Инциденты с персональными данными: разбираемся в деталях | Алексей Мунтян | *Редакция от 20.04.2023*

Алексей Мунтян, *15 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

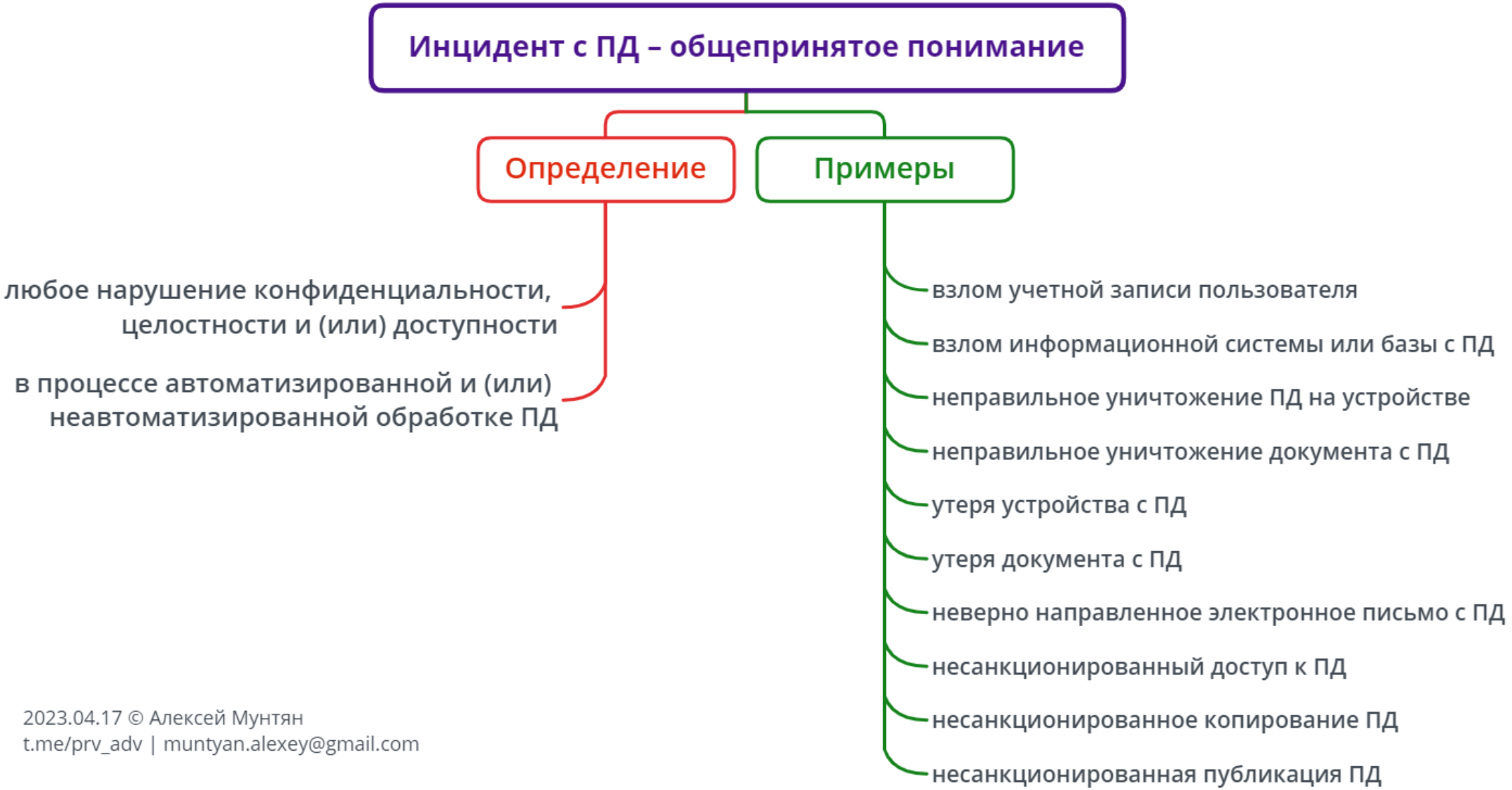
alexey.muntyan@privacy-advocates.ru

Telegram-канал

3 Реформа 152-ФЗ в 2022-2023гг.

2023.02.21 © Алексей Мунтян
t.me/prv_adv | muntyan.alexey@gmail.com

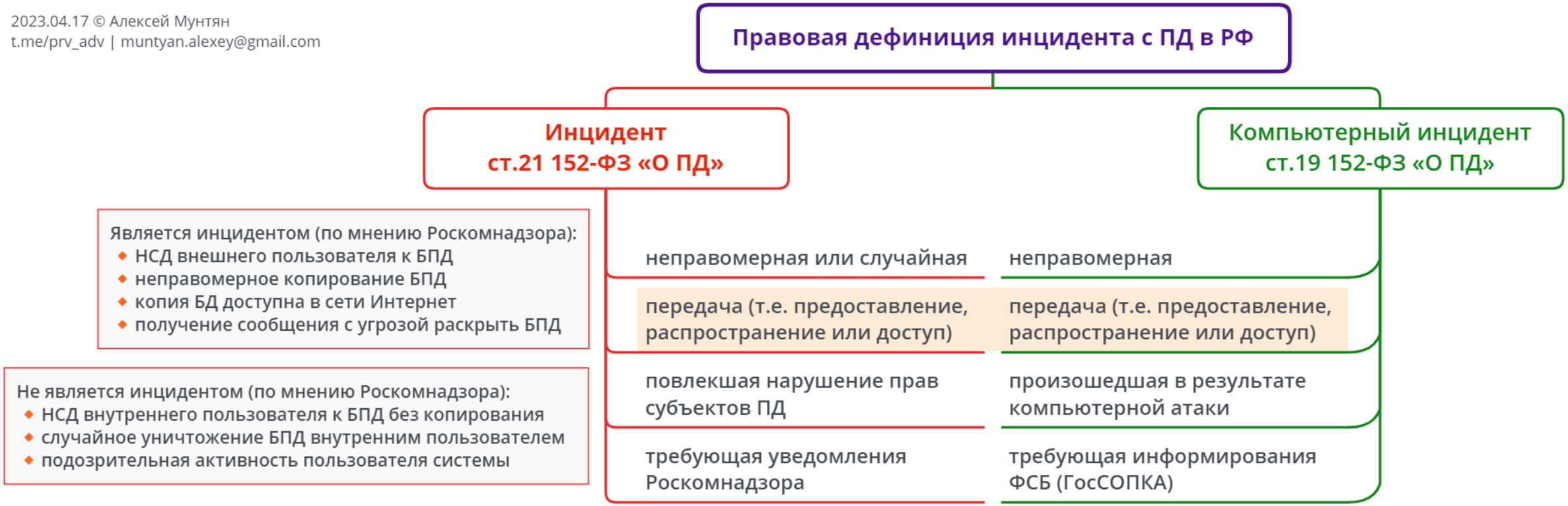
Инциденты с ПД – общепринятое понимание



2023.04.17 © Алексей Мунтян
t.me/prv_adv | muntyan.alexey@gmail.com

Инциденты с ПД – правовая дефиниция в РФ

2023.04.17 © Алексей Мунтян
t.me/prv_adv | muntyan.alexey@gmail.com



6 Управление инцидентом с ПД

2023.02.28 © Алексей Мунтян
t.me/prv_adv | muntyan.alexey@gmail.com

Инцидент с ПД

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

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

Инцидент выявляет оператор ИСПД

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

Приказ ФСБ от 13.02.2023 № 77 о порядке взаимодействия операторов с ГосСОПКА.
Направляются 1 или 2 уведомления:
- об обнаружении инцидента (24ч) - все операторы
- о результатах расследования (72ч) - операторы, использующие веб-портал Роскомнадзора

Уведомляется ФСБ

Уведомление на веб-портале pd.rkn.gov.ru/incidents/form/ - если у оператора нет соглашения с НКЦКИ (Роскомнадзор потом сам передает информацию в ФСБ)

Уведомление в ГосСОПКА при наличии 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

7 Ожидания Роскомнадзора от уведомления об инциденте с ПД

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
- **Контакты 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 несанкционированный доступ
  - 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

С момента выявления инцидента оператором, Роскомнадзором или иным заинтересованным лицом

Типичная аргументация оператора в суде по поводу инцидента

Типичная аргументация оператора в суде при условии установления факта инцидента

Содержание инцидента

- относительно небольшой масштаб инцидента (с т.з. количества затронутых субъектов ПД и записей о них)
- затронутые инцидентом ПД не содержат специальных и биометрических категорий, а также иных чувствительных данных
- затронутые инцидентом субъекты ПД не относятся к социально незащищенным группам населения

Объективная сторона инцидента

- инцидент произошёл у оператора впервые, оператор добросовестно выполнял все требования 152-ФЗ от 27.07.2006
- инцидент произошёл вследствие действий/бездействия контрагентов оператора или (и) действий злоумышленников
- оператор не получал жалоб, претензий, исков в связи с инцидентом
- оператор оценил нанесенный субъектам ПД уровень вреда как средний (см. приказ Роскомнадзора №178 от 27.10.2022)

Реагирование на инцидент

- своевременно и должным образом подготовлены и направлены в Роскомнадзор уведомления об инциденте
- оперативно и всесторонне организовано оповещение об инциденте всех заинтересованных лиц, включая субъектов ПД
- организован мониторинг публикаций скомпрометированной БПД и процесс инициирования удаления общедоступных копий БПД
- запланирован и реализован (реализуется) комплекс мер реагирования на инцидент и предотвращения инцидентов в будущем

2023.04.17 © Алексей Мунтян
t.me/prv_adv | muntyan.alexey@gmail.com

9 Перспективы усиления административной ответственности в 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, *15 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 четырех транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru