201901_edps_39.4_dpia_list_en.pdf (дата обращения: 27.08.2025).

260 Об утверждении Правил осуществления уведомления субъектов персональных данных о нарушении безопасности персональных данных [Электронный ресурс] : Приказ и. о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 9 августа 2024 года № 481/НҚ // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2400034919 (дата обращения: 19.08.2025).

261 Досье на проект Цифрового кодекса Республики Казахстан (апрель 2024 года) [Электронный ресурс] // ZAKON.KZ. – 2024. – URL: https://online.zakon.kz/Document/?doc_id=38933548 (дата обращения: 19.08.2025).

262 Досье на проект Закона Республики Казахстан «Об искусственном интеллекте» (январь 2025 года) [Электронный ресурс] // ZAKON.KZ. – 2025. – URL: https://online.zakon.kz/Document/?doc_id=34868071 (дата обращения: 19.08.2025).

263 Глава государства провел совещание по вопросам развития искусственного интеллекта [Электронный ресурс] // Официальный сайт Президента Республики Казахстан. – 2025. – URL: https://www.akorda.kz/ru/glava-gosudarstva-provel-soveshchanie-po-voprosam-razvitiya-iskusstvennogo-intellekta-1175749 (дата обращения: 19.08.2025).

264 China relaxes security review rules for some data exports [Электронный ресурс] // Reuters. – 2024. – URL: https://www.reuters.com/technology/cybersecurity/chinas-cyberspace-regulator-issues-rules-facilitate-cross-border-data-flow-2024-03-22/ (дата обращения: 19.08.2025).

265 Provisions on the Management of Deep Synthesis of Internet Information Services [Электронный ресурс] : [released on November 25, 2022] // The Central People's Government of the People's Republic of China. – URL: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm (дата обращения: 19.08.2025).

266 Interim Measures for the Administration of Generative Artificial Intelligence Services [Электронный ресурс] : [released on July 13, 2023] // Office of the Central Cyberspace Affairs Commission. – URL: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (дата обращения: 19.08.2025).

267 Regulations on the Administration of Algorithm Recommendations for Internet Information Services [Электронный ресурс] : [released on December 31, 2021] // The Central People's Government of the People's Republic of China. – URL: https://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm (дата обращения: 19.08.2025).

268 Об утверждении Концепции развития искусственного интеллекта на 2024-2029 годы [Электронный ресурс] : Постановление Правительства Республики Казахстан от 24 июля 2024 года № 592 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P2400000592 (дата обращения: 19.08.2025).

269 Елисеева Е. Депутаты одобрили законопроект об искусственном интеллекте [Электронный ресурс] / Е. Елисеева // ZAKON.KZ. – 2025. – URL: https://www.zakon.kz/obshestvo/6477337-deputaty-odobrili-zakonoproekt-ob-iskusstvennom-intellekte.html (дата обращения: 19.08.2025).

270 Estecahandy H. Geopolitics of Cryptocurrency Mining in Kazakhstan // Central Asian Survey. – 2024. – Vol. 43, No. 3. – pp. 327–345.

271 О цифровых активах в Республике Казахстан [Электронный ресурс] : Закон Республики Казахстан от 6 февраля 2023 года № 193-VII (с изменениями и дополнениями по состоянию на 30.06.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2300000193 (дата обращения: 19.08.2025).

272 Нацбанк: Официальный финансовый сектор не должен использовать криптовалюты [Электронный ресурс] // ZAKON.KZ. – 2018. – URL: https://www.zakon.kz/finansy/4924145-natsbank-ofitsialnyy-finansovyy-sektor.html (дата обращения: 19.08.2025).

273 Представители Минцифры рассказали о дальнейшем развитии искусственного интеллекта [Электронный ресурс] // Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. – 2025. – URL:

https://www.gov.kz/memleket/entities/mdai/press/news/details/742959?lang=ru (дата обращения: 19.08.2025).

274 International center for artificial intelligence [Электронный ресурс] // Alem.ai. – URL: https://alem.ai/ru/ (дата обращения: 19.08.2025).

275 О квалификации неоднократности и совокупности уголовных правонарушений [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 25 декабря 2006 года № 11 (с изменениями и дополнениями по состоянию на 11.12.2020 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P06000011S_ (дата обращения: 19.08.2025).

276 Об утверждении правил оказания услуг связи [Электронный ресурс] : Приказ и. о. Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171 (с изменениями и дополнениями по состоянию на 29.02.2024 г.) // // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1500010999 (дата обращения: 19.08.2025).

277 Кусаинова А. К. Гражданско-правовое регулирование отношений в сфере электронного документооборота в Республике Казахстан [Текст] : дис. … д-ра философии (PhD) : 6D030100 – Юриспруденция / А. К. Кусаинова ; КазНУ им. аль-Фараби. – Алматы : [б. и.], 2022. – 158 с.

278 О судебной экспертизе по уголовным делам [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 26 ноября 2004 года № 16 // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P04000016S_ (дата обращения: 19.08.2025).

279 О некоторых вопросах оценки доказательств по уголовным делам [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 20 апреля 2006 года № 4 (с изменениями и дополнениями по состоянию на 11.12.2020 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P06000004S_ (дата обращения: 19.08.2025).

280 Очередную серию тяжб с МФО и банком выиграла жительница Петропавловска [Электронный ресурс] // Северный Казахстан. – URL: https://izdatelstvo-sk.kz/news/ocherednuyu-seriyu-tyagbi-s-mfo7940/ (дата обращения: 19.08.2025).

281 О рассмотрении гражданского иска в уголовном процессе [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 20 июня 2005 года № 1 (с изменениями и дополнениями по состоянию на 11.12.2020 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P05000001S_ (дата обращения: 19.08.2025).

282 О применении судами законодательства о возмещении морального вреда [Электронный ресурс] : Нормативное постановление Верховного Суда

Республики Казахстан от 27 ноября 2015 года № 7 (с изменениями и дополнениями по состоянию на 28.11.2024 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P150000007S (дата обращения: 20.08.2025).

283 Citron D. K., Solove D. J. Privacy Harms // Boston University Law Review. – 2022. – Vol. 102. – pp. 793–863.

284 International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations [Электронный ресурс] / FATF. – Paris : FATF/OECD, 2012 (updated June 2025). – 150 p. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.pdf (дата обращения: 30.08.2025).

285 Guidance for a Risk-Based Approach: The Banking Sector [Электронный ресурс] / FATF. – Paris : FATF/OECD, 2014. – 50 p. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf (дата обращения: 30.08.2025).

286 О ратификации Конвенции Организации Объединенных Наций против транснациональной организованной преступности [Электронный ресурс] : Закон Республики Казахстан от 4 июня 2008 года № 40-IV // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z080000040_ (дата обращения: 20.08.2025).

287 Казахстан усиливает международное сотрудничество в борьбе с киберпреступностью на конференции OCTOPUS 2025 при поддержке ОБСЕ [Электронный ресурс] // ОБСЕ. – 2025. – URL: https://www.osce.org/ru/programme-office-in-astana/593225 (дата обращения: 20.08.2025).

288 О применении норм международных договоров Республики Казахстан [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 10 июля 2008 года № 1 (с изменениями и дополнениями по состоянию на 28.11.2024 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P08000001S_ (дата обращения: 20.08.2025).

289 Об утверждении Инструкции об оказании судами Республики Казахстан правовой помощи и обращении за правовой помощью к судам иностранных государств [Электронный ресурс] : Приказ Руководителя Департамента по обеспечению деятельности судов при Верховном Суде Республики Казахстан (аппарата Верховного Суда Республики Казахстан) от 11 мая 2016 года № 6001-16-7-6/196 (с изменениями и дополнениями по состоянию на 17.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1600013794 (дата обращения: 20.08.2025).

290 Explanatory Memoranda of the OECD Privacy Guidelines [Электронный ресурс] / OECD. – Paris : OECD Publishing, 2023. – 34 p. – (OECD Digital Economy

Papers; No. 360). – URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/10/explanatory-memoranda-of-the-oecd-privacy-guidelines_78b08164/ea4e9759-en.pdf (дата обращения: 20.08.2025).

291 Консультативный документ регуляторной политики к проекту Цифрового кодекса Республики Казахстан [Электронный ресурс] // Открытые НПА. – URL: https://legalacts.egov.kz/npa/view?id=14812473 (дата обращения: 20.08.2025).

292 О ратификации Соглашения о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными [Электронный ресурс] : Закон Республики Казахстан от 1 апреля 2022 года № 113-VII ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2200000113 (дата обращения: 27.08.2025).

293 Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1) [Электронный ресурс] : [adopted on 4 May 2020] / European Data Protection Board. – [Brussels], 2020. – 33 p. – URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (дата обращения: 20.08.2025).

294 Об утверждении Правил сбора, обработки персональных данных [Электронный ресурс] : Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ (с изменениями и дополнениями по состоянию на 23.04.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2000021498 (дата обращения: 20.08.2025).

295 Earning Digital Trust: Decision-Making for Trustworthy Technologies [Электронный ресурс] : Insight Report / World Economic Forum. – [Geneva], 2022. – 40 p. – URL: https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf (дата обращения: 20.08.2025).

296 Digital Trust: Supporting Individual Agency [Электронный ресурс] : White Paper / World Economic Forum. – [Geneva], 2024. – 22 p. – URL: https://www3.weforum.org/docs/WEF_Digital_Trust_Supporting_Individual_Agency_2024.pdf (дата обращения: 28.08.2025).

297 О внесении изменений и дополнений в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ «Об утверждении Правил сбора, обработки персональных данных» [Электронный ресурс] : Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 31 марта 2022 года № 102/НҚ // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2200027344 (дата обращения: 20.08.2025).

298 Об утверждении Правил функционирования государственного сервиса контроля доступа к персональным данным [Электронный ресурс] : Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2022 года № 144/НҚ // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2200027963 (дата обращения: 20.08.2025).

299 Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows [Электронный ресурс] : Briefing Paper / World Economic Forum. – [Geneva], 2023. – 14 p. – URL: https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf (дата обращения: 20.08.2025).

300 International data transfers [Электронный ресурс] // European Data Protection Board. – URL: https://edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en (дата обращения: 20.08.2025).

301 Judgment of the Court (Grand Chamber) of 16 July 2020. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Case C-311/18 [Электронный ресурс] // EUR-Lex. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311 (дата обращения: 20.08.2025).

302 Трансграничная передача персональных данных требует строгого соблюдения законодательства – эксперт [Электронный ресурс] // Kazakhstan Today. – 2025. – URL: https://www.kt.kz/rus/interview/transgranichnaya_peredacha_personalnyh_dannyh_trebuet_1377974477.html (дата обращения: 20.08.2025).

303 Об утверждении Правил проверки подлинности электронной цифровой подписи [Электронный ресурс] : Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 (с изменениями и дополнениями по состоянию на 30.12.2016 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1500012864 (дата обращения: 20.08.2025).

304 Electronic signatures [Электронный ресурс] : At a Glance / European Parliament. – [Brussels], 2022. – 2 p. – URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739238/EPRS_ATA(2022)739238_EN.pdf (дата обращения: 20.08.2025).

305 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [Электронный ресурс] // Official Journal of the European Union. – 2023. – L 191. – pp. 118–180. – URL: https://data.europa.eu/eli/reg/2023/1543/oj (дата обращения: 20.08.2025).

306 Guidelines and explanatory memorandum on electronic evidence in civil and administrative proceedings [Электронный ресурс] / Council of Europe. – [Strasbourg], 2019. – 33 p. – URL: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 (дата обращения: 20.08.2025).

307 Report of the Secretary-General: Roadmap for Digital Cooperation [Электронный ресурс] / United Nations. – [New York], 2020. – 39 p. – URL: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf (дата обращения: 28.08.2025).

308 Global Digital Compact: Zero Draft [Электронный ресурс] / United Nations. – [New York], 2024. – 13 p. – URL: https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Zero_Draft.pdf (дата обращения: 28.08.2025).

309 Guidelines on Artificial Intelligence and Data Protection [Электронный ресурс] / Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – Strasbourg, 2019. – 4 p. – URL: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (дата обращения: 17.09.2025).

310 О внесении изменений и дополнений в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2022 года № 144/НҚ «Об утверждении Правил функционирования государственного сервиса контроля доступа к персональным данным» [Электронный ресурс] : приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 17 июня 2025 года № 299/НҚ // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2500036295 (дата обращения: 22.09.2025).

311 О прокуратуре [Электронный ресурс] : Конституционный закон Республики Казахстан от 5 ноября 2022 года № 155-VII ЗРК (с изменениями и дополнениями по состоянию на 12.09.2023 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2200000155 (дата обращения: 17.09.2025).

312 About TPP [Электронный ресурс] // MIT Technology and Policy Program. – URL: https://tpp.mit.edu/about/ (дата обращения: 10.09.2025).

313 Technology Policy and Innovation [Электронный ресурс] // Columbia SIPA. – URL: https://www.sipa.columbia.edu/sipa-education/bulletin/tpi (дата обращения: 10.09.2025).

314 Science and Technology Policy [Электронный ресурс] // Stanford Public Policy. – URL: https://publicpolicy.stanford.edu/graduate/graduate-concentrations/science-and-technology-policy (дата обращения: 10.09.2025).

315 Science, Technology and Policy Studies Track [Электронный ресурс] // Harvard Kennedy School. – URL: https://www.hks.harvard.edu/educational-programs/doctoral-programs/phd-public-policy/science-technology-and-policy-studies (дата обращения: 10.09.2025).

316 Master in Technology and Global Affairs [Электронный ресурс] // Sciences Po PSIA. – URL: https://www.sciencespo.fr/psia/academics/masters/master-technology-global-affairs/ (дата обращения: 10.09.2025).

317 MSc Engineering and Policy Analysis [Электронный ресурс] // TU Delft. – URL: https://www.tudelft.nl/onderwijs/opleidingen/masters/epa/msc-engineering-and-policy-analysis (дата обращения: 10.09.2025).

318 Digital Technologies and Policy MPA [Электронный ресурс] // UCL. – URL: https://www.ucl.ac.uk/prospective-students/graduate/taught-degrees/digital-technologies-and-policy-mpa (дата обращения: 10.09.2025).

319 Tsinghua University Law School, Intellectual Property and Innovation Policy, Class of 2025 Admissions Guide [Электронный ресурс] // Tsinghua University Law School. – URL: https://www.law.tsinghua.edu.cn/info/1085/20245.htm (дата обращения: 10.09.2025).

320 Master [Электронный ресурс] // School of Public Policy and Management, UCAS. – URL: https://sppm.ucas.ac.cn/index.php/en/admission/master (дата обращения: 10.09.2025).

321 Цифровое право (IT Law) [Электронный ресурс] / Московский государственный юридический университет имени О.Е. Кутафина (МГЮА). – Москва. – URL: https://msal.ru/programs/vysshee-obrazovanie/magistratura/magisterskaya-programma-tsifrovoe-pravo-it-law/ (дата обращения: 10.09.2025).

322 Техноправо [Электронный ресурс] / Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). – Москва. – URL: https://msal.ru/programs/vysshee-obrazovanie/magistratura/tekhnopravo/ (дата обращения: 10.09.2025).

323 Цифровые финансовые технологии и право (FinTech Law) [Электронный ресурс] / Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). – Москва. – URL: https://msal.ru/programs/vysshee-obrazovanie/magistratura/tsifrovye-finansovye-tekhnologii-i-pravo-fintech-law-setevaya-forma-realizatsii-sovmestno-s-rudn/ (дата обращения: 10.09.2025).

324 Интеллектуальные права и право новых технологий [Электронный ресурс] / Московский государственный юридический университет имени О.Е. Кутафина (МГЮА). – Москва. – URL: https://msal.ru/programs/vysshee-obrazovanie/magistratura/magisterskaya-programma-intellektualnye-prava-i-pravo-novykh-tekhnologiy/ (дата обращения: 10.09.2025).

325 ИТ-юрист [Электронный ресурс] / Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ). – Москва. – URL: https://studyonline.hse.ru/it-lawyer (дата обращения: 10.09.2025).

326 Цифровое право / Legal Tech [Электронный ресурс] / Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ). – Москва. – URL: https://www.hse.ru/ma/dlaw (дата обращения: 10.09.2025).

327 Интеллектуальные права, искусственный интеллект и цифровые технологии [Электронный ресурс] // Юридический факультет МГУ имени М. В. Ломоносова. – URL: https://law.msu.ru/courses/72 (дата обращения: 10.09.2025).

328 Об утверждении Требований к деятельности организации по формированию и ведению базы данных [Электронный ресурс] : Постановление Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 июня 2007 года № 177 (с изменениями и дополнениями по состоянию на 01.01.2024 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V070004860_ (дата обращения: 28.08.2025).

329 Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах [Электронный ресурс] : Постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 (с изменениями и дополнениями по состоянию на 20.08.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1800016772 (дата обращения: 28.08.2025).

330 Об утверждении Требований к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности [Электронный ресурс] : Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 90 (с изменениями и дополнениями по состоянию на 27.11.2023 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2000021274 (дата обращения: 28.08.2025).

