



Реагирование на утечку персональных данных: выиграть или не проиграть?



Алексей Мунтян, *16 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель в Russian Privacy Professionals
Association - RPPA.ru

Внешний Data Protection Officer в нескольких
транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru



СберСпасибо: 52M	Tele2: 7.5M	Госуслуги+Почта России: 2.5M
Спортмастер: 46M	START: 7.5M	Твое: 2.3M
СДЭК: 26M+25M+100k	Whoosh: 7.2M	Tutu.ru: 2.2M
Гемотест: 31M	Яндекс Еда: 6.9M	Yappy: 2.1M
ФССП (долги, штрафы): 17.5M	Oriflame: 5.5M	Аскона: 2M
Красное&Белое: 17M	Московская электронная школа: 5.5M	Tiktop-free.com: 1.9M
Альфастрахование: 14M	kassy.ru: 4.9M	Delivery Club: 1.6M
DNS: 11M	Book24.ru: 4M	Ykt.ru: 1.4M
Почта России: 10M	Ситимобил: 3.9M	В Масштабе: 1.4M
NL International: 10M	Miltor: 3.8M	Kari: 1.2M
Читай Город: 9.5M	ОНЛАЙН ТРЕЙД.py: 3.7M	Кинокасса: 1.2M
Hearst Shkulev — E1/NGS/Rugion: 9.1M	Text.ru: 3.5M	AllLossLess.net: 1.2M
Здравсити: 9M	Mail.ru: 3.5M	Level.travel: 1.2M
Золото 585: 8.4M	Gloria Jeans: 3M	Pikabu: 1M
СОГАЗ: 7.9M	Суши Мастер: 2.8M	
Ашан: 7.8M	ДОМ.py: 2.7M	



Сотрудников российских компаний предупредили о новом виде мошенничества от лица ФСБ

ИБ-эксперт Бедеров: мошенники стали шантажировать компании РФ фейковыми утечками

Роман Кильдюшкин



© Depositphotos

Мошенники начали рассылать сотрудникам российских операторов персональных данных (банков, операторов сотовой связи, интернет-провайдеров и не только) фейковые уведомления об утечках якобы от ФСБ с целью шантажа и вымогательства денежных средств. Об этом «Газете.Ru» сообщил руководитель департамента информационно-аналитических исследований компании Т.Hunter Игорь Бедеров.

◇ Мошенники начали рассылать сотрудникам российских операторов персональных данных (банков, операторов сотовой связи, интернет-провайдеров и не только) фейковые уведомления об утечках якобы от ФСБ с целью шантажа и вымогательства денежных средств.

◇ В рамках новой схемы мошенники обращаются в компании под видом сотрудников ФСБ с запросом на проведение проверки, вызванной якобы утечкой персональных данных клиентов. Далее мошенники либо сразу предлагают уладить вопрос посредством взятки, либо под видом проверки получают сведения личного характера о работниках компании или другие виды защищенной информации и после приступают к шантажу.

◇ Для убедительности письма мошенников в новой схеме дополняются фотографиями распечатанных поручений и приказов ФСБ с печатями и подписями реальных госслужащих. По словам Бедерова, данные документы являются подделками.

