

Информационное письмо

Бизнесу приготовиться: давно ожидаемые законы по ужесточению ответственности за нарушения обработки ПДн окончательно приняты

4 декабря 2024 г.

Уважаемые дамы и господа!

Информируем Вас о принятии ряда важных законов, направленных на ужесточение административной ответственности и введение составов новых уголовных преступлений в сфере обработки персональных данных.

Увеличение штрафов за утечки ПДн и неуведомление Роскомнадзора

Р 30 ноября 2024 года Президентом РФ был подписан Федеральный закон № 420-ФЗ¹, который ужесточает административную ответственность за утечки персональных данных («ФЗ-420»).

Также ФЗ-420 дополняет КоАП РФ другими составами административных правонарушений и увеличивает размеры штрафов за правонарушения, уже предусмотренные действующими составами ст. 13.11 КоАП РФ.

Состав	Размеры штрафов для ЮЛ и ИП ² , рубли
Новые составы ст. 13.11 КоАП РФ	
Действие (бездействие), повлекшее неправомерную передачу (предоставление, распространение, доступ) персональных данных («утечка ПДн») ч. 12–14 ст. 13.11 КоАП РФ	
• от 1 000 до 10 000 субъектов ПДн и/или от 10 000 до 100 000 идентификаторов ³	от 3 до 5 млн
• от 10 000 до 100 000 субъектов ПДн и/или от 100 000 до 1 млн идентификаторов	от 5 до 10 млн
• более 100 000 субъектов ПДн и/или более 1 млн идентификаторов	от 10 до 15 млн

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

² Обращаем внимание, что по ч. 1.1 и ч. 8–18 ст. 13.11 КоАП ИП несут административную ответственность как ЮЛ. Между тем для составов ч. 10–18 КоАП РФ ответственность для должностных лиц негосударственных организаций не предусмотрена.

³ Под идентификатором понимается уникальное обозначение сведений о физическом лице, содержащееся в информационной системе персональных данных оператора и относящееся к такому лицу.

<p>Повторная утечка ПДн, если лицо ранее привлекалось по ч. 12–15 или по ч. 16–18 ст. 13.11 КоАП РФ</p> <p><i>ч. 15 ст. 13.11 КоАП РФ</i></p>	<p>от 1 до 3% размера выручки за календарный год, но не менее 20 млн и не более 500 млн</p>
<p>Утечка специальной категории ПДн</p> <p><i>ч. 16 ст. 13.11 КоАП РФ</i></p>	<p>от 10 до 15 млн</p> <p><i>*вне зависимости от количества субъектов ПДн, чьи ПДн утекли</i></p>
<p>Утечка биометрических ПДн</p> <p><i>ч. 17 ст. 13.11 КоАП РФ</i></p>	<p>от 15 до 20 млн</p> <p><i>*вне зависимости от количества субъектов ПДн, чьи ПДн утекли</i></p>
<p>Повторная утечка специальной категории ПДн или биометрических ПДн, если лицо ранее привлекалось по ч. 12–18</p> <p><i>ч. 18 ст. 13.11 КоАП РФ</i></p>	<p>от 1 до 3% размера выручки за календарный год, но не менее 25 млн и не более 500 млн</p>
<p>Неуведомление и/или несвоевременное уведомление Роскомнадзора об утечке ПДн</p> <p><i>ч. 11 ст. 13.11 КоАП РФ</i></p>	<p>от 1 до 3 млн</p>
<p>Неуведомление и/или несвоевременное уведомление Роскомнадзора о намерении осуществлять обработку ПДн</p> <p><i>часть 10 статьи 13.11 КоАП РФ</i></p>	<p>от 100 000 до 300 000</p>
<p>Новые размеры штрафов по ст. 13.11 КоАП РФ</p>	
<p>Незаконная обработка ПДн / обработка ПДн, несовместимая с целями их сбора</p> <p><i>ч. 1 ст. 13.11 КоАП РФ</i></p>	<p>от 150 000 до 300 000</p> <p><u>Повторное правонарушение:</u> от 300 000 до 500 000</p>

Смягчающие и отягчающие обстоятельства для повторных утечек по ч. 15 и ч. 18 ст. 13.11 КоАП РФ

Для повторных утечек по указанным составам отдельно закрепляются смягчающие и отягчающие вину обстоятельства.

Смягчающие обстоятельства

Вводится возможность снижения административного штрафа ниже нижнего порога за указанные составы – **до 0,1 %** от валовой выручки / собственных средств, но **не менее 15 и не более 50 млн руб.** при **одновременном** выполнении следующих условий:

- (А)** Ежегодные расходы на мероприятия по обеспечению информационной безопасности на протяжении 3 лет составляли не менее 0,1% от валовой выручки / собственных средств.

