Алексей Лукацкий

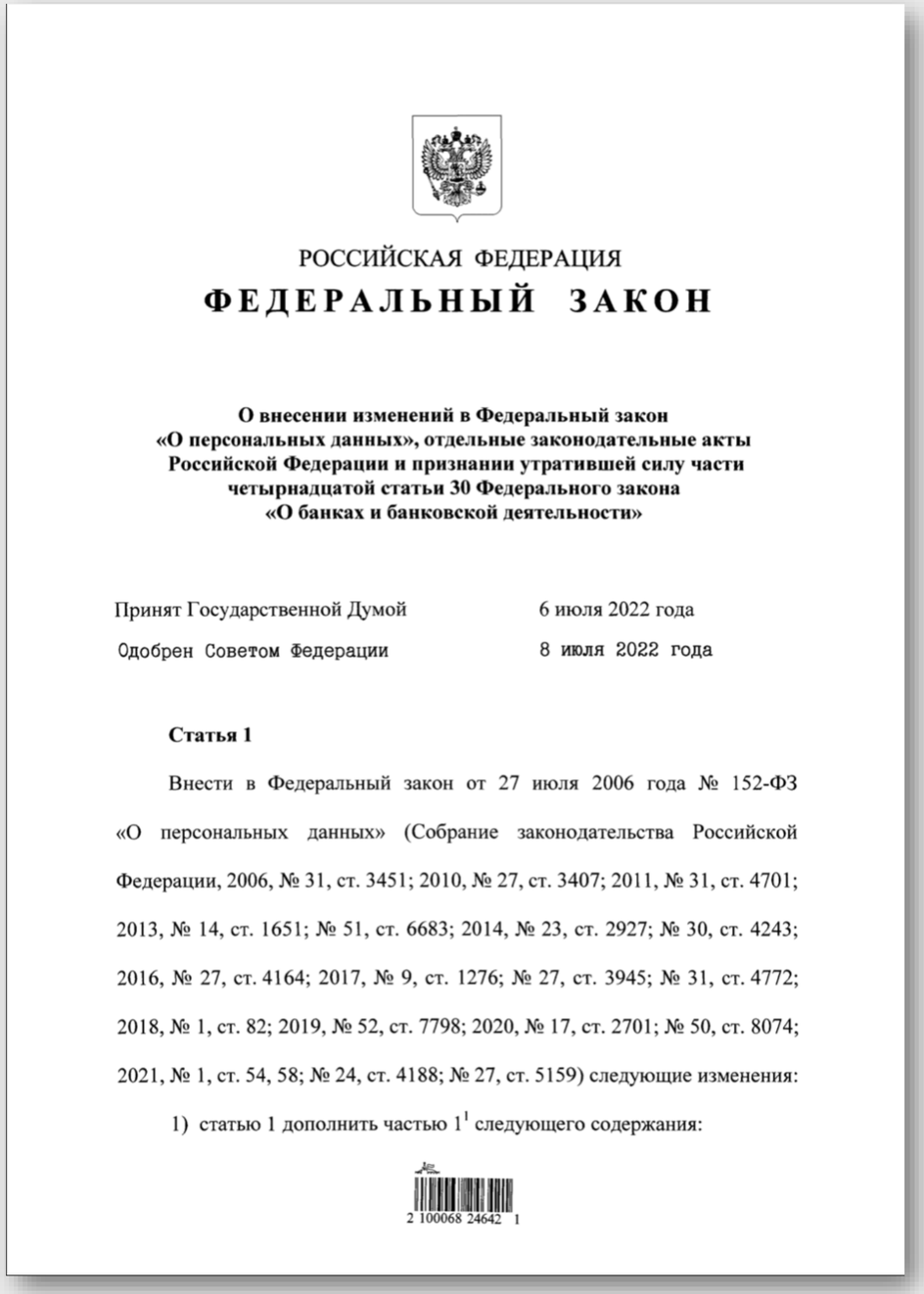
Бизнес-консультант по безопасности

Уведомление об утечках персданных

Что надо знать?

Новые требования закона о ПДн

- Принцип экстерриториальности
- Изменение правил трансграничной передачи данных
- Новые обязанности обработчика ПДн
- Изменение требований к согласию
- Изменение формы уведомления РКН о начале обработки ПДн
- Методика оценки вреда от РКН
- Методика уничтожения ПДн от РКН
- Информирование ФСБ и РКН об утечках ПДн
- Подключение операторов ПДн к ГосСОПКЕ



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»

Принят Государственной Думой 6 июля 2022 года

Одобрен Советом Федерации 8 июля 2022 года

Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2010, № 27, ст. 3407; 2011, № 31, ст. 4701; 2013, № 14, ст. 1651; № 51, ст. 6683; 2014, № 23, ст. 2927; № 30, ст. 4243; 2016, № 27, ст. 4164; 2017, № 9, ст. 1276; № 27, ст. 3945; № 31, ст. 4772; 2018, № 1, ст. 82; 2019, № 52, ст. 7798; 2020, № 17, ст. 2701; № 50, ст. 8074; 2021, № 1, ст. 54, 58; № 24, ст. 4188; № 27, ст. 5159) следующие изменения:

1) статью 1 дополнить частью 1^1 следующего содержания:

2 100068 24642 1

Вопрос стоит не «Утечет или нет?», а «Когда утечет?»

Утечки информации
Суд в Ростове-на-Дону вынес приговор Андрею Лукьянову, который занимался незаконной продажей детализаций телефонных соединений клиентов регионального оператора связи.

В компанию связи мужчина устроился в 2015 году и тогда же один из коллег предложил ему подработку. Лукьянову нужно было выяснить, на кого зарегистрирован номер, скопировать список звонков абонента и передать его заказчику.

Против него было возбуждено уголовное дело (“*Неправомерный доступ к компьютерной информации с использованием служебного положения*”) по 12 задокументированным фактам преступлений. В 2017 году он был уволен из компании по компрометирующим обстоятельствам.

Лукьянов полностью признал свою вину и дал показания на своих сообщников. Учитывая его раскаяние и помощь следствию, суд приговорил бывшего сотрудника компании к одному году лишения свободы условно.

Про случаи задержания и осуждения лиц, так или иначе связанных с торговлей персональными данными читайте в отчете: 👇

https://www.devicelock.com/ru/blog/pojmat-i-nakazat-kak-v-rossii-lovyat-i-nakazyvayut-za-nezakonnuyu-torgovlyu-personalnymi-dannymi-chast-2.html

> **Devicelock**
> **Поймать и наказать! Как в России ловят и наказывают за незаконную торговлю пер...**
> Почти год назад я делал подборку сообщений

Легальный доступ

Утечки информации
Вечером 1-го февраля 2020 г. система DeviceLock Data Breach Intelligence обнаружила сервер с открытой MongoDB не требующей аутентификации для подключения.

В свободно доступной базе данных было две «коллекции»:

1️⃣ *alpha_config_db* – 35,787 записей (42 Мб)
2️⃣ *stavcredit* – 8,279 записей (9 Мб)

Каждая запись содержит:

🌵 дата заявки
🌵 интересующая сумма кредита
🌵 интересующий срок кредитования
🌵 канал привлечения
🌵 ФИО
🌵 эл. почта
🌵 телефон
🌵 дата рождения
🌵 город
🌵 регион

В процессе анализа утечки удалось выяснить, что в обнаруженной MongoDB находятся данные клиентов кредитного брокера «*Альфа-кредит*» (*alpha-credit.com*), который собирает заявки на кредиты и помогает получить заем в банке.

Через 10 минут после обнаружения открытой MongoDB мы оповестили компанию об уязвимости, но доступ к данным был закрыт только вечером 04.02.2020. 🙈🤦‍♂️🤦‍♀️ По данным поисковика Shodan этот сервер попал в открытый доступ 31.01.2020. 😱

Корявый конфиг

📌Вот и закончились НОВОГОДНИЕ ПРАЗДНИКИ!
Мы, как и всегда работаем в прежнем режиме!

🏆 Скидка на все услуги 10% 🏆

💯 **Список услуг через ФНС**

ДРЕВО СВЯЗЕЙ:
- до 3-го колена
- до 6-го колена

💯 *КНИГА ПОКУПОК/ПРОДАЖ:
-За все периоды сдачи отчетности

💯 *ВЫПИСКИ*:*
- Месяц
- 6 месяцев
- 12 месяцев
- больше 12 месяцев

💯 **БАНКИ:**
🎯 *Альфа банк (физ/юр)*
🎯 *Тинькофф (физ/юр)*
🎯 *ВТБ (физ)*
🎯 *ПСБ (юр/физ)*
🎯 *Сбербанк (физ)*
🎯 *Убрир (юр)*
🎯 *Зенит (юр/мск)*
🎯 *Уралсиб (юр)*
🎯 *Авангард (юр)*
🎯 *Росбанк (юр/физ)*

Утечка на заказ

Нерезультативная безопасность

1. American Medical Collection Agency (03’19) – банкротство после утечки данных
2. Утечка 143 млн записей из Equifax (07’17) – ущерб составил 700 млн долларов
3. Взлом штаба демпартии США и утечка почты Хиллари Клинтон (2016) – влияние на результаты выборов (возможно)
4. Утечка 100 млн записей из Capital One – ущерб от 100 до 150 млн долларов
5. Утечка из Marriot / Starwood (03’20) – штраф 123 млн долларов
6. Target (05’14) – 61 млн долларов потерь от утечки данных в результате взлома, 100 млн долларов на изменение инфраструктуры и 18,5 млн долларов штрафа
7. Vastaamo Psychotherapy Centre (02’21) – банкротство после кражи данных пациентов и обвинений с их стороны

Что требует новая редакция закона?

Чтобы о чем-то сообщить, сначала это нужно обнаружить и собрать все сведения об инциденте!

Операторы ПДн должны уведомлять об инцидентах РКН в течение 24 часов

Подключение всех операторов ПДн к ГосСОПКЕ

Инциденты с ПДн ГосСОПКА передает в РКН

База инцидентов с ПДн будет вестись РКН. Доступ к базе будет иметь и ФСБ (по отдельно разработанным правилам)

Требования по уведомлению об инцидентах с ПДн в России похожи на европейские, но есть и отличия!

Уведомление – это вершина айсберга

Уведомление об инцидентах с ПДн

Мониторинг инцидентов с ПДн

Реагирование на инциденты с ПДн

Оценка вреда от инцидентов с ПДн

О каких инцидентах с ПДн уведомлять?

А что если не уведомлять? Оборотные штрафы?!

Как собрать данные об инциденте за короткое время?

Что такое инцидент ПДн?

Что такое утечка (breach) в европейском законодательстве?

- Доступ неавторизованных третьих лиц к ПДн
- Несанкционированное изменение ПДн
- Отправка ПДн неверному адресату
- Нарушение доступности ПДн
- Кража или утеря устройства с ПДн
- Вымогательское ПО (ransomware)

В российском законодательстве все зависит от того, кого мы уведомляем

РКН

- Неправомерное (случайное) копирование ПДн
- Копия базы данных с ПДн доступна в интернет
- Получено сообщение с угрозой раскрыть ПДн
- Случайная передача базы с ПДн третьим лицам

ФСБ

- Все инциденты с безопасностью ПДн, повлекшие за собой неправомерную передачу ПДн (исключая случайную), возникшие в результате компьютерной атаки

О чем не надо уведомлять РКН (а ФСБ?)

- Внутренний НСД к базе ПДн
- Подозрительная активность пользователя с ПДн
- Уничтожение (шифрование) ПДн
- Любые внутренние инциденты с ПДн

ФЗ-152 разделяет «инцидент с ПДн» (ст.21) и «компьютерный инцидент с ПДн» (ст.19)

РКН интересуют неправомерные и случайные действия, повлекшие за собой нарушение прав субъектов и нанесение им вреда, а ФСБ интересует только неправомерные действия, произошедшие в результате компьютерной атаки (можно без последствий)!

О чем надо уведомлять?

О чем уведомлять согласно европейским требованиям?

Если по телефону, то…

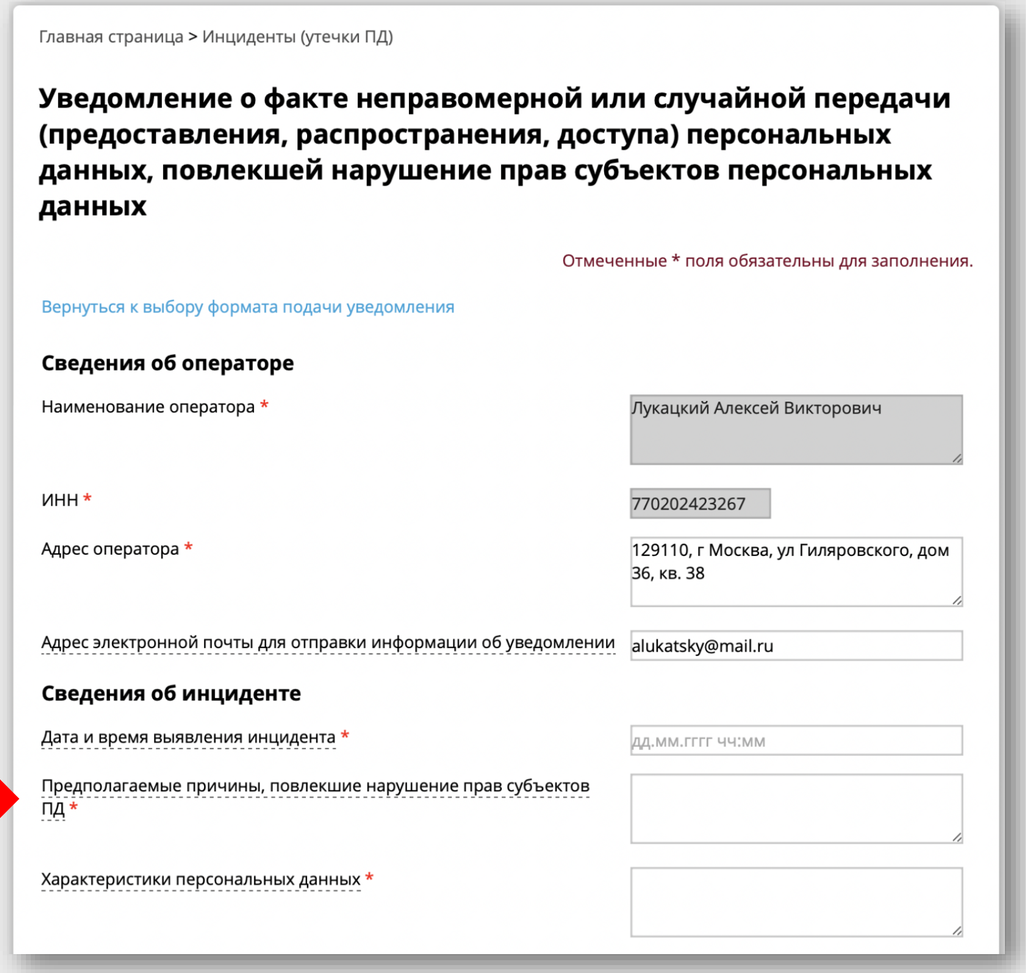
- Что произошло?
- Когда и как вы узнали об инциденте?
- Люди, которые могли пострадать в рамках инцидента?
- Что было сделано в ответ на инцидент?
- Контактное лицо
- Кому еще вы сообщили об инциденте?

О чем уведомлять согласно европейским требованиям?

Если онлайн, то…

- Что произошло?
- Как произошел инцидент?
- Как вы узнали об инциденте?
- Какие меры защиты предпринимались?
- Когда произошел инцидент?
- Когда был обнаружен инцидент?
- Категории ПДн
- Число записей/субъектов
- Категории субъектов
- Последствия для субъектов
- Был ли обучен персонал?
- Если была задержка в уведомлении, то почему?
- Какие действия были предприняты в ответ на инцидент?
- Вы уведомили субъектов об инциденте?
- Вы кому-то еще сообщили об инциденте?

Как и о чем уведомлять Роскомнадзор?



Главная страница > Инциденты (утечки ПД)

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Сведения об операторе

Наименование оператора *: Лукацкий Алексей Викторович

ИНН *: 770202423267

Адрес оператора *: 129110, г Москва, ул Гиляровского, дом 36, кв. 38

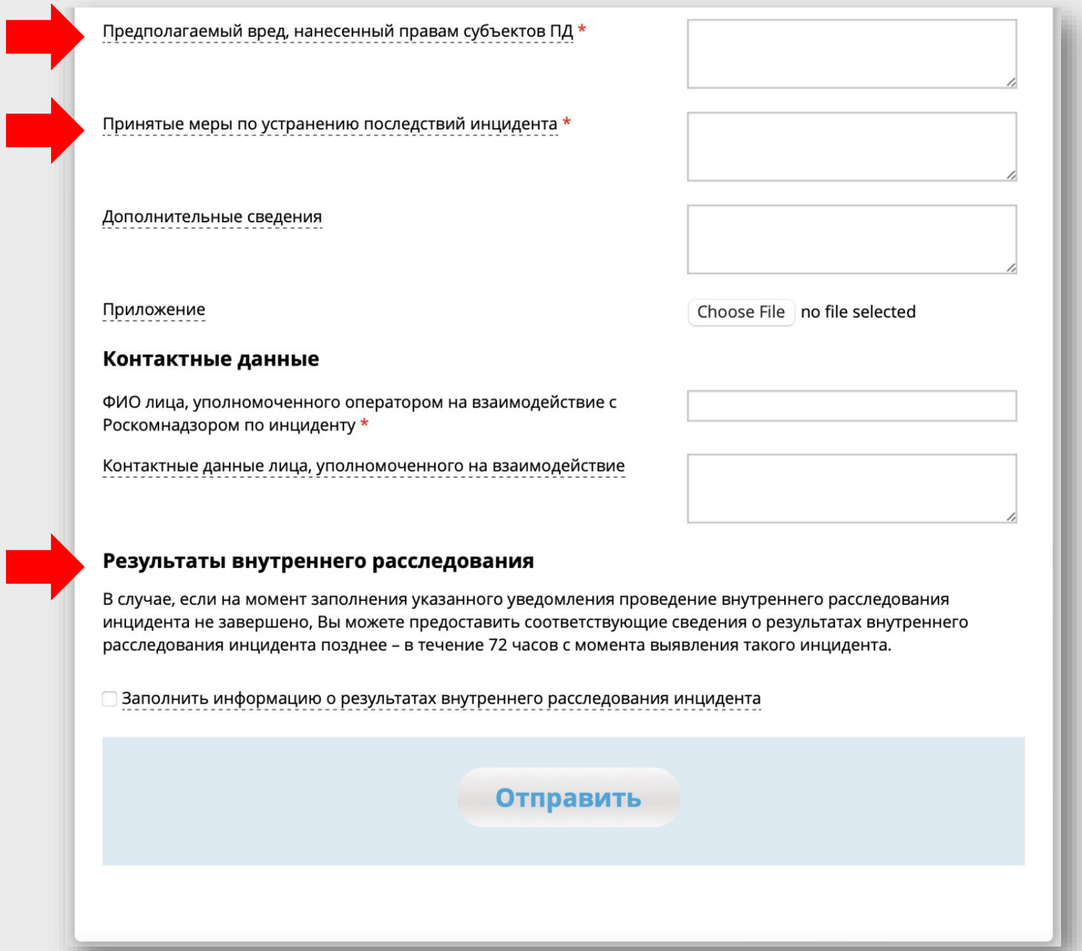
Адрес электронной почты для отправки информации об уведомлении: alukatsky@mail.ru

Сведения об инциденте

Дата и время выявления инцидента *: дд.мм.гггг чч:мм

Предполагаемые причины, повлекшие нарушение прав субъектов ПД *

Характеристики персональных данных *



Предполагаемый вред, нанесенный правам субъектов ПД *

Принятые меры по устранению последствий инцидента *

Дополнительные сведения

Приложение: Choose File no file selected

Контактные данные

ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту *

Контактные данные лица, уполномоченного на взаимодействие

Результаты внутреннего расследования

В случае, если на момент заполнения указанного уведомления проведение внутреннего расследования инцидента не завершено, Вы можете предоставить соответствующие сведения о результатах внутреннего расследования инцидента позднее – в течение 72 часов с момента выявления такого инцидента.

Заполнить информацию о результатах внутреннего расследования инцидента

Отправить

https://pd.rkn.gov.ru/incidents/form/

А как уведомлять ФСБ / ГосСОПКУ?

А как уведомлять ФСБ / ГосСОПКУ?

- Порядок на данный момент отсутствует!
- Но вряд ли он будет сильно отличаться от взаимодействия субъектов КИИ с ГосСОПКОЙ
- Не исключено, что все ограничится обменом данными между ФСБ и РКН

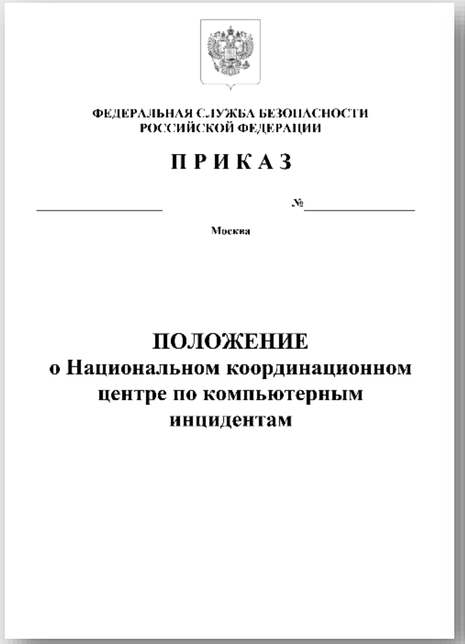
О чем уже сейчас надо сообщать в НКЦКИ?

Категории инцидентов	Типы инцидентов
Внедрение вредоносного программного обеспечения	Заражение ВПО
Распространение вредоносного программного обеспечения	Использование российского ресурса для распространения ВПО
	Попытки внедрения модулей ВПО
Нарушение или замедление работы контролируемого информационного ресурса	Компьютерная атака типа “отказ в обслуживании”
	Распределенная компьютерная атака типа “отказ в обслуживании”
	Несанкционированный вывод системы из строя
	Непреднамеренное отключение системы (без злого умысла)
Несанкционированный доступ в систему	Успешная эксплуатация уязвимости
	Компрометация учетной записи
Попытки несанкционированного доступа в систему или к информации	Попытки эксплуатации уязвимости
	Попытки авторизации в информационном ресурсе
Сбор сведений с использование ИКТ	Сканирование информационного ресурса
	Прослушивание (захват) сетевого трафика
	Социальная инженерия
Нарушение безопасности информации	**Несанкционированное разглашение информации**
	Несанкционированное изменение информации
Распространение информации с неприемлемым содержимым	Рассылка российским ресурсом спам-сообщений
	Публикация запрещенной законодательством РФ информации
Мошенничество с использованием ИКТ	Злоупотребление при использовании информационного ресурса
	Публикация мошеннического информационного ресурса
Наличие уязвимости или недостатков конфигурации	

Что означает присоединение к ГосСОПКЕ?

ИНФОРМИРОВАНИЕ	СОДЕЙСТВИЕ	ИСПОЛНЕНИЕ
Информирование об инцидентах вашего центра ГосСОПКИ	Содействие сотрудникам ФСБ в деятельности по реагированию на инциденты	Выполнение требований по установке и эксплуатации средств ГосСОПКИ (при наличии согласия ФСБ)

Чем регулируется ГосСОПКА?

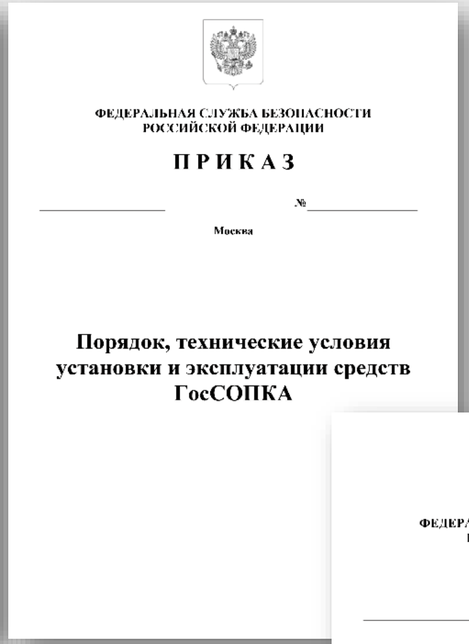

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

ПОЛОЖЕНИЕ
о Национальном координационном центре по компьютерным инцидентам

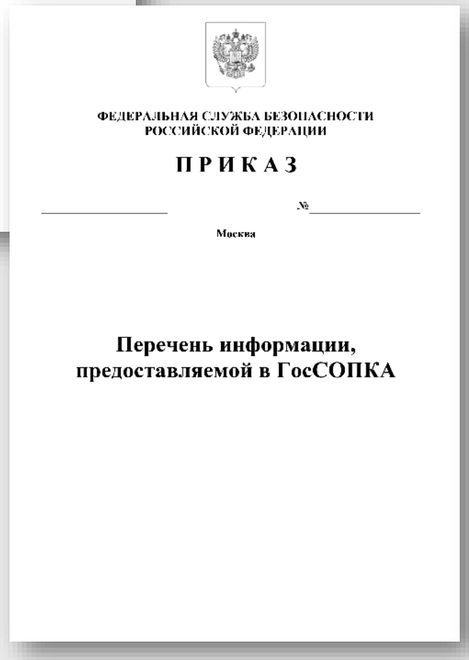

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

Порядок, технические условия установки и эксплуатации средств ГосСОПКА

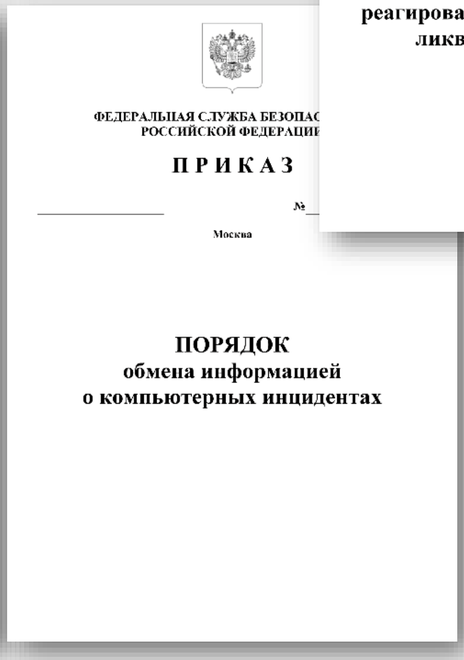

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

Перечень информации, предоставляемой в ГосСОПКА

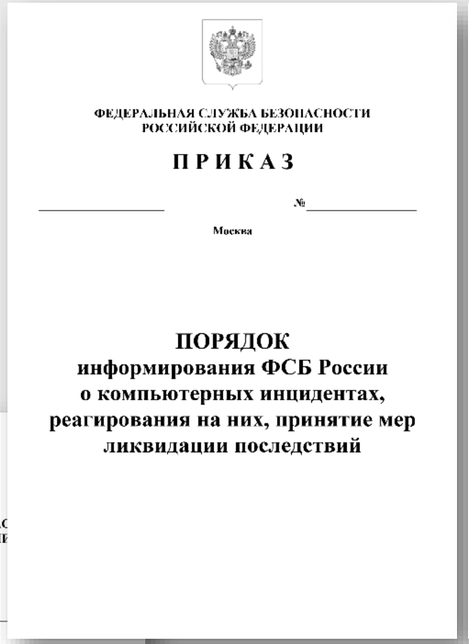

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАС
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_

