ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

УЦСБ

УЖЕСТОЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ 152-ФЗ

Инструкция для операторов ПДн

cybersec@ussc.ru

+7 (343) 379-98-34

sec.ussc.ru

Ужесточение ответственности за нарушение 152-ФЗ: инструкция для операторов ПДн

30 ноября был опубликован Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (далее – 420-ФЗ), который предусматривает увеличение штрафов за правонарушения, связанные с обработкой персональных данных (далее – ПДн), а также впервые вводит оборотные штрафы за утечки ПДн. Внесенные изменения вступят в силу 30.05.2025.

Какие составы правонарушений были введены? Как не нарушить требования Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – 152-ФЗ)? И что операторы ПДн могут сделать уже сейчас?

Отвечая на эти вопросы, мы подготовили инструкцию с рекомендациями для операторов ПДн по недопущению правонарушений и минимизации комплаенс и финансовых рисков.

Инструкция рекомендована к применению операторам ПДн: индивидуальным предпринимателям, юридическим лицам, государственным, муниципальным органам, которые организуют или осуществляют обработку ПДн самостоятельно или с привлечением других лиц (п.2 ст.3 152-ФЗ).

Перечень принятых сокращений

КоАП РФ	–	Кодекс об административных правонарушениях Российской Федерации
420-ФЗ	–	Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»
152-ФЗ	–	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Приказ ФСБ России № 77	–	Приказ Федеральной службы безопасности Российской Федерации от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»
ГосСОПКА	–	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Госуслуги	–	Портал государственных услуг Российской Федерации

Идентификатор	–	Уникальное обозначение сведений о физическом лице, необходимое для определения такого лица
КИИ	–	Критическая информационная инфраструктура
НКЦКИ	–	Национальный координационный центр по компьютерным инцидентам
ОГРН	–	Основной государственный регистрационный номер
ПДн	–	Персональные данные
Роскомнадзор	–	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
ФСБ России	–	Федеральная служба безопасности Российской Федерации

Основные определения

Биометрические ПДн – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн.

Выручка оператора – совокупность размера суммы выручки, полученной от реализации всех товаров (работ, услуг), за календарный год, предшествующий году, в котором было выявлено административное правонарушение[1].

Идентификатор – это уникальные обозначения сведений о физических лицах, необходимых для определения таких лиц, т.е. любая запись в базе данных, прямо или косвенно относящаяся к субъекту ПДн.

Обработка ПДн – это любое действие с ПДн: сбор, запись, хранение, накопление, распространение и иные операции.

Операторы ПДн – это любые организации, которые обрабатывают ПДн и определяют цели их обработки, состав необходимых для обработки ПДн и операции, совершаемые с ПДн.

ПДн – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Специальные категории ПДн – это данные касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости.

Утечка ПДн – это неправомерная передача (предоставление, распространение, доступ) ПДн лицам, не имеющим разрешения на доступ.

[1] либо за предшествующую дате выявленного административного правонарушения часть календарного года, в котором было выявлено административное правонарушение, если правонарушитель не осуществлял деятельность по реализации товаров (работ, услуг) в предшествующем календарном году

Ответственность за правонарушения

Принятые изменения уточняют составы правонарушений в рамках требований 152-ФЗ. В таблицах 1 и 2 мы привели краткую информацию о суммах возможных штрафов за такие правонарушения.

Таблица 1 – ужесточение действующих норм

№ п/п	Норма	Содержание нарушения	Для кого	Было (рублей)	Стало (рублей)
1	ч. 1 ст. 13.11	Обработка ПДн в случаях, не предусмотренных законодательством РФ в области ПДн, либо обработка ПДн, несовместимая с целями сбора	Граждане	2 тыс. – 6 тыс.	10 тыс. – 15 тыс.
			Должностные лица	10 тыс. – 20 тыс.	50 тыс. – 100 тыс.
			Юридические лица	60 тыс.– 100 тыс.	150 тыс. – 300 тыс.
2	ч. 1.1. ст. 13.11	Повторное совершение административного правонарушения, предусмотренного ч. 1 ст. 13.11	Граждане	4 тыс. – 12 тыс.	15 тыс. – 30 тыс.
			Должностные лица	10 тыс. – 50 тыс. 50 тыс. – 100 тыс. (для ИП)	100 тыс. – 200 тыс.
			Юридические лица	100 тыс. – 300 тыс.	300 тыс. – 500 тыс.