При этом привлекаемые подрядчики должны иметь соответствующую лицензию на ТЗКИ⁴ или лицензию на СКЗИ⁵. Аналогично при самостоятельном внедрении указанных мер оператор должен иметь соответствующую лицензию – при этом для целей технического обслуживания СКЗИ для собственных нужд лицензия не требуется.

⁴ Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации, п. 1 ч. 1 ст. 12 ФЗ «О лицензировании отдельных видов деятельности».

⁵ Лицензия ФСБ на услуги в области средств криптографической защиты информации, п. 5 ч. 1 ст. 12 ФЗ «О лицензировании отдельных видов деятельности».

- (В)** Проведение аудита, подтверждающего факт соблюдения требований к защите данных при обработке в информационных системах, в течение 12 месяцев до утечки.

Фактически это означает, что компаниям будет необходимо ежегодно проводить аудит своих ИСПДн.

- (С)** Отсутствиеотягчающих обстоятельств, предусмотренных для составов ч. 15 и ч. 18 ст. 13.11 КоАП РФ.

На иные правонарушения в сфере ПДн, включая на «первичные» утечки, будут распространяться общие смягчающие обстоятельства. Помимо этого, при наличии соответствующих оснований компании, как и ранее, смогут просить суд назначить штраф в размере ниже низшего предела или заменить его предупреждением.



Между тем, мы не исключаем, что суды будут учитывать наличие перечисленных выше обстоятельств при решении вопроса о возможном смягчении ответственности, как на «первичные» утечки, так и по иным составам ст. 13.11 КоАП РФ, и что они в конечном счете станут неким «стандартом добросовестности» для компаний.

Отягчающие обстоятельства

Отягчать ответственность по таким правонарушениям будут следующие обстоятельства:

- (А)** Продолжение противоправного поведения, несмотря на требования государственных органов по его прекращению.

ФЗ-420 не дает пояснений, что считать продолжением противоправного поведения при утечке ПДн. Можно предположить, что таким будет являться непрекращение неправомерной передачи или непринятие мер по исключению причин утечки и предотвращению последствий – однако последние действия формально не являются квалифицирующими для составов по ч. 15 и ч. 18 ст. 13.11 КоАП РФ.

- (В)** Лицо ранее привлекалось к ответственности по ч. 1–11 ст. 13.11 и/или ст. 13.6, ст. 13.12 КоАП РФ и на момент вынесения постановления по утечкам считается подвергнутым административному наказанию по прошлым правонарушениям (ст. 4.6 КоАП РФ).

Отмена «скидок»

Ранее действовавшая «скидка» в размере 50% для уплаты штрафа за правонарушение по ст. 13.11 КоАП РФ, выявленное в ходе государственного или муниципального контроля, отменяется.

Таким образом, за любые правонарушения по составам ст. 13.11 КоАП РФ юридическим лицам будет необходимо выплатить всю сумму назначенного штрафа.

Изменение подсудности для ст. 13.11 КоАП РФ

Подсудность составов ст. 13.11 КоАП РФ будет отнесена к арбитражным судам – напомним, что ранее они рассматривались мировыми судьями.

Изменение подсудности является скорее плюсом для компаний в силу большей бизнес-ориентированности специализации судей арбитражных судов и специфики рассматриваемых ими дел.

Иные нововведения

Также ФЗ-420 предусматриваются новые составы, связанные с нарушениями обработки биометрических ПДн в ЕБС и иных информационных системах:

Состав	Размеры штрафов, рубли
Нарушение порядка обработки биометрических ПДн в ЕБС и иных информационных системах ч. 2 ст. 13.11 ³ КоАП РФ	ДЛ – от 100 000 до 300 000 ЮЛ – от 500 000 до 1 млн
Непринятие организационных и технических мер по обеспечению безопасности биометрических ПДн в ЕБС и иных информационных системах	ДЛ – от 300 000 до 500 000 ЮЛ – от 1 млн до 1,5 млн

Состав	Размеры штрафов, рубли
<i>ч. 3 ст. 13.11³ КоАП РФ</i>	
Обработка биометрических ПДн без аккредитации <i>ч. 4 ст. 13.11³ КоАП РФ</i>	ДЛ – от 500 000 до 1 млн ЮЛ – от 1 млн до 2 млн
Отказ в заключении, исполнении, изменении или расторжении договора с потребителем в связи с его отказом от прохождения идентификации и/или аутентификации с использованием его биометрических ПДн <i>ст. 14.8 КоАП РФ</i>	ДЛ – от 50 000 до 100 000 ЮЛ – от 200 тысяч до 500 000

Помимо этого, для кредитных организаций вводится общее ограничение по размеру административных штрафов по составам КоАП РФ, исчисляемых из размера собственных средств кредитной организации – он не может превышать 3% размера собственных средств кредитной организации.

Вступление в силу

Изменения в КоАП РФ вступят в силу 30 мая 2025 года – спустя 180 дней после официального опубликования ФЗ-420.

