DATACASE | Privacy Tech
консалтинг в формате HD

Новые штрафы за нарушения в сфере персональных данных

Обзор изменений и рекомендации по подготовке к ним

декабрь 2024

30 ноября 2024 года Президент РФ подписал два ключевых закона, направленных на ужесточение ответственности за утечки персональных данных и другие нарушения в этой сфере: Федеральный закон № 420[1], который вносит изменения в Кодекс РФ об административных правонарушениях (далее – «**Изменения в КоАП**»), и Федеральный закон № 421[2], вносящий изменения в Уголовный кодекс РФ.

Изменения в Уголовный кодекс РФ вступили в силу 11 декабря 2024 года, а Изменения в КоАП вступят в силу 30 мая 2025 года. Поскольку новые штрафы охватывают широкий круг организаций и могут серьезно повлиять на бизнес, подготовку к изменениям стоит начать уже сейчас. Важно заранее актуализировать существующие процессы обработки персональных данных, обновить внутренние регламенты и внедрить дополнительные меры защиты.

В обзоре мы рассмотрели ключевые положения Изменений в КоАП и подготовили практические рекомендации, которые помогут вам подготовиться к изменениям и минимизировать возможные риски.

Увеличение штрафа по «общему» составу правонарушений

Штраф за неподачу уведомления об обработке в Роскомнадзор

Штраф за неподачу или несвоевременную подачу уведомления об утечке

Штрафы за утечку персональных данных

Штрафы за утечку специальных категорий персональных данных и биометрии

Оборотные штрафы за повторную утечку персональных данных

Новые «смягчающие обстоятельства» для случаев повторных утечек

Особое определение должностного и юридического лица для составов об утечках

По новым составам Роскомнадзор вправе возбудить дело без проведения проверки

Значительную часть дел по ст. 13.11 КоАП РФ будут рассматривать арбитражные суды

Отменена скидка за «раннюю» уплату штрафа

[1] Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс РФ об административных правонарушениях».

[2] Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс РФ».

Обзор изменений, внесенных в КоАП РФ

1. Увеличение штрафов по «общему» составу правонарушений

ч. 1, 1^1 ст. 13.11 КоАП РФ

Обработка персональных данных в случаях, не предусмотренных законодательством, или несовместимая с целями сбора персональных данных.

до 300 000 ₽
до 500 000 ₽ (повторно)

до 100 000 ₽
до 200 000 ₽ (повторно)

Изменения в КоАП увеличили размер административных штрафов, предусмотренных чч. 1 и 1^1 ст. 13.11 КоАП РФ для наиболее «общего» состава правонарушений в области обработки персональных данных. Данный состав предусматривает административную ответственность за обработку персональных данных в случаях, не предусмотренных законодательством, а также обработку, несовместимую с целями сбора персональных данных.

На практике именно этот состав правонарушений является одним из самых распространенных оснований для привлечения организаций и должностных лиц к административной ответственности. Чаще всего нарушения связаны с отсутствием согласия на обработку персональных данных, обработкой данных с превышением объема, который требуется для достижения заявленных целей, либо несоблюдением установленных сроков обработки персональных данных.

2. Штраф за неподачу уведомления об обработке персональных данных

ч. 10 ст. 13.11 КоАП РФ

Неуведомление или несвоевременное уведомление Роскомнадзора о намерении осуществлять обработку персональных данных.

до 300 000 ₽

до 50 000 ₽

Изменения в КоАП ввели специальную административную ответственность за неуведомление или несвоевременное уведомление Роскомнадзора о намерении осуществлять обработку персональных данных.

С 1 сентября 2022 года перечень случаев, когда операторы персональных данных вправе не подавать уведомление о начале обработки персональных данных в Роскомнадзор, был значительно сокращен. Соответственно, обязанность по подаче уведомления актуальна для подавляющего большинства операторов персональных данных.

Сейчас лица, не подавшие уведомление об обработке персональных данных, привлекаются к административной ответственности по ст. 19.7 КоАП РФ, которая предусматривает максимальный штраф в размере 5000 рублей. Таким образом, штраф за данное нарушение фактически увеличился в 60 раз.

3. Штраф за неуведомление или несвоевременное уведомление Роскомнадзора об утечке персональных данных

ч. 11 ст. 13.11 КоАП РФ

Неуведомление или несвоевременное уведомление Роскомнадзора об утечке персональных данных, которая повлекла нарушение прав субъектов персональных данных.

до 3 000 000 ₽

до 800 000 ₽

Операторы обязаны уведомлять Роскомнадзор об инцидентах (компьютерных и иных), которые повлекли нарушение прав субъектов персональных данных. Эта обязанность распространяется на случаи передачи (предоставления, распространения и доступа) персональных данных, которые произошли в результате намеренных действий или случайно.

Обязанность оператора персональных данных по уведомлению возникает с момента выявления инцидента и предполагает направление двух уведомлений в Роскомнадзор:

- первичного – в течение 24 часов, с базовой информацией об инциденте, и
- последующего – в течение 72 часов, с результатами внутреннего расследования инцидента.

Изменения в КоАП ввели административную ответственность за неуведомление (то есть неподачу уведомлений в Роскомнадзор), а также за подачу уведомлений с нарушением установленных сроков.

Операторы персональных данных также обязаны уведомлять ФСБ о компьютерных инцидентах, которые произошли в результате неправомерных действий. Поскольку в ч. 11 ст. 13.11 КоАП РФ прямо указано только на нарушение обязанности по уведомлению Роскомнадзора, новый штраф не охватывает нарушение обязательства по уведомлению ФСБ.

4. Штрафы за «утечку» персональных данных

чч. 12 – 14 ст. 13.11 КоАП РФ

Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) персональных данных определенного количества субъектов и (или) id:

1 000 – 10 000 субъектов и (или) 10 000 – 100 000 id

до 5 000 000 ₽

до 400 000 ₽

10 000 – 100 000 субъектов и (или) 100 000 – 1 000 000 id

до 10 000 000 ₽

до 500 000 ₽

Более 100 000 субъектов и (или) более 1 000 000 id

до 15 000 000 ₽

до 600 000 ₽

Изменения в КоАП предусмотрели несколько составов для случаев совершения действий (бездействия), повлекших неправомерную передачу (предоставление, распространение, доступ) информации, включающей персональные данные («**утечку**»).

Составы отличаются в зависимости от количества субъектов персональных данных и (или) идентификаторов («**id**»), которые были затронуты утечкой. Согласно примечанию к ст. 13.11 КоАП РФ, под id понимается уникальное обозначение сведений о физическом лице, содержащееся в информационной системе персональных данных оператора и относящееся к такому лицу. Пока отсутствует определенность относительно надлежащих способов определения «уникальности» соответствующих сведений, а также практического подхода к понятию id

в целом (например, будет ли являться id уникальный номер телефона, либо же речь будет идти только об id, присвоенных субъектам в рамках информационной системы).

Если количество субъектов и id, затронутых утечкой, меньше, чем предусмотрено новой ч. 12 ст. 13.11 КоАП РФ, то ответственность будет наступать по ч. 1, 1^1 или 2, 2^1 ст. 13.11 КоАП РФ (как это происходит в настоящее время).

Согласно положениям чч. 12-14 ст. 13.11 КоАП РФ, административная ответственность наступает за действия или бездействие, которые повлекли утечку персональных данных. Таким образом, административная ответственность должна наступать вне зависимости от того, какие усилия оператор прилагал для соблюдения требований законодательства в сфере обработки и защиты персональных данных. Однако полагаем, что такие усилия все же будут учитываться судами при рассмотрении споров (по крайней мере, в контексте определения размера штрафа).

4.1. Ответственность за утечку специальных категорий персональных данных и биометрии

ч. 16 ст. 13.11 КоАП РФ

Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей специальную категорию персональных данных.