Таблица 2 – новые нормы

№ п/п	Норма	Содержание нарушения	Для кого	Стало (рублей)
1	ч. 10 ст. 13.11	Невыполнение и (или) несвоевременное выполнение оператором обязанности по уведомлению Роскомнадзора о намерении осуществлять обработку ПДн	Граждане	5 тыс. – 10 тыс.
			Должностные лица	30 тыс. – 50 тыс.
			Юридические лица	100 тыс. – 300 тыс.
2	ч. 11 ст. 13.11	Невыполнение и (или) несвоевременное выполнение оператором обязанности по уведомлению Роскомнадзора в случае установления факта неправомерной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн	Граждане	50 тыс. – 100 тыс.
			Должностные лица	400 тыс. – 800 тыс.
			Юридические лица	1 млн. – 3 млн.
3	ч. 12 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн в объеме: – от 1 тыс. до 10 тыс. субъектов ПДн, – от 10 тыс. до 100 тыс. идентификаторов	Граждане	100 тыс. – 200 тыс.
			Должностные лица	200 тыс. – 400 тыс.
			Юридические лица	3 млн. – 5 млн.
4	ч. 13 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн в объеме: – от 10 тыс. до 100 тыс. субъектов ПДн, – от 100 тыс. до 1 млн. идентификаторов	Граждане	200 тыс. – 300 тыс.
			Должностные лица	300 тыс. – 500 тыс.
			Юридические лица	5 млн. – 10 млн.

5	ч. 14 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн в объеме: – более 100 тыс. субъектов ПДн, – более 1 млн. идентификаторов	Граждане	300 тыс. – 400 тыс.
			Должностные лица	400 тыс. – 600 тыс.
			Юридические лица	10 млн. – 15 млн.
6	ч. 15 ст. 13.11	Совершение административного правонарушения, предусмотренного ч. 12-14 ст. 13.11, лицами, которые ранее уже привлекались в соответствии с ч. 12-15, 16-18 ст. 13.11 Кодекса об административных правонарушениях (далее – КоАП РФ) за действия (бездействие), повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн	Граждане	400 тыс. – 600 тыс.
			Должностные лица	800 тыс. – 1,2 млн.
			Юридические лица	**от 1% до 3%**[2], но не менее 20 млн. и не более 500 млн.
7	ч. 16 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей **специальные категории** ПДн	Граждане	300 тыс. – 400 тыс.
			Должностные лица	1 млн. – 1,3 млн.
			Юридические лица	10 млн. – 15 млн.
8	ч. 17 ст. 13.11	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей **биометрические категории** ПДн	Граждане	400 тыс. – 500 тыс.
			Должностные лица	1,3 млн. – 1,5 млн.
			Юридические лица	15 млн. – 20 млн.
9	ч. 18 ст. 13.11	Совершение административного правонарушения, предусмотренного ч. 16 или 17 ст. 13.11, лицом, которое ранее уже привлекалось в соответствии с ч. 12-18 ст.13.11 КоАП РФ к административной ответственности	Граждане	500 тыс.– 800 тыс.
			Должностные лица	1,5 млн. – 2 млн.
			Юридические лица	**от 1% до 3%**[2], но не менее 25 и не более 500 млн.

Более подробно об изменениях читайте в статье на сайте УЦСБ.

Рекомендации

Далее в этой инструкции рассмотрим детально, что нужно делать операторам ПДн, чтобы не допустить правонарушений, предусмотренных введенными изменениями.

1. Операторы, подайте уведомление об обработке ПДн!

Принятые изменения (ч. 10 статьи 13.11 КоАП РФ) устанавливают административный штраф до 300 тыс. руб. за невыполнение и (или) несвоевременное выполнение оператором обязанности по уведомлению Роскомнадзора о намерении осуществлять обработку ПДн, предусмотренной ч. 1 ст. 22 152-ФЗ.