Уголовная ответственность за незаконный оборот и утечки ПДн



30 ноября 2024 года Президентом РФ также был подписан Федеральный закон № 421-ФЗ⁶, который предусматривает новые составы в УК РФ за преступления, связанные с незаконным оборотом ПДн и их утечками («ФЗ-421»):

Примеры составов по ст. 272.1 УК РФ ⁷	Наказание
Незаконное использование и/или передача (распространение, предоставление, доступ), сбор и/или хранение компьютерной информации, содержащей ПДн, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем ⁸ <i>ч. 1 ст. 272.1 УК РФ</i>	<ul style="list-style-type: none"> штраф до 300 тыс руб. или в размере иного дохода за период до 1 года либо принудительные работы на срок до 4 лет либо лишение свободы на срок до 4 лет <p>Если сопряжено с трансграничной передачей ПДн или носителей с ПДн⁹:</p> <ul style="list-style-type: none"> лишение свободы на срок до 8 лет + штраф до 2 млн руб. / иного дохода за период до 3 лет + возможность лишения права занимать определенные должности / заниматься определенной деятельностью на срок до 4 лет.
Создание и/или обеспечение функционирования информационного ресурса (в сети Интернет, информационной системы или ПО) для заведомо незаконного хранения, передачи (распространения, предоставления, доступа) компьютерной	штраф до 700 тыс руб. или в размере иного дохода за период до 2 лет с возможностью лишения права занимать определенные

⁶ Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

⁷ Обработка ПДн физическими лицами исключительно для личных и семейных нужд не подпадает под действие вводимого состава ст. 272.1 УК РФ.

⁸ В отдельных случаях предусмотрена более строгая ответственность, например, если данные преступные действия совершены с использованием специальных категорий ПДн, биометрических ПДн, или ПДн несовершеннолетних.

⁹ Под трансграничным перемещением носителей с ПДн понимается совершение действий по ввозу на территорию РФ и/или вывозу с территории РФ машиночитаемого носителя информации (в том числе магнитного и электронного), на который осуществлены запись и хранение такой информации.

<p>информации с ПДн, полученной незаконным путем</p> <p>ч. 6 ст. 272.1 УК РФ</p>	<p>должности / заниматься определенной деятельностью +</p> <ul style="list-style-type: none"> • принудительные работы на срок до 5 лет; либо • лишение свободы на срок до 5 лет.
----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Изменения в УК РФ вступят в силу 11 декабря 2024 года – через 10 дней со дня официального опубликования ФЗ-421.

Рекомендации по соответствию новому регулированию

У операторов есть 6 месяцев, чтобы оценить текущее соответствие процессов обработки ПДн и подготовиться к изменениям, в частности:



- Провести **аудит процессов обработки персональных данных, уделяя пристальное внимание своим ИСПДн**, и осуществить необходимые мероприятия в сфере информационной безопасности. Обязательно задокументировать результаты аудита, разработать план проведения ежегодных аудитов ИСПДн, регулярно проводить и документировать тренинги для работников по работе с ПДн.



- Еще не поздно разработать и внедрить **внутреннюю процедуру реагирования** на утечки персональных данных в компании, учитывая требования об уведомлении Роскомнадзора о подобных инцидентах и возможное информирование субъектов. В случае утечки **применять эти меры реагирования**, что может быть расценено судом как обстоятельство, смягчающее ответственность.



- Пересмотреть договоры / соглашения со сторонними организациями, привлекаемыми при обработке персональных данных (как с операторами, так и с обработчиками), на наличие обязанности об уведомлении оператора об утечках персональных данных, а также обязанности о принятии мер по **информационной безопасности**.



- Актуализировать **ЛНА** в сфере обеспечения информационной безопасности и проинформировать об этом работников.



- Направить в Роскомнадзор **уведомление об обработке** персональных данных, если ранее это не было сделано.
- Легализовать осуществляемую **трансграничную передачу ПДн**.

Мы надеемся, что информация, представленная в настоящем информационном письме, будет для Вас полезной. Если кто-либо из Ваших коллег также хотел бы получать наши информационные письма, пожалуйста, направьте ему [ссылку](#) на электронную форму подписки. Если Вы хотите узнать больше о нашей практике **Защиты данных и кибербезопасности**, напишите нам об этом в ответном письме. Мы будем рады направить Вам наши материалы.

Примечание: обращаем Ваше внимание на то, что информация, представленная в данном Информационном письме, основана на нашем анализе данных из открытых источников, а также на нашем понимании предусмотренных законодательных норм и практики правоприменения. Авторы данного письма, равно как и юридическая фирма АЛРУД, не несут ответственности за последствия, возникшие в результате принятия решений на основе данной информации.

В случае возникновения вопросов, пожалуйста, свяжитесь с Партнером АЛРУД

С уважением,
Юридическая фирма
АЛРУД



Мария Остащенко

Партнер

Коммерческое право,
Интеллектуальная собственность,
Защита данных и
кибербезопасность

E: mostashenko@alrud.com