Дата поступления рукописи в редакцию: 22.04.2026 г.
Дата принятия рукописи в печать: 03.05.2026 г.
DOI: 10.24412/2782-3830-2026-4-182-187

ЕРЕМИЧЕВ Ф.С.,
Аспирант Университета «Синергия»,
e-mail: fedor.eremichef@yandex.ru

ПРИНЦИП PRIVACY BY DESIGN КАК ОСНОВА ПРЕВЕНТИВНОЙ ГРАЖДАНСКО-ПРАВОВОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ: ПЕРСПЕКТИВЫ ИМПЛЕМЕНТАЦИИ В РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО

Аннотация. *В статье исследуется принцип Privacy by Design (защита конфиденциальности на этапе проектирования) как инструмент превентивной гражданско-правовой защиты персональных данных. Проводится анализ содержания принципа Privacy by Design в зарубежном законодательстве, прежде всего в статье 25 Общего регламента по защите данных Европейского союза (GDPR). Рассматривается институт уполномоченного по защите персональных данных (Data Protection Officer, DPO) как элемент институциональной реализации данного принципа. Обосновывается необходимость законодательного закрепления принципа Privacy by Design в российском законодательстве в качестве обязательного стандарта при разработке информационных систем, обрабатывающих персональные данные. Формулируются конкретные предложения по имплементации данного принципа и института DPO в Федеральный закон «О персональных данных».*

Ключевые слова*: Privacy by Design, персональные данные, превентивная защита, уполномоченный по защите данных, DPO, GDPR, информационная безопасность, аудит информационных систем.*

EREMICHEV F.S.,
Graduate student of Synergy University

PRIVACY BY DESIGN PRINCIPLE AS THE BASIS OF PREVENTIVE CIVIL PROTECTION OF PERSONAL DATA: PROSPECTS FOR IMPLEMENTATION IN RUSSIAN LEGISLATION

Annotation. *The article examines the Privacy by Design principle as a tool for preventive civil law protection of personal data. An analysis of the content of the Privacy by Design principle in foreign legislation, primarily in Article 25 of the General Data Protection Regulation (GDPR), is conducted. The institution of the Data Protection Officer (DPO) as an element of institutional implementation of this principle is considered. The necessity of legislative consolidation of the Privacy by Design principle in Russian legislation as a mandatory standard for the development of information systems processing personal data is substantiated. Specific proposals for the implementation of this principle and the DPO institution in the Federal Law "On Personal Data" are formulated.*

Key words: *Privacy by Design, personal data, preventive protection, Data Protection Officer, DPO, GDPR, information security, audit of information systems.*

Проблема защиты персональных данных в условиях цифровизации приобретает все большую остроту. Традиционные гражданско-правовые механизмы защиты, ориентированные на реагирование на уже совершенные нарушения (компенсация морального вреда, возмещение убытков), оказываются недостаточно эффективными в условиях, когда масштаб нарушений и объем скомпрометированных данных стремительно растут [1]. Принятие Федерального закона от 30 ноября 2024 года, вводящего оборотные штрафы за утечки персональных данных, ознаменовало новый этап в развитии отечественного законодательства в данной сфере, однако данная мера носит преимущественно карательный характер и не обеспечивает превентивной защиты [2].

В зарубежном праве важнейшим инструментом превентивной защиты персональных данных является принцип Privacy by Design (защита конфиденциальности на этапе проектирования), закрепленный в статье 25 GDPR. Данный принцип

предполагает встраивание механизмов защиты персональных данных в архитектуру информационных систем на этапе их проектирования, а не после выявления нарушений [3]. Институциональной формой реализации данного принципа является институт уполномоченного по защите персональных данных (Data Protection Officer, DPO), обеспечивающий внутренний контроль за соблюдением требований законодательства [4]. Целью настоящей статьи является обоснование необходимости имплементации принципа Privacy by Design и института DPO в российское законодательство.

Принцип Privacy by Design был впервые сформулирован канадским специалистом в области защиты данных Энн Кавукян в 1990-х годах и включает семь основополагающих принципов: проактивность, а не реактивность (предотвращение нарушений, а не реагирование на них); защита конфиденциальности по умолчанию (Privacy by Default); встроенность защиты в архитектуру системы; полная функциональность (обеспечение защиты без ущерба для функциональности системы); сквозная защита на протяжении всего жизненного цикла данных; видимость и прозрачность; уважение к пользователю (приоритет интересов пользователя при проектировании системы) [5].

Статья 25 GDPR закрепила принцип Privacy by Design в качестве обязательного правового требования. Контролер обязан как в момент определения средств обработки, так и в момент самой обработки внедрять надлежащие технические и организационные меры, разработанные для эффективной реализации принципов защиты данных (таких как минимизация данных) и интеграции необходимых гарантий в обработку для соблюдения требований GDPR и защиты прав субъектов данных. Кроме того, контролер обязан обеспечить, чтобы по умолчанию обрабатывались только те персональные данные, которые необходимы для каждой конкретной цели обработки (Privacy by Default) [3].

