

Инциденты с персональными данными: | **Алексей Мунтян**
разбираемся в деталях | *Редакция от 13.10.2022*



Инцидент с
персональными данными



Алексей Мунтян, 14 лет в Data Privacy

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

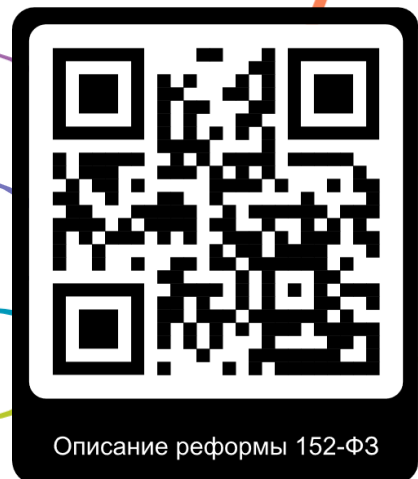
Внешний Data Protection Officer в двух транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru



Моя визитка



Экстерриториальность требований 152-ФЗ

Сокращение сроков обработки запросов субъектов ПД и Роскомнадзора

Право субъектов ПД на забвение

Новые требования к согласиям субъектов ПД

Новые требования к поручению обработки ПД

Новые требования к договорам с субъектами ПД

Новые требования к трансграничной передаче ПД

Роскомнадзором разработана рекомендованная форма уведомления о намерении осуществлять трансграничную передачу ПД

Приказ Роскомнадзора от 05.08.2022 №128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД"

Проект постановления Правительства РФ о порядке принятия решения о запрещении или ограничении трансграничной передачи ПД по представлению Роскомнадзора

Проект постановления Правительства РФ о порядке принятия решения о запрещении или ограничении трансграничной передачи ПД в целях защиты нравственности, здоровья, прав и законных интересов граждан

Проект постановления Правительства РФ о случаях, когда уведомление Роскомнадзора о трансграничной передаче ПД не требуется

Разработка Роскомнадзором требований (методики) в отношении оценки вреда субъектам ПД

Новые требования к локальным актам о ПД

Требования о взаимодействии с ГосСОПКА

Разработка ФСБ требований в отношении порядка взаимодействия операторов с ГосСОПКА, включая информирования ФСБ о компьютерных инцидентах

Совместная разработка ФСБ и Роскомнадзором порядка передачи информации о компьютерных инцидентах из ФСБ в Роскомнадзор

Требования об уведомлении в отношении инцидентов с ПД

Роскомнадзором разработана рекомендованная форма уведомления о факте неправомерной или случайной передачи ПД, повлекшей нарушение прав субъектов ПД

Возможна разработка Роскомнадзором порядка и условий взаимодействия с операторами в рамках ведения реестра учета утечек ПД

Новые требования к уничтожению ПД

Разработка Роскомнадзором требований в отношении подтверждения факта уничтожения ПД [проект НПА опубликован]

Новые требования к уведомлению об обработке ПД

Разработка Роскомнадзором новых форм уведомлений в отношении Реестра операторов [проект НПА опубликован]

с 2023.03

5 Уведомление об инцидентах с ПД

Требования о взаимодействии с ГосСОПКА

Разработка ФСБ требований в отношении порядка взаимодействия операторов с ГосСОПКА, включая информирования ФСБ о компьютерных инцидентах

Совместная разработка ФСБ и Роскомнадзором порядка передачи информации о компьютерных инцидентах из ФСБ в Роскомнадзор

Роскомнадзором разработана рекомендованная форма уведомления о факте неправомерной или случайной передачи ПД, повлекшей нарушение прав субъектов ПД

Требования об уведомлении в отношении инцидентов с ПД

Возможна разработка Роскомнадзором порядка и условий взаимодействия с операторами в рамках ведения реестра учета утечек ПД



Описание реформы 152-ФЗ

Локальным актам о ПД

Требования о взаимодействии с ГосСОПКА

Разработка ФСБ требований в отношении порядка взаимодействия операторов с ГосСОПКА, включая информирования ФСБ о компьютерных инцидентах

Совместная разработка ФСБ и Роскомнадзором порядка передачи информации о компьютерных инцидентах из ФСБ в Роскомнадзор

Роскомнадзором разработана рекомендованная форма уведомления о факте неправомерной или случайной передачи ПД, повлекшей нарушение прав субъектов ПД

Требования об уведомлении в отношении инцидентов с ПД

Возможна разработка Роскомнадзором порядка и условий взаимодействия с операторами в рамках ведения реестра учета утечек ПД

Новые требования к уничтожению ПД

Разработка Роскомнадзором требований в отношении подтверждения факта уничтожения ПД [проект НПА опубликован]

Новые требования к уведомлению об обработке ПД

Разработка Роскомнадзором новых форм уведомлений в отношении Реестра операторов [проект НПА опубликован]

Экстерриториальные требования

Сокращение сроков запросов субъектов ПД и Роскомнадзора

Право субъектов ПД на забвение


Новые требования к согласиям субъектов ПД

Новые требования к поручению обработки ПД

Новые требования к договорам с субъектами ПД

с 2023.03

6 Инциденты с ПД – общепринятое понимание

 Инцидент с ПД – это любое нарушение безопасности (конфиденциальности, целостности, доступности) ПД или требований законодательства о ПД или условий соглашений об обработке ПД.

**Обработка ПД
без законного
основания**

**Взлом
учетной
записи**

**Взлом
информационно
й системы или
базы данных**

**Неправильное
уничтожение ПД на
электронном
носителе**

**Неправильное
уничтожение
документа с ПД**

**Утеря
устройства с ПД**

**Утеря
документа с ПД**

**Неверно
направленное
электронное
письмо с ПД**

**Несанкциониро-
ванный доступ к
файлам с ПД**

**Несанкциониро-
ванная
публикация ПД**

**Несанкциониро-
ванная передача
ПД**

**Применение
методов
социальной
инженерии**

7 Инциденты с ПД – правовая дефиниция в РФ

<p>Инцидент с ПД ст.21 152-ФЗ «О ПД»</p>	<p>Компьютерный инцидент с ПД ст.19 152-ФЗ «О ПД»</p>
<p><u>передача</u> (т.е. предоставление, распространение или доступ) ПД</p>	
<p>неправомерная или случайная</p>	<p>неправомерная</p>
<p><u>повлекшая</u> нарушение прав субъектов ПД</p>	<p>произошедшая в <u>результате</u> компьютерной атаки</p>
<p>требующая уведомить Роскомнадзор</p>	<p>требующая проинформировать ФСБ (ГосСОПКА)</p>

По мнению Роскомнадзора

Требуется уведомление РКН

- ✓ Выявили неправомерное копирование базы данных
- ✓ Копия базы данных доступна в интернете
- ✓ Получено сообщение с угрозой раскрыть базу данных

Не требуется уведомление РКН

- ✗ НСД внутреннего пользователя к базе без копирования
- ✗ Случайное уничтожение базы внутренним пользователем
- ✗ Подозрительная активность пользователя системы

