KKMP LEGAL

30 мая 2025 г.

Ужесточение ответственности в сфере обработки персональных данных

30 мая 2025 года вступает в силу Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (далее – «**Закон**»), значительно ужесточающий ответственность за нарушение законодательства о персональных данных (далее – «**ПД**»).

I. ПРИЧИНЫ ПРИНЯТИЯ ЗАКОНА

Основная цель Закона – борьба с утечками ПД, которые приобрели в России массовый характер, а также стимулирование операторов ПД усиливать контроль за оборотом ПД и информационной безопасностью.

Если обратиться к истории принятия Закона, то по итогам заседания Совета по развитию гражданского общества и правам человека, состоявшегося 7 декабря 2022 года, Президентом Российской Федерации было дано поручение рассмотреть вопрос об ужесточении ответственности за незаконный оборот ПД и иные нарушения законодательства в области ПД.

В конце 2023 года в Государственную Думу были внесены законопроекты (№ 502104-8 и № 502113-8) об изменениях в КоАП РФ и УК РФ, которыми ужесточалась/ вводилась новая ответственность за утечки ПД (далее – «**Законопроекты**»).

Законопроекты вызвали общественные дискуссии и подверглись критике. Ранее мы писали о внесении Законопроектов в Государственную Думу.

Как следует из пояснительных записок к законопроектам, ПД стали постоянным «спутником» любых коммуникаций человека в Интернете. Проблемы обеспечения защиты таких данных, связанных с угрозами неправомерного доступа к ним, распространения и использования ПД в преступных целях, с каждым днем становятся все более актуальными:

- большая часть населения России является пользователями Интернета (130 млн), из них 106 млн пользуются социальными сетями;
- каждое четвертое преступление (с января по июль 2022 года) связано с использованием технологий, при этом количество преступлений с использованием ПД с каждым годом кратно растет;
- с января по август 2022 года произошли утечки 197 млн записей ПД, при этом ущерб превысил 8 млрд;
- в даркнете фигурируют ПД приблизительно 80% населения России;
- общий объем официально выявленных утечек ПД за 2022 год составил более 1130 млн записей.

За 2024 год Роскомнадзор зафиксировал 135 случаев утечек баз данных, в которых содержалось более 710 миллионов записей о россиянах.

При этом, как отмечают авторы Законопроектов, размер санкции был несоизмерим с последствиями от утечек – административный штраф составлял для юридических лиц до 100 тыс. рублей (ч. 1 ст. 13.11 КоАП РФ). В то же время какая-либо уголовная ответственность за утечки отсутствовала.

30 ноября 2024 года Президент Российской Федерации подписал закон, которым вносятся изменения в УК РФ[1]. Данный закон касается закрепления в УК РФ новой статьи (272.1), предусматривающей ответственность за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей ПД, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения. Изменения в УК РФ вступили в силу 11 декабря 2024 года, с более подробным обзором можно ознакомиться на нашем канале. Новая статья уже нашла свое применение: буквально несколько дней назад была опубликована новость о том, что в Петрозаводске следователи возбудили уголовное дело:

«Предварительно установлено, что в феврале 2025 года начальник одного из отделов филиала публично-правовой компании в Республике Карелия, имея доступ к федеральной государственной информационной системе, по просьбе знакомых незаконно передавал им для использования в личных целях содержащиеся в едином реестре недвижимости ПД лиц, а также сведения о принадлежащем им имуществе.».

Также 30 ноября 2024 года Президент Российской Федерации подписал Закон, который мы более подробно рассмотрим ниже.

II. ПОВЫШЕНИЕ ОТВЕТСТВЕННОСТИ ЗА СТАРЫЕ СОСТАВЫ

Старые составы правонарушений в сфере обработки ПД (ч.ч. 1 – 9 ст. 13.11 КоАП РФ) претерпели следующие изменения:

- повысилась ответственность за основной состав правонарушения[2] (ч. 1 ст. 13.11 КоАП РФ);
- повысилась ответственность за повторное совершение правонарушения, которое ранее квалифицировалось по ч. 1 ст. 13.11 КоАП РФ (ч. 1.1 ст. 13.11 КоАП РФ):

Измененная норма	Содержание нормы	Для граждан	Для должностных лиц	Для компаний
		Диапазон «от – до»		
Ч. 1 ст. 13.11 КоАП РФ	Нарушение законодательства о ПД	Было: 2-6 тыс. Стало: 10-15 тыс.	Было: 10-20 тыс. Стало: 50-100 тыс.	Было: 60-100 тыс. Стало: 150-300 тыс.
Ч. 1.1 ст. 13.11 КоАП РФ	Повторное совершение правонарушения, за которое лицо привлекалось по ч. 1 ст. 13.11 КоАП РФ	Было: 4-12 тыс. Стало: 15-30 тыс.	Было: 20-50 тыс. Стало: 100-200 тыс.	Было: 100-300 тыс. Стало: 300-500 тыс.

