Концепция проектируемой конфиденциальности для обеспечения безопасности персональных данных*

Жарова А.К.**

Аннотация. В статье анализируются концепция проектируемой конфиденциальности, нормативные и организационные требования, обеспечивающие конфиденциальность в информационных системах и службах. Проводится параллель между триадой, составляющей содержание проектируемой конфиденциальности, и положениями российского законодательства в целях создания условий прогнозирования, управления и предотвращения проблем, связанных с конфиденциальностью, уже на стадии разработки информационных технологий. Автором использовались **методы:** анализа и синтеза, диалектического развития, системного анализа, сравнительно-правовой и другие.

Результат. В статье сделан вывод, что безопасность российских пользователей информационных технологий должна обеспечиваться совместно правовым и техническим регулированием. Российская правовая система обеспечения конфиденциальности персональных данных соответствует триаде проектируемой конфиденциальности, но без работоспособной системы сертификации правовые требования не принесут необходимого результата. Для повышения эффективности правового регулирования необходимо включить в национальную систему сертификации информационных технологий стандарты продуктов или услуг в области кибербезопасности, в том числе безопасности аппаратного и программного обеспечения. Правовые нормы должны определять требования обеспечения конфиденциальности к разрабатываемым архитектуре информационной системы и аппаратно-программным решениям.

Ключевые слова: концепция, проектируемая конфиденциальность, информационные технологии, информационная безопасность, персональные данные, правовое регулирование, техническое регулирование, стандартизация, сертификация.

Abstract. The article analyzes the concept of projected confidentiality, regulatory and organizational requirements that ensure confidentiality in information systems and services. A parallel is drawn between the triad that makes up the content of the projected confidentiality and the provisions of Russian legislation in order to create conditions for forecasting, managing and preventing problems related to confidentiality already at the stage of information technology development. The author used the following **methods:** analysis and synthesis, the method of dialectical development, system analysis, comparative legal research method and others.

Result. The article concludes that the security of Russian users of information technology should be ensured jointly by legal and technical regulation. The Russian legal system for ensuring the confidentiality of personal data corresponds to the triad of projected confidentiality, but without a workable certification system, legal requirements will not bring the desired result. To improve the effectiveness of legal regulation, it is necessary to include standards for products or services in the field of cybersecurity, including hardware and software security, in the national information technology certification system. Legal regulations must determine the requirements for ensuring confidentiality for the developed architecture of the information system and hardware and software solutions.***

Keywords: concept, projected confidentiality, information technologies, information security, personal data, legal regulation, technical regulation, standardization, certification.

Обеспечение безопасности информации, используемой в целях профилирования деятельности человека, требует разработанной системы нормативных и организационных требований к информационным технологиям. Однако большинство технологий, используемых на территории РФ, разработаны зарубежными компаниями. В отличие от европейских государств, законодательство США не содержит общие требования к обеспечению

безопасности персональных данных [1]. Зачастую разработчики информационных технологий создают излишние технические решения, которые требуют доступ к персональным данным пользователя, например, доступ к микрофону, данным о местоположении, контактам пользователя и т.д., в свою очередь полученная информация позволяет создавать профиль деятельности человека без согласия самого субъекта.

* Статья подготовлена в соответствии с государственным заданием НИР № 0136-2021-0042 «Правовое регулирование цифровой экономики, искусственного интеллекта информационной безопасности».

** **Жарова Анна Константиновна**, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, доцент. E-mail: anna_jarova@mail.ru

Рецензент: Стрельцов Анатолий Александрович, член редколлегии журнала «Информационное право», заведующий отделом Института проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова, доктор юридических наук, доктор технических наук, профессор.

*** **The Concept of Projected Confidentiality (Privacy by Design) to Ensure the Security of Personal Data**

A. K. Zharova, Senior researcher of the sector of Criminal law, criminal procedure and criminology of the Institute of State and Law of the Russian Academy of Sciences, Doctor of Law, Associate Professor.

Reviewer: A. A. Streltsov, the Head of the Department for Institute of the information Security issues of the Moscow state University named after M. V. Lomonosov, doctor of Law, doctor of technical science, professor.

Концепция проектируемой конфиденциальности. В целях обеспечения информационной безопасности пользователей информационных технологий европейское законодательство реализует концепцию проектируемой конфиденциальности (Privacy by Design), основная цель которой – создать условия прогнозирования, управления и предотвращения проблем, связанных с конфиденциальностью, уже на стадии разработки информационных технологий. Данная концепция включает совокупность требований о защите информации, различные нормативные и организационные компоненты, обеспечивающие конфиденциальность в информационных системах и службах. Практика Евросоюза реализует принципы проектируемой конфиденциальности в правовых требованиях к информационным технологиям. Концепция проектируемой конфиденциальности была разработана в 1990-х годах в связи с постоянно растущими и системными проблемами информационных и коммуникационных технологий и крупномасштабных сетевых систем данных. В большинстве информационных источников в качестве автора этой концепции называют А. Кавоукиан. По сути, проектируемая конфиденциальность определена как механизм обеспечения приоритета права человека на безопасность личной жизни при разработке новых технологических инноваций.

А. Кавоукиан определяет проектируемую конфиденциальность [2] как защиту личной информации, которая не может быть обеспечена исключительно соблюдением нормативно-правовых актов. Если ранее считалось, что все проблемы в этой области могут быть решены путем внедрения специальных «технологий, защищающих конфиденциальность» [3], то в настоящее время только объединение норм правового, технического и организационного регулирования позволит достичь желаемого результата. Данная конфиденциальность определена триадой положений о защите персональных данных, возникающих при: 1) использовании информационных систем; 2) реализации деловых отношений; 3) использовании устройств, оборудования, сооружений и сетевой инфраструктуры [3]. Одним из методов обеспечения проектируемой конфиденциальности является минимизация запрашиваемых и используемых данных, закладываемая на стадии разработки программного обеспечения и информационных технологий [4]. Так, например, М. С. Крылова, исследуя принципы обработки персональных данных в праве Европейского союза, приходит к выводу, что минимизация запрашиваемых и используемых данных является мерой предупредительного характера в отношении защиты данных [5]. Но это только один из методов, реализуемых в проектируемой конфиденциальности.

Хотелось бы отметить, что проектируемая конфиденциальность реализуется в Общем положении ЕС о защите данных – GDPR. GDPR обязывает любых лиц, занимающихся профилированием деятельности человека, обеспечивать безопасность обрабатываемых данных; контроллеров – осуществлять технические и организационные меры для обеспечения конфиденциальности пользователей и прозрачности процесса обработки данных. Это, в свою очередь, позволяет субъектам данных получать разъяснения о видах обрабатываемых данных, алгоритмах их обработки и использования, в том числе корректировать собственные данные.

Принципы проектируемой конфиденциальности. Агентство Европейского Союза по кибербезопасности (ENISA) в 2014 г. опубликовало первый отчет в области проектируемой конфиденциальности, в котором конфиденциальность представлена через используемые стратегии защиты данных. В 2015 г. был представлен второй отчет [6], в котором проектируемая конфиденциальность представлена посредством анализа стратегий и инструментов проектирования в эпоху анализа больших данных. В 2019 г. ENISA опубликовало исследование семи принципов защиты данных по умолчанию в целях проектирования информационных технологий [7, 8]. В исследовании рекомендовано законодателям и организациям в области стандартизации учитывать принцип защиты данных по умолчанию для всех случаев регулирования обработки персональных данных. Правовые и технические нормы должны быть явными, параметры безопасности четко доведены до пользователей информационных технологий. В числе основополагающих принципов проектируемой конфиденциальности как фундаментальной человеческой ценности в целях обеспечения защиты личной информации и персонального контроля за ее использованием определены следующие основные положения.

1. Превентивные меры, а не только устранение последствий. Встраивание конфиденциальности в конструкцию информационной системы должно быть активным, а не ограничиваться лишь мерами по устранению последствий. Должны быть реализованы требования, которые позволяют предвидеть и предотвратить нарушение конфиденциальности. Иными словами, «личная информация должна быть защищена до того, как система запущена в работу, а не после выявления нарушений конфиденциальности» [3].

2. Конфиденциальность как стандартная установка по умолчанию. Информационная система должна защищать пользователя автоматически без ожидания таких настроек от пользователя. Решение об изменении настроек должен принимать только пользователь.

3. Конфиденциальность как часть инфраструктуры. Защита личной информации должна стать неотъемлемой частью архитектуры любой информационной системы или деловых отношений.

4. Полная функциональность с суммарным положительным результатом. Проектируемая конфиденциальность стремится учесть все законные интересы и цели «беспроеигрышным» способом. «Подход с нулевой суммой, при котором делаются ненужные компромиссы, является устаревшим» [3].

5. Защита личной информации на протяжении всего цикла ее сбора, хранения, обработки и уничтожения. Системы должны обеспечивать комплексную безопасность и полную защиту жизненного цикла – от приобретения до использования и безопасного уничтожения.

6. Доступность и открытость. Информационные технологии должны функционировать в соответствии с заявленными принципами и целями, что должно подтверждаться независимой проверкой. Все компоненты и операции должны быть открытыми и доступными как для пользователей, так и для субъектов, обеспечивающих данный вид сервиса.

7. Система должна быть ориентирована на пользователя. Разработчики и операторы информационных систем по умолчанию должны соблюдать стандарты обеспечения безопасности информации пользователей, их интересов, своевременно

уведомляя пользователей о сборе личной информации или изменениях в политике конфиденциальности, предоставляя им свободу выбора в удобной и понятной форме.

Концепция проектируемой конфиденциальности в России. В российском законодательстве положения проектируемой конфиденциальности определены в нескольких законах. Так, требования, связанные с защитой персональных данных при использовании информационных систем, устройств, оборудования, сооружений и сетевой инфраструктуры, определены в ст. 16. Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации), а также в ст. 19 Федерального закона от 27 июля 2006 г. «О персональных данных».

В соответствии с этими законами защита информации, в том числе персональных данных, представляет собой принятие правовых, организационных и технических мер, направленных на: «1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации».

В соответствии с Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, которые определяются уполномоченными на то государственными органами и закрепляются в ведомственных нормативных правовых актах.

Второе положение триады проектируемой конфиденциальности раскрывается в ст. 7 Федерального закона «О персональных данных». Так, «операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом».

Однако концепция проектируемой конфиденциальности, помимо правовых механизмов защиты информации, содержит также и технологические требования к разработчикам информационных технологий, заключающиеся в необходимости реализовывать логику архитектуры информационной технологии, которая позволит обеспечить защиту персональных данных на протяжении всего ее жизненного цикла [9].

Стандартизация технологий. В настоящее время нормативные требования к защите персональных данных на протяжении всего жизненного цикла информационной технологии в российском законодательстве не реализованы. Политика российского государства в данном направлении начала меняться с 2015 г. Требования, связанные с использованием отечественных информационных систем и устройств, оборудования, сооружений и сетевой инфраструктуры, начинают реализовываться в российском законодательстве. За период с 2015 г. по 2020 г. в Российской Федерации принято более 2000 правовых актов различных уровней в области обеспечения информационной безопасности в различных

областях общественных отношений. В 2019 г. приняты поправки в два закона, касающихся обеспечения информационной безопасности в области создания и использования программного обеспечения и обеспечения безопасной среды коммуникации на территории Российской Федерации [10]. С 2019 г. в РФ определено требование об обеспечении преимущественно отечественным программным обеспечением государственных органов и органов местного самоуправления, а также организаций, деятельность которых связана с критической информационной инфраструктурой. В ст. 138.1 УК РФ были приняты поправки в части приравнивания программного обеспечения к специальным техническим средствам. Созданы правовые условия для привлечения инвестиций в российскую экономику и повышения качества товаров, работ, услуг. Кроме того, с 1 июля 2020 г. вступил в силу закон о запрете продажи смартфонов, ноутбуков и других устройств без предустановленного российского программного обеспечения. В данном законе предусматривается создание списка обязательного программного обеспечения, которое должно устанавливаться на все устройства, продающиеся в России. Под ограничения попадают смартфоны, планшеты, компьютеры и телевизоры со Smart TV. Список таких устройств будет составлен и утвержден Правительством Российской Федерации.

Таким образом, можно отметить, что политика государства в области информационной безопасности повернулась в сторону необходимости обеспечения контроля за вводимыми в гражданский оборот информационными технологиями и приоритетного использования национальных информационных технологий. Первый шаг в концепции этой политики связан с разработкой системы национальных стандартов и определением перечня сферы экономических отношений, в которых будут осуществляться контроль и надзор за используемыми информационными технологиями, в основном эти сферы связаны с функционированием критической информационной инфраструктуры. Для остальных информационных технологий, используемых субъектами в сферах, отличных от критической информационной инфраструктуры, правовое регулирование пока меняется достаточно медленно.

Понимая сложность проблемы стандартизации и разнообразие участников этого процесса, Правительство Российской Федерации утвердило 29 октября 2019 г. Правила реализации федерального проекта «Информационная безопасность» в рамках национальной программы «Цифровая экономика Российской Федерации»¹, которые направлены на создание системы отраслевых правил использования киберфизических систем, разработку и принятие набора стандартов информационной безопасности и обработки больших массивов данных для минимизации рисков и угроз безопасного функционирования сетей связи общего пользования.

В европейской практике обеспечения информационной безопасности предлагается реализовать механизм контроля субъектами

¹ Постановление Правительства Российской Федерации от 29 октября 2019 г. № 1382 «Об утверждении Правил предоставления субсидий из федерального бюджета на достижение отдельных результатов федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» // СЗ РФ 2019. № 44. Ст. 6216.

персональных данных алгоритмов информационных технологий, обрабатывающих данные.

Правовой механизм направлен на реализацию требований проектируемой конфиденциальности в части обеспечения защиты данных на технологическом уровне.

Впервые реализация данного механизма была предложена в документе 2017 г., подготовленном информационным комиссаром Великобритании [11], в котором предлагалось ввести «алгоритмическую ответственность», являющуюся стратегическим решением проблемы обеспечения защиты персональных данных.

По сути, «алгоритмическая ответственность» позволяет реализовать правовой механизм контроля со стороны субъектов персональных данных используемых алгоритмов машинного обучения. Субъект персональных данных в любой момент может убедиться, что алгоритмы выполняют именно те действия, которые от них ждут.

Однако ни в российской научной литературе, ни в программных государственных документах пока не отражена данная тенденция обеспечения информационной безопасности.

Хотелось бы отметить, что такая новация является интересной, и вполне возможно, что подобное объединение правового и технического регулирования принесет хорошие результаты, поскольку на разработчиков будет возложена ответственность за разработку неточных и непрозрачных алгоритмов, а у пользователей появится легальная возможность контролировать результаты, получаемые в процессе обработки информации, относимой к их персональным данным.

Конечно, возможны и сложности при реализации такого решения, поскольку это потребует формирования специальных органов, отвечающих за контроль и надзор в этой области отношений.

Российская правовая система обеспечения конфиденциальности персональных данных соответствует триаде проектируемой конфиденциальности, но без работоспособной системы сертификации правовые требования не принесут необходимого результата.

Для обеспечения безопасности российских пользователей информационных технологий необходимо включить в национальную систему сертификации информационных технологий стандарты продуктов или услуг в области кибербезопасности, в том числе безопасности аппаратного и программного обеспечения.

Принципы проектируемой конфиденциальности можно реализовать только при взаимодействующей системе правового и технического регулирования в области обеспечения информационной безопасности, поскольку большинство принципов обеспечивается правовыми нормами, определяющими требования к архитектуре информационной системы и аппаратно-программным решениям обеспечения конфиденциальности.

Литература

1. Жарова А. К. Источники понятий «персональные данные» и частная жизнь лица в российском праве / А. К. Жарова, В. М. Елин // Вестник Академии права и управления. 2017. № 1(64). С. 69–78.
2. Privacy by Design. 7 основополагающих принципов. URL: https://online.zakon.kz/Document/?doc_id=31633216#pos=31;0 (дата обращения: 11.05.2021).
3. Annual Report 1995. URL: https://www.ipc.on.ca/wp-content/uploads/Resources/up-ar_95e.pdf (дата обращения: 11.05.2021).
4. Елин В. М. «Облачные услуги» и особенности их правового регулирования в Российской Федерации / В. М. Елин // Информационное право. 2017. № 4. С. 28–33.
5. Крылова М. С. Принципы обработки персональных данных в праве Европейского союза / М. С. Крылова // Актуальные проблемы российского права. 2017. № 10. С. 175–181.
6. ENISA. URL: <https://www.enisa.europa.eu/topics/data-protection/privacy-by-design> (дата обращения: 11.05.2021).
7. Regulation EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF> (дата обращения: 11.05.2021).
8. Recommendations on Shaping Technology According to GDPR Provisions – Exploring the Notion of Data Protection by Default. URL: <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> (дата обращения: 11.05.2021).
9. Big Data, Artificial Intelligence, Machine Learning and Data Protection. URL: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> (дата обращения: 11.05.2021).
10. Федеральный закон от 22 декабря 2020 г. № 460-ФЗ (ред. от 11 июня 2021 г.) «О внесении изменений в Федеральный закон «О техническом регулировании» и Федеральный закон «О внесении изменений в статью 4 Закона Российской Федерации «О защите прав потребителей».
11. Leizerov S. Information and Privacy Commissioner of Ontario / S. Leizerov, E. Shangina. URL: www.ipc.on.ca (дата обращения: 11.05.2021).

References

1. Zharova A. K. Istochniki ponyatij «personal'nye dannye» i chastnaya zhizn' lica v rossijskom prave [Sources of the Concepts of «Personal Data» and the Private Life of a Person in Russian Law] / A. K. Zharova, V. M. Elin // Vestnik Akademii prava i upravleniya – Bulletin of the Academy of Law and Management. 2017. № 1(64). S. 69–78.
4. Elin V. M. «Oblachnye uslugi» i osobennosti ih pravovogo regulirovaniya v Rossijskoj Federacii [«Cloud Services» and Features of Their Legal Regulation in the Russian Federation] / V. M. Elin // Informacionnoe pravo – Information law. 2017. № 4. S. 28–33.
5. Krylova M. S. Principy obrabotki personal'nyh dannyh v prave Evropejskogo soyuza [Principles of Personal Data Processing in the Law of the European Union] / M. S. Krylova // Aktual'nye problemy rossijskogo prava – Actual problems of Russian law. 2017. № 10. S. 175–181.