до 15 000 000 ₽

до 1 300 000 ₽

ч. 17 ст. 13.11 КоАП РФ

Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей биометрические персональные данные.

до 20 000 000 ₽

до 1 500 000 ₽

Изменения в КоАП ввели отдельные составы административной ответственности за утечку специальных категорий персональных данных и биометрических данных. В отличие от персональных данных, которые не относятся к этим категориям, Изменения в КоАП не дифференцируют штраф в зависимости от объема специальных категорий персональных данных и биометрических данных, подвергшихся утечке.

4.2. Ответственность за повторную утечку

ч. 15 ст. 13.11 КоАП РФ

Совершение правонарушения по чч. 12–14 ст. 13.11 КоАП РФ лицом, подвергнутым административному наказанию по чч.12–18 ст. 13.11 КоАП РФ.

до 3 % от выручки
(не меньше 20 000 000 ₽ и не больше 500 000 000 ₽)

до 1 200 000 ₽

ч. 18 ст. 13.11 КоАП РФ

Совершение правонарушения по чч. 16–17 ст. 13.11 КоАП РФ лицом, подвергнутым административному наказанию по чч.12–18 ст. 13.11 КоАП РФ.

до 3 % от выручки
(не меньше 25 000 000 ₽ и не больше 500 000 000 ₽)

до 2 000 000 ₽

Изменения в КоАП также ввели административную ответственность за повторное совершение правонарушения. Правонарушение считается совершенным повторно, если оно совершено в течение 1 года со дня исполнения постановления о назначении административного наказания (например, со дня уплаты административного штрафа) по однородному правонарушению.

Для юридических лиц ответственность за повторное правонарушение установлена в виде «оборотного» штрафа.

5. Особенности назначения административного наказания

5.1. Новые «смягчающие обстоятельства»

Изменения в КоАП предусмотрели перечень обстоятельств, при которых может быть снижен административный штраф по ч. 15 и ч. 18 ст. 13.11 КоАП РФ (то есть только для случаев повторных правонарушений **(!)**).

Если указанные ниже условия **выполнены одновременно до вынесения постановления о наложении административного штрафа**, то штраф назначается в размере 1/10 минимального размера штрафа, предусмотренного за соответствующее правонарушение, но не ниже 15 млн. рублей и не более 50 млн. рублей:

а) Ежегодные расходы на мероприятия по обеспечению информационной безопасности в течение 3 лет до года выявления правонарушения составляют не менее 1/10 % годового совокупного размера выручки либо размера собственных средств (капитала) кредитной организации. При этом такие мероприятия должны выполняться сторонней организацией или самим оператором при наличии соответствующей лицензии.

б) У оператора есть документальное подтверждение соблюдения требований к защите персональных данных в информационной системе персональных данных, полученное в течение 12 месяцев до момента выявления правонарушения;

в) В действиях лица, привлекаемого к административной ответственности, отсутствуют отягчающие обстоятельства, а именно:

- лицо не должно продолжать противоправное поведение, несмотря на требование прекратить его;
- на момент совершения правонарушения лицо не должно считаться подвергнутым наказанию по чч. 1-11 ст. 13.11, ст. 13.6 и 13.12 КоАП РФ.

Для всех остальных случаев будет действовать общий перечень смягчающих обстоятельств.

5.2. Лица, привлекаемые к ответственности

В новых примечаниях к ст. 13.11 КоАП РФ предусмотрен особый подход к определению должностного и юридического лица для целей применения чч. 10-18 ст. 13.11 КоАП РФ:

- под должностным лицом понимается должностное лицо государственного или муниципального органа, а также некоммерческой организации;
- под юридическим лицом понимается юридическое лицо, которое **НЕ** является государственным или муниципальным органом, а также некоммерческой организацией.

Таким образом, к коммерческим организациям будут применяться более высокие штрафы, в то время как их должностные лица не будут привлекаться к ответственности по всем новым составам правонарушений. В государственном секторе и некоммерческих организациях ответственность, напротив, будет носить персональный характер, поскольку будет возлагаться на должностных лиц.

5.3. Изменение порядка возбуждения и рассмотрения дел

Изменения в КоАП предусмотрели право Роскомнадзора возбуждать дела об административных правонарушениях по чч. 10-18 ст. 13.11 КоАП РФ без проведения контрольных (надзорных) мероприятий при получении от физического или юридического лица, совершившего правонарушение, данных, подтверждающих событие правонарушения. Например, такими данными может быть и само уведомление об утечке, которое оператор персональных данных должен подавать в Роскомнадзор.

Помимо этого, дела по ст. 13.11 КоАП РФ будут рассматривать арбитражные суды вместо мировых судов, если нарушение совершено юридическими лицами, их должностными лицами или иными работниками, а также ИП.

Также в случаях привлечения к административной ответственности по ст. 13.11 КоАП РФ за нарушение, выявленное в ходе контрольных (надзорных) мероприятий, отменяется возможность уплатить штраф со скидкой в 50%. Независимо от срока уплаты штрафа, он должен уплачиваться в полном объеме.

Подготовка к изменениям: дорожная карта

Описанные изменения касаются практически всего спектра регуляторных требований в области обработки персональных данных, начиная с оснований для обработки данных и заканчивая вопросами информационной безопасности. Поэтому подготовка к вступлению изменений в силу должна предусматривать комплексное усиление комплаенса по всем направлениям. Особое внимание необходимо уделить таким потенциальным нарушениям, которые могут повлечь значительные финансовые санкции.

1. Инвентаризация процессов обработки персональных данных

Эффективное управление основаниями обработки персональных данных, подача уведомления о начале обработки таких данных и даже выстраивание системы технической защиты информации **невозможно**, если отсутствует актуальная картина обработки данных. Поэтому любому оператору следует начать с выявления актуальных процессов обработки персональных данных, их оптимизации (при наличии такой возможности) и документирования.

Результатом проведенного аудита должен стать актуальный реестр (список, перечень) процессов обработки персональных данных, который будет описывать в отношении каждого выявленного процесса состав обрабатываемых персональных данных, категории субъектов, способы, сроки обработки и хранения, а также другие существенные параметры обработки данных.

Реестр позволит не только выполнить конкретные нормативные требования к документированию процессов обработки данных (п. 2 ч. 1 ст. 18.1 152-ФЗ), но и будет являться «картой», облегчающей выполнение иных регуляторных требований.

2. Определение и внедрение надлежащих оснований обработки данных

Опираясь на ранее составленный реестр процессов обработки персональных данных, оператор может подобрать для каждого процесса соответствующее основание обработки (например, исполнение договорных обязательств, выполнение требований закона, согласие субъекта или иное). В тех случаях, когда таким основанием является согласие субъекта, необходимо также выбрать подходящий способ его получения и обеспечить сохранность доказательств его получения.

Подобрав подходящие основания обработки для каждой цели обработки персональных данных и внедрив механизмы получения согласий субъектов (где это требуется), оператор может избежать возможных штрафов, предусмотренных ч. 1 ст. 13.11 КоАП РФ.

Особое внимание следует уделить не только самому факту получения согласий, но и актуальным требованиям, выработанным в правоприменительной практике. Как известно, форма согласия и контекст его получения могут существенно влиять на предъявляемые к нему требования (например, в части допустимых способов идентификации субъекта или возможности объединения в одном согласии нескольких целей обработки персональных данных). Игнорирование указанных нюансов может обесценить все усилия оператора в области сбора согласий субъектов.

3. Формирование уведомлений о начале (изменении параметров) обработки персональных данных

Операторам, которые еще не успели уведомить Роскомнадзор о начале обработки персональных данных, следует сделать это до того момента,

как санкции за соответствующее правонарушение увеличатся в десятки раз. Тем операторам, которые подали такое уведомление ранее, следует убедиться в том, что ранее заявленные сведения являются актуальными.

Важно обеспечить, чтобы содержание уведомления соответствовало иным документам оператора в области обработки персональных данных. Так, цели, заявленные в уведомлении, должны соответствовать целям, указанным в локальных нормативных актах, согласиях на обработку персональных данных, публичных политиках и иных документах оператора.

4. Внедрение базовых мер защиты информации

Новые составы правонарушений не предполагают привлечение оператора к административной ответственности за невыполнение нормативных требований к технической защите персональных данных как таковых. Огромные штрафы ждут только тех, чьи ошибки в выстраивании системы информационной безопасности привели к эффективной утечке персональных данных. Это позволяет операторам в первую очередь сосредоточиться не на буквальном выполнении подзаконных актов в области технической защиты информации (например, Приказа ФСТЭК России № 21), а на устранении или снижении ключевых практических рисков, угрожающих их инфраструктуре.

Из года в год исследования крупнейших игроков рынка информационной безопасности показывают, что основная масса утечек данных происходит в связи с нарушением базовых правил защиты информации (несвоевременная установка обновлений, использование «заводских» паролей и т.д.). Как следствие, последовательное внедрение даже самых примитивных практик в области защиты информации может существенно повысить уровень защищенности компании.

5. Внедрение контролей, позволяющих поддерживать надлежащий уровень комплаенса

Вопреки распространенному заблуждению, соответствие требованиям законодательства не достигается посредством утверждения стопки локальных нормативных актов с последующей подачей уведомления о начале обработки персональных данных. Одной из основных задач оператора является поддержание состояния комплаенса с течением времени (а в идеале повышение его уровня). Предпринимая описанные выше меры, оператору необходимо параллельно внедрять механизмы контроля за их соблюдением, актуальностью и эффективностью. Это включает практики регулярных внутренних аудитов, инициативное информирование сотрудников о новых процессах обработки персональных данных, а также технические тестирования защищенности инфраструктуры.

Описанный выше перечень шагов не является исчерпывающим. Однако в условиях ограниченных ресурсов и времени он может позволить существенно снизить вероятность привлечения оператора и его должностных лиц к административной ответственности.

Мы с радостью готовы оказать вам и вашим коллегам содействие в реализации описанных шагов. Уже сейчас наш сервис PrivacyLine существенно упрощает выполнение большинства из описанных шагов, начиная с основного – инвентаризации процессов обработки данных. В тех случаях, когда запрос клиента требует индивидуального подхода, к вашим услугам консультации наших специалистов, имеющих многолетний опыт работы в области защиты персональных данных.

Антон Брагинец

Генеральный директор DataCase, директор по развитию Privacy Tech

anton.braginets@datacase.pro

Ксения Смирнова

Генеральный директор Privacy Tech

kseniya.smirnova@privacy-tech.ru

Подписывайтесь на telegram канал: https://t.me/privacy_tech

Сервис PrivacyLine

Сервис, который позволяет выполнять требования 152-ФЗ в формате «единого окна»

Возможности сервиса

Учет

Ведите реестры процессов, ИСПДн, хранилищ документации, получателей и обработчиков персональных данных в соответствии с требованиями 152-ФЗ в формате «единого окна».

Выгрузка

Выгружайте необходимые данные в удобном формате для создания документов: согласий, договоров, политик, локальных актов, отчетов и других.

База знаний

Используйте экспертную базу знаний с ответами на актуальные вопросы в сфере персональных данных, шаблонами документов, типовыми формами согласий и договоров.

История аудита

Сохраняйте историю взаимодействия с владельцами бизнес-процессов, связанных с обработкой персональных данных, а также проведенных аудитов соответствия требованиям 152-ФЗ.

Гостевой доступ

Предоставляйте гостевой доступ коллегам для проверки, заполнения или актуализации отдельных разделов реестров.

Справочники и подсказки

Используйте встроенные справочники параметров обработки и подсказки к полям, чтобы заполнять реестры быстрее и без существенных затрат на погружение в сложную терминологию.

PrivacyLine включен в Реестр российского программного обеспечения (№ 23683)

Подробнее см. на privacy-tech.ru