САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ

САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

Сборник трудов

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпуск 11

Санкт-Петербург
2022

УДК (002:681):338.98

Р32

Региональная информатика и информационная безопасность.

Р32 Сборник трудов. Выпуск 11 / СПОИСУ. – СПб., 2022. – 645 с.

ISBN 978-5-00182-048-2

В сборник включены статьи участников Санкт-Петербургской международной конференции «Региональная информатика» и Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», проведенных при поддержке Правительства Санкт-Петербурга, объединенных в рубрики: Государственная политика в сфере информатизации и информационной безопасности; Теоретические проблемы информатики и информатизации; Телекоммуникационные сети и технологии; Информационная безопасность; Правовые аспекты информатизации и информационной безопасности; Информационно-психологическая безопасность; Информационные технологии на транспорте; Информационные технологии в образовании, Информационные технологии в медицине и здравоохранении; Информационные технологии в экологии; Информационные технологии управления объектами морской техники и морской инфраструктуры, Информационные технологии в дизайне, печати и медиаиндустрии; Информационные технологии в социокомпьютинге; Информационные технологии в критических инфраструктурах; Молодежная научная школа «интеллектуальные безопасные информационные системы и технологии».

Сборник статей предназначен для широкого круга руководителей и специалистов органов государственной власти и местного самоуправления, промышленности, науки, образования, бизнеса, аспирантов и студентов высших учебных заведений, специализирующихся в вопросах информатизации, связи, информационной безопасности и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

ISBN 978-5-00182-048-2

Публикуется в авторской редакции

Подписано в печать 30.11.2022. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 74,5. Тираж 400 экз. Заказ № 17956
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-048-2

ST. PETERSBURG INTERREGIONAL CONFERENCE
INFORMATION SECURITY OF RUSSIAN REGIONS

ST. PETERSBURG INTERNATONAL CONFERENCE
REGIONAL INFORMATICS

Proceedings

REGIONAL INFORMATICS AND INFORMATION SECURITY

The Issue No 11

St. Petersburg
2022

УДК 004.056

НОРМАТИВНО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Сторожик Виктор Сергеевич
Арктический и антарктический научно-исследовательский институт
Беринга, ул., 38, Санкт-Петербург, 199397, Россия
e-mail: vstorozhik@yandex.ru

Аннотация. В статье рассматриваются особенности реализации требований международного законодательства, нормативных правовых актов Российской Федерации, нормативных правовых актов и методических документов Роскомнадзора России, ФСБ России и ФСТЭК России, определяющих порядок обеспечения безопасности персональных данных при их обработке в информационных системах.

Ключевые слова: безопасность; защита; информация; информационная система; информационная технология; категория персональных данных; норма; оператор; меры защиты; персональные данные; право; система безопасности; средства защиты; угроза безопасности информации; уровень защищенности.

REGULATORY AND METHODOLOGICAL SUPPORT OF PERSONAL DATA SECURITY DURING THEIR PROCESSING IN INFORMATION SYSTEMS

Storozhik Viktor
Arctic and Antarctic Research Institute
38 Bering St, St. Petersburg, 199397, Russia
e-mail: vstorozhik@yandex.ru

Abstract. The article discusses the specifics of the implementation of the requirements of international legislation, regulatory legal acts of the Russian Federation, regulatory legal acts and methodological documents of Roskomnadzor of Russia, the FSB of Russia and the FSTEC of Russia, which determine the procedure for ensuring the security of personal data during their processing in information systems.

Keywords: security; protection; information; information system; information technology; category of personal data; norm; operator; protection measures; personal data; law; security system; means of protection; threat to information security; security level.

Введение. Доктрина информационной безопасности Российской Федерации к основным национальным интересам в информационной сфере относит защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем [1].

В Стратегии национальной безопасности Российской Федерации отмечено, что использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российский информационных ресурсов к воздействию из-за рубежа, и поставлена задача обеспечения защиты конституционных прав и свобод человека и гражданина при обработке персональных данных [2].

В докладе Президента Российской Федерации на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» подчеркнуто, что принципиально важно свести на нет риски утечек конфиденциальной информации и персональных данных граждан [3].

Правоотношения в области обеспечения безопасности персональных данных (ПДн) регулируются российским и международным законодательством.

В соответствии со ст. 15 Конституции Российской Федерации общепризнанные принципы и нормы международного права, и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора [4].

Первый международный нормативный правовой акт в области обеспечения безопасности ПДн «Основные положения Организации по экономическому сотрудничеству и развитию о защите неприкосновенности частной жизни и международных обменов ПДн» был принят в 1980 г. [5]. В нем зафиксированы общие принципы (вытекающие из необходимости защиты прав и свобод граждан), на которых должно основываться национальное законодательство о ПДн, а также установлены барьеры, препятствующие неконтролируемому международному обороту ПДн. Документ распространял свое действие лишь на незначительное число развитых стран, присоединившихся к Организации по экономическому сотрудничеству и развитию.

Для существенного расширения состава стран-участниц в области обеспечения безопасности ПДн в 1981 г. была принята «Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» (Конвенция) [6]. В ней были заложены международные законодательные основы обработки ПДн: использование ПДн только для определенных целей и в пределах определенных сроков, неизбыточность и актуальность обрабатываемых ПДн и особенности их трансграничной передачи, обеспечение защиты ПДн, гарантированные права гражданина - обладателя личных данных.

В последующие годы был принят ряд международных нормативных правовых актов, уточняющих и дополняющих положения Конвенции:

1. В 1990 году Генеральной ассамблеей ООН было принято «Руководство ООН относительно компьютерных файлов ПДн», которое частично дублирует положения Конвенции и ориентировано на страны «третьего мира» [7].

2. Директива 95/46/ЕС Европейского парламента и Совета Европейского союза 1995 г. О защите прав частных лиц применительно к обработке ПДн и о свободном движении таких данных [8], которая содержит нормы, обязательные к применению в национальных законодательствах стран-членов Евросоюза. Принципы и нормы защиты прав и свобод частных лиц, в особенности право на частную жизнь, содержащиеся в ней, закрепляют и усиливают принципы, содержащиеся в Конвенции. При этом, директива не определяет какие конкретно технические решения следует использовать для защиты ПДн и предоставляет странам-членам Евросоюза право для самостоятельного регулирования.

3. Директива 97/66/ЕС Европейского парламента и Совета Европейского союза 1997 г. [9], регулирующая использование ПДн и защиту неприкосновенности частной жизни в сфере телекоммуникаций. Ее положения уточняют и дополняют директиву 95/46/ЕС, и направлены на обеспечение свободной передачи ПДн при обеспечении защиты частной жизни.

В директивах [8, 9] определено, что юридические, нормативные и технические требования, выдвигаемые в целях обеспечения защиты ПДн, прав частных лиц и законных интересов юридических лиц, должны быть четко сбалансированы и не должны создавать помех для развития рынка.

4. Генеральный (общий) регламент о защите ПДн (General Data Protection Regulation, GDPR). В октябре 2018 г. странами-участницами был подписан Протокол № 223 о внесении изменений в Конвенцию [10],

который в соответствии с вызовами текущего времени актуализировал Конвенцию в части защиты биометрических и генетических данных, новых прав физических лиц в контексте алгоритмического принятия решений искусственным интеллектом, требований защиты данных уже на этапе проектирования информационных систем, обязанности операторов ПДн уведомлять уполномоченный надзорный орган об утечках данных. Гражданам предоставлена возможность получать квалифицированную помощь надзорного органа по вопросам защиты их ПДн.

Российская Федерация подписала Конвенцию в 2001 г. и ратифицировала её в 2005 г. [11]. На основании 4-й статьи Конвенции был принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [12], который дублировал основные положения Конвенции, а также вносил ряд дополнительных требований по обработке ПДн.

С учетом возникающих вызовов в 2011 г. в 152-ФЗ были внесены существенные изменения базовых положений о защите ПДн [13], а в 2014 г. - требования о запрете первичной обработки ПДн за пределами территории Российской Федерации [14].

Государственная Дума Российской Федерации 24 мая 2022 г. приняла в первом чтении законопроект [15], которым предусматриваются дополнительные меры по защите ПДн, обязывающие операторов ПДн незамедлительно сообщать в уполномоченные органы обо всех кибератаках и утечках, а также информировать соответствующие органы о намерении передачи ПДн за рубеж, устанавливающие прямой запрет отказывать гражданам в оказании услуг, если они не готовы предоставить свои ПДн, ограничивающие обработку биометрических ПДн несовершеннолетних и совершенствующие порядок трансграничной передачи ПДн. Также законопроектом предусмотрена экстерриториальность применения российского законодательства о ПДн и устанавливается возможность вмешательства уполномоченных органов власти в вопросы обеспечения безопасности обработки ПДн российских граждан на территории других государств.

Уполномоченным органом Российской Федерации по защите прав субъектов ПДн является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), подведомственная Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) [16].

В соответствии со статьей 19 152-ФЗ операторы информационной системы персональных данных (ИСПДн) обязаны принимать необходимые правовые, организационные и технические меры для защиты ПДн, при этом обеспечение безопасности ПДн достигается:

1) Определением угроз безопасности ПДн при их обработке в ИСПДн;

2) Применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

3) Использованием прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (СЗИ);

4) Оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

5) Учетом машинных носителей ПДн;

6) Обнаружением фактов несанкционированного доступа к ПДн и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;

7) Восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) Регламентацией правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

9) Контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

В рамках реализации требований части 3 статьи 19 152-ФЗ Правительством Российской Федерации установлены:

1) Уровни защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных [17];

2) Требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн [17];

3) Требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн [18].

Всего установлено четыре уровня защищенности ПДн, которые зависят: от типа угроз, актуальных для ИСПДн; категории обрабатываемых ПДн; количества обрабатываемых ПДн и принадлежности этих ПДн сотрудникам оператора.

Выделяют три типа угроз:

Угрозы 1-го типа актуальны для ИС, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИС.

Угрозы 2-го типа актуальны для ИС, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИС.

Угрозы 3-го типа актуальны для ИС, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИС.

Выделяются следующие категории ПДн: специальные, биометрические, общедоступные, иные.

По количеству ПДн субъектов выделяют случаи, когда производится обработка более чем 100 000 субъектов ПДн и менее чем 100 000 субъектов ПДн.

Требования к защите ПДн зависят от уровня защищенности ПДн.

Всего установлено восемь требований: от четырех - у четвертого уровня защищенности до восьми - у первого уровня защищенности.

Таким образом, в ИСПДн любого уровня защищенности ПДн необходимо реализовать следующие требования:

1. Организацию режима обеспечения безопасности помещений, в которых размещена ИС, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

2. Обеспечение сохранности носителей ПДн;

3. Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей;

4. Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Контроль выполнения требования к защите ПДн при их обработке в ИСПДн осуществляет оператор (самостоятельно или с привлечением организаций, имеющих лицензию ФСТЭК России на оказание услуг по технической защите конфиденциальной информации) не реже 1 раза в 3 года.

Система защиты персональных данных ИСПДн должна использовать меры, необходимые для выполнения требований к защите ПДн для установленного уровня защищенности ПДн.

В соответствии с нормами части 4 статьи 19 152-ФЗ эти меры устанавливают в пределах своих полномочий ФСТЭК России (обеспечение безопасности ПДн не криптографическими мерами) и ФСБ России (обеспечение безопасности ПДн при использовании криптографических методов защиты информации) [19, 20].

Приказом ФСТЭК России от 17 февраля 2013 г. № 21 утверждены Состав и содержание конкретных организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн для обеспечения соответствующего уровня защищенности ПДн [21]. Это позволяет оператору ПДн выполнить требование части 1 статьи 19 152-ФЗ об обязанности принимать необходимые правовые, организационные и технические меры при обработке ПДн или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним и неправомерных действий в отношении ПДн.

В приказе № 21 выделены следующие группы мер:

- Идентификация и аутентификация субъектов доступа и объектов доступа;
- Управление доступом субъектов доступа к объектам доступа;
- Ограничение программной среды;
- Защита машинных носителей ПДн;
- Регистрация событий безопасности;
- Антивирусная защита;
- Обнаружение вторжений;
- Контроль (анализ) защищенности ПДн;
- Обеспечение целостности ИС и ПДн;
- Обеспечение доступности ПДн;
- Защита среды виртуализации;
- Защита технических средств;
- Защита ИС, ее средств, систем связи и передачи данных;
- Выявление инцидентов и реагирование на них;
- Управление конфигурацией ИС и системы защиты ПДн.

При этом состав и содержание каждой меры с учетом обеспечиваемых уровней защищенности ПДн приводится в приложении к приказу № 21 [21]. В приложении к приказу № 21 также приводятся наборы базовых мер, которые необходимы для применения в определенных уровнях защищенности ПДн, а также набор дополнительных мер, которые оператор может выбирать по своему усмотрению.

Приказом №21 предусмотрен следующий алгоритм выбора и применения мер для обеспечения безопасности ПДн:

1. Формируется базовый набор мер для обеспечения заданного уровня защищенности ПДн в соответствии с базовыми наборами мер, приведенными в приложении для установленного уровня защищенности ПДн в рассматриваемой системе;

2. Производится адаптация базового набора мер, предполагающая исключение нерелевантных «базовых» мер в зависимости от особенностей структурно-функциональных характеристик ИС и использующихся информационных технологий;

3. Уточняется адаптированный базовый набор мер путем включения в набор мер, не определенных как базовые, но обеспечивающих нейтрализацию актуальных угроз безопасности ПДн, или исключение из адаптированного набора мер в случае отсутствия соответствующих актуальных угроз;

4. Осуществляется дополнение уточненного адаптированного базового набора мерами, установленными иными применимыми нормативными правовыми актами в области защиты информации. Приказ в пункте 10 содержит важное замечание о возможности оператора применять компенсирующие меры при невозможности технической реализации или экономической нецелесообразности применения мер из базового набора, что предоставляет определенную гибкость при выборе новых и обосновании использования уже внедренных СЗИ для обеспечения безопасности ПДн.

Если защищаемая ИСПДн является государственной информационной системой (ГИС), то меры по обеспечению безопасности ПДн должны приниматься в соответствии с требованиями приказа ФСТЭК России от 11 февраля 2013 г. № 17 [22].

Приказ № 17 устанавливает требования к обеспечению безопасности информации ограниченного доступа в ГИС, при этом в п. 5 подчеркивается, что при обработке ПДн в ГИС следует руководствоваться требованиями, установленными Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 [17]. Приказ обязывает операторов ГИС использовать только сертифицированные СЗИ и проводить аттестацию ГИС на соответствие требованиям по защите информации. Данный документ предполагает выполнение операторами следующих мероприятий для обеспечения защиты информации: формирование требований к защите информации; разработка, внедрение и аттестация системы защиты информации ИС; обеспечение защиты информации в ходе эксплуатации ИС и при выводе ИС из эксплуатации [22]. Кроме Приказа № 17 при реализации соответствующих мер защиты информации также необходимо руководствоваться методическим документом ФСТЭК России «Меры защиты информации в государственных информационных системах», в котором более детально раскрываются состав и содержание мер [23].

Если защищаемая ИСПДн является значимым объектом критической информационной инфраструктуры [24, 25], то меры по обеспечению безопасности должны приниматься в соответствии с требованиями приказа ФСТЭК России от 25 декабря 2017 г. № 239 [26]. А затем дополняться мерами, которые предусмотрены в соответствии с приказом ФСТЭК России от 17 февраля 2013 г. № 21.

Для определения угроз безопасности ПДн при их обработке в ИСПДн оператору следует опираться на следующие методические документы ФСТЭК России:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [27];

2. Методика оценки угроз безопасности информации [28].

ФСБ России во исполнение части 4 статьи 19 152-ФЗ приказом от 10 июля 2014 г. № 378 утвержден Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации (СКЗИ), необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности [29].

Методические рекомендации ФСБ России по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 г., предназначены для государственных органов и операторов, использующих СКЗИ и разрабатывающих соответствующие модели угроз [30].

Операторам ИСПДн также необходимо руководствоваться методическими документами ФСБ России:

1. Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных [31];

2. Методическими рекомендациями по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации [32].

В соответствии с частью 5 статьи 19 152-ФЗ на уровне субъектов Российской Федерации, в федеральных органах исполнительной власти, Банке России, должны быть разработаны нормативные правовые акты и определены актуальные угрозы безопасности ПДн.

Указанные требования были реализованы Банком России, рядом федеральных органов исполнительной власти и внебюджетных государственных фондов. Действует стандарт Банка России отраслевого применения СТО БР ИББС-1.0-2010 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения [33], в котором предъявлены требования по обработке и обеспечению безопасности ПДн в соответствии с отраслевой моделью. В Минцифры России применяются: Модель угроз и нарушителя безопасности ПДн, обрабатываемых в типовых ИСПДн отрасли [34] и Модель угроз и нарушителя безопасности ПДн, обрабатываемых в специальных ИСПДн отрасли, в Министерстве здравоохранения Российской Федерации используется Модель угроз типовой медицинской ИС типового лечебно-профилактического учреждения [35].

