ДИСКУССИОННЫЕ СТАТЬИ | DISCUSSION PAPERS

Современная наука и инновации.
2023. № 4 (44). С. 274-284.
Modern Science and Innovations.
2023; 4(44):274-284.

ДИСКУССИОННЫЕ СТАТЬИ / DISCUSSION PAPERS

Научная статья / Original article

УДК 681.51: 621.18-5
https://doi.org/10.37493/2307-910X.2023.4.33

Елена Александровна Овчинникова
[Elena A. Ovchinnikova][1]*,
Елена Анатольевна Семенова
[Elena A. Semenova][2],
Валентина Викторовна Цаплева
[Valentina V. Tsapleva][3]

Анализ правовых и организационных основ планирования системы безопасности персональных данных

Analysis of the legal and organizational framework for ensuring the security of personal data

[1, 2, 3]Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, Россия / Siberian State University of telecommunications and Information Science, Novosibirsk, Russia

****Автор, ответственный за переписку: Елена Александровна Овчинникова, 9538685137@mail.ru / Corresponding author: Elena A. Ovchinnikova, 9538685137@mail.ru***

Аннотация. *В работе выполнен анализ особенностей применения правовых основ обеспечения безопасности ПДн, а также раскрыты существенные организационные аспекты планирования системы защиты ПДн в организации. Авторами анализируются отдельные аспекты правового регулирования, оказывающие существенное влияние на выбор организационных мер защиты ПДн: установление пределов действия законодательства РФ в области ПДн; установление категорий ПДн и соответствующих им основных источников правового регулирования; особенности нормативно-правового регулирования обработки отдельных категорий ПДн. Структурно и логически работа разделена на две основные части: правовые меры обеспечения безопасности ПДн, организационные меры планирования защиты ПДн. Авторами статьи проведен анализ правовых и организационно-плановых мер по обеспечению безопасности персональных данных, которые могут быть реализованы в организации.*

Ключевые слова: персональные данные, система защиты, меры защиты, конфиденциальность, угроза, уровень защиты

Для цитирования: *Овчинникова Е. А., Семенова Е. А., Цаплева В. В. Анализ правовых и организационных основ планирования системы безопасности персональных данных // Современная наука и инновации. 2023. № 4 (44). С. 274-284. https://doi.org/10.37493/2307-910X.2023.4.33*

Abstract. *The paper analyzes the features of the application of the legal framework for ensuring the security of PD, as well as reveals the essential organizational aspects of planning a PD protection system in an organization. The authors analyze certain aspects of legal regulation that have a significant impact on the choice of organizational measures to protect PD: setting the limits of the RF legislation in the field of PD; establishment of categories of PD and the main sources of legal regulation corresponding to them; features of legal regulation of the processing of certain categories of PD. Structurally and logically, the work is divided into two main parts: legal measures to ensure the security of PD, organizational measures for planning the protection of PD. In general, the authors of the article analyze legal, organizational and planning measures to ensure the security of personal data that can be implemented in an organization.*

Keywords: personal data, protection system, protection measures, confidentiality, threat, level of protection

For citation: *Ovchinnikova EA, Semenova EA, Shebzukhova TA, Tsapleva VV. Analysis of the legal and organizational framework for ensuring the security of personal data. Modern Science and Innovations. 2023;4(44):274-284. (In Russ.).* https://doi.org/10.37493/2307-910X.2023.4.33

Введение. Российское государство предоставляет и гарантирует своим гражданам широкий спектр прав, к ним, в частности, относится информационное право на неприкосновенность частной жизни, личную и семейную тайну (ч. 1, ст. 23 Конституции РФ) [5]. Безопасность информации о человеке и его частной жизни обеспечивается посредством комплекса мер правового, организационного и технического характера (ч. 1, ст. 16 ФЗ РФ от 27.07.2006 № 149) [9]. Рассмотрим ключевые аспекты в рамках каждой из групп, указанных мер применительно к персональным данным (ПДн).

Материалы и методы исследований. Правовые меры обеспечения безопасности ПДн. Основой функционирования общественных отношений в той или иной их сфере или области является установление общеобязательных правовых предписаний (субъектный состав, правовой статус, условия его реализации, пределы действия нормативных предписаний и др.), которые закрепляются в нормативно-правовых актах различного уровня. Институциональное регулирование области персональных данных имеет определенное содержание и объем, опосредованный правовым характером самих сведений (рисунок 1).

Обеспечение безопасности отдельных видов информации может быть достигнуто путем ограничения доступа к информации, устанавливаемое посредством федеральных законов на разумных и справедливых началах. Применение (состав и объем) режимных мер не может противоречить обозначенным целям, как например, целям защиты прав граждан (ч. 1, ст. 9 ФЗ РФ от 27.07.2006 № 149) [9]. Поэтому так важно соблюсти баланс информационной открытости и конфиденциальности, а также удобство правоприменения в областях информационной сферы.