Практическая реализация принципа Privacy by Design в информационных системах включает ряд конкретных мер. На этапе проектирования это проведение оценки воздействия на защиту данных (DPIA) для выявления рисков и определения мер по их минимизации, определение минимально необходимого объема персональных данных для достижения каждой цели обработки, проектирование архитектуры системы с учетом принципа разделения данных, встраивание механизмов псевдонимизации и анонимизации данных, проектирование механизмов реализации прав субъектов данных (доступ, удаление, переносимость, ограничение обработки) [6].

На этапе разработки это использование безопасных методов программирования, проведение тестирования безопасности, внедрение механизмов шифрования данных при хранении и передаче, реализация многофакторной аутентификации и контроля доступа, ведение журналов всех операций с персональными данными. На этапе эксплуатации это регулярное обновление программного обеспечения и устранение уязвимостей, мониторинг безопасности в режиме реального времени, регулярное проведение аудитов информационных систем, обучение персонала правилам обработки и защиты персональных данных, разработка и тестирование планов реагирования на инциденты [7].

В российском законодательстве принцип Privacy by Design не закреплен в качестве обязательного требования. Статья 19 Федерального закона от 27 июля 2006 года N 152-ФЗ «О персональных данных» обязывает оператора принимать необходимые правовые, организационные и технические меры для защиты персональных данных, однако не конкретизирует, какие именно меры являются необходимыми, и не устанавливает требования о встраивании механизмов защиты в архитектуру информационных систем на этапе их проектирования [8]. Подзаконные акты (приказы ФСТЭК России, ФСБ России) устанавливают технические требования к защите персональных данных в информационных системах, однако их соблюдение не гарантирует отсутствия утечек и не освобождает оператора от ответственности.

Институт уполномоченного по защите данных (Data Protection Officer, DPO), закрепленный в статьях 37–39 GDPR, является одним из наиболее значимых нововведений Регламента. Назначение DPO обязательно в трех случаях: когда обработка осуществляется публичным органом или организацией; когда основная деятельность контролера или процессора состоит в операциях по обработке, которые по своей природе, объему и/или целям требуют регулярного и систематического мониторинга субъектов данных в крупном масштабе; когда основная деятельность контролера или процессора состоит в крупномасштабной обработке специальных категорий данных [4].

DPO должен обладать экспертными знаниями в области законодательства и практики защиты данных, быть независимым в осуществлении своих функций, не получать указаний от руководства относительно выполнения своих задач и подчиняться непосредственно высшему руководству контролера или процессора. К задачам DPO относятся: информирование и консультирование контролера и работников по вопросам защиты данных, мониторинг соблюдения GDPR,

консультирование по вопросам оценки воздействия на защиту данных (DPIA), взаимодействие с надзорным органом, выполнение функции контактного лица для надзорного органа [9].

Опыт функционирования института DPO в Европейском союзе за период с момента вступления GDPR в силу демонстрирует его высокую эффективность. Организации, назначившие квалифицированного DPO, демонстрируют существенно более низкий уровень нарушений и утечек персональных данных по сравнению с организациями, не имеющими такого специалиста. Это обусловлено тем, что DPO обеспечивает постоянный внутренний контроль за соблюдением требований законодательства, выявляет и устраняет нарушения на ранней стадии, консультирует руководство и сотрудников по вопросам обработки данных, а также взаимодействует с надзорным органом [10].

В российском законодательстве институт DPO не закреплен. Статья 22.1 Федерального закона N 152-ФЗ предусматривает обязанность оператора назначить ответственного за организацию обработки персональных данных, однако данная норма не устанавливает квалификационных требований к такому лицу, не обеспечивает его независимость и не определяет его функции с достаточной степенью детализации [8].

Для сравнительного анализа института DPO в различных юрисдикциях обратимся к *таблице 1.*

Таблица 1. Сравнительный анализ института уполномоченного по защите персональных данных

Параметр	ЕС (GDPR)	КНР (PIPL)	Россия (ФЗ-152)
Обязательность	Да (для определенных категорий)	Да (для крупных операторов)	Нет (только ответственный за организацию обработки)
Квалификация	Экспертные знания в области права и IT	Не детализировано	Не установлена
Независимость	Да (запрет на указания, защита от увольнения)	Ограниченная	Не обеспечена
Функции	Мониторинг, консультирование, DPIA, взаимодействие с регулятором	Мониторинг, взаимодействие	Организация обработки (не детализировано)
Подотчетность	Высшему руководству	Руководству	Не определена

Как следует из таблицы 1, российское законодательство существенно уступает зарубежным аналогам по уровню институциональной защиты персональных данных. Отсутствие обязательного института DPO, квалификационных требований и гарантий независимости ответственного лица является существенным пробелом, требующим законодательного восполнения.

На основе проведенного исследования предлагается следующая модель имплементации принципа Privacy by Design в российское законодательство. Предлагается включение в Федеральный закон N 152-ФЗ новой статьи, обязывающей операторов при проектировании и разработке информационных систем, предназначенных для обработки персональных данных, внедрять технические и организационные меры, обеспечивающие реализацию принципов обработки персональных данных и защиту прав субъектов данных [8]. Данное требование должно распространяться как на новые информационные системы, так и на существенную модернизацию существующих систем.

Кроме того, предлагается включение обязанности проведения оценки воздействия на защиту данных (DPIA) перед началом обработки, которая может представлять высокий риск для прав и свобод субъектов данных. К таким видам обработки относятся масштабная обработка специальных категорий данных, систематический мониторинг общедоступных мест, автоматизированное принятие решений, включая профилирование, порождающее юридические последствия для субъекта данных. Данное предложение основано на положительном опыте применения статьи 35 GDPR, предусматривающей аналогичное требование [3].

Предлагается также установление обязанности обеспечения защиты данных по умолчанию (Privacy by Default): настройки конфиденциально-

сти информационных систем должны быть установлены на максимальный уровень защиты по умолчанию, а пользователь должен иметь возможность самостоятельно снизить уровень защиты, если пожелает. Данное требование направлено на устранение практики, при которой операторы устанавливают минимальный уровень защиты по умолчанию, рассчитывая на то, что большинство пользователей не будут изменять настройки [11].

Предлагается установление ответственности за нарушение принципа Privacy by Design: если утечка персональных данных произошла вследствие того, что оператор не внедрил надлежащие технические и организационные меры на этапе проектирования информационной системы, это должно рассматриваться как отягчающее обстоятельство при определении размера ответственности [2].

В отношении института DPO предлагается следующая модель для российского законодательства. DPO обязаны назначить организации, осуществляющие обработку персональных данных значительного числа субъектов, государственные органы и органы местного самоуправления, организации, основная деятельность которых связана с систематическим масштабным мониторингом субъектов данных, а также организации, осуществляющие масштабную обработку специальных категорий персональных данных или биометрических данных [4].

DPO должен иметь высшее юридическое образование или высшее образование в области информационных технологий с дополнительной подготовкой в области права, стаж работы в сфере защиты персональных данных не менее трех лет, подтвержденную квалификацию. DPO не может быть уволен или подвергнут дисциплинарному взысканию за выполнение своих функций, подчиняется непосредственно единоличному исполнительному органу организации, не может совмещать свои функции с должностями, создающими конфликт интересов [9].

Предлагается также введение обязательного периодического аудита информационных систем, обрабатывающих персональные данные, с привлечением независимых аудиторов. Аудит должен проводиться не реже одного раза в год для крупных операторов и не реже одного раза в два года для средних операторов. Результаты аудита должны быть доступны уполномоченному органу и могут использоваться в качестве доказательства надлежащего исполнения оператором обязанностей по защите персональных данных [12].

Для наглядного представления предлагаемой модели превентивной защиты персональных данных обратимся к *рисунку 1.*

Как показано на рисунке 1, предлагаемая модель превентивной защиты включает три взаимосвязанных элемента: принцип Privacy by Design, обеспечивающий встраивание механизмов защиты в архитектуру информационных систем; институт DPO, обеспечивающий постоянный внутренний контроль; обязательный аудит, обеспечивающий независимую проверку соблюдения требований. Совместное функционирование данных элементов позволяет создать комплексную систему превентивной защиты, направленную на предотвращение нарушений, а не на реагирование на уже совершенные нарушения.

Рисунок 1. Модель превентивной гражданско-правовой защиты персональных данных

Для оценки ожидаемого эффекта от реализации предлагаемых мер обратимся к *таблице 2.*

Таблица 2. Ожидаемый эффект от имплементации принципа Privacy by Design и института DPO

Мера	Основание	Ожидаемый эффект
Privacy by Design	Ст. 25 GDPR, опыт ЕС	Снижение числа утечек, повышение качества защиты
Privacy by Default	Ст. 25(2) GDPR	Минимизация обрабатываемых данных
Обязательный DPO	Ст. 37–39 GDPR, PIPL	Внутренний контроль, снижение нарушений
Обязательная DPIA	Ст. 35 GDPR	Выявление рисков до начала обработки
Обязательный аудит	Лучшие практики	Независимая проверка, доказательство добросовестности

Как следует из таблицы 2, реализация предлагаемых мер позволит создать комплексную систему превентивной защиты персональных данных, направленную на предотвращение нарушений и снижение их масштабов. Каждая из мер имеет подтвержденное зарубежным опытом обоснование и направлена на решение конкретной проблемы в системе защиты персональных данных.

Проведенное исследование позволяет сформулировать следующие основные выводы. Принцип Privacy by Design является наиболее перспективным инструментом превентивной гражданско-правовой защиты персональных данных, обеспечивающим встраивание механизмов защиты в архитектуру информационных систем на этапе их проектирования. Данный принцип, закрепленный в статье 25 GDPR, доказал свою эффективность в зарубежной практике и нуждается в имплементации в российское законодательство [3].

Институт уполномоченного по защите персональных данных (DPO), закрепленный в статьях 37–39 GDPR, обеспечивает постоянный внутренний контроль за соблюдением требований законодательства и является необходимым элементом институциональной реализации принципа Privacy by Design. Введение обязательного института DPO для организаций, обрабатывающих персональные данные значительного числа субъектов, позволит существенно повысить уровень защиты персональных данных в Российской Федерации [4].

Обязательный периодический аудит информационных систем обеспечивает независимую проверку соблюдения требований безопасности и может использоваться как доказательство добросовестности оператора при определении размера ответственности. Совместная реализация принципа Privacy by Design, института DPO и обязательного аудита создаст комплексную систему превентивной защиты, направленную на предотвращение нарушений и снижение их масштабов [12].

Реализация предлагаемых мер требует внесения изменений в Федеральный закон «О персональных данных» и принятия соответствующих подзаконных актов, конкретизирующих требования к содержанию и порядку проведения DPIA, квалификационные требования к DPO, порядок проведения обязательного аудита и требования к аудиторским организациям. Представляется целесообразным поэтапное введение данных требований с предоставлением операторам переходного периода для приведения своих информационных систем и организационных процессов в соответствие с новыми требованиями [8].

Список литературы:

[1] Богатырева А.Т., Перепадя О.А., Чуниха А.А. Современные тенденции развития института персональных данных в условиях цифровизации // Право и государство: теория и практика. 2024. №9 (237).

[2] Федеральный закон от 30.11.2024 N 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Art. 25, 35.

[4] Regulation (EU) 2016/679 (GDPR). Art. 37–39.

[5] Cavoukian A. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada, 2009. Revised 2011.

[6] Чурилов А.Ю. Принципы общего Регламента Европейского союза о защите персом нальных данных (GDPR): проблемы и перспективы имплементации // Сибирское юридическое обозрение. 2019. №1.

[7] Свиридова Е.А. Правовые механизмы защиты персональных данных в информационно-телекоммуникационных системах // Современное право. 2023. №3. С. 58–62.

[8] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) «О персональных данных».

[9] Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer, 2017. 383 p.

[10] Соколова М.Е. Первые успехи нового европейского общего Регламента по защите персональных данных // Современная Европа. 2020. №2.

[11] Деико С.В. Доктринальные аспекты правовой защиты персональных данных в условиях цифровизации экономических отношений // Государственная служба. 2024. №2 (148). С. 55–61.

[12] Исаев А.С., Хлюпина Е.А. Правовые основы организации защиты персональных данных. СПб: НИУ ИТМО, 2014. 106 с.

References:

[1] Bogatyreva A.T., Perapadya O.A., Chunikha A.A. Current trends in the development of the institution of personal data in the context of digitalization// Law and the state: theory and practice. 2024. №9 (237).

[2] Federal Law of 30.11.2024 No. 420-FZ “On Amendments to the Code of Administrative Offenses of the Russian Federation.”

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Art. 25, 35.

[4] Regulation (EU) 2016/679 (GDPR). Art. 37–39.

[5] Cavoukian A. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada, 2009. Revised 2011.

[6] Churilov A.Yu. Principles of the General Regulation of the European Union on the Protection of Personal Data (GDPR): Problems and Prospects of Implementation//Siberian Legal Review. 2019. №1.

[7] Sviridova E.A. Legal mechanisms for the protection of personal data in information and telecommunication systems//Modern law. 2023. №3. S. 58-62.

[8] Federal Law of 27.07.2006 N 152-FZ (as amended by 24.06.2025) “ On Personal Data.”

[9] Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer, 2017. 383 p.

[10] M.E. Sokolova. The first successes of the new European General Regulation on the Protection of Personal Data//Modern Europe. 2020. №2.

[11] Deiko S.V. Doctrinal aspects of the legal protection of personal data in the context of digitalization of economic relations//Public Service. 2024. №2 (148). S. 55-61.

[12] Isaev A.S., Khlyupina E.A. Legal basis for the organization of personal data protection. St. Petersburg: NRU ITMO, 2014. 106 s.