В соответствии с частью 7 статьи 19 152-ФЗ Правительством Российской Федерации от утверждены Правила согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности ПДн, актуальных при обработке ПДн в ИСПДн, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с ФСБ России и ФСТЭК России [36].

В рамках обеспечения работ по методическому руководству при разработке нормативных правовых актов определяющих угрозы безопасности персональных данных в органах государственной власти субъектов Российской Федерации территориальные органы ФСТЭК России (управления по федеральным округам) обеспечивают рассмотрение на предмет соответствия требованиям законодательства Российской Федерации об информации, информационных технологиях, и о защите информации, а также законодательства о ПДн, поступивших в их адрес проектов нормативных правовых актов с приложением пояснительной записки, в которой обосновывается актуальность угроз ПДн - в виде модели угроз и описания ИС, оказывают методическую помощь разработчикам и в течение 10 дней с даты регистрации направляют в центральный аппарат ФСТЭК России результаты проведенного анализа и предложения о возможности согласования представленных проектов нормативных правовых актов.

В соответствии с частью 3 статьи 18.1 152-ФЗ постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 утвержден Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, который определяет первоочередные мероприятия при обработке ПДн и содержит перечень организационно-распорядительных документов, которые следует разрабатывать операторам [37].

Постановлением Правительства от 15 сентября 2008 г. № 687 утверждено Положение об особенностях обработки ПДн, осуществляемой без использования средств автоматизации, в котором дано определение понятия «обработка персональных данных, осуществляемая без использования средств автоматизации», а также указаны особенности организации такой обработки и меры по обеспечению безопасности при обработке ПДн без использования средств автоматизации [38].

Цель и особенности обработки ПДн государственных гражданских служащих регламентируются Указом Президента Российской Федерации 30 мая 2005 г. № 609 [39].

Операторам ИСПДн при обеспечении безопасности ПДн также необходимо руководствоваться требованиями нормативных правовых актов Роскомнадзора [40-44].

Заключение. Таким образом, выполнение требований международного законодательства, нормативных правовых актов Российской Федерации, нормативных правовых актов и методических документов Роскомнадзора России, ФСБ России и ФСТЭК России, определяющих порядок обеспечения безопасности персональных данных при их обработке в информационных системах, позволяет операторам информационных систем персональных данных решить задачу обеспечения защиты конституционных прав и свобод человека и гражданина при обработке персональных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства».
4. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.).
5. Основные положения Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональных данных, 1980.
6. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.).
7. Руководство ООН относительно компьютерных файлов персональных данных (принято Генеральной Ассамблеей ООН 14 декабря 1990 г.).
8. Директива 95/46/ЕС Европейского парламента и Совета Европейского союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (Страсбург, 24 октября 1995 г.).
9. Директива 97/66/ЕС Европейского парламента и Совета Европейского союза о использовании персональных данных и защите неприкосновенности частной жизни в сфере телекоммуникаций (Страсбург, 15 декабря 1997 г.).
10. Протокол № 223 о внесении изменений в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 18 октября 2018 г.).
11. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

12. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
13. Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных».
14. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных».
15. Законопроект № 101234-8 «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных».
16. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
17. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
18. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
19. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 (ред. от 08 декабря 2021 г.) «Вопросы Федеральной службы по техническому и экспортному контролю».
20. Указ Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации» (с изменениями и дополнениями).
21. Приказ ФСТЭК России от 17 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
23. Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11 февраля 2014 г.
24. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
25. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
26. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60).
27. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 15 февраля 2008 г.
28. Методика оценки угроз безопасности информации, утверждена ФСТЭК России 5 февраля 2021 г.
29. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности».
30. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432.
31. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.
32. Методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены 8 Центром ФСБ России 21 февраля 2008 г. № 149/54-144.
33. Стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0.
34. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли, одобрена решением секции № 1 научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2.
35. Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения, Минздравсоцразвития России, 2009.
36. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № 940 «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю».
37. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
38. Постановление Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
39. Указ Президента Российской Федерации 30 мая 2005 г. № 609 «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
40. Приказ от 19 августа 2011 г. № 706 «Об утверждении рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».
41. Приказ от 20 июня 2012 г. № 621 «О консультативном совете при уполномоченном органе по защите прав субъектов персональных данных».
42. Приказ от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».
43. Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
44. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденные 13 декабря 2013 г.