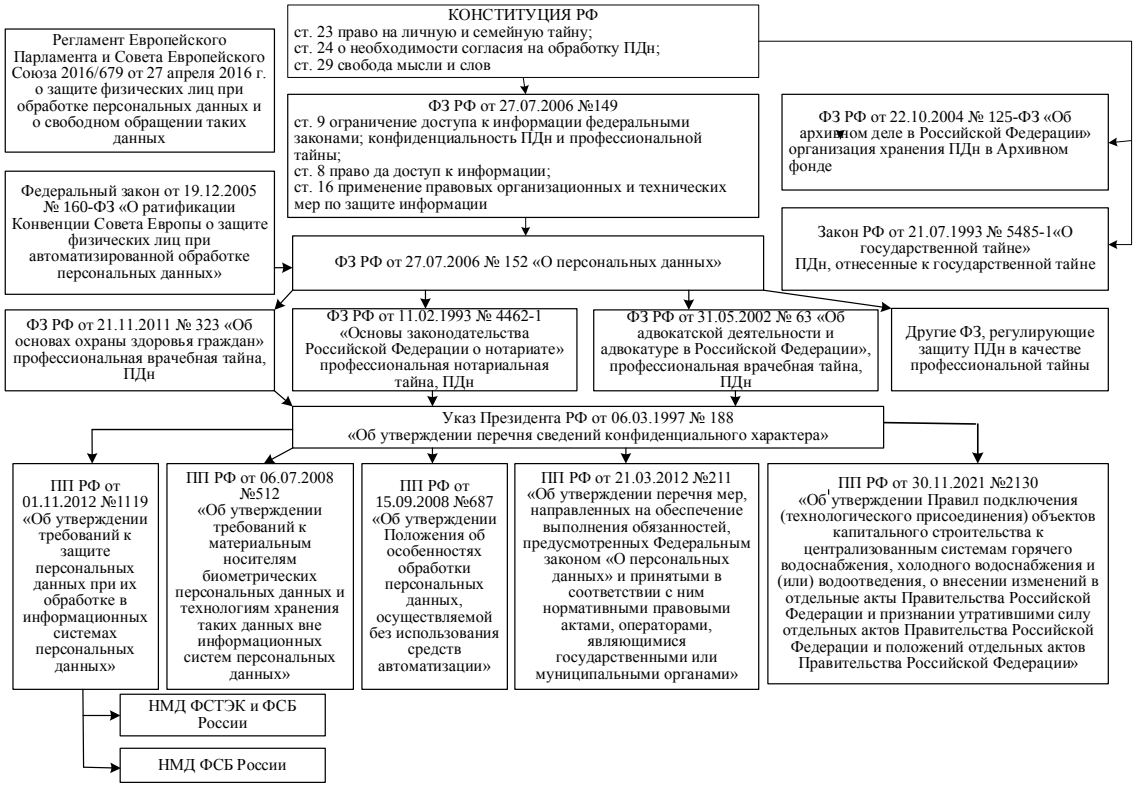

Рисунок 1 – Правовые основы обеспечения безопасности ПДн
Figure 1 – The legal basis for ensuring the safety of PD

Правовые основы безопасности ПДн закреплены в законе федерального уровня от 27.07.2006 № 152 «О персональных данных» (ФЗ РФ), согласно которому, сбор и обработка ПДн должны осуществляться в соответствии с целями деятельности организации, исключая при этом избыточность обрабатываемой и сохраняемой информации [19].

Для обеспечения безопасного обращения ПДн требуется четкое установление пределов действия ФЗ РФ, в частности территориальных, а также по субъектам и объектам правоотношений.

По территориальным пределам действия следует обратить внимание на существенные проблемы в отношении защиты прав российских операторов ПДн на международном уровне. Территориальные и субъектные пределы действия как ФЗ РФ, так и законодательства ЕС в отношении стороны-негражданина весьма расплывчаты. При этом особенности законодательств таковы, что и персональные данные граждан РФ, и операторы ПДн – физические и юридические лица РФ, участвующие в правоотношениях, более уязвимы нежели европейские. Рассмотрим некоторые особенности подробнее.

Результаты исследований и их обсуждение. В юрисдикции ФЗ РФ находятся иностранные частные или юридические лица на основании соглашения (договора) одной из сторон, которого являются граждане РФ. Таким образом, в силу трансграничного характера современной экономической деятельности, а также по смыслу категории «соглашение», в области действия ФЗ РФ может оказаться любой иностранный субъект, поддерживающий экономические связи с гражданином РФ, который при этом не определен. Напротив, в европейском законодательстве, стороны-неграждане ЕС четко обозначены, но таким образом, что включают практически всех лиц, прямо или опосредовано контактирующих с субъектом ЕС, что придает ему и определенность, и трансграничность.

Проблематичным является практическое применение российского законодательства. Поскольку, в отличие от России, которая является добросовестным субъектом международных отношений и не только принимает, но и исполняет нормы международного права, являющиеся составной частью ее правовой системы (ч. 4, ст. 15 Конституции) [5], международные субъекты попросту игнорируют российские правовые и правоприменительные предписания. Соответственно вероятность применения РФ юридической ответственности и более того ее реализации в отношении субъекта-негражданина довольно низкая. В свою очередь объемы санкций, предусмотренных законодательством РФ в области ПДн, существенно ниже в сравнении с европейскими. Таким образом, возможность избежать или проигнорировать санкции еще более снижает эффективность правовой защиты субъектов и операторов ПДн РФ.

Как отмечалось ранее основы правовой защиты ПДн закреплены в Федеральном законе «О персональных данных», который выделяет отдельные категории информации по своему содержанию, соответствующие персональным данным, но находящиеся вне пределов его действия [9]. Обозначенный подход также фиксируется в Указе Президента РФ от 06.03.1997 № 188, в утвержденном им перечне сведений конфиденциального характера [13]. Правовая защита сведений, находящихся вне пределов действия ФЗ РФ, должна обеспечиваться другими федеральными законами. Рассмотрим отдельные категории таких сведений в соответствии с источниками их регулирования:

• в зависимости от особенностей обработки ПДн, действие ФЗ РФ не распространяется на данные, обрабатываемые без использования средств автоматизации, если их обработка не соответствует характеру операций, совершаемых с использованием средств автоматизации или по установленному для их использования в информационной системе (ИС) алгоритму (ч. 1, ст. 1 ФЗ РФ) [19];

• поскольку предметом ФЗ РФ являются правоотношения, очевидно, что обработка ПДн физическими лицами в личных и семейных целях не входит в область его действия, более того она безразлична для позитивного права (п. 1, ч. 2, ст. 1 ФЗ РФ) [19];

• реализация функций архива по управлению и использованию документов Архивного фонда, содержащих ПДн (п. 2, ч. 2, ст. 1 ФЗ РФ), регулируется ФЗ РФ от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации» [8] за исключением деятельности по распространению в сети Интернет персональных данных, содержащихся в архивных документах, которая регулируются федеральными законами № 149 и № 152 [15, 19];

• ПДн (п. 4, ч. 2, ст. 1 ФЗ РФ), отнесенные к сведениям, составляющим государственную тайну (Закон РФ от 21.07.1993 № 5485-1«О государственной тайне») [18].

Безопасность определенных категорий сведений профессионального характера (профессиональная и служебная тайна) обеспечивается нормами ФЗ РФ, а также законодательством в сфере их обращения, рассмотрим некоторые из них (ст. 6 ФЗ РФ) [19]:

• профессиональная тайна – сведения, обрабатываемые в процессе реализации профессиональной деятельности, ограничение доступа к которым установлено Конституцией и федеральными законами РФ (п. 4 Указа Президента РФ от 06.03.1997 № 188) [13]: врачебная тайна (ст. 13 ФЗ РФ от 21.11.2011 № 323 «Об основах охраны здоровья граждан») [12], нотариальная тайна (ст. ФЗ РФ от 11.02.1993 № 4462-1 «Основы законодательства Российской Федерации о нотариате») [21], адвокатская тайна (ст. 8 ФЗ РФ от 31.05.2002 № 63 «Об адвокатской деятельности и адвокатуре в Российской Федерации») [7], тайна связи, включающая переписку, телефонные переговоры, почтовые отправления, телеграфные и иные сообщения) (ст. 63 ФЗ РФ от 07.07.2003 № 126 «О связи» [20], ст. 13 УПК РФ [24]) и др.

• информация о деятельности судов, содержащая ПДн (ч. 3 ст. 1 ФЗ РФ), а также сведения (п. 2 Указа Президента РФ от 06.03.1997 № 188) [13], составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых применяются меры государственной защиты (ФЗ РФ от 22.12. 2008 № 262 «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [11], ст. 5 ФЗ РФ от 20.04.1995 № 45 «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» [17], ст. 9 ФЗ РФ от 20.08.2004 № 119 «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства») [16];

• сведения (п. 7 Указа Президента РФ от 06.03.1997 № 188), содержащиеся в личных делах, осужденных (Уголовно-исполнительный кодекс Российской Федерации) [13];

• защита персональных данных работников осуществляется на основании ФЗ РФ и положений главы 14 ТК РФ [22], отдельные механизмы реализации защиты сведений о работниках, соискателях на замещение вакантных должностей, а также лицах, находящихся в кадровом резерве разъяснены Роскомнадзором от 14 декабря 2012 г. [9];

• сведения (п. 7 Указа Президента РФ от 06.03.1997 № 188), содержащиеся в банке данных службы судебных приставов, являются общедоступными, поэтому обеспечивается сохранение их основных свойств за исключением конфиденциальности (ст. 6 ФЗ РФ от 02.10.2007 № 229 «Об исполнительном производстве») [10]. Так в процессе обработки таких персональных данных должны быть обеспечены основные, присущие информации ценностные характеристики, а именно: целостность, точность, достоверность, актуальность (ч. 6, ст. 5 ФЗ РФ) [13, 19].

В связи с тем, что по своей природе персональные данные не отделимы от субъекта, оператор должен обеспечить их хранение в той форме, которая позволяет идентифицировать непосредственно субъекта персональных данных. Исключением являются условия, предусмотренные п. 9., ч. 1, ст. 6 ФЗ РФ, применяемые к обработке обезличенных ПДн [19].

В соответствии с Конституцией России, по смыслу части 1 статьи 24, одной из основополагающих мер защиты ПДн является необходимость получения согласия субъекта на соответствующие действия. Данное условие закреплено в статьях 6 (п. 1, ч. 1), 7 и 9 ФЗ РФ, а также в ст. 3 ФЗ РФ от 27.07.2006 № 149 (п. 7) непосредственно в отношении ПДн, за исключением обозначенных в статье 6 случаев, когда субъект не в состоянии дать такое согласие или обработка ПДн необходима в интересах государства и третьих лиц. В случае, если оператор поручает обработку ПДн третьим лицам, последние в соответствии с ч. 4, ст. 6 ФЗ РФ не обязаны получать согласие, так как ответственность перед субъектом продолжает нести непосредственно оператор [9, 19].

Вместе с тем, не стоит забывать, что граждане являются частью общества, поэтому публичность становится неотъемлемым их свойством, а, следовательно, в определенной степени затрагивает и их персональные данные. Таким образом, конфиденциальность, в силу природы ПДн, не может быть абсолютной. В этой связи законодатель выделяет следующие категории, указывающие на возможность распространения (неограниченности) отдельных ПДн [19]:

• ПДн, разрешенные субъектом для их распространения на основании согласия (ст. 10 ФЗ РФ);

• общедоступные источники ПДн, которые формируются в целях информационного обеспечения, также с письменного согласия субъекта персональных данных и могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и другую информацию, сообщаемую субъектом (ч. 1, ст. 8 ФЗ РФ).

Категория «общедоступные ПДн» в законе не закреплена, но о них говорится в Постановлении Правительства РФ от 01.11.2012 № 1119 в контексте определения информационной системы, обрабатывающей общедоступные персональные данные. Постановление также четко указывает на критерий общедоступности ПДн, а именно их получение только из общедоступных источников, которые в соответствии с ФЗ РФ формируются на основании письменного согласия субъекта [15].

Федеральный закон выделяет отдельные категории персональных данных, в отношении которых применяются меры защиты, учитывающие особенности их содержания. К примеру, обработка специальных ПДн осуществляется при наличии установленных в статье 10 случаев и незамедлительно прекращается при устранении соответствующих причин (ч. 4, ст. 10 ФЗ РФ) [19].

Основополагающей мерой правовой защиты, в том числе и ПДн, является установление правового статуса субъектов – участников правовых отношений. Так, на оператора возлагается обязанность по применению всего комплекса мер для защиты ПДн от неправомерного или случайного доступа и осуществлению действий, направленных на изменение свойств сведений (ч. 1, ст. 19 ФЗ РФ) [19].

В силу особой значимости объекта защиты и непосредственной его связи с гражданскими правами и свободами устанавливается федеральный государственный контроль (надзор) за обработкой ПДн, осуществляемый Роскомнадзором – органом по защите прав субъектов ПДн и прокуратурой – единой государственной системой органов, осуществляющих надзор за соблюдением законов Российской Федерации (ст.ст. 23, 23.1 ФЗ РФ) [19].

Одним из универсальных правовых механизмов предупреждения нарушений является установление ответственности, а именно: дисциплинарной, гражданско-правовой, административной и уголовной.

Таким образом, на основании закрепленных в федеральном законодательстве базовых правовых основ защиты ПДн Правительством РФ вырабатываются требования для разработки соответствующих организационных и технических мер, применяемых для защиты персональных данных, на бумажных носителях без использования средств

автоматизации (ПП РФ от 15.09.2008 № 687) и обрабатываемых в информационных системах персональных данных (ИСПДн) (ПП РФ от 01.11.2012 № 1119) [15].

Организационные меры планирования защиты ПДн. Безопасность персональных данных обеспечивается оператором, который на основании согласия субъекта ПДн или федерального закона осуществляет их обработку. По закону оператор может делегировать полномочия по обработке ПДн третьему лицу, которое и буде, в таком случае, осуществлять их защиту. При этом ответственность за безопасность сведений несет оператор, независимо от того, кем осуществляется их обработка. Применяемые для защиты обрабатываемых в информационных системах ПДн организационные и технические меры реализуются в зависимости от уровней защищенности в рамках, установленных Правительством РФ требований (ПП от 01.11.2012 № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных») [15]. Целью выполнения требований является нейтрализация актуальных угроз безопасности информации (ч. 4, ст. 19 ФЗ РФ) [19].

Организация функционирования системы защиты ПДн (СЗИ) осуществляется в рамках нескольких циклов (ГОСТ 27001-2021): планирование и разработка; внедрение и сопровождение; контроль и мониторинг; восстановление, модернизация и повышение эффективности. Рассмотрим каким образом осуществляется планирование разработки СЗИ с учетом предъявляемых к защите ПДн требований.

Учитывая публичный характер охраны ПДн, может быть реализована только та СЗИ, которая выстроена на основании установленных Правительством требований. Также не следует забывать, что защита информации является лишь обслуживающим механизмом реализации основной деятельности организации, следовательно, различные СЗИ должны быть встроены в общий процесс и учитывать его задачи.

Прежде формирования мер защиты необходимо обследовать действующую информационно систему (состав и используемые информационные технологии), а также провести инвентаризацию обрабатываемых в ней ПДн. ПДн весьма сложный объект, поэтому недостаточно лишь составить перечень непосредственно сведений. Главным образом необходимо установить категории и объем обрабатываемых данных, а также обоснованность их обработки. Обработка персональных данных может осуществляться на основании федерального закона, согласия субъекта или договора (соглашения). Категории и объем обрабатываемых данных должны соответствовать целям обработки и не быть избыточными. При организации обработки ПДн следует учитывать особую важность объекта защиты и публичный характер обеспечения его безопасности, в том числе предусмотренную законом ответственность. Так, например, обработка ПДн несовместимая с целями их сбора влечет административную ответственность в размере до 6000 – на физических лиц, до 20000 – на должностных лиц и до 100000 – на юридических лиц (ст. 13.11 КоАП) [4].

После проведения инвентаризации обрабатываемой информации проводится обследование ИС, в рамках которого должны быть установлены ее следующие параметры: структура информационной системы (автономные, локальные, распределенные); наличие подключений к сетям общего пользования, в том числе сети Интернет; режим обработки ПДн (однопользовательский, многопользовательский); наличие разграничения прав доступа к ПДн в информационной системе; территориальное расположение элементов информационной системы (РФ, на территории других государств).

Далее, на основании полной информации о системе устанавливаются актуальные угрозы информационной безопасности и осуществляется их классификация по трем уровням безопасности. Для установления и анализа угроз ИБ используется перечень актуальных угроз из банка данных угроз безопасности информации ФСТЭК России (БДУ). Вместе с тем объединения операторов вправе определять дополнительные угрозы безопасности с учетом особенностей, используемых ими ИСПДн (ч. 6 ст. 19 ФЗ РФ) [19].

Всего установлено три типа угроз. Угрозы первого и второго типа связаны с наличием недокументированных возможностей в системном программном обеспечении (1-й тип) и в прикладном программном обеспечении (2-й тип). Угрозы 3-го типа могут быть реализованы в ИС, для которых не актуальны угрозы с приведенными выше недокументированными возможностями (ПП РФ № 1119) [15].

Рассмотрим требования к построению системы защиты ИСПДн. Разработка системы защиты ИСПДн требует установления уровня (ПП РФ № 1119 – для ИСПДн) или класса (ПП РФ от 06.07.2015 № 676 – для ГИС) ее защищенности на основании типа угроз с учетом оценки возможного вреда в случае их реализации, а также категорий ПДн [15], их принадлежность и объем базы данных таблица 1.

Таблица 1 – Критерии, определяющие уровень защищенности ПДн
Table 1 – Criteria determining the level of PD security

УЗ	Тип угрозы	Категории ПД	Принадлежность ПД	Объем базы
УЗ-1	I	иные	-	-
		специальные		
		биометрические		
	II	специальные	не сотрудники	более 100000
УЗ-2	I	общедоступные	-	-
	II	специальные	сотрудники	-
			не сотрудники	менее 100000
	II	биометрические	-	-
	II	общедоступные	не сотрудники	более 100000
	II	иные	не сотрудники	более 100000
	III	специальные	не сотрудники	более 100000
УЗ-3	II	общедоступные	сотрудники	-
			не сотрудники	менее 100000
	II	иные	сотрудники	-
			не сотрудники	менее 100000
	III	специальные	сотрудники	-
			не сотрудники	менее 100000
		биометрические	-	-
		иные	не сотрудники	более100000
УЗ-4	III	общедоступные	-	-
	III	иные	сотрудники	
		иные	не сотрудники	менее 100000

Особое значение для построения СЗИ имеет проведение анализа актуальных угроз ИБ и его формализация в виде модели угроз ИБ. В зависимости от назначения ИСПДн, обрабатываемых в ней данных и применяемых для защиты средств (СКЗИ) принято разделять модели угроз ФСБ и ФСТЭК. Мы же рассматриваем требования ПП РФ № 1119 [15], которое на предусматривает в своем составе применение средств криптографической защиты, поэтому достаточно использовать нормативную базу ФСТЭК: утвержденные Постановлением Правительства РФ меры по обеспечению безопасности ПДн [15], Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008) [1], учитываются измененные в соответствии с ПП РФ № 1119 требования; Методика оценки угроз безопасности информации (утверждена ФСТЭК России 05.02.2021) [6]; БДУ ФСТЭК России [2].

Таким образом, обследование действующей ИСПДн, обработка и анализ полученных результатов, определение уровней защиты системы и оценка угроз ее безопасности (построение моделей угроз и нарушителя) являются основой для разработки комплекса соответствующий организационных и технических мер.

Заключение. При построении системы защиты ПДн первоначально следует учитывать территориальную и юрисдикционную принадлежность субъекта персональных данных. Трансграничный характер современных социальных связей определяет

институциональные особенности правого регулирования отдельных предметных областей, в частности ПДн. Основы европейского правового регулирования ПДн имплементированы в российское законодательство, что нисколько не освобождает оператора от необходимости применять непосредственно европейскую законодательную базу. Следует отметить, что европейский регламент весьма казуистичен и включает отдельные предписания, которые прямо не обозначены в законодательстве о персональных данных РФ, в тоже время его нарушение может привести к существенным санкциям. Поэтому эффективность обеспечения безопасности ПДн непосредственно зависит от тщательности изучения нормативной базы в неразрывной связи со структурными особенностями информационной системы.

ЛИТЕРАТУРА

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) : Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] ФСТЭК России. URL: https://bdu.fstec.ru/documents/16 (дата обращения: 25.03.2023).
2. Банк данных угроз безопасности информации [Электронный ресурс] ФСТЭК России. URL: https://bdu.fstec.ru/threat (дата обращения: 25.03.2023).
3. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» : дата введения 2008-02-01 (недействующий). URL: https://docs.cntd.ru/document/1200058325 (дата обращения: 24.03.2023).
4. Кодекс Российской Федерации об административных правонарушениях [федер. Закон: принят Гос. Думой 20 декабря 2001 г.: по состоянию на 2 октября 2018 г.]. М.: Собрание законодательства Российской Федерации, 2002. № 1 (часть. I). ст. 1.
5. Конституция: Осн. Закон Рос. Федерации от 12 дек. 2003 г. [Электронный ресурс] КонсультатПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 05.04.2023).
6. Методика оценки угроз безопасности информации: Методический документ. – утвержден ФСТЭК России 5 февр. 2021 г. [Электронный ресурс] ФСТЭК России. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5- fevralya-2021 (дата обращения: 30.03.2023).
7. Об адвокатской деятельности и адвокатуре в Российской Федерации : федер. закон принят Гос. Думой 26 апр. 2002 г. № 63-ФЗ: по состоянию на 10 нояб. 2022 г. [Электронный ресурс] КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_36945// (дата обращения: 01.04.2023).
8. Об Архивном деле в Российской Федерации [федер. закон: принят Гос. Думой 1 октября 2004 г.: по состоянию на 28 декабря 2017 г.]. М.: Собрание законодательства Российской Федерации, 2004. № 43. ст. 4169.
9. Об информации, информационных технологиях и о защите информации : федер. закон принят Гос. Думой 8 июля 2006 г. № 149-ФЗ: по состоянию на 27 июля 2006 г. [Электронный ресурс] КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.04.2022).
10. Об исполнительном производстве: федер. закон принят Гос. Думой 14 сентяб. 2007 г. № 229-ФЗ: по состоянию на 29 декаб. 2022 г. [Электронный ресурс] КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_71450/ (дата обращения: 01.04.2023).
11. Об обеспечении доступа к информации о деятельности судов в Российской Федерации [федер. закон: принят Гос. Думой 10 декабря 2008 г.: по состоянию на 28 декабря 2017 г.]. М.: Собрание законодательства Российской Федерации, 2008. № 32. ст. 6217.
12. Об основах охраны здоровья граждан Российской Федерации : федер. закон принят Гос. Думой 1 нояб. 2011 г. № 323-ФЗ: по состоянию на 19 декаб. 2022 г. [Электронный ресурс] КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 01.04.2023).
13. Об утверждении перечня сведений конфиденциального характера [указ Президента: утвержден Президентом 6 мата 1997 г.: по состоянию на 13 июля 2015 г.]. М.: Собрание законодательства Российской Федерации, 1997. № 188. ст. 1127.
14. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18 февр. 2013 г. № 21. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18- fevralya-2013-g-n-21 (дата обращения 19.03.2023 г.).
15. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных утв. Постановлением Правительства РФ 1 нояб. 2012 г. № 1119. URL: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 08.04.2023).
16. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства: федер. закон принят Гос. Думой 31 июля 2004 г. № 119-ФЗ: по состоянию на 1 июля 2021

г. [Электронный ресурс] КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_48959/ (дата обращения: 01.04.2023).

17. О государственной защите судей, должностных лиц правоохранительных и контролирующих органов: федер. закон принят Гос. Думой 22 марта 1995 г. № 45-ФЗ: по состоянию на 1 июля 2021 г. [Электронный ресурс] КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_6425/ (дата обращения: 01.04.2023).

18. О государственной тайне : закон РФ: принят Гос. Думой 21 июля 1993 г.: по состоянию на 9 марта 2021 г.]. [Электронный ресурс] КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 21.04.2023).

19. О персональных данных [Федер. закон: принят Гос. Думой 8 июля 2006 г.: по состоянию на 25 ноября 2009 г.]. М.: Собрание законодательства Российской Федерации, 2006. № 31. Ч. 1. ст. 3451.

20. О связи [Федер. закон: принят Гос. Думой 18 июня 2003 г.: по состоянию на 3 августа 2018 г.]. М.: Собрание законодательства Российской Федерации, 2003. № 28. ст. 2895.

21. Основы законодательства Российской Федерации о нотариате : закон утв. ВС РФ 11.02.1993 № 4462-1: по состоянию на 28 декаб 2022 г. [Электронный ресурс] КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_1581/ (дата обращения: 01.04.2023).

22. Трудовой кодекс Российской Федерации : федер. закон от 30 декаб. 2001 г. № 197-ФЗ по сост. на 2 июля 2021 г. [Электронный ресурс] «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_75545/ac2912085b2f68971c7dc84be6ccb 8a5291f10f5/#dst100106 (дата обращения 23.03.2022).

23. Уголовно-исполнительный кодекс Российской Федерации : федер. закон принят Гос. Думой 18 декаб. 1996 г. № 1-ФЗ по сост. на 29 декаб. 2022 г. [Электронный ресурс] «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_75545/ac2912085b2f68971c7dc84be6ccb 8a5291f10f5/#dst100106 (дата обращения 23.03.2022).

24. Уголовно-процессуальный кодекс Российской Федерации [федер. Закон: принят Гос. Думой 22 ноября 2001 г.: по состоянию на 25 ноября 2013 г.]. М.: Собрание законодательства Российской Федерации, 2001. № 52. ст. 4921.

REFERENCES

1. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh (vypiska): Utverzhdena zamestitelem direktora FSTEHK Rossii 15 fevralya 2008 g. [Ehlektronnyi resurs] FSTEHK Rossii. Available from: https://bdu.fstec.ru/documents/16 [Accessed 25 March 2023].

2. Bank dannykh ugroz bezopasnosti informatsii [Ehlektronnyi resurs] FSTEHK Rossii. Available from: https://bdu.fstec.ru/threat [Accessed 25 March 2023].

3. GOST R ISO/MEHK 27001-2006 “Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti [Ehlektronnyi resurs] Sistemy menedzhmenta informatsionnoi bezopasnosti”: data vvedeniya 2008-02-01 (nedeistvuyushchii). Available from: https://docs.cntd.ru/document/1200058325 [Accessed 24 March 2023].

4. Kodeks Rossiiskoi Federatsii ob administrativnykh pravonarusheniyakh [feder. Zakon: prinyat Gos. Dumoi 20 dekabrya 2001 g.: po sostoyaniyu na 2 oktyabrya 2018 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2002. No. 1 (chast' I). St. 1.

5. Konstitutsiya: Osn. Zakon Ros. Federatsii ot 12 dek. 2003 g. [Ehlektronnyi resurs] Konsul'taTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_28399/ [Accessed 5 April 2023].

6. Metodika otsenki ugroz bezopasnosti informatsii: Metodicheskii dokument. utverzhden FSTEHK Rossii 5 fevr. 2021 g. [Ehlektronnyi resurs] FSTEHK Rossii. Rezhim dostupa: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5- fevralya-2021 [Accessed 30 March 2023].

7. Ob advokatskoi deyatel'nosti i advokature v Rossiiskoi Federatsii: feder. zakon prinyat Gos. Dumoi 26 apr. 2002 g. № 63-FZ: po sostoyaniyu na 10 noyab. 2022 g. [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_36945// [Accessed 1 April 2023].

8. Ob Arkhivnom dele v Rossiiskoi Federatsii [feder. zakon: prinyat Gos. Dumoi 1 oktyabrya 2004 g.: po sostoyaniyu na 28 dekabrya 2017 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2004. No. 43. St. 4169.

9. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: feder. zakon prinyat Gos. Dumoi 8 iyulya 2006 g. No. 149-FZ: po sostoyaniyu na 27 iyulya 2006 g. [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_61798/ [Accessed 1 April 2023].

10. Ob ispolnitel'nom proizvodstve: feder. zakon prinyat Gos. Dumoi 14 sentyab. 2007 g. No. 229-FZ: po sostoyaniyu na 29 dekab. 2022 g. [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: https://www.consultant.ru/document/cons_doc_LAW_71450/ [Accessed 1 April 2023].

11. Ob obespechenii dostupa k informatsii o deyatel'nosti sudov v Rossiiskoi Federatsii [feder. zakon: prinyat Gos. Dumoi 10 dekabrya 2008 g.: po sostoyaniyu na 28 dekabrya 2017 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2008. No. 32. St. 6217.

12. Ob osnovakh okhrany zdorov'ya grazhdan Rossiiskoi Federatsii: feder. zakon prinyat Gos. Dumoi 1 noyab. 2011 g. No. 323-FZ: po sostoyaniyu na 19 dekab. 2022 g. [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: https://www.consultant.ru/document/cons_doc_LAW_121895/ [Accessed 1 April 2023].

13. Ob utverzhdenii perechnya svedenii konfidentsial'nogo kharaktera [ukaz Prezidenta: utverzhden Prezidentom 6 mata 1997 g.: po sostoyaniyu na 13 iyulya 2015 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 1997. № 188. St. 1127.

14. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Prikaz FSTEHK Rossii ot 18 fevr. 2013 g. No. 21. [Ehlektronnyi resurs] Available from: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 [Accessed 19 March 2023].

15. Ob utverzhdenii trebovanii k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh utv. Postanovleniem Pravitel'stva RF 1 noyab. 2012 g. № 1119. [Ehlektronnyi resurs] Available from: http://www.consultant.ru/document/cons_doc_LAW_137356/ [Accessed 8 April 2023].

16. O gosudarstvennoi zashchite poterpevshikh, svidetelei i inykh uchastnikov ugolovnogo sudoproizvodstva: feder. zakon prinyat Gos. Dumoi 31 iyulya 2004 g. No. 119-FZ: po sostoyaniyu na 1 iyulya 2021 g. – [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_48959/ [Accessed 1 April 2023].

17. O gosudarstvennoi zashchite sudei, dolzhnostnykh lits pravookhranitel'nykh i kontroliruyushchikh organov: feder. zakon prinyat Gos. Dumoi 22 marta 1995 g. No. 45-FZ: po sostoyaniyu na 1 iyulya 2021 g. – [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_6425/ [Accessed 1 April 2023].

18. O gosudarstvennoi taine: zakon RF: prinyat Gos. Dumoi 21 iyulya 1993 g.: po sostoyaniyu na 9 marta 2021 g.]. [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_2481/ [Accessed 21 April 2023].

19. O personal'nykh dannykh [Feder. zakon: prinyat Gos. Dumoi 8 iyulya 2006 g.: po sostoyaniyu na 25 noyabrya 2009 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2006. № 31. CH. 1. St. 3451.

20. O svyazi [Feder. zakon: prinyat Gos. Dumoi 18 iyunya 2003 g.: po sostoyaniyu na 3 avgusta 2018 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2003. No. 28. St. 2895.

21. Osnovy zakonodatel'stva Rossiiskoi Federatsii o notariate: zakon utv. VS RF 11.02.1993 № 4462-1: po sostoyaniyu na 28 dekab 2022 g. [Ehlektronnyi resurs] Konsul'tanTPlyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_1581/ [Accessed 1 April 2023].

22. Trudovoi kodeks Rossiiskoi Federatsii: feder. zakon ot 30 dekab. 2001 g. № 197-FZ po sost. na 2 iyulya 2021 g. [Ehlektronnyi resurs] Konsul'tant Plyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_75545/ac2912085b2f68971c7dc84be6ccb 8a5291f10f5/#dst100106 [Accessed 23 March 2023].

23. Ugolovno-ispolnitel'nyi kodeks Rossiiskoi Federatsii: feder. zakon prinyat Gos. Dumoi 18 dekab. 1996 g. No. 1-FZ po sost. na 29 dekab. 2022 g. [Ehlektronnyi resurs] Konsul'tant Plyus. Available from: http://www.consultant.ru/document/cons_doc_LAW_75545/ac2912085b2f68971c7dc84be6ccb 8a5291f10f5/#dst100106 [Accessed 23 March 2023].

24. Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii [feder. Zakon: prinyat Gos. Dumoi 22 noyabrya 2001 g.: po sostoyaniyu na 25 noyabrya 2013 g.]. M.: Sobranie zakonodatel'stva Rossiiskoi Federatsii, 2001. No. 52. St. 4921.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Елена Александровна Овчинникова – кандидат юридических наук, доцент кафедры защиты информации в социальных системах, Институт безопасности, Сибирский государственный университет телекоммуникаций и информатики, ул. Кирова, 86, г. Новосибирск, 630102, 9538685137@mail.ru

Елена Анатольевна Семенова – кандидат технических наук, доцент, декан факультета инновационной инженерии и технологии гостеприимства, Пятигорский институт (филиал), Северо-Кавказский федеральный университет

Валентина Викторовна Цаплева – кандидат технических наук, доцент, заведующий кафедрой систем управления и информационных технологий, Пятигорский институт (филиал) Северо-Кавказский федеральный университет

INFORMATION ABOUT THE AUTHORS

Elena A. Ovchinnikova – Associate Professor, Siberian State University of telecommunications and Information Science, 86, Kirov St., Novosibirsk, Russia, 9538685137@mail.ru

Elena A. Semenova – Cand. Sci. (Techn.), Associate Professor, Dean of the Faculty of Innovative Engineering and Hospitality Technology, Pyatigorsk Institute (branch), North Caucasus Federal University, Pyatigorsk, Russia

Valentina V. Tsapleva – Cand. Sci. (Techn.), Associate Professor, Head of the Department of Management Systems and Information Technologies, Pyatigorsk Institute (branch), North Caucasus Federal University, Pyatigorsk, Russia

Вклад авторов: все авторы внесли равный вклад в подготовку публикации.
Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.
Conflict of interest: the authors declare no conflicts of interests.

Статья поступила в редакцию: 28.09.2023;
одобрена после рецензирования: 17.11.2023;
принята к публикации: 08.12.2023.

The article was submitted: 28.09.2023;
approved after reviewing: 17.11.2023;
accepted for publication: 08.12.2023.