<https://www.gazeta.ru/tech/news/2023/12/15/21928249.shtml>





Проект изменений в ст.13.11 КоАП РФ (на 04.12.2023 - https://sozd.duma.gov.ru/bill/502104-8)		
Часть	Состав правонарушения	Санкция (штраф)
1 ^{update}	Обработка ПД в не предусмотренных законом случаях, либо обработка ПД, несовместимая с целями сбора ПД	ФЛ: 10-15 тыс. Р; ДЛ: 50-100 тыс. Р; ЮЛ: 150-300 тыс. Р
1.1 ^{update}	Повторная ¹ обработка ПД в не предусмотренных законом случаях, либо повторная обработка ПД, несовместимая с целями сбора ПД	ФЛ: 15-30 тыс. Р; ДЛ: 100-200 тыс. Р; ИП/ЮЛ: 300-500 тыс. Р
10 ^{new}	Неуведомление и (или) несвоевременное уведомление Роскомнадзора об обработке ПД	ФЛ: 5-10 тыс. Р; ДЛ ² : 30-50 тыс. Р; ИП/ЮЛ ³ : 100-300 тыс. Р
11 ^{new}	Неуведомление и (или) несвоевременное уведомление Роскомнадзора об утечке ПД ⁴ , повлекшей нарушение прав субъектов ПД	ФЛ: 50-100 тыс. Р; ДЛ: 400-800 тыс. Р; ИП/ЮЛ: 1-3 млн. Р
12 ^{new}	Действия (бездействия) оператора, повлекшие утечку ПД 1-10 тыс. субъектов и/или 10-100 тыс. идентификаторов ⁵	ФЛ: 100-200 тыс. Р; ДЛ: 800-1000 тыс. Р; ИП/ЮЛ: 3-5 млн. Р
13 ^{new}	Действия (бездействия) оператора, повлекшие утечку ПД 10-100 тыс. субъектов и/или 100-1000 тыс. идентификаторов	ФЛ: 200-300 тыс. Р; ДЛ: 1-1,5 млн. Р; ИП/ЮЛ: 5-10 млн. Р
14 ^{new}	Действия (бездействия) оператора, повлекшие утечку ПД >100 тыс. субъектов и/или >1000 тыс. идентификаторов	ФЛ: 300-400 тыс. Р; ДЛ: 1,5-2 млн. Р; ИП/ЮЛ: 10-15 млн. Р
15 ^{new}	Повторная утечка ПД, предусмотренная ч.ч.12-14 ст.13.11 КоАП	ФЛ: 400-600 тыс. Р; ДЛ: 2-4 млн. Р; ИП/ЮЛ: 0,1-3% от годового оборота (мин. 15 млн. Р и макс. 500 млн. Р)
16 ^{new}	Действия (бездействия) оператора, повлекшие утечку специальных категорий и/или биометрических ПД	ФЛ: 400-500 тыс. Р; ДЛ: 2-3 млн. Р; ИП/ЮЛ: 15-20 млн. Р
17 ^{new}	Повторная утечка специальных категорий и/или биометрических ПД оператором, который ранее наказывался по ч.ч.12-14, 16 ст.13.11 КоАП	ФЛ: 500-800 тыс. Р; ДЛ: 3-5 млн. Р; ИП/ЮЛ: 0,1-3% от годового оборота (мин. 20 млн. Р и макс. 500 млн. Р)

Отягчающие обстоятельства:

- повторное уведомление и (или) несвоевременное уведомление Роскомнадзора об утечке ПД, повлекшей нарушение прав субъектов ПД;
- продолжение правонарушения по ч.ч.12-17 ст.13.11 КоАП, несмотря на требование уполномоченных лиц прекратить его (п.1 ч.1 ст.4.3 КоАП).

¹ Совершение правонарушения в течение 1 года с момента, когда за аналогичное правонарушение это лицо уже ранее было наказано (см. ст.4.6 КоАП).

² **Должностное лицо** – должностное лицо государственного или муниципального органа, сотрудник государственного или муниципального учреждения (для ч.ч.10-17 ст.13.11 КоАП).

³ **Юридическое лицо** – юридическое лицо, не являющееся государственным или муниципальным органом/учреждением (для ч.ч.10-17 ст.13.11 КоАП).

⁴ **Утечка ПД** – факт неправомерной передачи (предоставления, распространения, доступа) ПД.

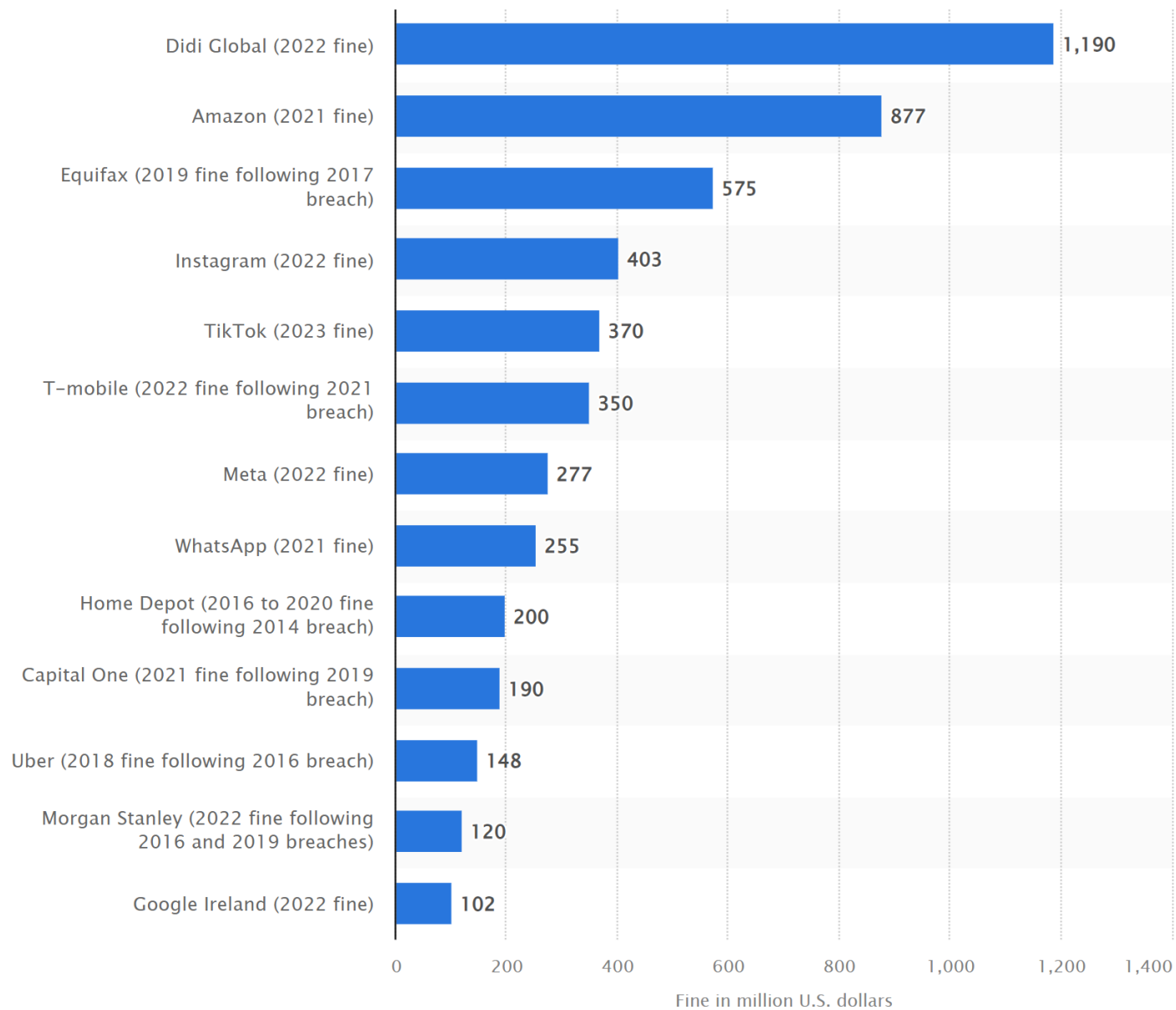
⁵ **Идентификатор** – уникальные обозначения сведений о физическом лице, необходимые для определения такого лица.

Проект новой ст.272 ¹ в УК РФ (на 04.12.2023 - https://sozd.duma.gov.ru/bill/502113-8)		
Часть	Состав преступления	Наказание
1	Незаконные ¹ использование и (или) передача (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации с ПД, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем	<ul style="list-style-type: none"> • штраф до 300 тыс. ₽ • принудительные работы до 4 лет • лишение свободы до 4 лет
2	Деяние по ч.1, совершенное в отношении компьютерной информации со специальными категориями ПД и (или) биометрическими ПД	<ul style="list-style-type: none"> • штраф до 700 тыс. ₽ или доход осужденного за 1 год + лишение права занимать определенные должности или заниматься определенной деятельностью до 2 лет • принудительные работы до 5 лет • лишение свободы до 5 лет
3	Деяния по ч.1 и (или) ч.2, совершенные: <ul style="list-style-type: none"> а) из корыстной заинтересованности; б) повлекшее причинение крупного ущерба; в) группой лиц по предварительному сговору; г) с использованием своего служебного положения 	<ul style="list-style-type: none"> • штраф до 1 млн ₽ или доход осужденного за 1 год + лишение права занимать определенные должности или заниматься определенной деятельностью до 3 лет • принудительные работы до 5 лет + штраф до 1 млн ₽ или доход осужденного за 2 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 3 лет • лишение свободы до 6 лет + штраф до 1 млн ₽ или дохода осужденного за 2 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 3 лет
4	Деяния по ч.ч. 1, 2 или 3, сопряженные с трансграничной передачей компьютерной информации с ПД и (или) трансграничным перемещением ² носителей с ПД	лишение свободы до 8 лет + штраф до 2 млн ₽ или доход осужденного за 3 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 4 лет
5	Деяния по ч.ч. 1, 2 или 3, если они повлекли тяжкие последствия ³ , либо были совершены организованной группой	лишение свободы до 10 лет + штраф до 3 млн ₽ или доход осужденного за 4 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 5 лет
6	Создание и(или) обеспечение функционирования информационных ресурсов (сайта в сети «Интернет» и (или) страницы сайта в сети «Интернет», информационной системы, программы для ЭВМ), заведомо предназначенных для незаконного хранения, передачи (распространения, предоставления, доступа) компьютерной информации с ПД	<ul style="list-style-type: none"> • штраф до 700 тыс. ₽ или доход осужденного за 2 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 2 лет • принудительные работы до 5 лет + штраф до 700 тыс. ₽ или доход осужденного за 2 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 2 лет • лишение свободы до 5 лет + штраф до 700 тыс. ₽ или дохода осужденного за 2 года + лишение права занимать определенные должности или заниматься определенной деятельностью до 2 лет

¹ Действие статьи не распространяется на случаи обработки ПД физическими лицами исключительно для личных и семейных нужд.

² **Трансграничное перемещение** – ввоз на территорию РФ и (или) вывозу из РФ машиночитаемого носителя информации (в том числе магнитного и электронного), на который осуществлена запись и хранение компьютерной информации с ПД.

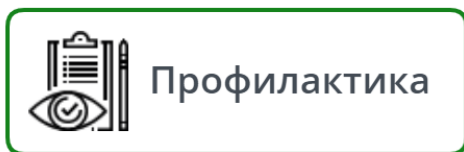
³ **Тяжкие последствия** – временная приостановка или нарушение работы оператора ПД, нарушение целостности ИСПД, распространение компьютерной информации с ПД неограниченному кругу лиц и (или) предоставление или доступ к ней третьим лицам с целью причинения вреда жизни, здоровью, имуществу, правам и законным интересам человека и гражданина, ущерба обороне и (или) безопасности государства, охране правопорядка и иным охраняемым федеральными законами ценностям.



Штрафы за утечки - это здорово!..
...для всех, кроме людей и компаний

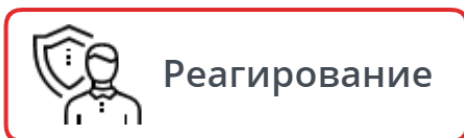


2023.11.10 © Алексей Мунтян | t.me/prv_adv



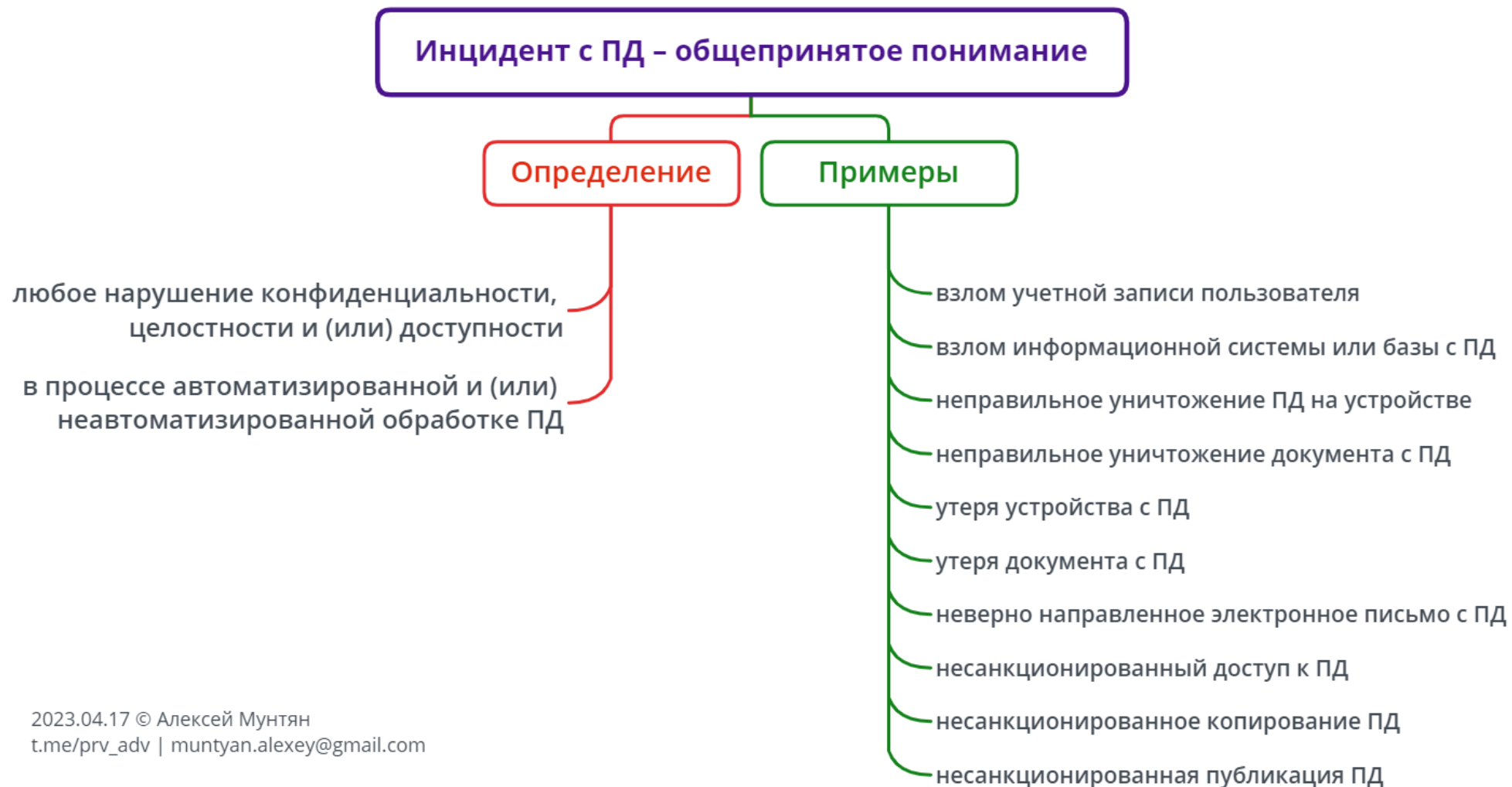
- Создание портала для повышения осведомленности
- Скидки и льготы (хотя бы для СМБ) на приобретение сертифицированных средств защиты информации

- Проектируемая защита ПД
- Лучшие практики обеспечения ИБ
- Чек-листы и тесты для самоконтроля



- Создание ИТ-платформы для централизованной подготовки и направления в суд коллективных исков пострадавших от утечки
- Отказ от объективного вменения, то есть от привлечения оператора к ответственности за утечку без установления его вины (см. ст.2.1 КоАП РФ)
- Стимулирование развития рынка страхования киберрисков в отношении ответственности операторов перед субъектами ПД и третьими лицами в случае инцидента с ПД





Правовая дефиниция инцидента с ПД в РФ

Инцидент ч.3.1 ст.21 152-ФЗ «О ПД»

Является инцидентом по приказу РКН от 14.11.2022 №187:

- ♦ БПД доступна неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) ПД

Является инцидентом (по мнению Роскомнадзора):

- ♦ НСД внешнего пользователя к БПД
- ♦ НСД, связанный с уязвимостями ПО системы
- ♦ неправомерное копирование БПД
- ♦ копия БПД (актуальная или скомпрометированная ранее) доступна в сети Интернет
- ♦ получение сообщения с угрозой раскрыть БПД

Не является инцидентом (по мнению Роскомнадзора):

- ♦ НСД внутреннего пользователя к БПД без копирования
- ♦ случайное уничтожение БПД внутренним пользователем
- ♦ подозрительная активность пользователя системы

Источник: pd.rkn.gov.ru/incidents/form и t.me/rkn_tg/320

Компьютерный инцидент ч.12 ст.19 152-ФЗ «О ПД»

передача (т.е. предоставление, распространение или доступ)

неправомерная или случайная

неправомерная

повлекшая нарушение прав
субъектов ПД

произошедшая в результате
компьютерной атаки

требующая уведомления
Роскомнадзора

требующая информирования
ФСБ (ГосСОПКА)





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

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)

24 часа

72 часа

С момента выявления инцидента оператором, Роскомнадзором или иным заинтересованным лицом



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 ПД
- затронутые инцидентом субъекты ПД не относятся к социально незащищенным группам населения



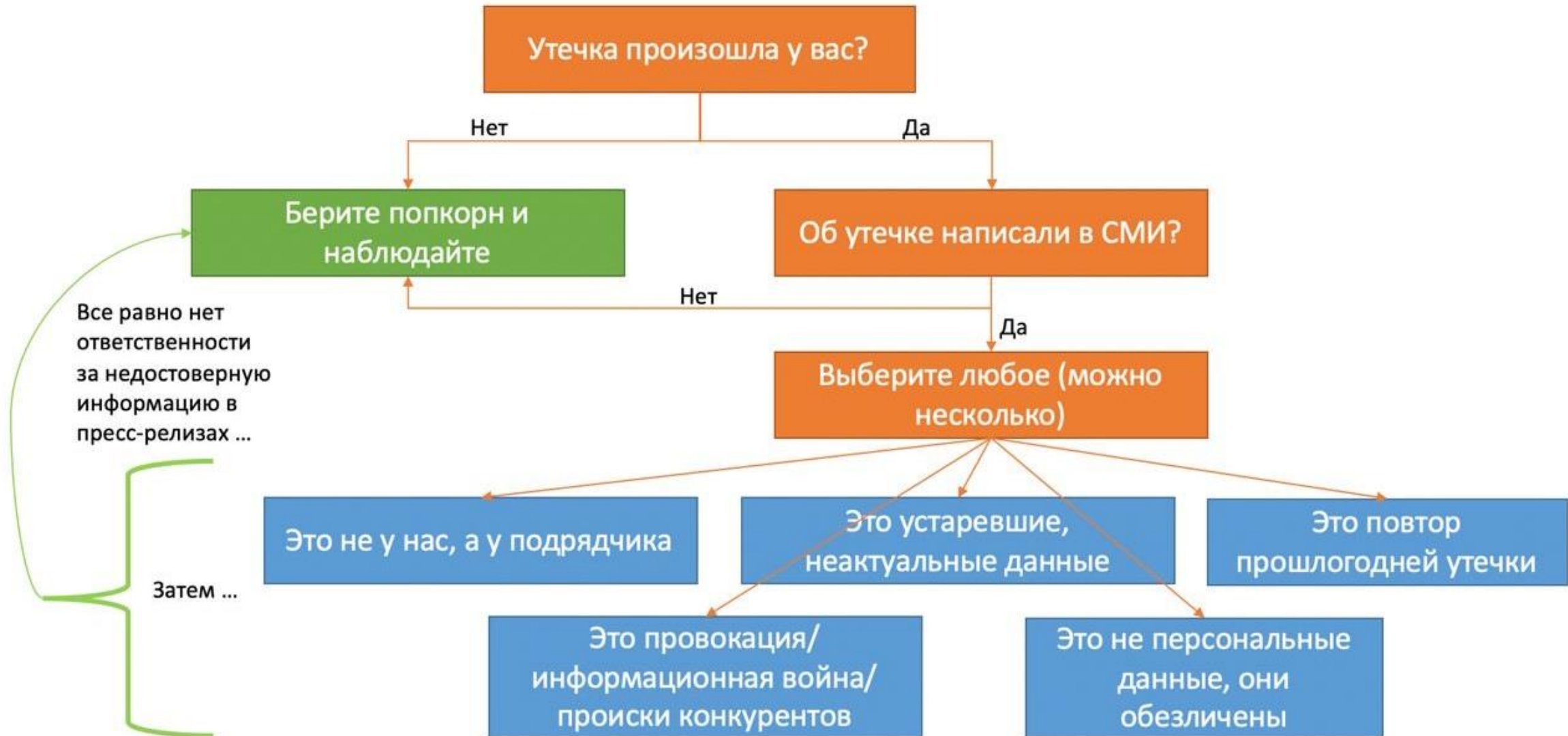
Объективная сторона инцидента

- инцидент произошёл у оператора впервые, оператор добросовестно выполнял все требования 152-ФЗ
- 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 (абз.2 п.2.2 приказа Роскомнадзора №178 от 27.10.2022)

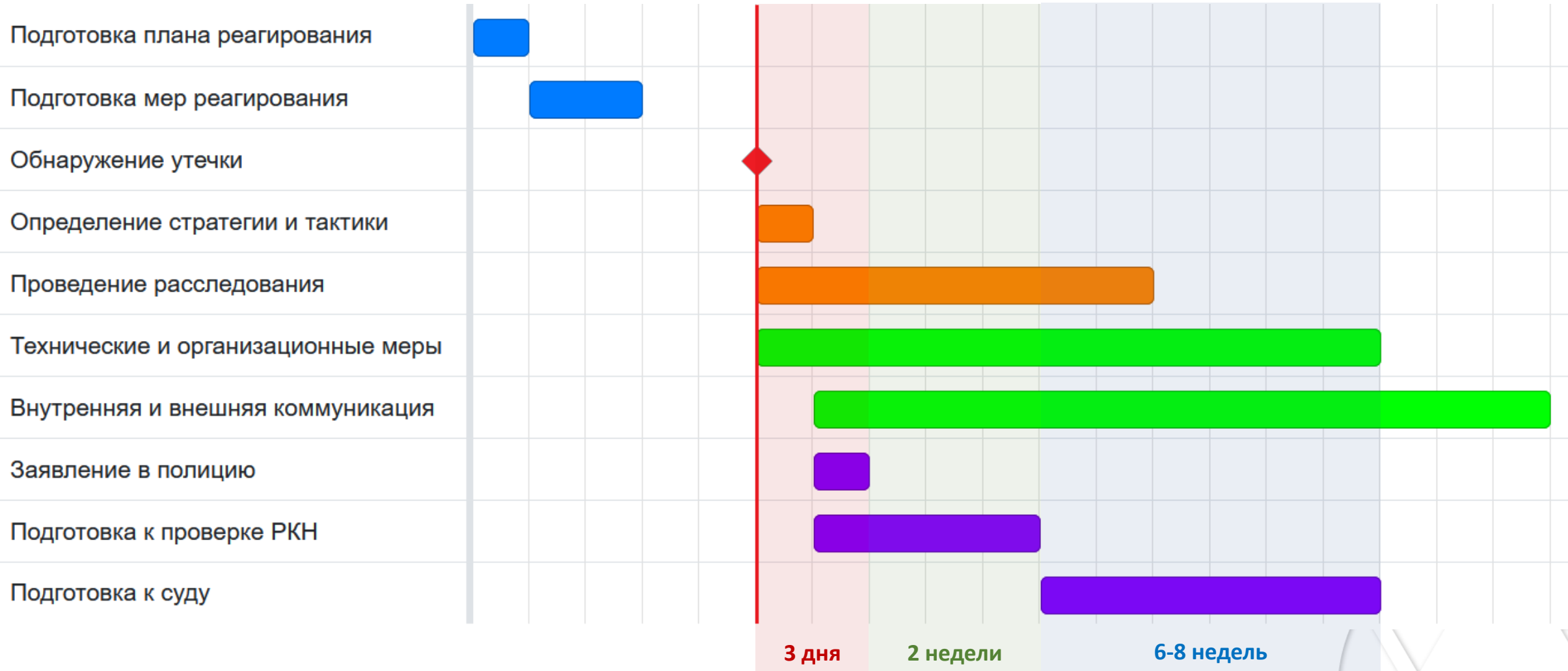


Реагирование на инцидент

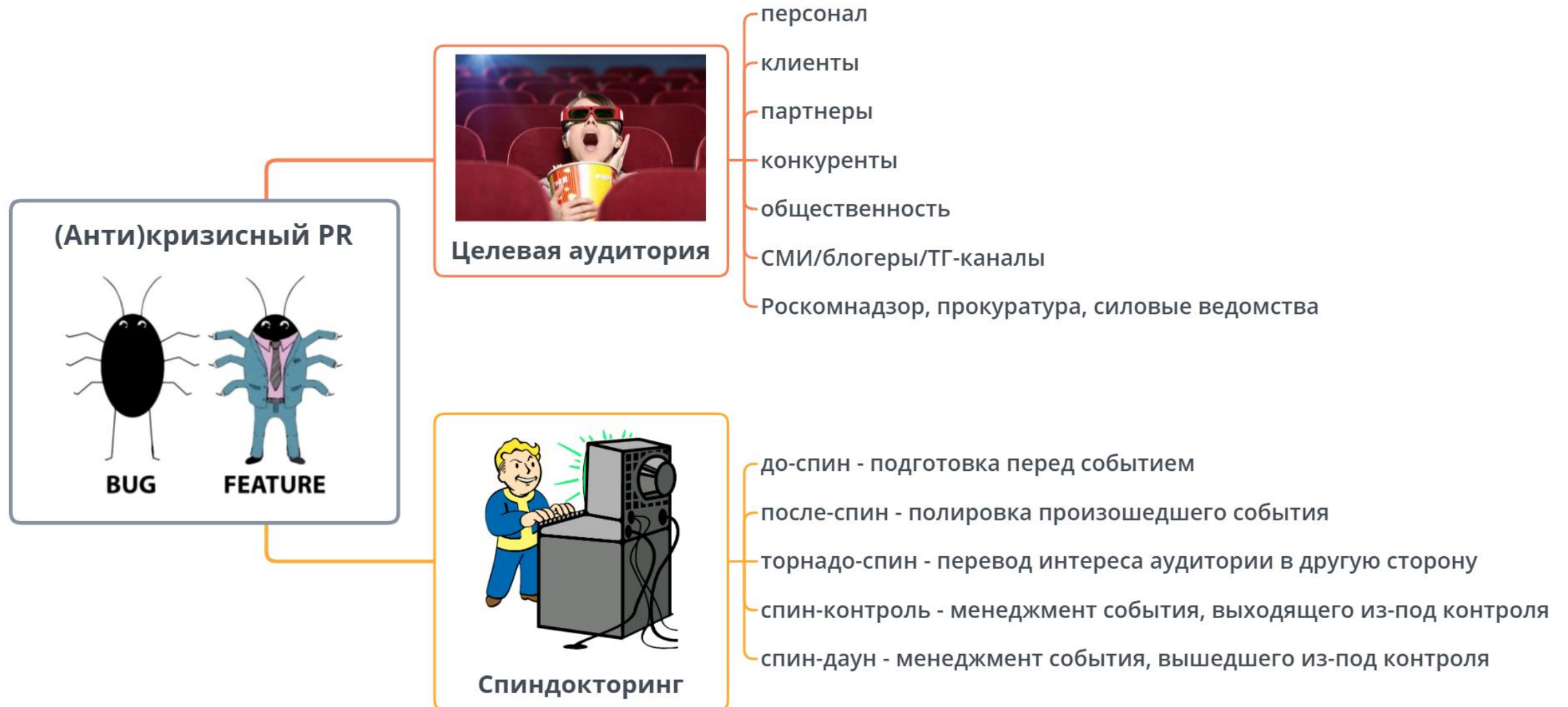
- своевременно и должным образом подготовлены и направлены в Роскомнадзор уведомления об инциденте
- надлежащим образом и добросовестно осуществлено взаимодействие с Роскомнадзором в ходе проведения им контрольно-надзорного мероприятия
- оперативно и всесторонне организовано оповещение об инциденте всех 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
- осуществлена компенсация вреда, причиненного субъектам ПД вследствие инцидента
- в правоохранительные органы подано заявление в отношении неустановленного лица (группы лиц), получившего правомерный доступ к ПД







Реальная длительность жизненного цикла утечки



Игра на избегание неудач

Минимизация издержек от утечки



Игра на победу

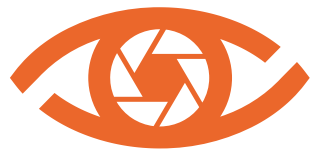
Максимизация пользы от утечки





Скачать презентацию





**Privacy
Advocates**

Всегда рады сотрудничеству!

+7 (903) 762-64-15 | corp@privacy-advocates.ru | t.me/prv_adv



Telegram-канал