Сведения об инциденте

Предполагаемые причины, повлекшие нарушение

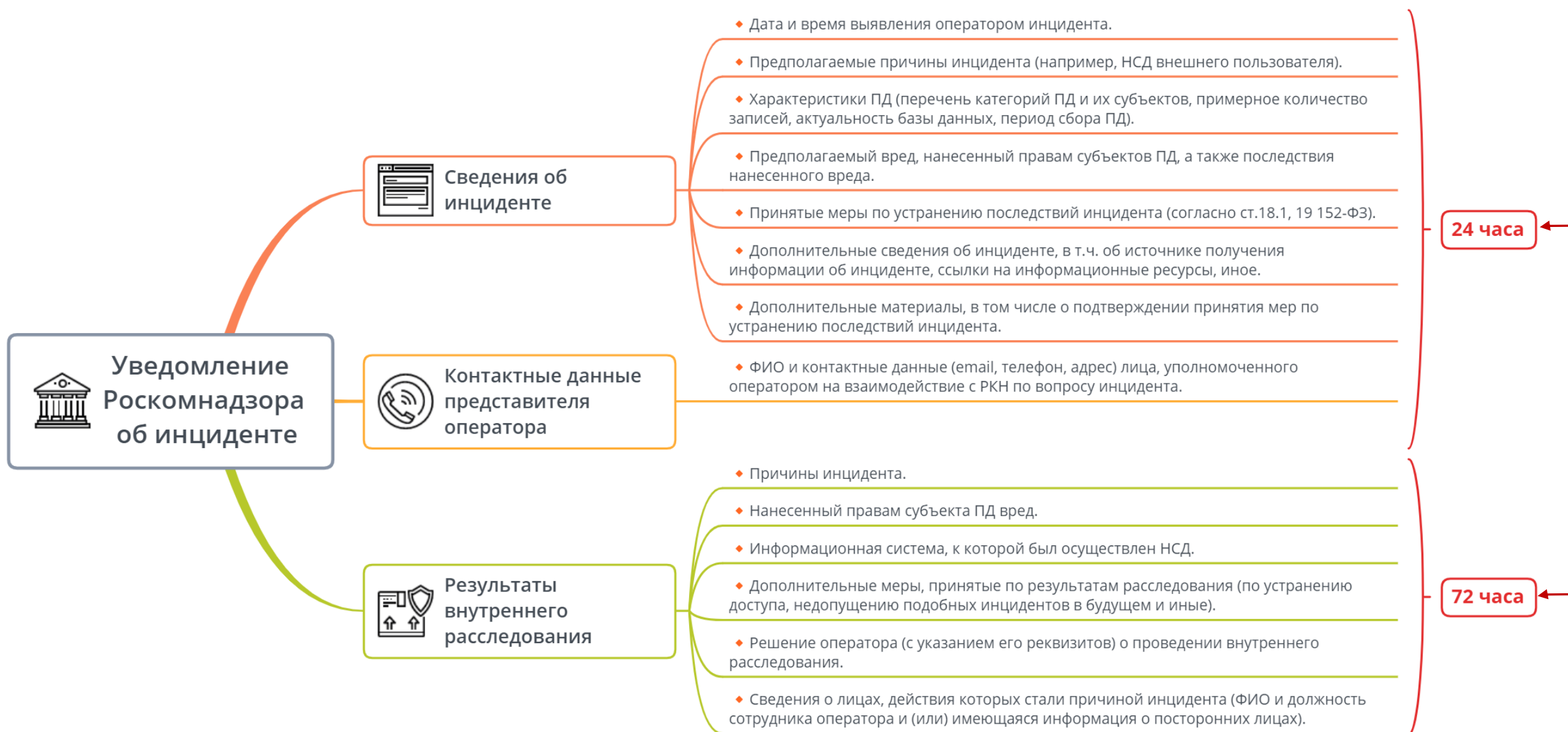
укажите предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных, например, несанкционированный доступ внешнего пользователя, несанкционированный доступ, связанный с уязвимостями программного обеспечения информационной системы и иные



Примечание

В некоторых сценариях могут сочетаться признаки обоих видов инцидентов, например, неправомерная передача (доступ) ПД, произошедшая в результате компьютерной атаки, повлекшая нарушение прав субъектов ПД, требующая уведомить Роскомнадзор и проинформировать ФСБ (ГосСОПКА).

С момента выявления инцидента оператором, Роскомнадзором или иным заинтересованным лицом





Проект изменений в КоАП РФ

ч.10 ст.13.11: для утечки ПД от 10.000 до 100.000 записей в отношении субъектов ПД, штраф для должностных лиц – от 200.000₽ до 400.000₽, а штраф для ИП и юрлиц – 0,02% от годового оборота, но не менее 1.000.000₽.

ч.11 ст.13.11: для утечки ПД более 100.000 записей в отношении субъектов ПД, штраф для должностных лиц – от 400.000₽ до 600.000₽, а штраф для ИП и юрлиц – до 1% от годового оборота, но не менее 2.000.000₽.

Ст.2.4 КоАП РФ

Административная ответственность должностных лиц требует выполнения ими «распорядительных» или «административно-хозяйственных» функций.

Смягчающие обстоятельства:

- ↑ Оператор ранее направил в Роскомнадзор результаты добровольной оценки соответствия уровня защищенности ИСПД требованиям законодательства.
- ↑ Инцидент с ПД не связан с неисполнением оператором требований в области ПД и защиты информации.

Отягчающие обстоятельства:

- ↓ Инцидент с особо чувствительными ПД (например, медицинскими данными) или биометрическими ПД.
- ↓ Оператор не направил вовремя уведомление об инциденте в Роскомнадзор.
- ↓ Оператор не способствовал административному или уголовному расследованию инцидента.
- ↓ Оператор не предоставил сведения об инциденте по запросу Роскомнадзора.
- ↓ Оператор ранее не направил в Роскомнадзор уведомление об обработке ПД.

Благодарю за ваше внимание



Алексей Мунтян, *14 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

Внешний Data Protection Officer в двух транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru