Инциденты с персональными данными: разбираемся в деталях

Алексей Мунтян

Редакция от 16.02.2023

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 четырёх транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru

Telegram-канал

Реформа 152-ФЗ

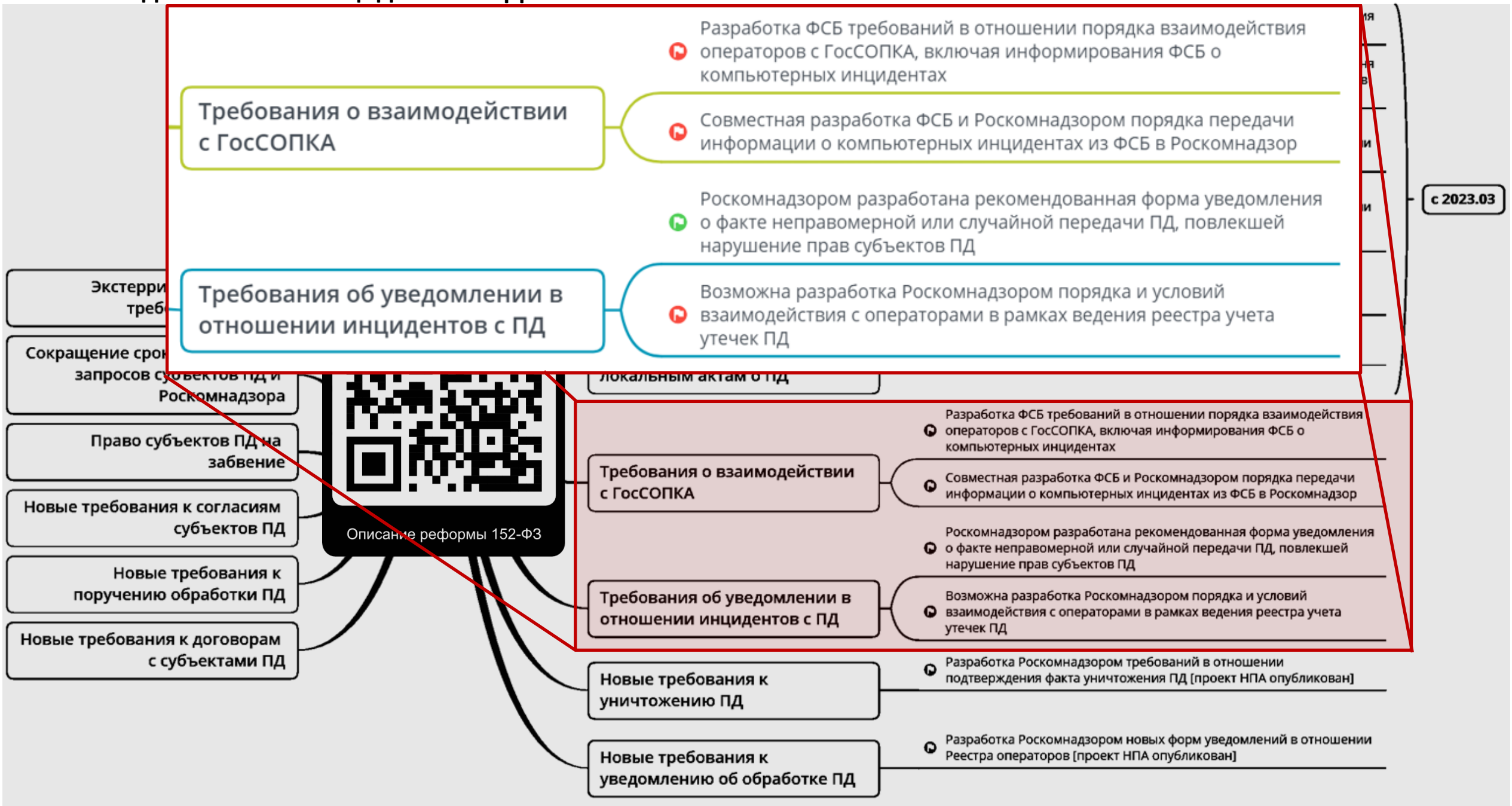
Описание реформы 152-ФЗ

- 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"
  - Постановление Правительства РФ о порядке принятия решения о запрещении или ограничении трансграничной передачи ПД по представлению Роскомнадзора (опубликован проект НПА)
  - Постановление Правительства РФ о порядке принятия решения о запрещении или ограничении трансграничной передачи ПД в целях защиты нравственности, здоровья, прав и законных интересов граждан (опубликован проект НПА)
  - Постановление Правительства РФ о случаях, когда уведомление Роскомнадзора о трансграничной передаче ПД не требуется (опубликован проект НПА)
- Новые требования к локальным актам о ПД
  - Приказ 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"
- Требования о взаимодействии с ГосСОПКА
  - Приказ ФСБ России о порядке взаимодействия операторов с ГосСОПКА, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПД (опубликован проект НПА)
  - Совместная разработка ФСБ и Роскомнадзором порядка передачи информации о компьютерных инцидентах из ФСБ в Роскомнадзор (опубликован проект НПА)
- 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
  - Приказ Роскомнадзора от 14.11.2022 №187 "Об утверждении Порядка и условий взаимодействия Роскомнадзора с операторами в рамках ведения реестра учета инцидентов с ПД"
- Новые требования к уничтожению ПД
  - Приказ Роскомнадзора от 28.10.2022 №179 "Об утверждении Требований к подтверждению уничтожения персональных данных"
- Новые требования к уведомлению об обработке ПД
  - Приказ Роскомнадзора от 28.10.2022 №180 "Об утверждении форм уведомлений о намерении осуществлять обработку ПД, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПД, о прекращении обработки ПД"

с 2023.03

4 Уведомление об инцидентах с ПД



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 информационной 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**

Инциденты с ПД – правовая дефиниция в РФ

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

По мнению Роскомнадзора

Требуется уведомление РКН	Не требуется уведомление РКН
Выявили неправомерное копирование базы данных	НСД внутреннего пользователя к базе без копирования
Копия базы данных доступна в интернете	Случайное уничтожение базы внутренним пользователем
Получено сообщение с угрозой раскрыть базу данных	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).

7 Уведомление Роскомнадзора об инциденте (утечке) с ПД

Ч.3.1 СТ.21 152-ФЗ «В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных»

- ✓ ВЫЯВИЛИ НЕПРАВОМЕРНОЕ КОПИРОВАНИЕ БАЗЫ ДАННЫХ
- ✓ КОПИЯ БАЗЫ ДАННЫХ ДОСТУПНА В ИНТЕРНЕТ
- ✓ ПОЛУЧЕНО СООБЩЕНИЕ С УГРОЗОЙ РАСКРЫТЬ БАЗУ ДАННЫХ
- ✗ НСД ВНУТРЕННЕГО ПОЛЬЗОВАТЕЛЯ К БАЗЕ БЕЗ КОПИРОВАНИЯ
- ✗ СЛУЧАЙНОЕ УНИЧТОЖЕНИЕ БАЗЫ ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЕМ
- ✗ ПОДОЗРИТЕЛЬНАЯ АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ

24 ЧАСА — СООБЩЕНИЕ ОБ УТЕЧКЕ
ХАРАКТЕРИСТИКИ ДАННЫХ, ОБСТОЯТЕЛЬСТВА ИНЦИДЕНТА, ОТВЕТСТВЕННЫЙ ЗА ВЗАИМОДЕЙСТВИЕ

72 ЧАСА — РЕЗУЛЬТАТ РАССЛЕДОВАНИЯ
ПРИЧИНЫ УТЕЧКИ, ВИНОВНЫЕ ЛИЦА

Ожидания Роскомнадзора от уведомления об инциденте с ПД

С момента выявления инцидента оператором, Роскомнадзором или иным заинтересованным лицом

Уведомление Роскомнадзора об инциденте

Сведения об инциденте

- Дата и время выявления оператором инцидента.
- Предполагаемые причины инцидента (например, НСД внешнего пользователя).
- Характеристики ПД (перечень категорий ПД и их субъектов, примерное количество записей, актуальность базы данных, период сбора ПД).
- Предполагаемый вред, нанесенный правам субъектов ПД, а также последствия нанесенного вреда.
- Принятые меры по устранению последствий инцидента (согласно ст.18.1, 19 152-ФЗ).
- Дополнительные сведения об инциденте, в т.ч. об источнике получения информации об инциденте, ссылки на информационные ресурсы, иное.
- Дополнительные материалы, в том числе о подтверждении принятия мер по устранению последствий инцидента.

Контактные данные представителя оператора

- ФИО и контактные данные (email, телефон, адрес) лица, уполномоченного оператором на взаимодействие с РКН по вопросу инцидента.

24 часа

Результаты внутреннего расследования

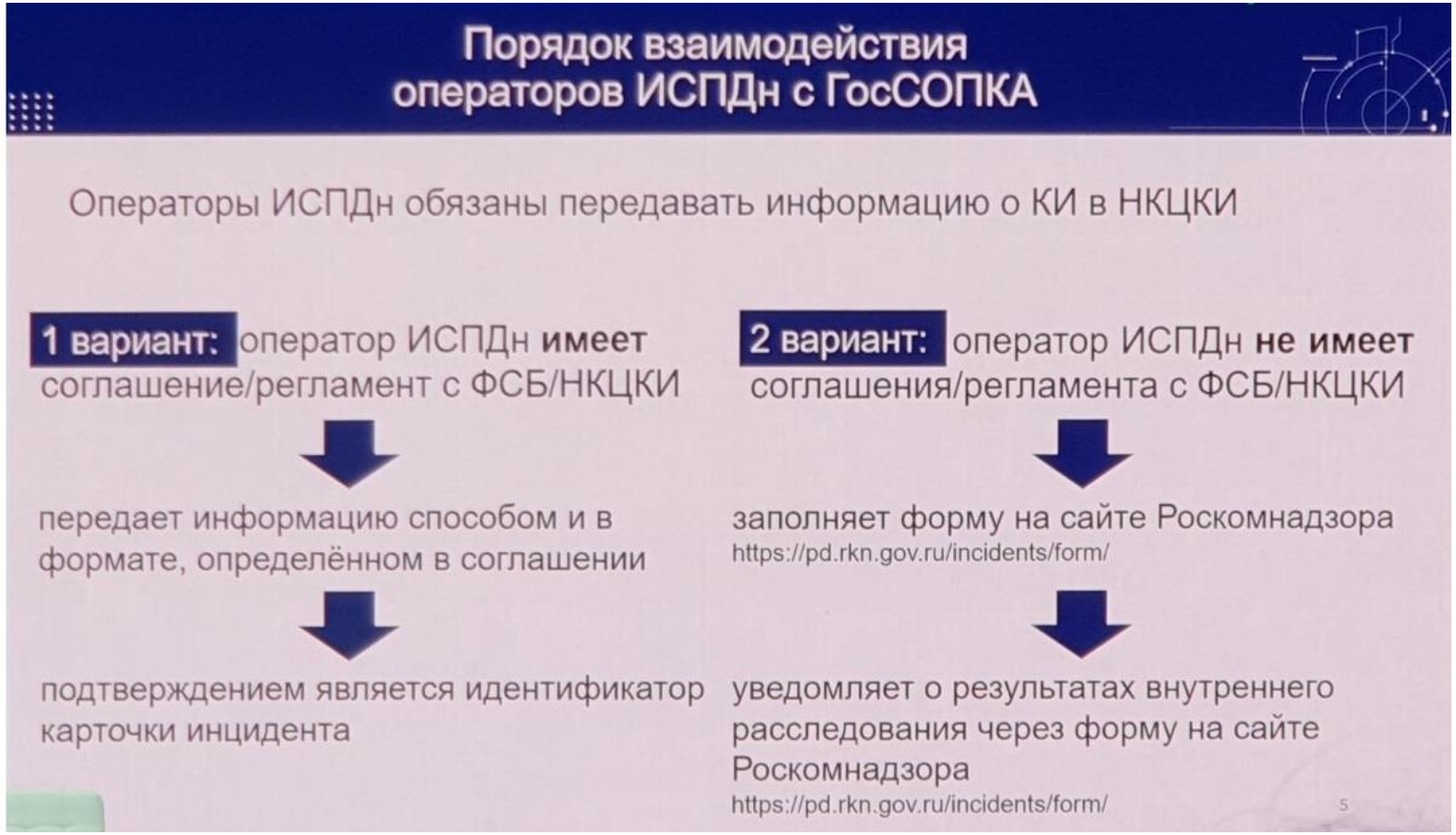
- Причины инцидента.
- Нанесенный правам субъекта ПД вред.
- Информационная система, к которой был осуществлен НСД.
- Дополнительные меры, принятые по результатам расследования (по устранению доступа, недопущению подобных инцидентов в будущем и иные).
- Решение оператора (с указанием его реквизитов) о проведении внутреннего расследования.
- Сведения о лицах, действия которых стали причиной инцидента (ФИО и должность сотрудника оператора и (или) имеющаяся информация о посторонних лицах).

72 часа

9 Взаимодействие с ГосСОПКА

SOC-форум 2022. А. Раевский (НКЦКИ):

- Проект порядка информирования ФСБ о компьютерных инцидентах с ПД опубликован 30.12.2022 на Госпортале.
- Предполагается, что будет два варианта взаимодействия (см. фото слайда презентации). Первый вариант будет аналогичен существующему порядку для субъектов КИИ. Во втором случае информирование будет осуществляться через сайт Роскомнадзора.
- НКЦКИ будет вправе запрашивать дополнительную информацию об инциденте у оператора (безотносительно трека, по которому в НКЦКИ поступает информация - напрямую или через Роскомнадзор).



SOC-форум 2022. С. Корелов (НКЦКИ):
За непредоставление информации о компьютерных инцидентах с ПД в ФСБ России планируется ввести административную откровенность.
У НКЦКИ (ФСБ России), как отметил спикер, имеются возможности выявления тех, кто будет скрывать такую информацию.

10 Уведомление об инциденте с ПД

- Что является инцидентом с ПД:
  - НСД внешнего пользователя к БПД
  - неправомерное копирование БПД
  - копия БД доступна в сети Интернет
  - получение сообщения с угрозой раскрыть БПД
- Что не является инцидентом с ПД:
  - НСД внутреннего пользователя к БПД без копирования
  - случайное уничтожение БПД внутренним пользователем
  - подозрительная активность пользователя системы

Инцидент с ПД

Неправомерная или случайная передача (предоставление, распространение, доступ) ПД, повлекшая нарушение прав субъектов ПД

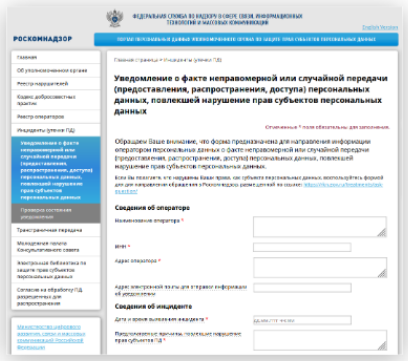
Инцидент может выявить:
- оператор ПД
- Роскомнадзор
- иное заинтересованное лицо

За неуведомление:
- пока что штраф до 5,000 ₽ (ст.19.7 КоАП)
- возможно будет отягчающим обстоятельством при назначении оборотного штрафа за инцидент

Приказ Роскомнадзора от 14.11.2022 №187.
Направляются 2 уведомления:
- о факте инцидента (24ч)
- о результатах расследования (72ч)

Уведомляется Роскомнадзор

Уведомление на веб-портале pd.rkn.gov.ru/incidents/form/



Компьютерный инцидент, повлекший неправомерную передачу (предоставление, распространение, доступ) ПД

Инцидент выявляет оператор ИСПД

За неуведомление:
- пока что штраф до 5,000 ₽ (ст.19.7 КоАП)
- возможно будет предусмотрена отдельная административная ответственность

Проект приказа ФСБ России о порядке взаимодействия операторов с ГосСОПКА.
Направляются 2 уведомления:
- о факте инцидента (24ч)
- о результатах расследования (72ч)

Уведомляется ФСБ

Уведомление на веб-портале pd.rkn.gov.ru/incidents/form/

Уведомление в ГосСОПКА согласно условиям соглашения/регламента между оператором ИСПД и НКЦКИ (пп.4.8 п.4 Положения о НКЦКИ)

- ГОСТ Р 59709-2022 - Управление компьютерными инцидентами. Термины и определения
- ГОСТ Р 59710-2022 - Управление компьютерными инцидентами. Общие положения
- ГОСТ Р 59711-2022 - Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами
- ГОСТ Р 59712-2022 - Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты

11 Перспективы усиления административной ответственности к 2023г.

Проект изменений в ст.13.11 КоАП РФ (*на 14.12.2022*)			
Часть	**Состав правонарушения**	**Санкция**	**Определение размера санкции**
10	Утечка ПД[1] в размере 10-100 тыс. записей в отношении субъектов ПД и (или) содержащей ПД 1-10 тыс. субъектов ПД	Штраф для ДЛ[2]: 300-600 тыс. ₽ Штраф для ИП/ЮЛ: 1-5 млн. ₽	Минимальный размер штрафа налагается при наличии смягчающих обстоятельств и при отсутствии отягчающих обстоятельств
11	Утечка ПД в размере >100 тыс. записей в отношении субъектов ПД и (или) содержащей ПД >10 тыс. субъектов ПД	Штраф для ДЛ: 600-800 тыс. ₽ Штраф для ИП/ЮЛ: 5-10 млн. ₽	
12	Рецидив утечки ПД, предусмотренной ч.10 или ч.11 ст.13.11 КоАП	Штраф для ДЛ: 800-1000 тыс. ₽	
		Штраф для ИП/ЮЛ: 1-3% от годового оборота, (минимум 5 млн. ₽ и максимум 500 млн. ₽)	
		Штраф для ИП/ЮЛ: 0,1% от годового оборота, (минимум 5 млн. ₽ и максимум 500 млн. ₽)	Наличие смягчающих обстоятельств, отсутствие отягчающих обстоятельств, а также компенсация не менее чем 2/3 пострадавшим[3] субъектам ПД возможного вреда в срок до 30 дней с даты утечки ПД и в размере не менее 0,5% от годового оборота (минимум 7 млн. ₽)

[1] **Утечка ПД** – несанкционированный доступ и (или) копирование, предоставление и (или) распространение баз данных (или их части), относящихся к субъектам ПД и позволяющих без использования дополнительной информации определить принадлежность содержащихся в них ПД конкретному субъекту ПД.

[2] **Должностные лица** – указанные в ст.2.4 КоАП лица, которые постоянно, временно или в соответствии со специальными полномочиями осуществляют функции представителя власти, а равно лиц, выполняющих организационно-распорядительные или административно-хозяйственные функции.

[3] Глава Минцифры РФ Максут Шадаев (https://tass.ru/ekonomika/16586731): «Если с 2/3 граждан урегулировано, то это будет смягчающим обстоятельством».

Смягчающие обстоятельства:

↑ Оператор ранее направил в Роскомнадзор результаты добровольной оценки соответствия уровня защищенности ИСПД требованиям законодательства

↑ Утечка не связана с неисполнением оператором требований в области ПД и защиты информации

Отягчающие обстоятельства:

↓ Утечка специальных категорий ПД (в т.ч. медицинских данных) или биометрических ПД

↓ Оператор не направил вовремя уведомление об утечке в Роскомнадзор

↓ Оператор не способствовал административному или уголовному расследованию утечки

↓ Оператор не предоставил сведения об утечке 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