331 Об утверждении Правил подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций [Электронный ресурс] : Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 12 сентября 2022 года № 67 (с изменениями и дополнениями по состоянию на 20.08.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2200029639 (дата обращения: 28.08.2025).

332 Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан [Электронный ресурс] : Постановление Правления Национального Банка Республики Казахстан от 12 ноября 2019 года № 188 (с изменениями и дополнениями по состоянию на 25.07.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1900019632 (дата обращения: 28.08.2025).

333 Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчетов, а также Требований, предъявляемых кредитными бюро к поставщикам информации и получателям кредитных отчетов [Электронный ресурс] : Постановление Правления Национального Банка Республики Казахстан от 27 сентября 2018 года № 228 (с изменениями и дополнениями по состоянию на 16.08.2024 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1800017702 (дата обращения: 28.08.2025).

334 Защита персональных данных [Электронный ресурс] // PwC в Казахстане. – URL: https://www.pwc.com/kz/ru/services/data-privacy.html (дата обращения: 20.08.2025).

335 ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines [Электронный ресурс] // ISO. – URL: https://www.iso.org/standard/71670.html (дата обращения: 21.08.2025).

336 Scheider S., Lauf F., Möller, F., Otto B. A Reference System Architecture with Data Sovereignty for Human-Centric Data Ecosystems // Business & Information Systems Engineering. – 2023. – Vol. 65, No. 5. – pp. 577–595.

337 Добровольный отказ от получения банковских займов, микрокредитов [Электронный ресурс] // Egov.kz : Государственные услуги и информация онлайн. – URL: https://egov.kz/cms/ru/services/pass_fcb (дата обращения: 21.08.2025).

338 European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01) [Электронный ресурс] // Official Journal of the European Union. – 2023. – C 23. – pp. 1–7. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2023:023:FULL (дата обращения: 28.08.2025).

339 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [Электронный ресурс] // Official Journal of the European Union. – 2022. – L 152. – pp. 1–44. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868 (дата обращения: 28.08.2025).

340 Butin D., Le Métayer D. Log Analysis for Data Protection Accountability // International Symposium on Formal Methods. – Cham : Springer International Publishing, 2014. – pp. 163–178.

341 Butin D., Chicote M., Le Métayer, D. Log Design for Accountability // 2013 IEEE Security and Privacy Workshops. – IEEE, 2013. – pp. 1–7.

342 Llanos J. T., Carr M., Rana O. Using the Blockchain to Enable Transparent and Auditable Processing of Personal Data in Cloud-Based Services: Lessons from the Privacy-Aware Cloud Ecosystems (PACE) Project // Computer Law & Security Review. – 2023. – Vol. 51. – Article ID 105873. – pp. 1–18.

343 Karjalainen T. All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm // European Data Protection Law Review. – 2022. – Vol. 8. – pp. 19–30.

344 Mantelero A., Vaciago G., Esposito, M. S., Monte N. The Common EU Approach to Personal Data and Cybersecurity Regulation // International Journal of Law and Information Technology. – 2020. – Vol. 28, No. 4. – pp. 297–328.

345 Об утверждении Правил интеграции с государственным сервисом контроля доступа к персональным данным [Электронный ресурс] : Приказ и. о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 8 июля 2022 года № 236/НҚ (с изменениями и дополнениями по состоянию на 30.05.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2200028786 (дата обращения: 21.08.2025).

346 Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры [Электронный ресурс] : Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ (с изменениями и дополнениями по состоянию на 23.04.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V1800017019 (дата обращения: 21.08.2025).

347 Brownsword R. Law Disrupted, Law Re-Imagined, Law Re-Invented // Technology and Regulation. – 2019. – Vol. 2019. – pp. 10–30.

348 Marchant G. E. Governance of Emerging Technologies as a Wicked Problem // Vanderbilt Law Review. – 2020. – Vol. 73. – pp. 1861–1877.

349 Wang Y. Do Not Go Gentle into That Good Night: The European Union’s and China’s Different Approaches to the Extraterritorial Application of Artificial Intelligence Laws and Regulations // Computer Law & Security Review. – 2024. – Vol. 53. – Article ID 105965. – pp. 1–13.

350 Veale M., Zuiderveen Borgesius, F. Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach // Computer Law Review International. – 2021. – Vol. 22, No. 4. – pp. 97–112.

351 Cafaggi F. New Foundations of Transnational Private Regulation [Электронный ресурс] / F. Cafaggi ; Robert Schuman Centre for Advanced Studies. – Florence : European University Institute, 2010. – 40 p. – (EUI Working Papers ; RSCAS 2010/53 ; Private Regulation Series-04). – URL: https://cadmus.eui.eu/server/api/core/bitstreams/18807b59-5f6a-5b47-a9d6-9c5d9cab36e2/content (дата обращения: 11.09.2025).

352 Scott C., Cafaggi F., Senden L. The Conceptual and Constitutional Challenge of Transnational Private Regulation // Journal of Law and Society. – 2011. – Vol. 38, No. 1. – pp. 1–19.

353 Klonick K. The New Governors: The People, Rules, and Processes Governing Online Speech // Harvard Law Review. – 2017. – Vol. 131. – pp. 1599–1670.

354 Douek E. Content Moderation as Systems Thinking // Harvard Law Review. – 2022. – Vol. 136, No. 2. – P. 526–607.

355 Chander A., Lê U. P. Data Nationalism // Emory Law Journal. – 2014. – Vol. 64. – pp. 679–739.

356 Kuner C. Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law // International Data Privacy Law. – 2015. – Vol. 5, No. 4. – pp. 235–245.

357 Allen H. J. Regulatory Sandboxes // George Washington Law Review. – 2019. – Vol. 87, No. 3. – pp. 579–645.

358 Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation / D. A. Zetzsche [et al.] // Fordham Journal of Corporate & Financial Law. – 2017. – Vol. 23, No. 1. – pp. 31–103.

359 Buocz T., Pfotenhauer S., Eisenberger I. Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety? // Law, Innovation and Technology. – 2023. – Vol. 15, No. 2. – pp. 357–389.

360 A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications / J. Truby [et al.] // European Journal of Risk Regulation. – 2022. – Vol. 13, No. 2. – pp. 270–294.

361 Institutional Development and the Astana International Finance Center in Kazakhstan / H. Yeung [et al.] // Washington University Global Studies Law Review. – 2020. – Vol. 19. – pp. 53–83.

362 Ionescu D. P., Eliantonio M. Soft Law Behind the Scenes: Transparency, Participation and the European Union's Soft Law Making Process in the Field of Climate Change // European Journal of Risk Regulation. – 2023. – Vol. 14, No. 2. – pp. 292–312.

363 Rangone N., Megale L. Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making // European Journal of Risk Regulation. – 2025. – pp. 1–16.

364 Vander Maelen C. Codes of (Mis)conduct? An Appraisal of Articles 40–41 GDPR in View of the 1995 Data Protection Directive and Its Shortcomings // European Data Protection Law Review. – 2020. – Vol. 6, No. 2. – pp. 231–242.

365 Lachaud E. What GDPR Tells About Certification // Computer Law & Security Review. – 2020. – Vol. 38. – Article ID 105457. – pp. 1–12.

366 Koulierakis E. Certification as Guidance for Data Protection by Design // International Review of Law, Computers & Technology. – 2024. – Vol. 38, No. 2. – pp. 245–263.

367 The Strengthened Code of Practice on Disinformation 2022 [Электронный ресурс] // European Commission. – URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-

democracy/strengthened-eu-code-practice-disinformation_en (дата обращения: 21.08.2025).

368 Mündges S., Park K. But Did They Really? Platforms' Compliance with the Code of Practice on Disinformation in Review // Internet Policy Review. – 2024. – Vol. 13, No. 3. – pp. 1–21.

369 Ebers M. Truly risk-based regulation of artificial intelligence: how to implement the EU's AI Act // European Journal of Risk Regulation. – 2024. – pp. 684–703.

370 Gstrein O. J., Haleem N., Zwitter A. General-purpose AI regulation and the European Union AI Act // Internet Policy Review. – 2024. – Vol. 13, No. 3. – pp. 1–26.

371 Neuwirth R. J. Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA) // Computer Law & Security Review. – 2023. – Vol. 48. – Article ID 105798. – pp. 1–14.

372 Arcila B. B. AI Liability in Europe: How Does It Complement Risk Regulation and Deal with the Problem of Human Oversight? // Computer Law & Security Review. – 2024. – Vol. 54. – Article ID 106012. – pp. 1–17.

373 Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [Электронный ресурс] // Official Journal of the European Union. – 2024. – L 2024/2853. – URL: https://data.europa.eu/eli/dir/2024/2853/oj (дата обращения: 21.08.2025).

374 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) [Электронный ресурс] // EUR-Lex. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496 (дата обращения: 21.08.2025).

375 Withdrawal of Commission Proposals [Электронный ресурс] // Official Journal of the European Union. – 2025. – C 2025/5423. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52025XC05423 (дата обращения: 21.08.2025).

376 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [Электронный ресурс] // Official Journal of the European Union. – 2018. – L 303. – P. 59–68. – URL: https://data.europa.eu/eli/reg/2018/1807/oj (дата обращения: 21.08.2025).

377 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [Электронный ресурс] // EUR-Lex. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010 (дата обращения: 21.08.2025)

378 Hinrichs O. Consumer Law and the Regulation of the Free Flow of Data: Upsetting the Balance of the European Data Protection Framework // Journal of European Consumer and Market Law. – 2024. – Vol. 13, No. 2. – pp. 1–18.

379 Migliorini S. China’s Interim Measures on Generative AI: Origin, Content and Significance // Computer Law & Security Review. – 2024. – Vol. 53. – Article ID 105985. – pp. 1–7.

380 Creemers R. China’s Emerging Data Protection Framework // Journal of Cybersecurity. – 2022. – Vol. 8, No. 1. – Article ID tyac011. – pp. 1–12.

381 Pang C. K. A Comparative Analysis of Artificial Intelligence Regulation: Implications for Singapore // Singapore Academy of Law Journal. – 2025. – Vol. 37, No. 1. – pp. 189–232.

382 Zou M., Zhang L. Navigating China’s Regulatory Approach to Generative Artificial Intelligence and Large Language Models // Cambridge Forum on AI: Law and Governance. – 2025. – Vol. 1. – Article ID e8. – pp. 1–16.

383 Measures for the Security Administration of the Application of Facial Recognition Technology [Электронный ресурс] : [released on March 21, 2025] // Cyberspace Administration of China. – URL: https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm (дата обращения: 21.08.2025).

384 Dong H., Chen J. Meta-Regulation: An Ideal Alternative to the Primary Responsibility as the Regulatory Model of Generative AI in China // Computer Law & Security Review. – 2024. – Vol. 54. – Article ID 106016. – pp. 1–16.

385 Saktaganova A. B., Saktaganova I. S. Theoretical and Legal Foundations of the Formation of the Legal Definition of Artificial Intelligence: Challenges and Prospects // Bulletin of the Karaganda University. Law Series. – 2025. – Vol. 30, No. 1(117). – pp. 68–79.

386 Тлембаева Ж. У. О некоторых подходах к правовому регулированию искусственного интеллекта // Вестник Института законодательства и правовой информации Республики Казахстан. – 2021. – № 2 (65). – С. 61–74.

387 Yelegen A. Y. Trends in Regulating the Capabilities of Artificial Intelligence in the Field of Medicine in the Era of Globalizing International Law // Bulletin of the L. N. Gumilyov Eurasian National University. Law Series. – 2023. – Vol. 145, No. 4. – pp. 153–162.

388 Дячук М. И. Регуляторная песочница в Республике Казахстан: пути совершенствования // Вестник Института законодательства и правовой информации Республики Казахстан. – 2022. – № 3 (70). – С. 196–204.

389 De Terwangne C. Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data // Computer Law & Security Review. – 2021. – Vol. 40. – Article ID 105497. – pp. 1–18.

390 Сырлыбаева Ф. М. Некоторые вопросы защиты информационных прав работника // Вестник Евразийского национального университета имени Л. Н. Гумилёва. Серия: Право. – 2022. – Т. 140, № 3. – С. 72–80.

391 Омурчиева Э. М., Саудабаева Д. Е. Проблемы применения законодательства Республики Казахстан о персональных данных: риски для

работодателя // Вестник Института законодательства и правовой информации Республики Казахстан. – 2024. – № 2 (77). – С. 111–121.

392 Greenleaf G. Kazakhstan Enacts Central Asia's Second Data Privacy Law [Электронный ресурс] // Privacy Laws & Business International Report. – 2013. – No. 124. – P. 23–24. – (UNSW Law Research Paper No. 2013-59). – URL: https://ssrn.com/abstract=2319178 (дата обращения: 21.08.2025).

393 О судебной практике по делам о мошенничестве [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 года № 6 (с изменениями и дополнениями по состоянию на 22.12.2022 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P170000006S (дата обращения: 21.08.2025).

394 О судебной практике по делам о хищениях [Электронный ресурс] : Нормативное постановление Верховного Суда Республики Казахстан от 11 июля 2003 года № 8 (с изменениями и дополнениями по состоянию на 28.09.2023 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/P03000008S_ (дата обращения: 21.08.2025).

395 Верховный суд предложил списывать кредиты некоторым казахстанцам [Электронный ресурс] // Tengrinews.kz. – URL: https://tengrinews.kz/kazakhstan_news/verhovnyiy-sud-predlojil-spisyivat-kredityi-nekotoryim-kazahstantsam-553672/ (дата обращения: 21.08.2025).

396 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (ETS No. 224) [Электронный ресурс] : [done at Strasbourg, 12.V.2022] // Council of Europe. – URL: https://rm.coe.int/1680a49dab (дата обращения: 22.08.2025).

397 Кодекс деловой этики членов ОЮЛ «Ассоциация микрофинансовых организаций Казахстана» [Электронный ресурс] : [утвержден Протоколом Общего собрания членов Объединения юридических лиц «Ассоциация микрофинансовых организаций Казахстана» от 8 июня 2022 г.]. – URL: https://amfok.kz/Кодекс%20этики%2008062022.pdf (дата обращения: 22.08.2025).

398 Политика по правам человека АО «Банк ЦентрКредит» [Электронный ресурс] : утв. постановлением Совета директоров от 08.09.2023 г. № 0908/2 (в редакции от 30.07.2024 г. № 0730/3) // Официальный сайт АО «Банк ЦентрКредит». – URL: https://www.bcc.kz/storage/app/media/О%20банке/ESG/Documents/rus_политика%20по%20правам%20человека.pdf (дата обращения: 22.08.2025).

399 Кодекс этики и делового поведения в АО «Народный Банк Казахстана» [Электронный ресурс] : [утвержден протоколом заочного заседания Совета директоров АО «Народный Банк Казахстана» от 18 июля 2022 года № 34]. – URL: https://halykbank.kz/storage/app/media/Korporotivniy/2022/7/rus_%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%20%D1%8D%D1%82%D0%B8%D0%BA%D0%B8%20%D0%B8%20%D0%B4%D0%B5%D0%BB%D0%BE%D0%B2

%D0%BE%D0%B3%D0%BE%20%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%BD%D0%B0%20%D1%80%D1%83%D1%81%D1%81.%D1%8F%D0%B7%D1%8B%D0%BA%D0%B5.pdf (дата обращения: 22.08.2025).

400 О техническом регулировании [Электронный ресурс] : Закон Республики Казахстан от 30 декабря 2020 года № 396-VI ЗРК (с изменениями и дополнениями по состоянию на 19.05.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2000000396 (дата обращения: 22.08.2025).

401 Об утверждении Правил осуществления государственных закупок [Электронный ресурс] : Приказ Министра финансов Республики Казахстан от 9 октября 2024 года № 687 (с изменениями и дополнениями по состоянию на 21.08.2025 г.) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: https://adilet.zan.kz/rus/docs/V2400035238 (дата обращения: 22.08.2025).

402 Interactive Range и АО «Государственная техническая служба» при поддержке МЦРИАП РК запускают онлайн Bootcamp и CTF по кибербезопасности для школьников 9-12 классов [Электронный ресурс] // Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. – URL: https://www.gov.kz/memleket/entities/mdai/press/news/details/1043566?lang=ru (дата обращения: 22.08.2025).

403 Цифровая гигиена и борьба с фейками: в Академии МВД проходит конкурс по кибербезопасности [Электронный ресурс] // Министерство внутренних дел Республики Казахстан. – URL: https://www.gov.kz/memleket/entities/qriim/press/news/details/1024992?lang=ru (дата обращения: 22.08.2025).

404 Central Asia Fintech Summit 2024: в Алматы впервые пройдет крупнейшее финтех-мероприятие региона [Электронный ресурс] // Национальная Платежная Корпорация. – URL: https://npck.kz/central-asia-fintech-summit-2024/ (дата обращения: 22.08.2025).

405 Президент Казахстана и Наследный принц Абу-Даби приняли участие в бизнес-форуме «Казахстан – ОАЭ» [Электронный ресурс] // Официальный сайт Президента Республики Казахстан. – 2025. – URL: https://akorda.kz/ru/prezident-kazahstana-i-naslednyy-princ-abu-dabi-prinyali-uchastie-v-biznes-forume-kazahstan-oae-124574 (дата обращения: 22.08.2025).