Москва

ПОРЯДОК
обмена информацией о компьютерных инцидентах

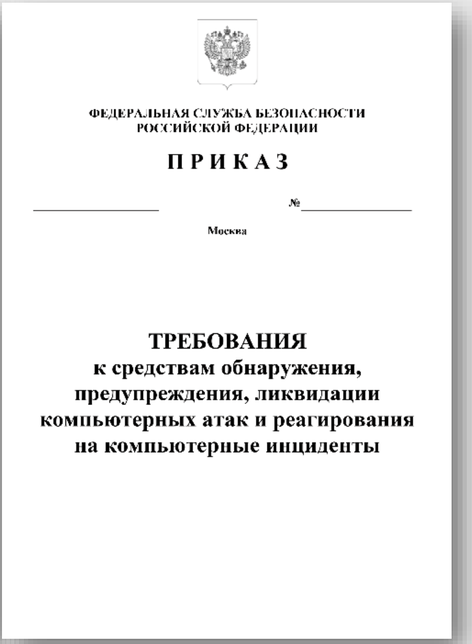

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

ПОРЯДОК
информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятие мер ликвидации последствий


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

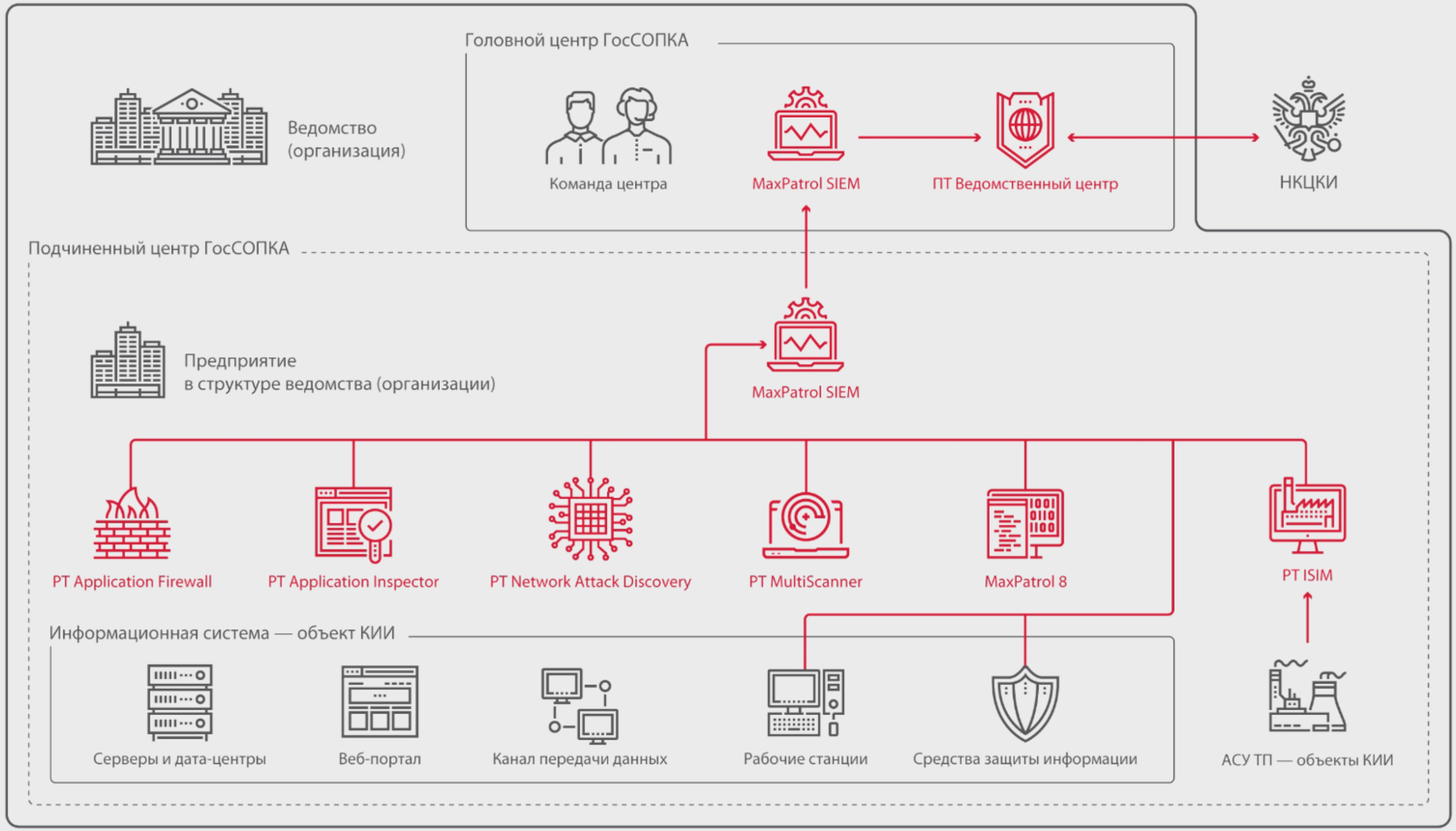
Москва

ТРЕБОВАНИЯ
к средствам обнаружения, предупреждения, ликвидации компьютерных атак и реагирования на компьютерные инциденты

Как информировать ГосСОПКУ (НКЦКИ)?

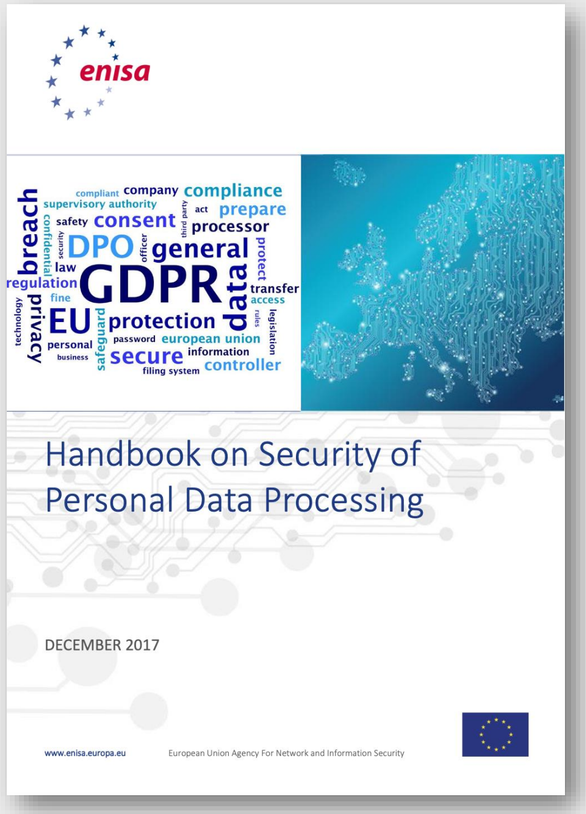
Напрямую

Через центр ГосСОПКИ



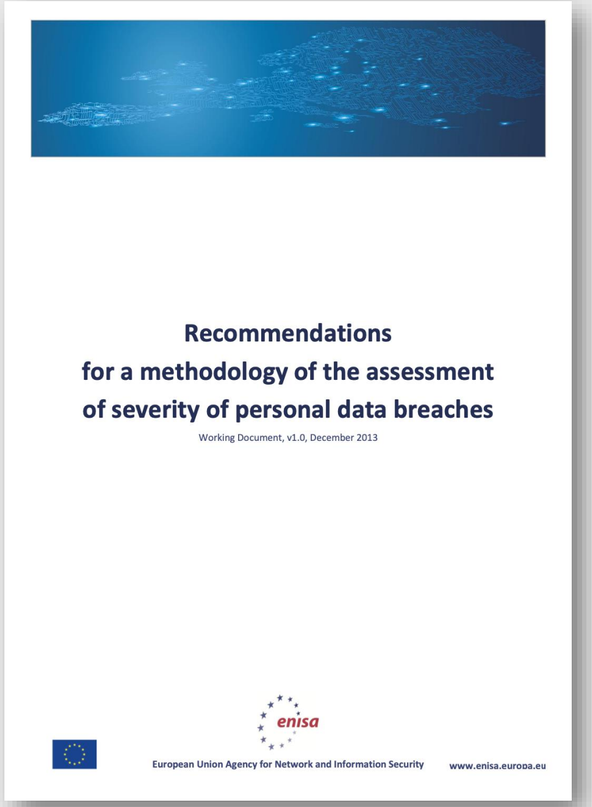
Как оценить ущерб от инцидента ПДн?

Как оценить ущерб/риски для ПДн (в Европе)?



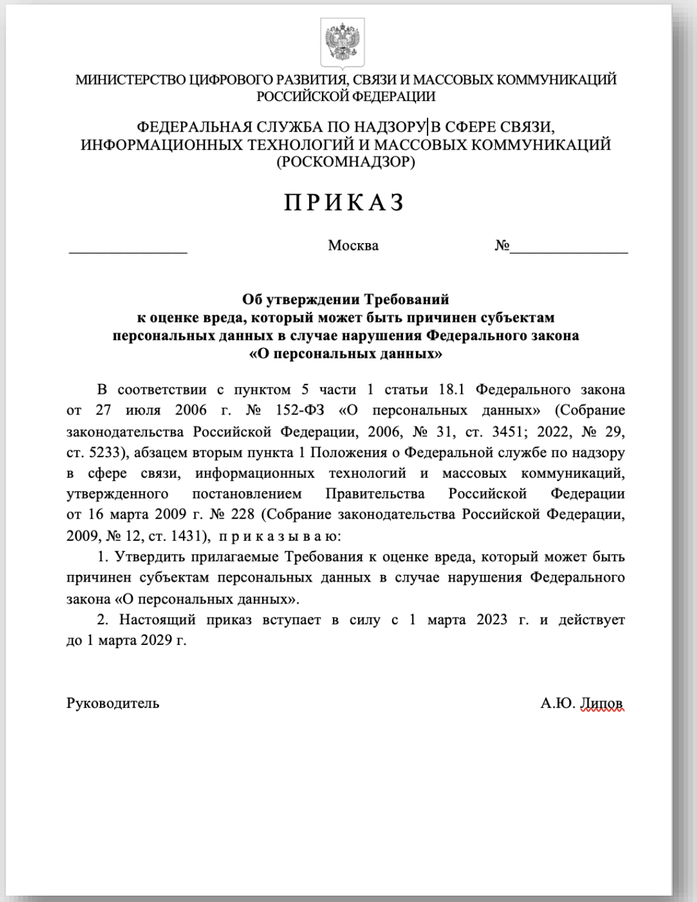
https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

- Кейс: выплата зарплаты
- Кейс: рекрутинг
- Кейс: оценка персонала
- Кейс: заказ и доставка товаров
- Кейс: маркетинг и реклама
- Кейс: предоставление услуг
- Кейс: контроль доступа
- Кейс: видеонаблюдение
- Кейс: медицинские услуги и телемедицина
- Кейс: дистанционное образование



https://www.enisa.europa.eu/publications/dbn-severity

Как оценить ущерб/риски для ПДн (в России)?



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)

ПРИКАЗ

_____ Москва №_____

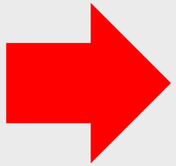
Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

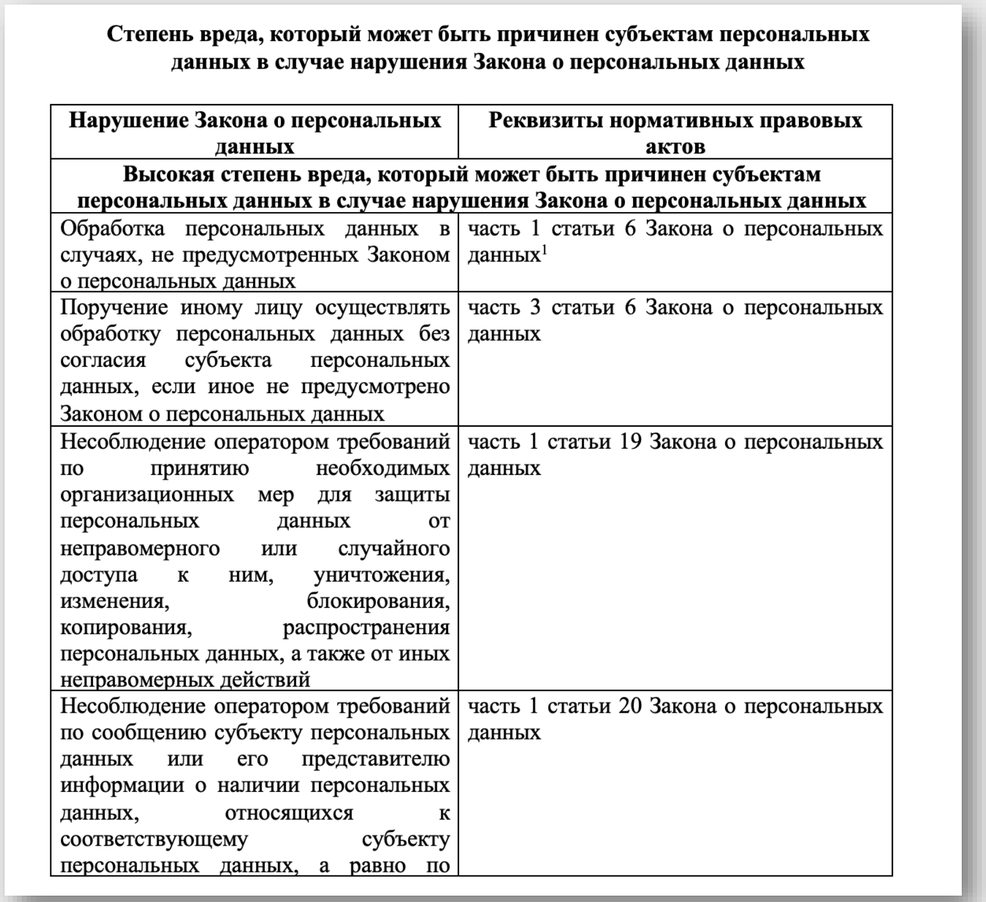
В соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233), абзацем вторым пункта 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431), п р и к а з ы в а ю:

1. Утвердить прилагаемые Требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

2. Настоящий приказ вступает в силу с 1 марта 2023 г. и действует до 1 марта 2029 г.

Руководитель А.Ю. Липов





Степень вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных

Нарушение Закона о персональных данных	Реквизиты нормативных правовых актов
Высокая степень вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных	
Обработка персональных данных в случаях, не предусмотренных Законом о персональных данных	часть 1 статьи 6 Закона о персональных данных[1]
Поручение иному лицу осуществлять обработку персональных данных без согласия субъекта персональных данных, если иное не предусмотрено Законом о персональных данных	часть 3 статьи 6 Закона о персональных данных
Несоблюдение оператором требований по принятию необходимых организационных мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий	часть 1 статьи 19 Закона о персональных данных
Несоблюдение оператором требований по сообщению субъекту персональных данных или его представителю информации о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а равно по	часть 1 статьи 20 Закона о персональных данных

Это важно не только для регуляторов, но и для бизнеса

НЕДОПУСТИМОЕ СОБЫТИЕ	СЦЕНАРИИ РЕАЛИЗАЦИИ	ЦЕЛЕВЫЕ СИСТЕМЫ	КРИТЕРИИ РЕАЛИЗАЦИИ
Утечка персональных данных более 10 тысяч клиентов компании, повлекшая штраф в размере 4% от оборота	▪ Несанкционированный доступ к серверу баз данных с ПДн ▪ Кража ноутбука с ПДн ▪ Взлом через подрядчика (supply chain attack)	▪ CRM-система ▪ 1С:ERP или SAP ▪ Система управления лояльностью	▪ Доступ к CRM-системе с с привилегиями на копирование данных на внешний носитель ▪ Доступ к 1С или SAP с правами на выгрузку или отправку данных внешнему пользователю ▪ Доступ к ноутбуку сотрудника отдела продаж ▪ Доступ к резервной копии базы данных при условии отсутствия ее шифрования

Когда надо уведомлять?

Когда уведомлять?

РКН

- О факте инцидента – в течение 24 часов
- О результатах расследования – в течение 72 часов

ФСБ

- Сроки пока не определены. Вероятно в течение 24 часов (как в рамках ГосСОПКИ и КИИ)

Какие нормативные акты нас еще ждут?

Свежие проекты НПА по уведомлению

- Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных

https://regulation.gov.ru/projects#npa=132272

- Об утверждении Порядка передачи информации о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных

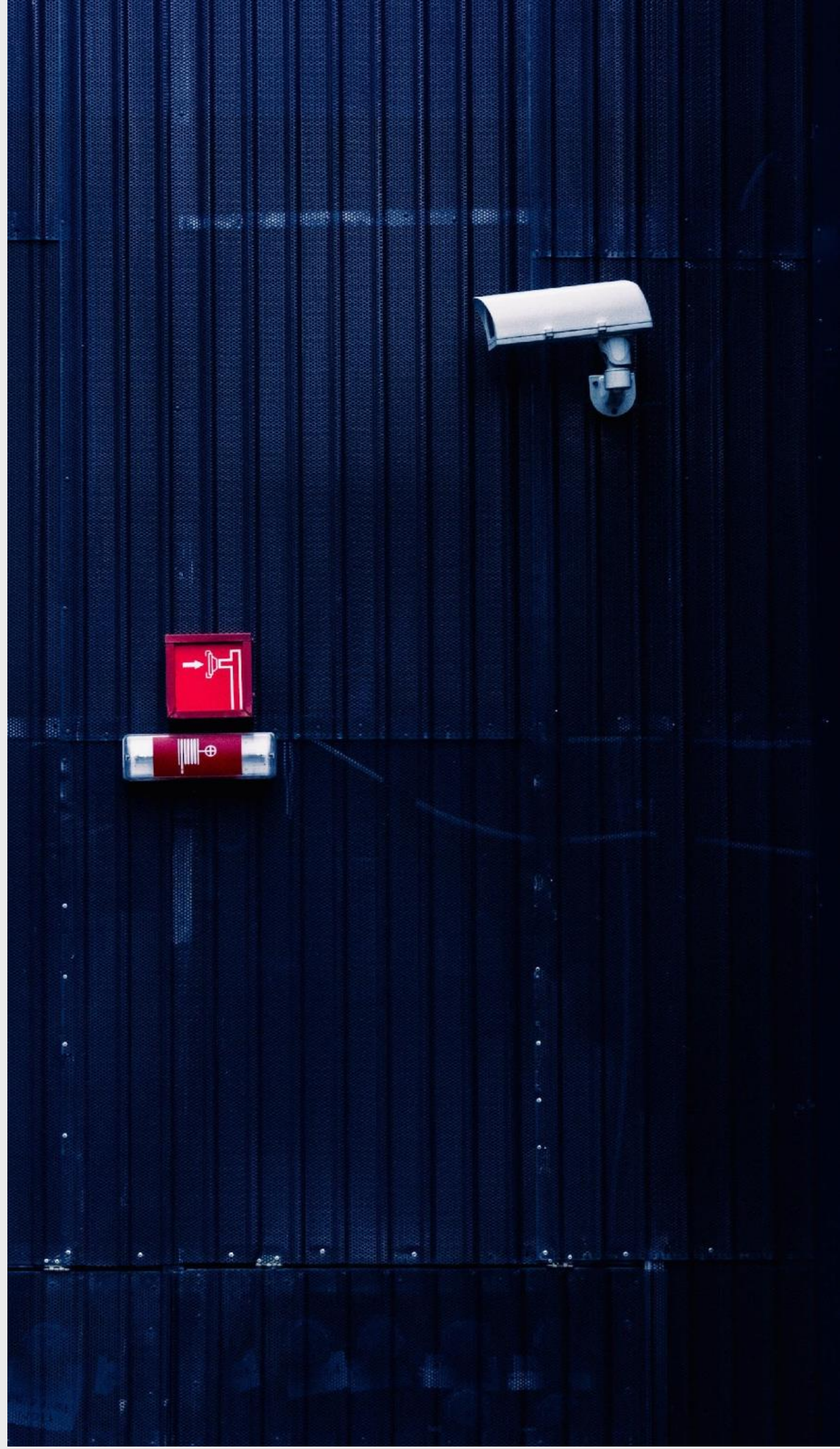
https://regulation.gov.ru/projects#npa=132338

- Guidelines 9/2022 on personal data breach notification under GDPR

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en

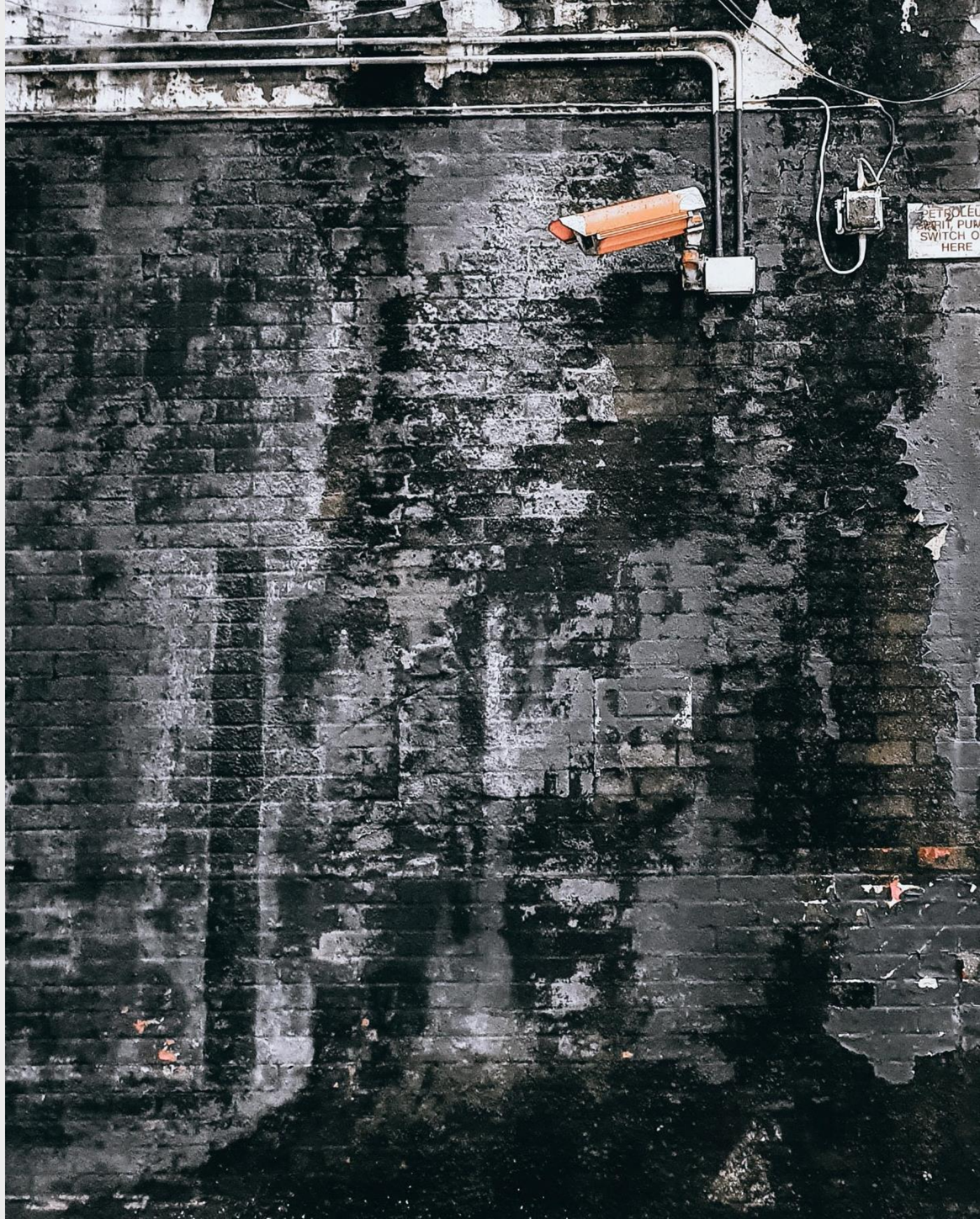
Об утверждении Порядка и условий взаимодействия…

- Уведомление пострадавшим оператором РКН и передача сведений о факте инцидента и о результатах расследования
- 2 уведомления – первичное (о факте) и дополнительное (о результатах расследования)
- Уведомление направляется в бумажном виде и в электронной форме
- РКН уведомляет оператора о факте получения уведомления
- Определены сроки ответов на запросы РКН в случае неполноты данных в уведомлениях



Об утверждении Порядка передачи информации…

- Обмен информации по форме РКН между РКН и ФСБ
- Передача в течение трех дней с момента получения уведомления
- РКН и ФСБ должны определить структурные подразделения и лиц, ответственных за передачу
- Ответственные лица и подразделения определяют форматы и каналы передачи



А если не уведомлять?

Планируется введение оборотных штрафов за утечки ПДн!

1% за первую утечку и 4% за сокрытие факта утечки, но это не точно!

Планируемые штрафы

Ст.13.11 – ч. 10 – утечка ПДн 10 000 до 100 000 записей (не субъектов) – штраф для должностных лиц – от 200 до 400 тысяч рублей; штраф для ИП и юрлиц – 0,02% от годового оборота, но не менее 1 000 000 рублей

Ст.13.11 – ч. 11 – утечка ПДн более 100 000 записей (не субъектов) – штраф для должностных лиц – от 400 до 600 тысяч рублей; штраф для ИП и юрлиц – до 1% от годового оборота, но не менее 2 000 000 рублей

Сокрытие факта утечки – до 4% от годового оборота

Обстоятельства

Отягчающие

- Инцидент со специальными или биометрическими категориями ПДн
- Оператор не уведомил вовремя РКН
- Оператор не способствовал расследованию
- Оператор не предоставил данные об инциденте по запросу РКН
- Оператор ранее не не направил в РКН уведомление о начале обработки ПДн

Смягчающие

- Оператор направил ранее в РКН результаты добровольной оценки соответствия уровня защищенности ИСПДн требованиям законодательства
- Инцидент с ПДн не связан с неисполнением оператором требования в области защиты прав субъектов ПДн и технической защиты ПДн

А если утечка фейковая или на базе уже ранее утекших данных?

Упс… А если база оказалась фейком?

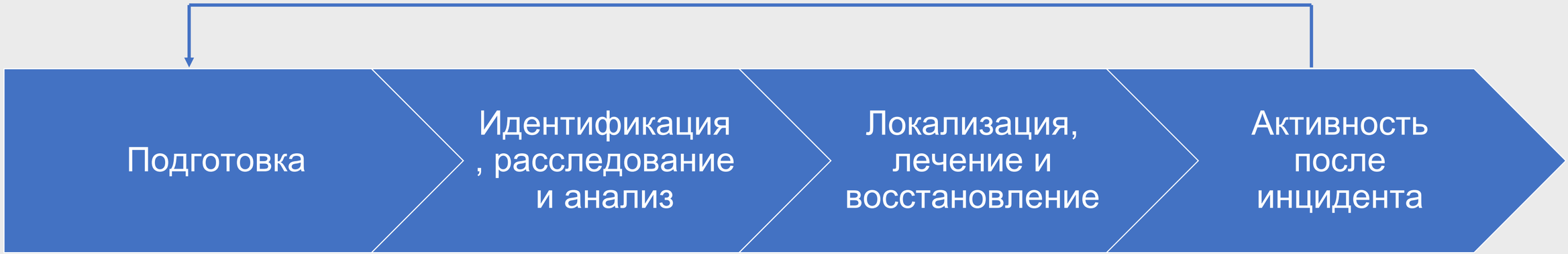
- Утечка фейковая – отправить в РКН дополнительное уведомление с результатами расследования
- Утечка принадлежит другому оператору – отправить в РКН дополнительное уведомление с результатами расследования
- Утечка ранее была зафиксирована – отправить в РКН уведомление согласно ч.3.1 ст.21 ФЗ-152

Уведомление – это финальный шаг в реагировании на инциденты

Как выстроить процесс управления инцидентами?

Управление любым инцидентом, включая и инциденты с ПДн, – это следование определенной процедуре, которую необходимо регулярно тестировать на работоспособность

Процесс реагирования на инциденты



Политики, партнеры, планы, плейбуки и практика (5П)

Форензика, TTP/TTП и индикаторы компрометации (IOC)

Поиск причины, управление кризисной ситуацией, реагирование на инцидент, общение со СМИ, уведомление регулятора

С чего начать реагирование на инциденты с ПДн?

- Как вы распознаете инцидент с ПДн?
- Вы понимаете, что инцидент с ПДн – это не только утечка?
- У вас есть план реагирования на инциденты с ПДн?
- Кто отвечает за инциденты с ПДн?
- Кто входит в группу реагирования?
- Персонал обладает нужными навыками?

Думайте об инциденте не в контексте «если», а в контексте «когда»

План реагирования на инциденты должен содержать следующие моменты

- Ключевые контакты
- Механизмы коммуникаций
- Критерии эскалации
- Блок-схема процессов
- Дежурные процедуры на типичные инциденты с ПДн
- Упрощенные чек-листы
- Процедура взаимодействия с правоохранительными органами и регулирующими органами
- Шаблоны необходимых форм

Обнаружение, предупреждение и ликвидация последствий компьютерных атак

MP VM — MP Vulnerability Management
PT AI — PT Application Inspector

MP SIEM — MaxPatrol SIEM
PT NAD — PT Network Attack Discovery

PT AF — PT Application Firewall
PT ISIM — PT Industrial Security Incident Manager

Немного про мониторинг утечек информации

Если все-таки утечка, то по каким каналам?

- Email
- Мессенджеры
- Веб-почта
- FTP
- Флешки
- Бумажные носители
- Камеры
- Соцсети
- DNS
- API
- Сайты
- SSL/TLS
- Неправильная классификация
- Файловые шары
- Облака
- Физическая кража
- Подглядывание

Вы уверены, что вам надо фокусироваться на DLP?

DLP борется с утечками ПДн!

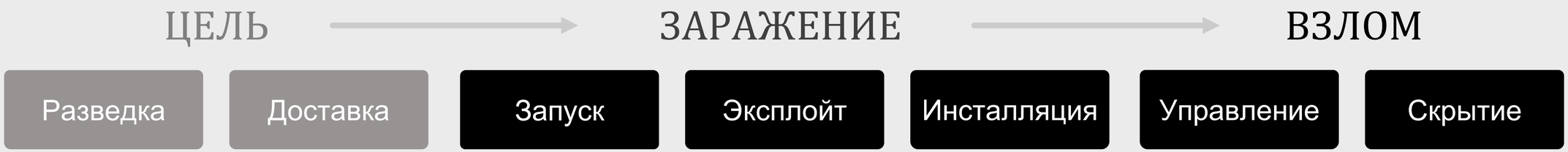
А РАЗВЕ DLP НЕ ПОМОЖЕТ БОРОТЬСЯ С УТЕЧКАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Увы ☹ Каналов и способов утечки гораздо больше, чем может покрыть DLP

Важно понимать, что утечка – это провал предварительных мер ИБ

- Никогда утечка не является точечным действием и всегда состоит из ряда связанных между собой шагов
- Отражение/нейтрализация утечек могут осуществляться на любом этапе и пропуск первых этапов не означает провал ИБ
- Ключевой задачей ИБ является мониторинг различных этапов совершения утечки и блокирование самого важного из них, ради которого злоумышленник все и затевал (тут и работает DLP)

Пример: шифровальщик Sodinokibi (REvil), крадущий данные



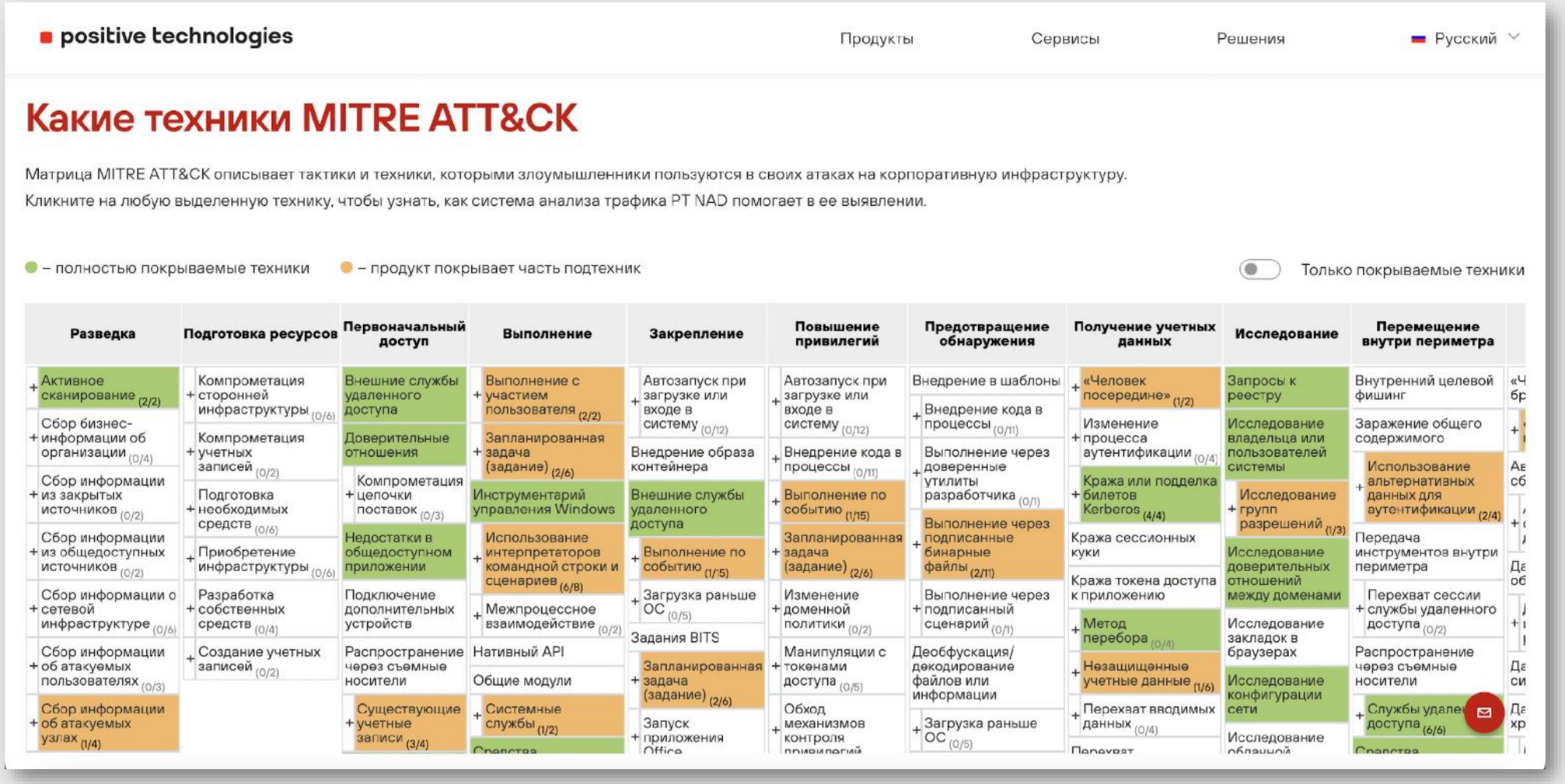
Незащищенные и уязвимые сервисы (RDP, VPN, SharePoint)
Фишинг
Украденные пароли

→ Cobalt Strike
Webshell
VPN abuse

→ Mimikatz
ProcDump
Пароли

→ WMIEXEC
SMBEXEC
PsExec
RDP
CrackMapExec

Универсальный язык для описания техник и тактик хакеров



positive technologies

Продукты Сервисы Решения Русский

Какие техники MITRE ATT&CK

Матрица MITRE ATT&CK описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру.
Кликните на любую выделенную технику, чтобы узнать, как система анализа трафика PT NAD помогает в ее выявлении.

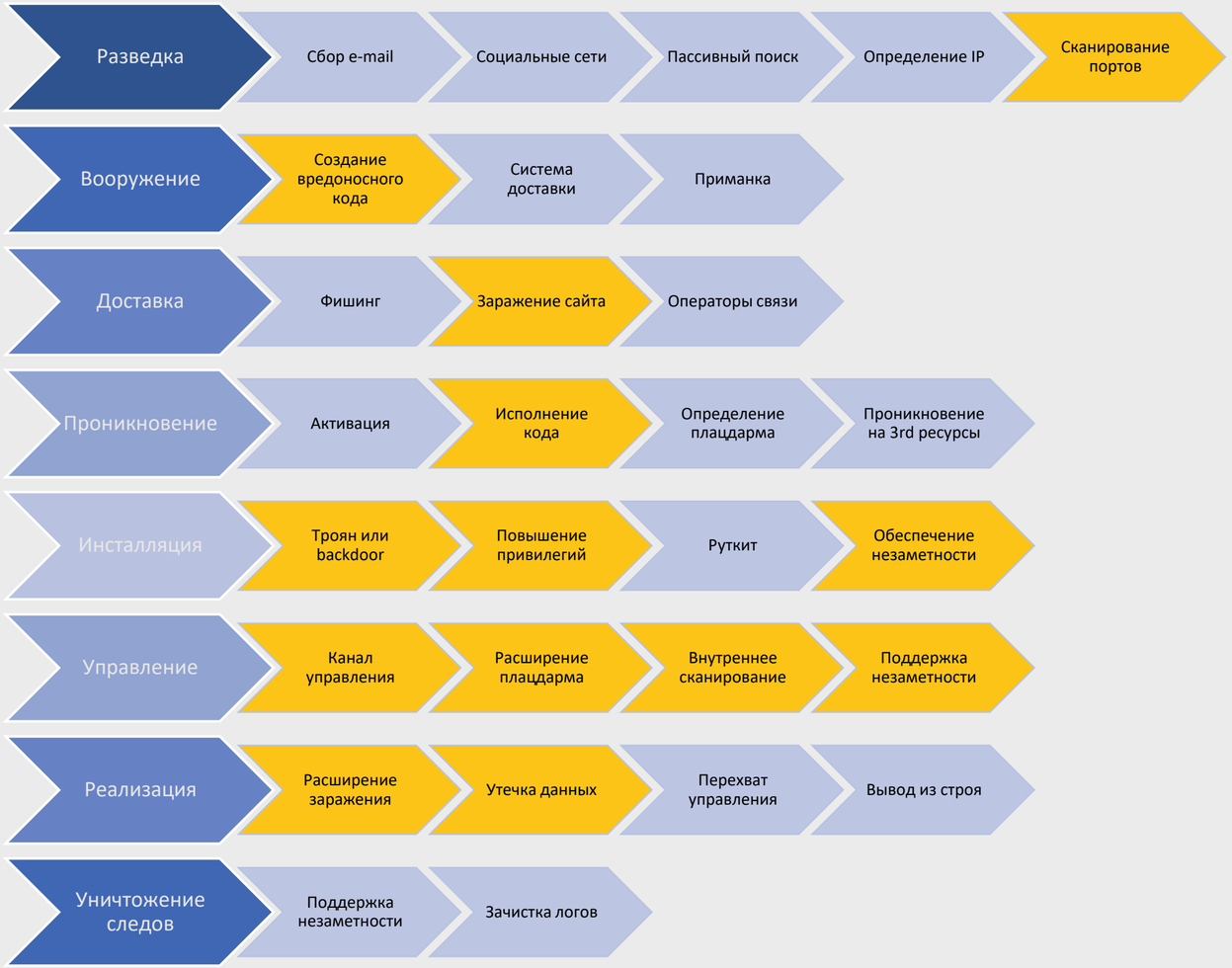
– полностью покрываемые техники – продукт покрывает часть подтехник Только покрываемые техники

Разведка	Подготовка ресурсов	Первоначальный доступ	Выполнение	Закрепление	Повышение привилегий	Предотвращение обнаружения	Получение учетных данных	Исследование	Перемещение внутри периметра
+ Активное сканирование (2/2)	+ Компрометация сторонней инфраструктуры (0/6)	Внешние службы удаленного доступа	+ Выполнение с участием пользователя (2/2)	+ Автозапуск при загрузке или входе в систему (0/12)	+ Автозапуск при загрузке или входе в систему (0/12)	Внедрение в шаблоны	+ «Человек посередине» (1/2)	Запросы к реестру	Внутренний целевой фишинг
+ Сбор бизнес-информации об организации (0/4)	+ Компрометация учетных записей (0/2)	Доверительные отношения	+ Запланированная задача (задание) (2/6)	Внедрение образа контейнера	+ Внедрение кода в процессы (0/11)	+ Внедрение кода в процессы (0/11)	+ Изменение процесса аутентификации (0/4)	Исследование владельца или пользователей системы	Заражение общего содержимого
+ Сбор информации из закрытых источников (0/2)	+ Подготовка необходимых средств (0/6)	+ Компрометация цепочки поставок (0/3)	Инструментарий управления Windows	Внешние службы удаленного доступа	+ Выполнение по событию (1/15)	+ Выполнение через доверенные утилиты разработчика (0/1)	+ Кража или подделка билетов Kerberos (4/4)	+ Исследование групп разрешений (1/3)	+ Использование альтернативных данных для аутентификации (2/4)
+ Сбор информации из общедоступных источников (0/2)	+ Приобретение инфраструктуры (0/6)	Недостатки в общедоступном приложении	+ Использование интерпретаторов командной строки и сценариев (6/8)	+ Выполнение по событию (1/15)	+ Запланированная задача (задание) (2/6)	+ Выполнение через подписанные бинарные файлы (2/11)	Кража сессионных куки	Исследование доверительных отношений между доменами	Передача инструментов внутри периметра
+ Сбор информации о сетевой инфраструктуре (0/6)	+ Разработка собственных средств (0/4)	Подключение дополнительных устройств	+ Межпроцессное взаимодействие (0/2)	+ Загрузка раньше ОС (0/5)	+ Изменение доменной политики (0/2)	+ Выполнение через подписанный сценарий (0/1)	Кража токена доступа к приложению	Исследование закладок в браузерах	+ Перехват сессии службы удаленного доступа (0/2)
+ Сбор информации об атакуемых пользователях (0/3)	+ Создание учетных записей (0/2)	Распространение через съемные носители	Нативный API	Задания BITS	+ Манипуляции с токенами доступа (0/5)	Деобфускация/ декодирование файлов или информации	+ Метод перебора (0/4)	Исследование конфигурации сети	Распространение через съемные носители
+ Сбор информации об атакуемых узлах (1/4)		+ Существующие учетные записи (3/4)	Общие модули	+ Запланированная задача (задание) (2/6)	+ Обход механизмов контроля привилегий	+ Загрузка раньше ОС (0/5)	+ Незащищенные учетные данные (1/6)	Исследование облачной	+ Службы удаленного доступа (6/6)
			+ Системные службы (1/2)	+ Запуск приложения Office			+ Перехват вводимых данных (0/4)		Средства
			Средства				Перехват		

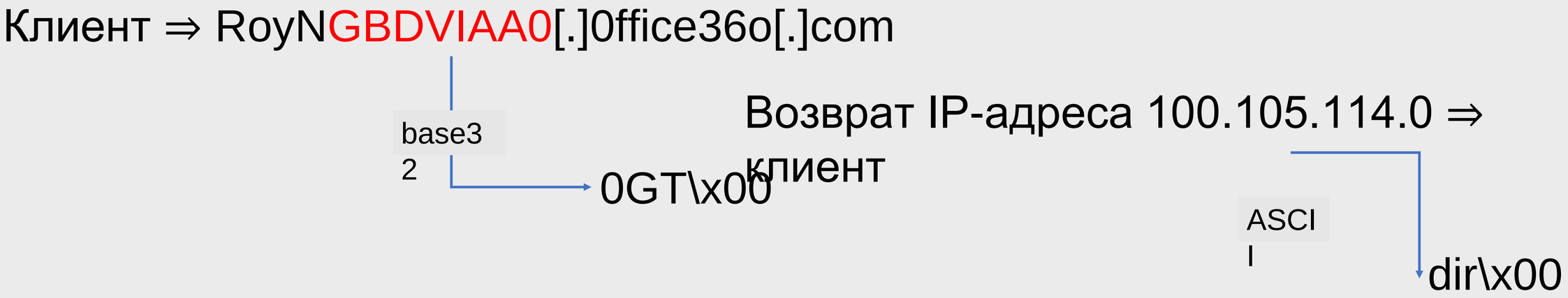
https://mitre.ptsecurity.com/ru-RU/techniques

Утечка данных у Equifax (потеря 700 миллионов долларов)

- Невыстроенный процесс управления уязвимостями
  - Список лиц, которым направлялось уведомление US CERT, был устаревшим
  - Сканер уязвимостей не смог обнаружить уязвимостей на веб-портале
- Скрытие активности в шифрованном канале
- Отсутствие сегментации в сети
- Логины и пароли в открытом виде
- Ненастроенное средство инспекции сетевого трафика с просроченным сертификатом

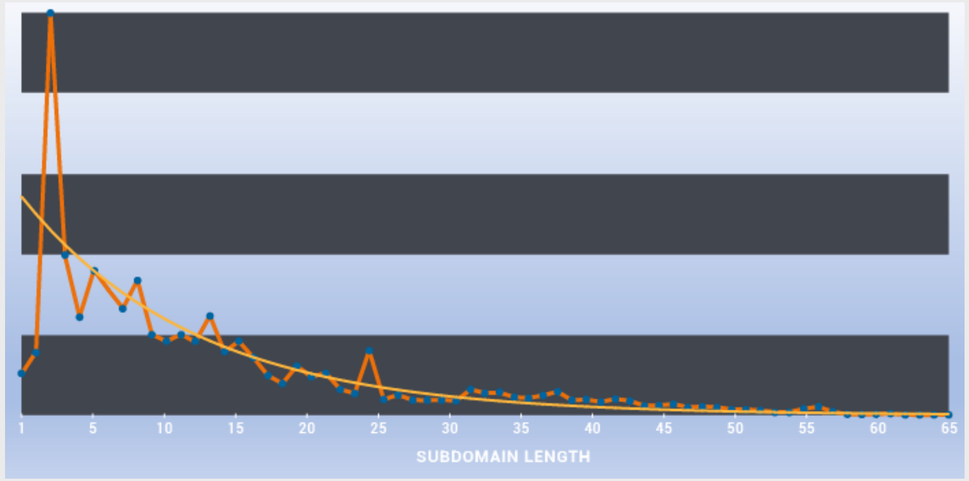


Кампания DNSpionage: нетрадиционный канал утечки

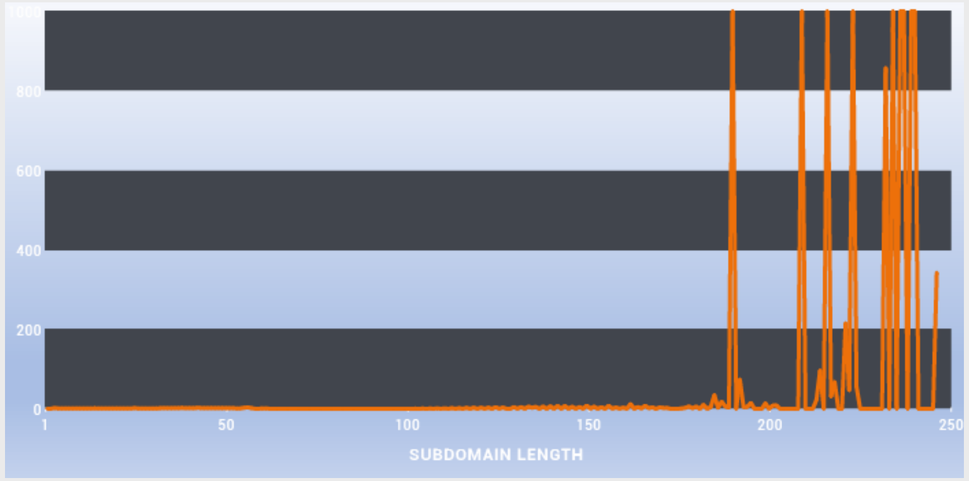


gLtAGJDVIAJAKZXWY000[.]0ffice36o[.]com -> GJDVIAJAKZXWY000 -> “2GT\x01 Vol»
TwGHGJDVIATVNVSSA000[.]0ffice36o[.]com -> GJDVIATVNVSSA000 -> «2GT\x02 ume»
1QMUGJDVIA3JNYQGI000[.]0ffice36o[.]com -> GJDVIA3JNYQGI000 -> «2GT\x03 in d»
iucCGJDVIBDSNF3GK000[.]0ffice36o[.]com -> GJDVIBDSNF3GK000 -> «2GT\x04 rive»
viLxGJDVIBJAIMQGQ000[.]0ffice36o[.]com -> GJDVIBJAIMQGQ000 -> «2GT\x05 C h»

Утечка номеров кредитных карт через DNS



Нормальное распределение длин поддоменов



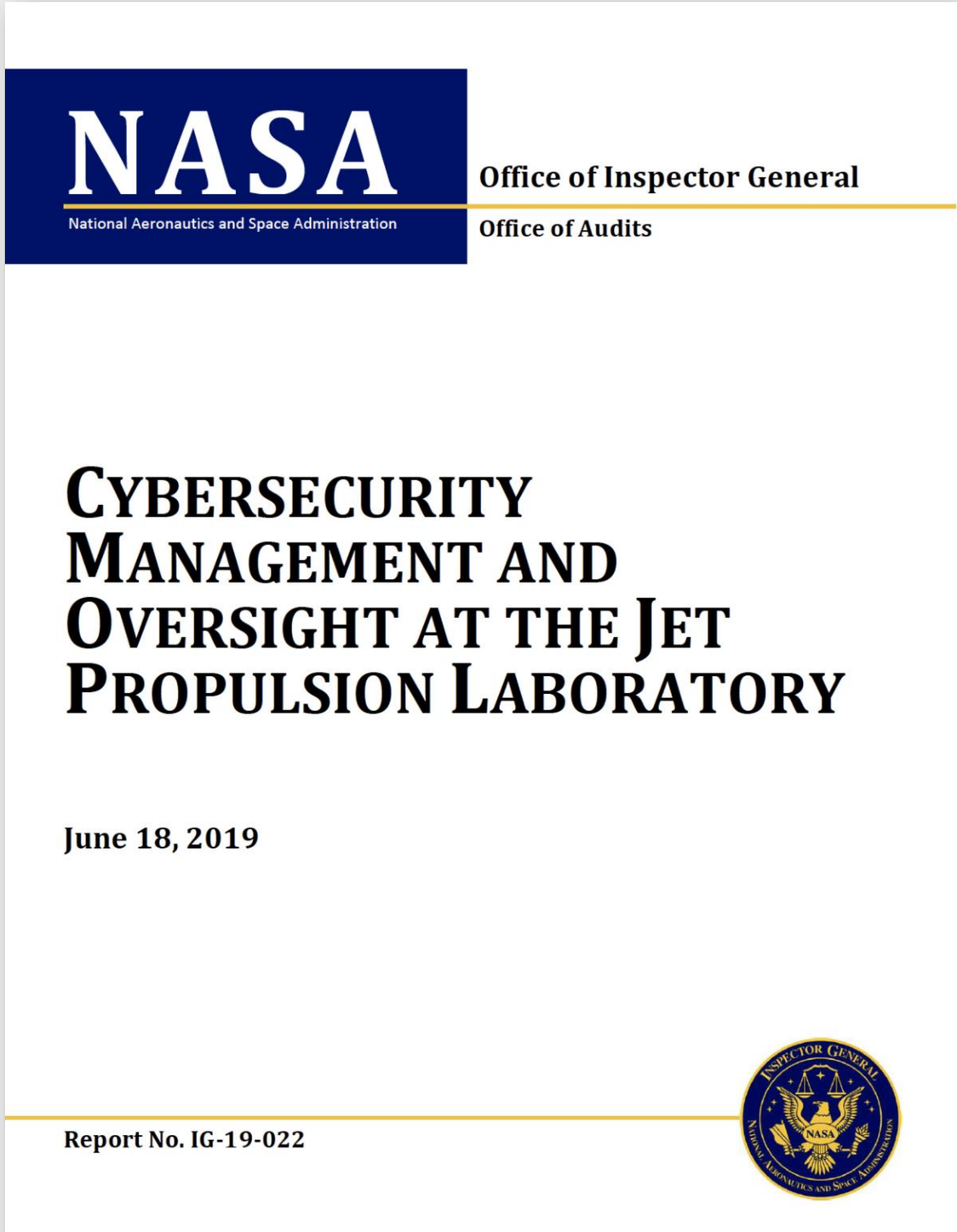
Аномалии в названии поддоменов

log.nu6timjqgq4dimbuhe.3ikfsb---отредактировано---cg3.7s3bnxqmavqy7sec.dojfgj.com
log.nu6timjqgq4dimbuhe.otlz5y---отредактировано---ivc.v55pgwcschs3cbee.dojfgj.com

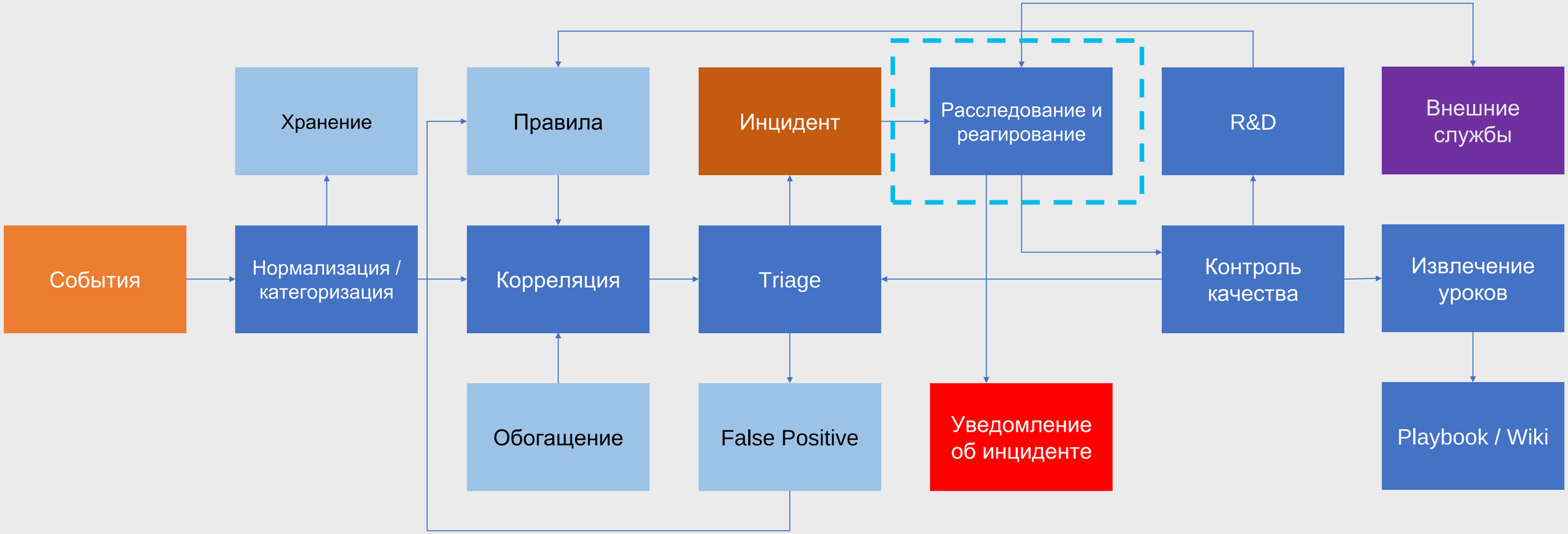
Что скрывается в этой строке на 231 символ?