2 от совокупного размера суммы выручки, полученной от реализации всех товаров (работ, услуг), за календарный год, предшествующий году, в котором было выявлено административное правонарушение либо за предшествующую дате выявленного административного правонарушения часть календарного года, в котором было выявлено административное правонарушение, если правонарушитель не осуществлял деятельность по реализации товаров (работ, услуг) в предшествующем календарном году.

Напомним, что уведомлять Роскомнадзор не нужно, если оператор осуществляет обработку ПДн:

- без использования средств автоматизации;
- в случаях, предусмотренных законодательством о транспортной безопасности;
- включенных в государственные автоматизированных информационные системы или в государственные информационные системы ПДн, созданные в целях защиты безопасности государства и общественного порядка.

В иных случаях необходимо подать уведомление о намерении осуществлять обработку ПДн для включения в Реестр операторов ПДн. Направить уведомление в Роскомнадзор можно одним из следующих способов:

- в бумажном виде;
- в электронном виде с использованием усиленной квалифицированной электронной подписи;
- в электронном виде с использованием средств аутентификации Портала государственных услуг Российской Федерации (далее – Госуслуг).

***Важно**: уведомлять Роскомнадзор необходимо не только о начале обработки ПДн, но и об изменениях в порядке обработки или о ее прекращении (в течение 10 рабочих дней с даты внесения изменений или прекращения обработки) (ч.7 ст.22 152-ФЗ). Формы уведомлений представлены на сайте Роскомнадзора.*

Чтобы проверить наличие уведомления об обработке, следует обратиться к реестру операторов, размещенному на сайте Роскомнадзора по вкладкам: «Персональные данные» – «Портал персональных данных Уполномоченного органа по защите прав субъектов персональных данных» – «Реестр операторов» – «Реестр», после чего ввести в предназначенные поля наименование организации, идентификационный номер налогоплательщика или регистрационный номер. Информацию из реестра также можно получить в поисковой строке на портале по запросу в виде названия или основного государственного регистрационного номера (далее – ОГРН) оператора.

2. Назначьте ответственного за обработку ПДн

В соответствии с п. 1 ст. 18.1 152–ФЗ оператору необходимо назначить ответственного за организацию обработки ПДн, а также ответственного за обеспечение безопасности ПДн в информационной системе ПДн согласно п. 14 и п. 15 ПП-1119.

Обязанности ответственного за организацию обработки ПДн установлены в п. 4 ст. 22.1 152-ФЗ:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о ПДн, в том числе требований к защите ПДн;
- доводить до сведения работников оператора положения законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Обязанности ответственного за обеспечение безопасности ПДн в информационной системе ПДн на уровне законодательства не определены.

Важно: *не только определить ответственного за обработку ПДн и ответственного за обеспечение безопасности ПДн, но и назначить их приказом. Также необходимо разработать для этих лиц должностные инструкции, которые будут определять права, функциональные обязанности и ответственность.*

3. Сократите объемы обрабатываемых ПДн

В ч. 12, 13, 14[3] ст. 13.1 КоАП РФ предусмотрена ответственность за действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн. При этом размер штрафа зависит от объема неправомерно переданных ПДн количества субъектов и идентификаторов.

Законодатель обращает внимание, что сбор и обработка ПДн должны носить исключительно целевой характер.

Оператору рекомендуется:

– определить минимально необходимый состав ПДн для достижения целей обработки;
– минимизировать состав обрабатываемых ПДн;
– организовать сбор только необходимых ПДн.

Важно: *содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки и не должны быть избыточными.*

4. Легализуйте передачу ПДн

Оператор может понести ответственность за действия (бездействие), повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей ПДн. Для снижения риска утечки ПДн оператору необходимо проанализировать процессы передачи ПДн в целях их соответствия требованиям 152-ФЗ.

[3] во всех частях есть оговорка о том, что эти действия (бездействие) не должны содержать признаков уголовно наказуемого деяния.

Передача ПДн по договору поручения

В случае передачи ПДн другому оператору с целью их дальнейшей обработки, согласно п. 3 ст. 6 152-ФЗ операторам необходимо разработать или актуализировать поручение на обработку ПДн с указанием следующих сведений:

- перечень обрабатываемых ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн по поручению оператора ПДн;
- цели обработки ПДн;
- требования, предусмотренные ст.19 152-ФЗ, к защите обрабатываемых ПДн;
- обязанность лица, которому поручается обработка ПДн, соблюдать конфиденциальность информации и требования, предусмотренные ч. 5 ст. 18 и ст.18.1 152-ФЗ, а также предоставлять информацию, подтверждающую выполнение этих требований;
- требование об уведомлении оператора ПДн о неправомерной обработке ПДн.

Если передача ПДн осуществляется по договору поручения, предусмотренному в рамках ч. 3, 4 и 5 ст. 6 152-ФЗ, оператору необходимо также получить согласие субъекта на обработку ПДн с указанием:

- в качестве действия с ПДн – передачу;
- реквизитов получателя.

Важно: *получатель при этом не обязан запрашивать отдельное согласие субъекта на обработку его ПДн, но* ***полная ответственность*** *за деятельность получателя* ***лежит на операторе****. Получатель, со своей стороны, несёт ответственность перед оператором за свою деятельность. Исключение составляет случай, когда обработка ПДн поручена иностранному физическому или юридическому лицу (ч. 6 ст. 6 152-ФЗ). В этом случае ответственность за деятельность указанных лиц перед субъектом ПДн возлагается как на самого оператора, так и на лицо, выполняющее обработку по его поручению.*

Передача ПДн без договора поручения

Если передача осуществляется без поручения, например, по договору, ответственность распределяется между оператором и получателем в соответствии с конкретными действиями, произведенными каждой из сторон.

Иными словами, если передача осуществляется на законных основаниях, и для передачи ПДн от субъекта ПДн получены все необходимые согласия на обработку его ПДн (в том числе на обработку ПДн, разрешенных субъектом ПДн для распространения) ответственность за утечку ПДн после их передачи будет нести получатель.

В случае, если передача ПДн не является законной, то есть не получены необходимые согласия субъектов и обработка не соответствует условиям, предусмотренным п. 2-11 ч. 1 ст. 6 152-ФЗ, а также п. 2-10 ч. 2, ч. 2.1 ст. 10 и ч. 2 ст. 11 152-ФЗ для специальных категорий ПДн и биометрических ПДн соответственно и ч. 15 ст. 10.1 152-ФЗ для ПДн, разрешенных субъектом для распространения, ответственность за незаконную передачу **несет оператор ПДн**.

5. Распространяйте ПДн с согласия

Распространение ПДн может быть правомерным. В ст. 10.1 152-ФЗ предусмотрены основания для распространения ПДн.

В целях законного распространения ПДн оператору необходимо:

- взять отдельное согласие на обработку ПДн, разрешенных субъектом ПДн для распространения;
- в открытом доступе разместить информацию об условиях обработки и о наличии запретов на обработку ПДн, разрешенных субъектом ПДн для распространения.

Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, может быть предоставлено оператору непосредственно или с использованием информационной системы Роскомнадзора. Требования к содержанию согласия установлены в Приказе Роскомнадзора от 24.02.2021 №18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».

Важно: *обязанность предоставить доказательства законности распространения ПДн лежит на каждом лице, осуществившем их распространение.*

Важно: *требования не применяются в случае обработки ПДн в целях выполнения возложенных законодательством РФ на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.*

6. Оцените вред субъектам ПДн в случае утечки ПДн

До наступления утечки ПДн оператору необходимо согласно ст. 18.1 152-ФЗ провести оценку вреда, который может быть причинен субъектам ПДн в случае нарушения 152-ФЗ (далее – оценка вреда) с целью оценки достаточности принимаемых мер, направленных на защиту ПДн. Если меры защиты не обеспечивают требуемый уровень защищенности ПДн, то оператору ПДн необходимо усилить меры в целях минимизации рисков утечки ПДн.

Оценка вреда проводится согласно Приказу Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

Ответственному за организацию обработки ПДн либо специально образуемой комиссией для проведения оценки вреда необходимо определить одну из трех **степеней вреда** (высокая, средняя, низкая). Результаты оценки вреда необходимо оформлять соответствующим актом.

В Акт оценки вреда необходимо включить:

- наименование или фамилию, имя, отчество (при наличии) и адрес оператора ПДн;
- дату издания акта оценки вреда;
- дату проведения оценки вреда;
- фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;
- степень вреда, которая может быть причинена субъекту ПДн.

Важно: *результаты оценки вреда учитываются в уведомлении о неправомерной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн.*

7. Внедрите процесс реагирования на утечки ПДн

Изменения (ч. 11 ст. 13.11 КоАП РФ) также устанавливают административный штраф до 3 млн. руб. за невыполнение и (или) несвоевременное выполнение оператором ПДн обязанности по уведомлению Роскомнадзора в случае установления факта неправомерной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, предусмотренной ч. 3.1 ст. 21 152-ФЗ.

Напомним, что операторы ПДн должны взаимодействовать с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) и Федеральной службой безопасности Российской Федерации (далее – ФСБ России) через Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ).

Порядок взаимодействия операторов ПДн с НКЦКИ регламентирован Приказом ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» (далее – Приказ ФСБ России № 77).

Субъекты КИИ

Если оператор ПДн является субъектом критической информационной инфраструктуры (далее – КИИ), то в соответствии с ч. 2 Приказа ФСБ России № 77, информация о компьютерных инцидентах направляется в НКЦКИ с использованием технической инфраструктуры или по электронной почте, факсу, номеру телефона, указанным на официальном сайте НКЦКИ, **в течение 24 х часов** с момента обнаружения инцидента. В случае, когда компьютерный инцидент связан

со **значимым объектом КИИ**, допустимый срок информирования НКЦКИ составляет **не более 3-х часов** с момента обнаружения. Об инциденте необходимо сообщить следующее:

- дата, время, место нахождения или географическое местоположение объекта КИИ, на котором произошел компьютерный инцидент;
- наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;
- связь с другими компьютерными инцидентами (при наличии);
- состав технических параметров компьютерного инцидента;
- последствия компьютерного инцидента.

Не субъекты КИИ

Операторы ПДн, не являющиеся субъектами КИИ, в соответствии с ч. 3 Приказа ФСБ России № 77, направляют информацию о компьютерных инцидентах путем заполнения на официальном сайте уведомления Роскомнадзора в установленные сроки (ч. 3.1 ст. 21 152-ФЗ):

- **в течение 24-х** часов с момента обнаружения инцидента – информацию о компьютерном инциденте, с указанием информации о:
  - предполагаемых причинах, повлекших нарушение прав субъектов ПДн;
  - предполагаемом вреде, нанесенном субъектам ПДн;
  - принятых мерах по устранению последствий инцидента;
  - контактном лице оператора ПДн, которое будет взаимодействовать с Роскомнадзором.
- **в течение 72-х часов** – о результатах внутреннего расследования, с указанием информации о лицах, причастных к инциденту (при наличии).

Важно: *для своевременного уведомления об утечке ПДн необходимо провести ряд мероприятий:*

- *необходимо разработать/актуализировать* ***порядок реагирования*** *на компьютерные инциденты, повлекшие за собой нарушение прав субъектов ПДн;*
- *подготовить условия для* ***мониторинга инцидентов*** *с ПДн;*
- *обеспечить* ***реагирование на инциденты*** *с ПДн;*
- *провести* ***оценку вреда субъектам*** *ПДн от утечки ПДн.*

В качестве подтверждения получения информации о компьютерном инциденте (утечке ПДн) НКЦКИ присваивает компьютерным инцидентам уникальные идентификаторы, которые направляет операторам ПДн в течение 24-х часов с момента их присвоения по тем же каналам, по которым информация об инциденте была отправлена оператором ПДн.

Способы информирования Роскомнадзора и НКЦКИ представлены в таблице 3.