Индивидуальные предприниматели будут нести ответственность как юридические лица за повторную утечку ПД (ч. 1.1 ст. 13.11 КоАП РФ) и за несоблюдение требований о локализации (ч. 8, 9 ст. 13.11 КоАП РФ).

---

[1] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

[2] Под основным составом в силу ч. 1 ст. 13.11 КоАП РФ понимается обработка ПД в случаях, не предусмотренных законодательством Российской Федерации в области ПД, либо обработка ПД, несовместимая с целями сбора ПД.

III. ПОЯВЛЕНИЕ НОВЫХ СОСТАВОВ

Появились новые составы за неуведомление Роскомнадзора о намерении осуществлять обработку ПД (ч. 10 ст. 13.11 КоАП РФ), за неуведомление Роскомнадзора об утечке ПД (ч. 11 ст. 13.11 КоАП РФ), а также за утечки ПД (ч.ч. 12-18 КоАП РФ).

Новая норма	Содержание нормы	Для граждан	Для должностных лиц	Для компаний
		Диапазон «от – до»		
Ч. 10 ст. 13.11 КоАП РФ	Неуведомление Роскомнадзора о намерении осуществлять обработку ПД	5-10 тыс.	30-50 тыс.	100-300 тыс.
Ч. 11 ст. 13.11 КоАП РФ	Неуведомление Роскомнадзора об утечке ПД	50-100 тыс.	400-800 тыс.	1-3 млн.
Ч. 12 ст. 13.11 КоАП РФ	Утечка ПД (от 1 тыс. до 10 тыс. субъектов либо от 10 тыс. до 100 тыс. идентификаторов)	100-200 тыс.	200-400 тыс.	3-5 млн.
Ч. 13 ст. 13.11 КоАП РФ	Утечка ПД (от 10 тыс. до 100 тыс. субъектов либо от 100 тыс. до 1 млн. идентификаторов)	200-300 тыс.	300-500 тыс.	5-10 млн.
Ч. 14 ст. 13.11 КоАП РФ	Утечка ПД (более 100 тыс. субъектов либо более 1 млн. идентификаторов)	300-400 тыс.	400-600 тыс.	10-15 млн.
Ч. 15 ст. 13.11 КоАП РФ	Повторная утечка ПД	400-600 тыс.	800 тыс. – 1,2 млн.	1 – 3 % совокупной выручки, но не менее 20 млн. и не более 500 млн.
Ч. 16 ст. 13.11 КоАП РФ	Утечка специальных категорий ПД	300-400 тыс.	1-1,3 млн.	10-15 млн.
Ч. 17 ст. 13.11 КоАП РФ	Утечка биометрии	400-500 тыс.	1,3-1,5 млн.	15-20 млн.
Ч. 18 ст. 13.11 КоАП РФ	Повторная утечка специальных категорий ПД или биометрии	500-800 тыс.	1,5-2 млн.	1 – 3 % совокупной выручки, но не менее 25 млн и не более 500 млн.

Новые составы имеют ряд особенностей, о которых речь пойдет ниже.

1.1. Субъекты

Важно отметить, что новые составы (ч.ч. 10-18 ст. 13.11 КоАП РФ) имеют особый субъектный состав по сравнению со старыми (ч.ч. 1 – 9 ст. 13.11 КоАП РФ):

- под должностными лицами понимаются сотрудники государственного или муниципального органа либо некоммерческой организации;

- под юридическими лицами понимаются операторы - юридические лица, не являющееся государственным или муниципальным органом либо некоммерческой организацией.

Получается, что, если утечку допустила коммерческая организация, ее должностные лица к административной ответственности привлечены не будут. Если же утечку допустил государственный / муниципальный орган или некоммерческая организация – они не будут привлечены к ответственности как юридические лица, но их должностные лица получат административные штрафы.

Риски привлечения к административной ответственности единоличных исполнительных органов коммерческих организаций и лиц, ответственных за информационную безопасность и обработку ПД, не поменялись (но при этом не исключаются риски гражданско-правового характера, например, взыскание убытков с генерального директора). Что касается штрафов для должностных лиц государственных / муниципальных органов и некоммерческих организаций, они могут показаться значительными. В этом случае остается открытым вопрос – какое должностное лицо будет привлечено к ответственности – ответственный за информационную безопасность или руководитель? КоАП РФ не дает ответа на этот вопрос, в каждом конкретном случае необходимо будет определять должностные обязанности и объем ответственности.

Также важно отметить, что индивидуальные предприниматели будут отвечать за утечки как юридические лица. Эта мера кажется внутренне противоречивой, поскольку государство поддерживает снижение административной нагрузки на малый и средний бизнес. С одной стороны, в 2022 году вводится ст. 4.1.2 КоАП РФ[3], позволяющая снижать размер ответственности субъектам малого и среднего предпринимательства – юридическим лицам. С другой, вводятся такие высокие штрафы для индивидуальных предпринимателей. И это в противовес общему правилу КоАП РФ о том, что индивидуальные предприниматели несут ответственность как должностные лица[4] (ст. 2.4 КоАП РФ).

Возможно, подход государства заключается в том, что если индивидуальный предприниматель обрабатывает ПД более 1 тыс. субъектов, то предполагается, что он получает высокую прибыль. Такой подход является спорным, поскольку за несколько лет у ИП с небольшими оборотами может скопиться клиентская база более 1 тыс. человек.

1.2. Понятие «идентификатор»

Как уже было отмечено в таблице, размер штрафа за утечки зависит, в том числе, от количества идентификаторов, которые в КоАП РФ определены как «уникальное обозначение сведений о физическом лице, содержащееся в информационной системе ПД оператора и относящееся к такому лицу».

Понятие «индентификатор» является довольно неопределенным. Вполне вероятно, что под ним понимаются отдельные категории ПД. Например, в сеть утекла клиентская база, в которой содержалась информация о клиентах: ФИО, телефон, почта, номер карты лояльности. В таком случае, на 1 субъекта ПД будут приходиться 4 идентификатора.

---

[3] Статья касается назначения административного наказания в виде административного штрафа социально ориентированным некоммерческим организациям и являющимся субъектами малого и среднего предпринимательства юридическим лицам, отнесенным к малым предприятиям, в том числе к микропредприятиям.

[4] Размер административных штрафов для должностных лиц кратко меньше, чем размер штрафов для юридических лиц.

Поскольку размер ответственности теперь зависит от количества идентификаторов, у операторов появится дополнительный стимул минимизировать сбор излишних ПД, если это выходит за пределы обозначенных целей обработки.

1.3. Утечка специальных категорий ПД и биометрии

Как мы отметили в таблице, Законом введены новые составы – это утечка специальных категорий ПД (ч. 16 ст. 13.11 КоАП РФ), утечка биометрии (ч. 17 ст. 13.11 КоАП РФ), а также их повторная утечка (ч. 18 ст. 13.11 КоАП РФ). Указанные составы применяются независимо от того, какое количество ПД или идентификаторов подверглось утечке. Это означает, что даже формальная утечка ПД одного субъекта может повлечь серьезные последствия. В связи с этим, мы рекомендуем уделить особое внимание защите и обработке ПД данных категорий.

1.4. Отягчающие обстоятельства

В случае повторных утечек при назначении наказания учитываются следующие отягчающие обстоятельства (ч.15, ч.18 ст. 13.11 КоАП РФ):

- лицо продолжило противоправное поведение, несмотря на требование уполномоченных на то лиц прекратить его;

- лицо ранее привлекалось к ответственности по ч.ч. 1–11 ст. 13.11 КоАП РФ и/или ст. 13.6[5], ст. 13.12[6] КоАП РФ и на момент вынесения постановления об административном правонарушении считается подвергнутым административному наказанию по прошлым правонарушениям[7].

Получается, что законодатель рассматривает утечку ПД как длящееся нарушение. В таком случае продолжением противоправного поведения для операторов, допустивших утечку, считается неуведомление или ненадлежащее уведомление Роскомнадзора об утечке, а также неисполнение иных обязанностей, предусмотренных ч. 3.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «**Закон о персональных данных**»), например, непроведение внутреннего расследования.

1.5. Смягчающие обстоятельства

Как и отягчающие обстоятельства, специальные смягчающие обстоятельства применимы только при назначении наказания за повторные утечки (ч.15, ч.18 ст. 13.11 КоАП РФ). Так, ответственность ниже минимального предела (1/10 минимального размера, но в любом случае от 15 млн до 50 млн) может быть предусмотрена при одновременном соблюдении следующих условий:

- ежегодные расходы оператора на мероприятия по обеспечению информационной безопасности, проведенные организациями, имеющими лицензию, либо самостоятельно оператором, если у него есть лицензия, равны 0.1% годовой выручки в течение 3 лет;

- оператор проводил аудит соблюдения требований к защите ПД и документировал его результаты за 12 месяцев до утечки;

- отсутствуют отягчающие обстоятельства.

Применение новых смягчающих обстоятельств вызывает на практике ряд вопросов:

- Первый вопрос связан с составом расходов на информационную безопасность. Что к ним относится? Являются ли расходы на проведение тренингов мероприятиями по обеспечению информационной безопасности? А приобретение серверов? Установка новой пропускной

---

5 Ст. 13.6 КоАП РФ. Использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям.

6 Ст. 13.12 КоАП РФ. Нарушение правил защиты информации.

7 В соответствии с ч. 1 ст. 4.6 КоАП РФ лицо, которому назначено административное наказание за совершение административного правонарушения, считается подвергнутым данному наказанию со дня вступления в законную силу постановления о назначении административного наказания до истечения одного года со дня окончания исполнения данного постановления

системы? Пока что вопрос зависит от оценки правоприменительным органом конкретных обстоятельств дела.

- Второй вопрос, логично вытекающий из первого, связан с доказательствами, которыми оператор должен подтверждать расходы на проведение мероприятий по обеспечению информационной безопасности. Если он заключает договор с подрядной организацией, имеющей лицензию, стоимость будет прописана в договоре или спецификациях. Другое дело, если оператор имеет лицензию и проводит такие мероприятия самостоятельно. В данном случае могут возникнуть сложности с документальным подтверждением расходов.

- Третий вопрос связан с проведением аудита – должен ли оператор проводить его самостоятельно или с привлечением третьих лиц? Пока ответа на данный вопрос нет, необходимо ждать официальных разъяснений. Скорее всего, оператор может провести такой аудит самостоятельно при условии тщательного документирования (поскольку иное не установлено в КоАП РФ).

Если вспомнить историю принятия Закона, то изначально активно обсуждался вопрос компенсаций субъектам ПД за утечки. Предполагалось, что указанная мера позволит «смягчить» наказание. Однако, как ответил министр цифрового развития, связи и массовых коммуникаций России Максут Шадаев, данная норма не вошла в Закон, поскольку «ни по одному составу административных правонарушений нет такой нормы»[8].

Обращаем внимание, что компенсации несмотря на то, что не вошли в текст Закона, все равно могут являться смягчающим обстоятельством. Это обусловлено общим правилом, установленным ст. 4.2 КоАП РФ, в частности, смягчающим обстоятельством является предотвращение лицом, совершившим административное правонарушение, вредных последствий административного правонарушения.

Кроме того, правоприменительный орган, рассматривающий дело об административном правонарушении, может признать смягчающими обстоятельствами иные обстоятельства, которые не указаны в КоАП РФ (ч. 2 ст. 4.2). Здесь важно сказать, что принятие мер, которые установлены законодательством (например, реагирование на инцидент, принятие внутренней документации в сфере информационной безопасности и т.д.) как обязанности оператора, не будут рассматриваться в качестве смягчающих обстоятельств.

1.6. Неприменение «скидки» на штраф

Многие автолюбители знают, что если заплатить штраф сразу, то на него будет действовать «скидка» 50%. В отношении административной ответственности за нарушение законодательства о ПД такая скидка теперь перестала распространяться на ст. 13.11 КоАП РФ, как на старые составы, так на новые (ч.ч. 1.3-3 ст. 32.2 КоАП РФ).

1.7. «Стандарты осмотрительности» при организации обработки ПД

При применении новых составов основная сложность заключается в том, чтобы определить, какой оператор будет признан виновным в утечке. Как будет установлена вина, если оператор добросовестно соблюдал обязанности, предусмотренные Законом о персональных данных, и подвергся хакерской атаке злоумышленников?

Исходя из ч. 1 ст. 2.1 КоАП РФ административным правонарушением признается противоправное, виновное действие (бездействие). В силу ч. 2 указанной статьи юридическое лицо признается виновным в совершении административного правонарушения, если будет установлено, что у него имелась возможность для соблюдения правил и норм, но данным лицом не были приняты все зависящие от него меры по их соблюдению.

Формулировка «все зависящие меры» достаточно широкая и непонятно, какие меры должен предпринять оператор, чтобы исключить свою вину. Не существует «универсального рецепта», исключающего вину оператора, в каждом конкретном случае меры будут подлежать индивидуальной оценке. К сожалению, «все зависящие меры» - категория достаточно

[8] https://www.vedomosti.ru/technology/articles/2024/11/19/1076023-kompensatsii-utechki-ne-budet?from=copy_text

субъективная. Возможно, в дальнейшем будут официальные разъяснения или стандарты, которые будут выработаны практикой.

Однако уже сейчас можно ориентироваться на определенные «стандарты осмотрительности»:

- учитывая, (1) что оператор в силу ч. 1 ст. 18.1 Закона о персональных данных самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено законодательством, а также учитывая, (2) что ст. 19 Закона о персональных данных содержит открытый перечень мер по обеспечению безопасности ПД, оператору желательно соблюдать как можно больше перечисленных в указанных статьях мер;

- определенным «стандартом осмотрительности» будет соблюдение условий, которые необходимы для смягчения ответственности по новым правилам – расходы на информационную безопасность и аудит (см. подробнее п. 1.5 Обзора);

- операторы могут ориентироваться на отраслевые стандарты, к которым относится, к примеру, Отраслевой стандарт защиты данных Ассоциации больших данных. В указанном случае необходимо оценивать рынок и деятельность оператора.

IV. Рекомендации

Для минимизации рисков привлечения к ответственности за нарушение Закона о персональных данных рекомендуем совершить следующие действия, направленные на усиление комплаенса в сфере ПД (с учетом изложенного выше, перечень не рассматривается как исчерпывающий):

- подать уведомления в Роскомнадзор (о намерении осуществлять обработку ПД, о трансграничной передаче);

- назначить ответственных лиц за обработку ПД;

- утвердить внутреннюю документацию, а именно политики и положения (об обработке ПД, о защите конфиденциальной информации, об информационной безопасности, процедуры реагирования на утечки и компьютерные инциденты и т.д.), формы согласий;

- проводить ежегодный аудит процессов обработки ПД;

- вести реестр информационных систем, чтобы понимать какие процессы обработки ПД есть в организации, откуда может произойти утечка;

- регулярно проводить работу с персоналом – знакомить под роспись с внутренней документацией, проводить тренинги;

- документировать любые траты на информационную безопасность/ защиту ПД, будь то замена оборудования, обучение или разработка документации;

- застраховать риски, связанные с обработкой ПД (киберриски);

- провести аудит договоров с контрагентами, разграничить ответственность за утечки;

- по возможности провести проверку контрагентов и принять регламент проверки.

В случае утечки рекомендуем действовать проактивно:

- предпринять все действия реагирования на утечку, предусмотренные в качестве обязанностей оператора (уведомить Роскомнадзора, провести внутреннее расследование, устранить последствия и др.),

- не скрывать факт утечки, а предупредить субъектов ПД, чьи данные утекли, вести активный диалог с ними;

- фиксировать любые обращения пользователей и действия, предпринятые в связи с обращениями;

- при возможности компенсировать ущерб субъектам ПД;
- подать заявление о совершении преступления в правоохранительные органы;
- подать запрос в Роскомнадзор с просьбой заблокировать ресурс, на котором размещены утекшие ПД.

Даже если совершение указанных действий не исключит административную ответственность, будут убедительные аргументы для того, чтобы ее снизить: обосновать наличие смягчающих обстоятельств либо снизить ответственность ниже минимального предела.

* * *

Мы будем рады ответить на ваши вопросы по данной тематике.

Анна Максименко
Партнер
Anna.Maximenko@kkmp.legal

Антон Селиверстов
Юрист
Anton.Seliverstov@kkmp.legal