Взлом NASA

- В апреле 2018 хакеры проникли во внутреннюю сеть NASA и украли 500 МБ данных
- В качестве точки входа использовался портативный компьютер Raspberry Pi, установленный в сети NASA



Поэтому должен быть выстроен полноценный мониторинг разных источников телеметрии



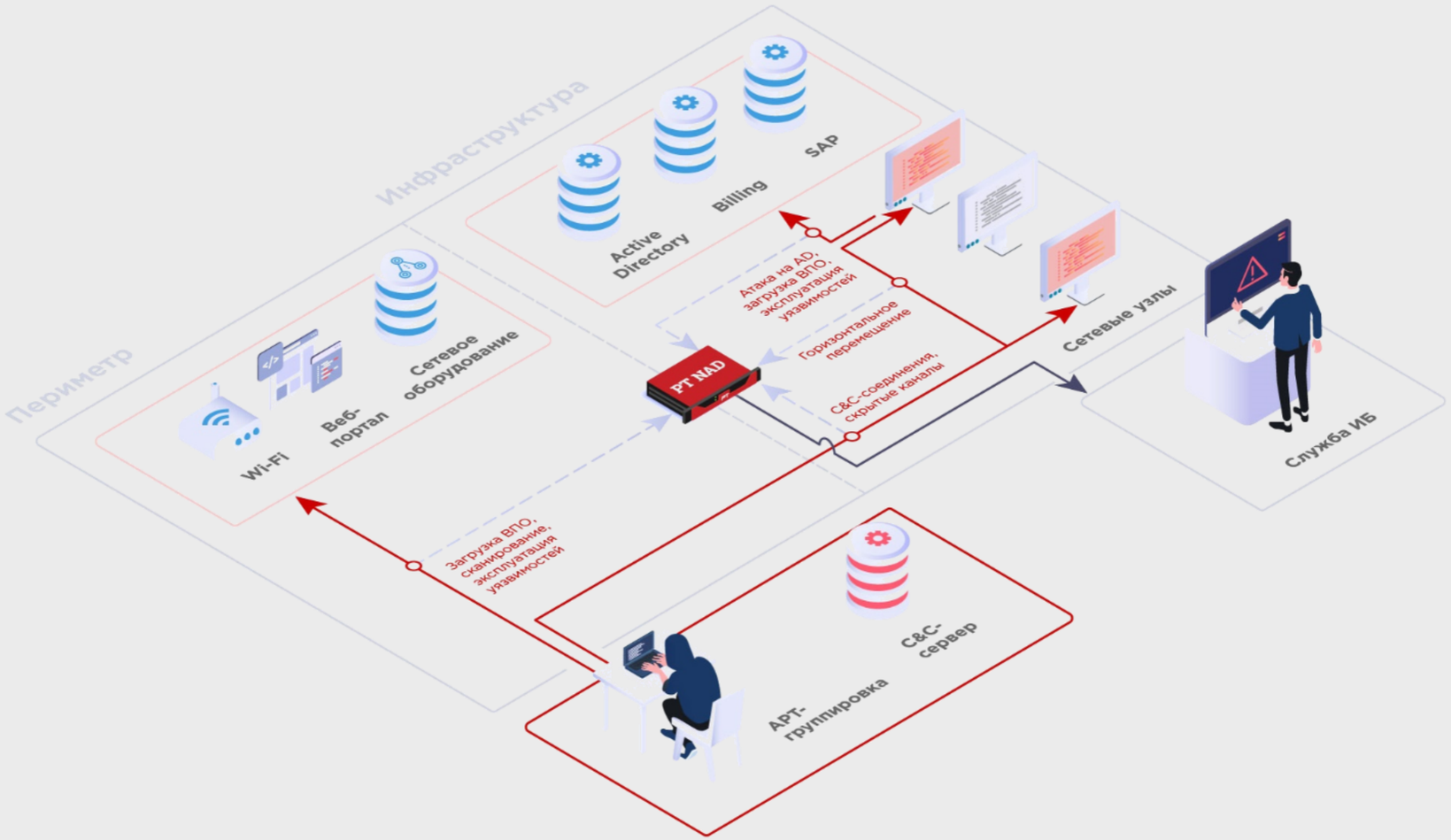
Какие средства мониторинга (источники телеметрии) важны?

- Security Information Event Management (SIEM)
  MP SIEM
- eXtended Detection & Response (XDR) / EDR / NDR
  PT EDR / XDR / NAD
- Enterprise Digital Rights Management (EDRM)
- DBMS Monitoring
- Cloud Access Security Broker (CASB)
- Data Access Governance (DAG) и Data Centric Access and Protection (DCAP)

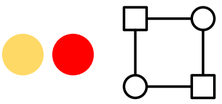
Пример: PT NAD

PT NAD захватывает и разбирает трафик на периметре и в инфраструктуре

Это позволяет выявлять активность злоумышленника и на самых ранних этапах проникновения в сеть, и во время попыток закрепиться и развить атаку внутри сети



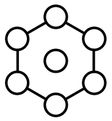
- Правила обнаружения угроз
- Модули глубокой аналитики
- Машинное обучение
- Ретроспективный анализ
- Поведенческая аналитика



Перемещения злоумышленника внутри сети

Хакерский инструментарий

Активность вредоносного ПО

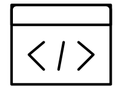


Эксплуатацию уязвимостей в сети

Сокрытие активности от средств защиты

Угрозы в зашифрованном трафике

Нарушения регламентов ИБ



Связь с автоматически сгенерированными доменами

Признаки атак, не обнаруженных ранее

Новые устройства в сети

PT NAD ВЫЯВЛЯЕТ

Анализ отсутствия источников телеметрии и качества детекта

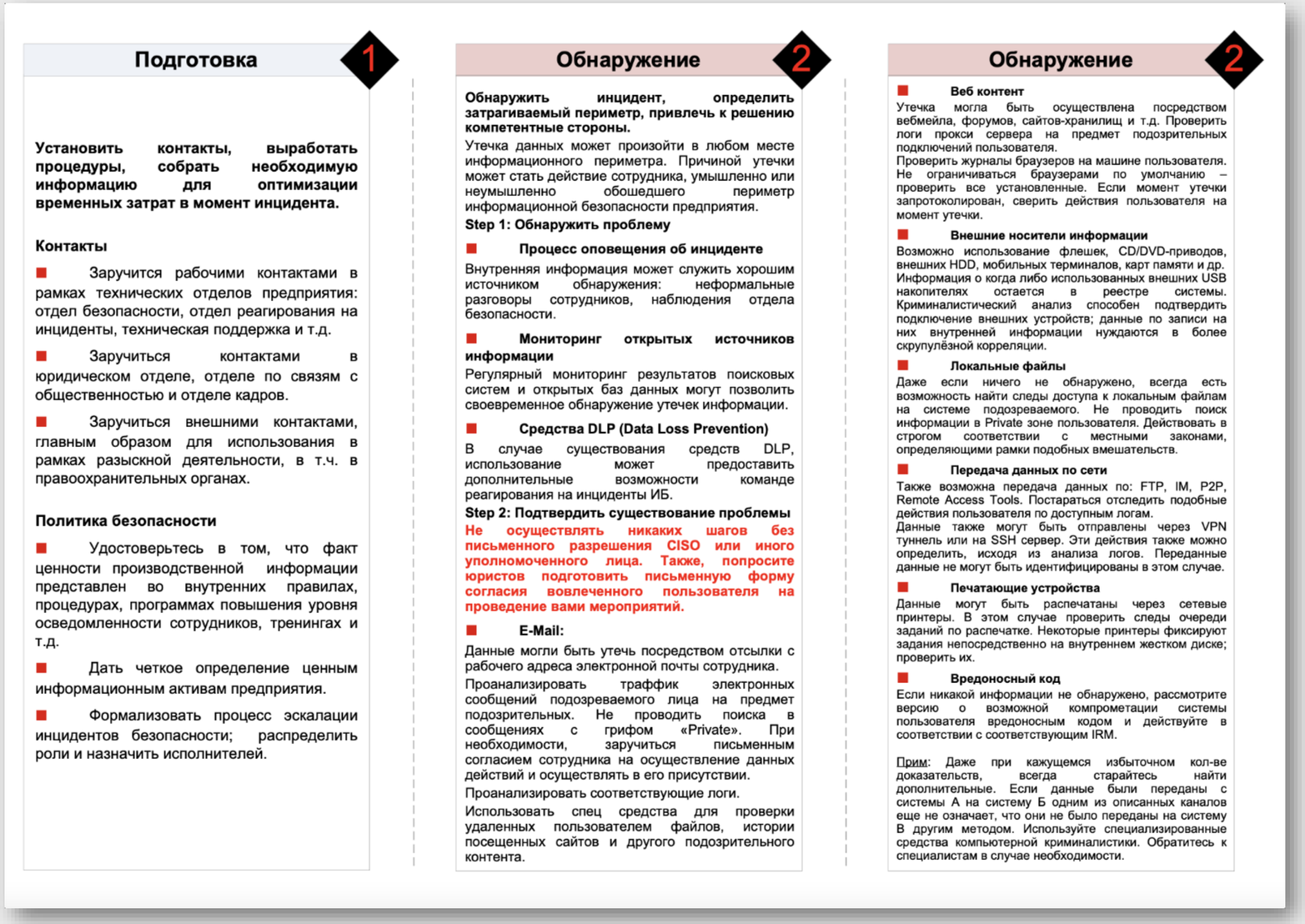
- Необходимо знать имеющиеся источники событий ИБ, из которых будут формироваться инциденты
- Необходимо понимать имеющиеся технологии обнаружения угроз (не вторжений / атак) и используемые ими источники телеметрии

Покрытие телеметрией техник MITRE ATT&CK

Как не делать лишних шагов вправо/влево, следуя четкой процедуре?

Пример плейбука по утечке данных (рус)

- Что мы пытаемся защитить?
- Какие у нас угрозы?
- Как мы детектируем их?
- Как мы реагируем?



Подготовка 1

Установить контакты, выработать процедуры, собрать необходимую информацию для оптимизации временных затрат в момент инцидента.

Контакты

- Заручится рабочими контактами в рамках технических отделов предприятия: отдел безопасности, отдел реагирования на инциденты, техническая поддержка и т.д.
- Заручиться контактами в юридическом отделе, отделе по связям с общественностью и отделе кадров.
- Заручиться внешними контактами, главным образом для использования в рамках разыскной деятельности, в т.ч. в правоохранительных органах.

Политика безопасности

- Удостоверьтесь в том, что факт ценности производственной информации представлен во внутренних правилах, процедурах, программах повышения уровня осведомленности сотрудников, тренингах и т.д.
- Дать четкое определение ценным информационным активам предприятия.
- Формализовать процесс эскалации инцидентов безопасности; распределить роли и назначить исполнителей.

Обнаружение 2

Обнаружить инцидент, определить затрагиваемый периметр, привлечь к решению компетентные стороны.

Утечка данных может произойти в любом месте информационного периметра. Причиной утечки может стать действие сотрудника, умышленно или неумышленно обошедшего периметр информационной безопасности предприятия.

Step 1: Обнаружить проблему

- **Процесс оповещения об инциденте**

Внутренняя информация может служить хорошим источником обнаружения: неформальные разговоры сотрудников, наблюдения отдела безопасности.

- **Мониторинг открытых источников информации**

Регулярный мониторинг результатов поисковых систем и открытых баз данных могут позволить своевременное обнаружение утечек информации.

- **Средства DLP (Data Loss Prevention)**

В случае существования средств DLP, использование может предоставить дополнительные возможности команде реагирования на инциденты ИБ.

Step 2: Подтвердить существование проблемы

Не осуществлять никаких шагов без письменного разрешения CISO или иного уполномоченного лица. Также, попросите юристов подготовить письменную форму согласия вовлеченного пользователя на проведение вами мероприятий.

- **E-Mail:**

Данные могли быть утечь посредством отсылки с рабочего адреса электронной почты сотрудника.

Проанализировать траффик электронных сообщений подозреваемого лица на предмет подозрительных. Не проводить поиска в сообщениях с грифом «Private». При необходимости, заручиться письменным согласием сотрудника на осуществление данных действий и осуществлять в его присутствии.

Проанализировать соответствующие логи.

Использовать спец средства для проверки удаленных пользователем файлов, истории посещенных сайтов и другого подозрительного контента.

Обнаружение 2

- **Веб контент**

Утечка могла быть осуществлена посредством вебмейла, форумов, сайтов-хранилищ и т.д. Проверить логи прокси сервера на предмет подозрительных подключений пользователя.
Проверить журналы браузеров на машине пользователя. Не ограничиваться браузерами по умолчанию – проверить все установленные. Если момент утечки запротоколирован, сверить действия пользователя на момент утечки.

- **Внешние носители информации**

Возможно использование флешек, CD/DVD-приводов, внешних HDD, мобильных терминалов, карт памяти и др. Информация о когда либо использованных внешних USB накопителях остается в реестре системы. Криминалистический анализ способен подтвердить подключение внешних устройств; данные по записи на них внутренней информации нуждаются в более скрупулёзной корреляции.

- **Локальные файлы**

Даже если ничего не обнаружено, всегда есть возможность найти следы доступа к локальным файлам на системе подозреваемого. Не проводить поиск информации в Private зоне пользователя. Действовать в строгом соответствии с местными законами, определяющими рамки подобных вмешательств.

- **Передача данных по сети**

Также возможна передача данных по: FTP, IM, P2P, Remote Access Tools. Постараться отследить подобные действия пользователя по доступным логам.
Данные также могут быть отправлены через VPN туннель или на SSH сервер. Эти действия также можно определить, исходя из анализа логов. Переданные данные не могут быть идентифицированы в этом случае.

- **Печатающие устройства**

Данные могут быть распечатаны через сетевые принтеры. В этом случае проверить следы очереди заданий по распечатке. Некоторые принтеры фиксируют задания непосредственно на внутреннем жестком диске; проверить их.

- **Вредоносный код**

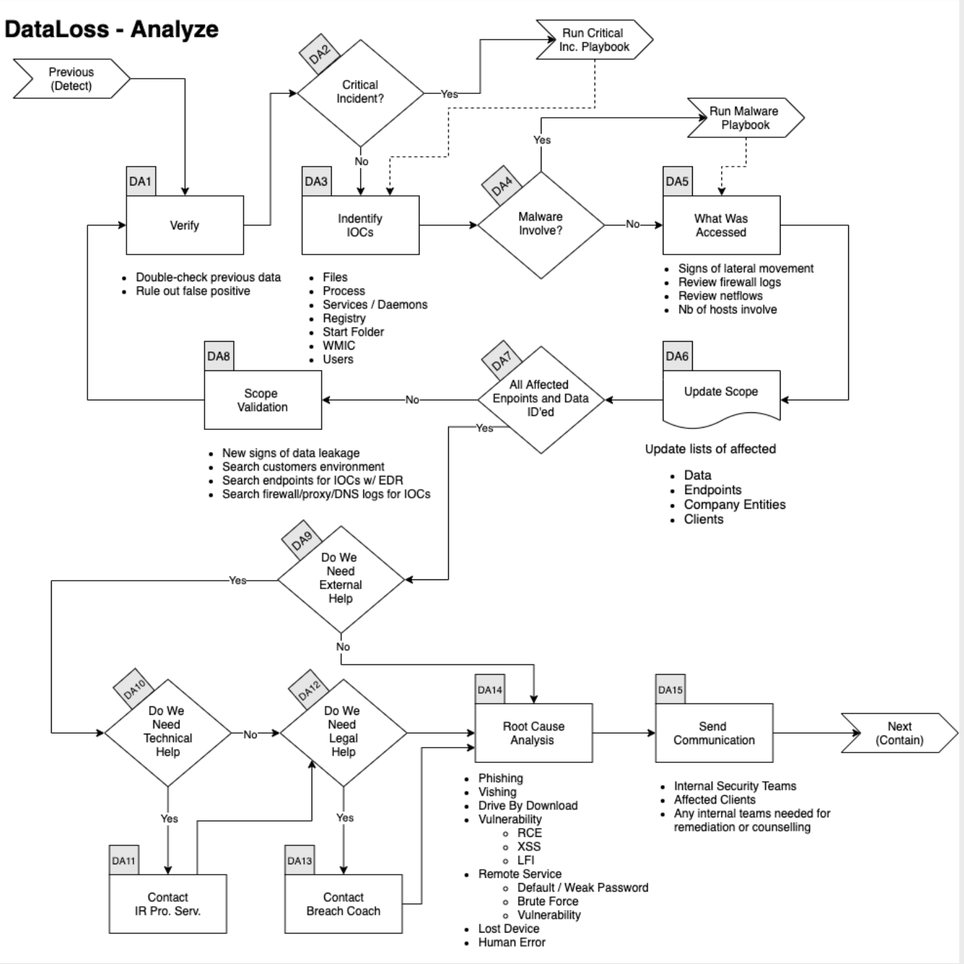
Если никакой информации не обнаружено, рассмотрите версию о возможной компрометации системы пользователя вредоносным кодом и действуйте в соответствии с соответствующим IRM.

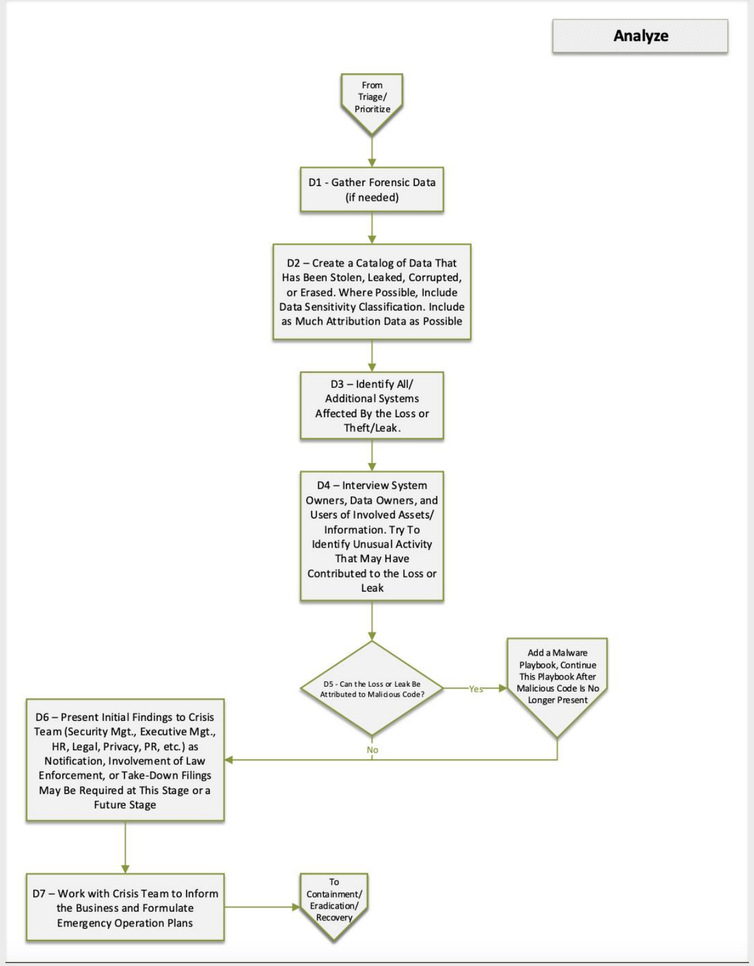
Прим: Даже при кажущемся избыточном кол-ве доказательств, всегда старайтесь найти дополнительные. Если данные были переданы с системы А на систему Б одним из описанных каналов еще не означает, что они не было переданы на систему В другим методом. Используйте специализированные средства компьютерной криминалистики. Обратитесь к специалистам в случае необходимости.

Пример плейбука по утечке данных (англ)

Data Loss Playbook

Пример визуализации плейбука по утечке данных (англ)





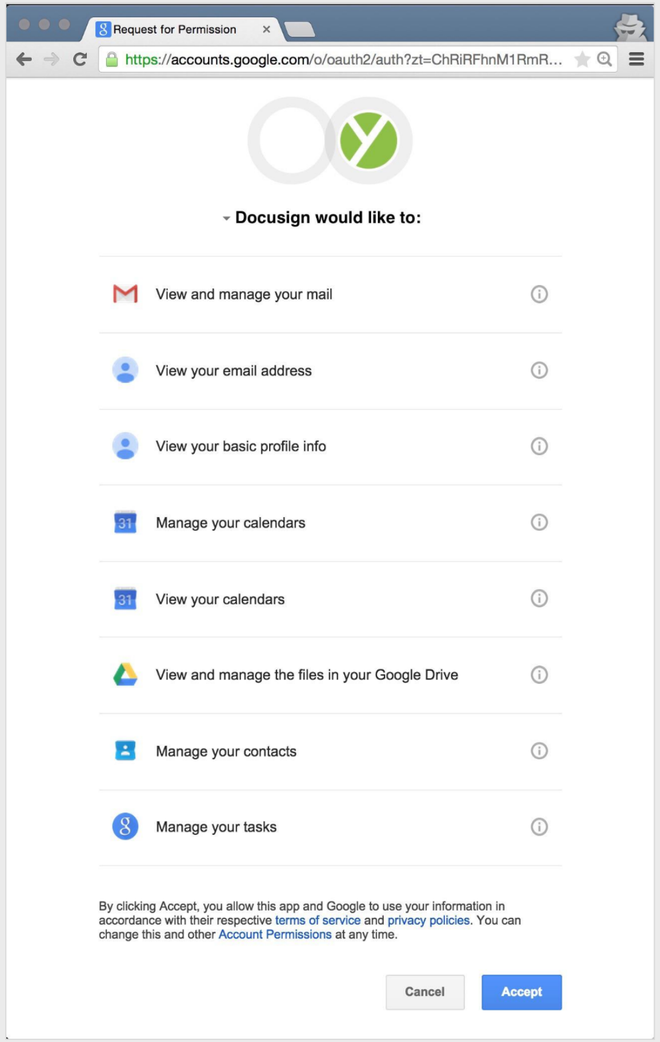
Фрагменты этапа анализа инцидента с ПДн

А реагирование – это часть системы обеспечения безопасности ПДн

Информирование об утечках ПДн – это часть процесса

…который начинается с ответа на вопросы

1. Кто (или что) имеет доступ к данным?
2. Откуда он (или оно) имеет доступ?
3. Какой доступ он (или оно) имеет?
4. Когда он (или оно) должен иметь доступ?
5. Что он (или оно) могут делать в рамках своего доступа?
6. А кто (или что) мне угрожает?
7. А что он (или оно) может сделать?
8. …



Вопросов на самом деле больше

Текущий статус

- Что мы уже знаем?
- Какие защитные меры мы применяем сейчас?
- У нас есть доказательства наличия проблем с утечками?

Информация

- Где она?
- Что требует защиты?
- Цели защиты?
- Драйвера защиты?

Риски и угрозы

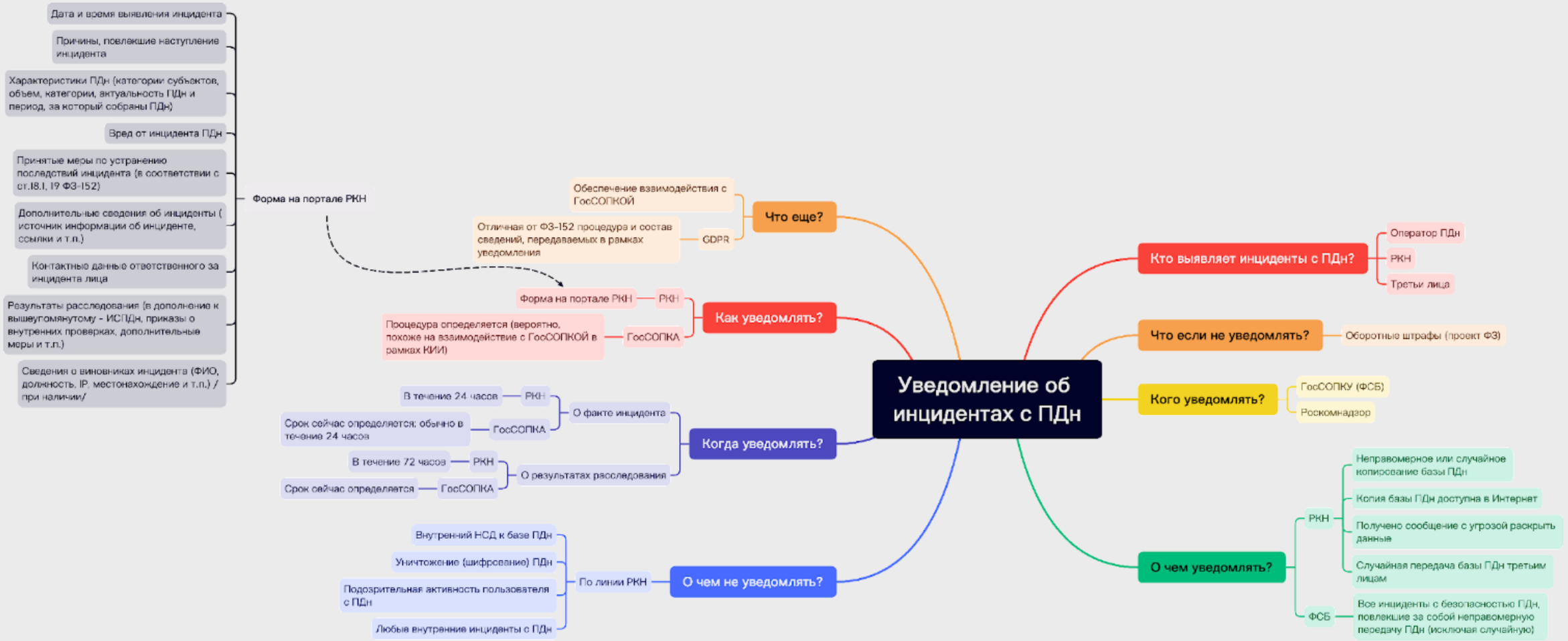
- Потенциальные риски и угрозы?
- Какие риски существуют?
- У нас есть план реагирования на инциденты?
- Планируем ли мы изменить нашу ИТ-архитектуру, например, уйти в облака?

Факторы успеха

- Может DLP решить наши цели?
- Какие преимущества мы получим с помощью DLP?
- Как будет определена удача от DLP?
- Какие условия для удачного внедрения?
- Кто должен быть вовлечен и насколько глубоко?
- Будет DLP работать в нашей культуре?
- Что может помешать?


Но это уже другая история

В качестве первичного резюме



Скачать картинку: https://t.me/alukatsky/6411

В качестве полного резюме

- Уведомление регулятора об инциденте с ПДн – это верхушка айсберга!
- Учитывайте тактику, техники и процедуры (TTP), используемые злоумышленниками
- Учитывайте жизненный цикл утечки (kill chain)
- Начните пересмотр стратегии борьбы с утечками, сфокусированной не вокруг DLP
- Идентифицируйте слабые звенья в организации, в сети, в системе защиты
- Думайте как злоумышленники – действовать как безопасники (применяйте Red Team / Blue Team)
- Внедрите сегментацию инфраструктуры – 50% успеха
- Внедрите мониторинг всей инфраструктуры – вторые 50% успеха

В качестве полного резюме

- Сбалансируйте технологии борьбы с утечками (предотвращение, обнаружение и реагирование) – вместо соотношения 80-15-5 перейдите к 33-33-34
- Задумайтесь о безопасности внутренней сети также, как защищается периметр, а также о безопасности облаков (включая доступ к ним) и мобильных устройств
- Мониторьте даже то, чего якобы нет (Wi-Fi, мобильные устройства, 3G/4G-модемы, облака и т. п.)
- Внедрите систему Threat Intelligence (Darknet, форумы, Telegram-каналы) для раннего предупреждения об утечках
- Займитесь повышением осведомленности персонала

alukatsky@ptsecurity.com

ptsecurity.com

Спасибо за внимание

О Positive Technologies

20 лет
исследований и опыта в обеспечении кибербезопасности

300+
экспертов в крупнейшем исследовательском центре в Европе

10 лет
проводим самые крупные в России и Европе киберучения

80%
отечественных компаний рейтинга «Эксперт-400» используют наши продукты и услуги

Positive Technologies уже 20 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира.
В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».
Следите за нами в соцсетях,а также в разделе «Новости» на сайте ptsecurity.com.