Таблица 3 – способы информирования Роскомнадзора и ГосСОПКА

№ п/п	Оператор	Кого уведомлять	Как уведомлять	Когда уведомлять
1	Субъект КИИ	НКЦКИ	– e-mail: incident@cert.gov.ru; – тел.: +7 (916) 901-07-42; – факс: 7 (499) 144-64; – средства технической инфраструктуры	3 часа – *уведомление об инциденте со значимым объектом КИИ (для субъекта КИИ)* 24 часа – *уведомление об утечке/инциденте*
2	Не субъект КИИ	Роскомнадзор (передает сведения в НКЦКИ)	Уведомления на сайте Роскомнадзора	24 часа – *уведомление об утечке/инциденте* 72 часа – *уведомление о результатах внутреннего расследования*

8. Оцените эффективность принимаемых мер по защите ПДн

Самые большие штрафы, предусмотренные введенными поправками, установлены за повторные утечки ПДн. При этом для частей ч. 15 и ч. 18 статьи 13.11 КоАП РФ предусмотрено смягчающие обстоятельства, одним из которых является – документальное подтверждение соблюдения требований к защите ПДн при их обработке в информационных системах ПДн.

В соответствии с п. 4 ч. 2 ст. 19 152–ФЗ обеспечение безопасности ПДн достигается, в частности, оценкой эффективности принимаемых мер по обеспечению безопасности ПДн. Оценка эффективности мер безопасности ПДн может быть проведена в формате комплекса организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие системы защиты ПДн требованиям по защите ПДн.

В соответствии с п. 6 Приказа ФСТЭК России № 21, оценка эффективности реализованных в рамках системы защиты ПДн мер по обеспечению безопасности ПДн может проводится оператором ПДн самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Оценка эффективности реализованных мер защиты ПДн может быть проведена также в форме аттестации с соблюдением требований:

- Приказа ФСТЭК России 29.04.2021 № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
- Национального стандарта ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» (для служебного пользования).

Иными словами, фактом подтверждения соблюдения требований по защите ПДн могут являться, например, Акт оценки эффективности системы защиты ПДн или Аттестат соответствия требованиям по обеспечению безопасности ПДн.

Важно: *с учетом предусмотренной ответственности в КоАП РФ рекомендуем проводить мероприятия по оценке эффективности не реже одного раза в год.*

Для получения положительного заключения по результатам оценки эффективности оператору необходимо реализовать ряд мер по организации обработки и обеспечению безопасности ПДн, предусмотренных 152-ФЗ и его подзаконными актами.

Подготовительные работы к оценке эффективности будут включать следующие работы:

- обследование процессов организации обработки и обеспечения безопасности ПДн;
- определение уровня защищенности ПДн в информационных системах ПДн;
- моделирование угроз безопасности ПДн;
- разработка технического задания на систему защиты ПДн;
- проектирование системы защиты ПДн.

После получения полной информации об актуальных угрозах и мерах защиты, позволяющих их нейтрализовать, необходимо выполнить следующие этапы:

- внедрить технические меры защиты ПДн;
- внедрить организационные меры защиты ПДн;
- провести оценку эффективности принятых мер по защите ПДн;
- поддерживать необходимых уровень защищенности ПДн в информационной системе ПДн в процессе эксплуатации.

Заключение

В целях минимизации рисков нарушения 152-ФЗ оператору необходимо:

- подать уведомление о намерении осуществлять обработку ПДн и поддерживать его в актуальном состоянии;
- назначить ответственного за организацию обработки ПДн;
- сократить объем обрабатываемых ПДн;
- проверить корректность и законность действий при передаче ПДн;
- провести оценку вреда субъектам ПДн от утечки ПДн;
- внедрить процесс реагирования на утечки ПДн:
  - подготовить условия для мониторинга утечек ПДн;
  - уведомлять Роскомнадзор в случае установления факта неправомерной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн;
  - расследовать причины утечки ПДн и принимать мери по минимизации последствий от них.
- применять необходимые и достаточные меры по обеспечению безопасности ПДн, установленные действующим законодательством РФ, включая:
  - **регламентацию процессов** обработки и защиты ПДн;
  - **внедрение** организационных и технических **мер защиты** ПДн;
  - проведение ежегодной **оценки эффективности** системы защиты ПДн.