PRO iP VIDEO

Тема доклада:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/ЗАЩИЩЕННОСТЬ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Погоржельский Станислав Игоревич

Технический пресейл по услугам кибербезопасности
для ИТ-Инфраструктуры ПАО МегаФон

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

О ЧЁМ МЫ С ВАМИ ПОГОВОРИМ

- Правовые аспекты ИБ и защищенности систем видеонаблюдения
- За что несёт ответственность проектировщик при реализации системы видеонаблюдения
- Какие правила ИБ нужно учесть в реализации ИТ ландшафта систем видеонаблюдения. Примеры инструментария и нюансов

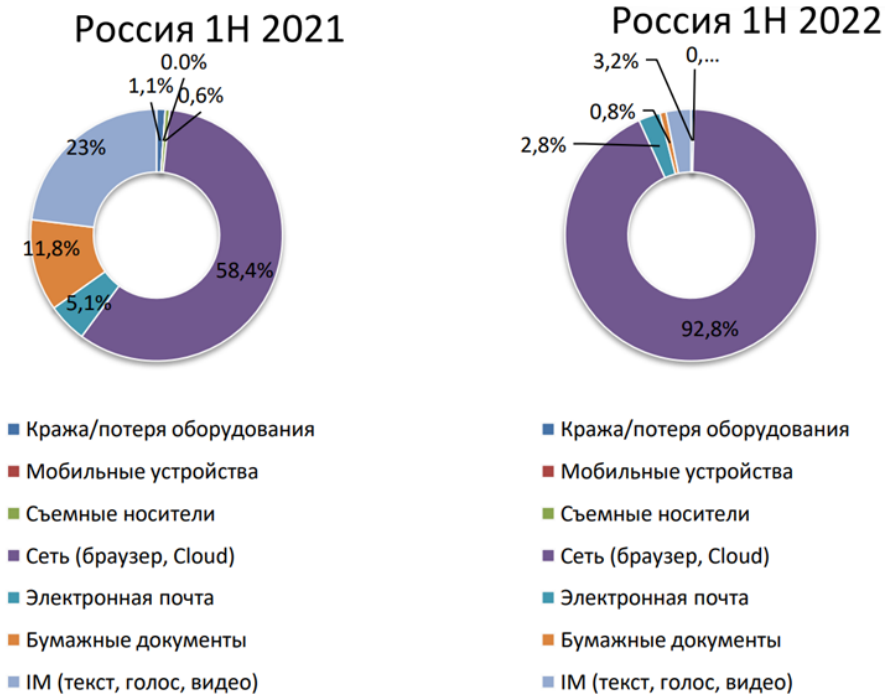
ДОГОВОРИМСЯ О ТЕРМИНАХ

- ИБ – информационная безопасность
- ЦОД/ИТ ландшафт – собирательный образ ИТ инфраструктуры
- МСЭ - Межсетевой экран
- СОВ – система обнаружения вторжений
- Сигнатуры – набор правил/процедур защиты ИБ
- ПДн – персональный данные
- ПО – программное обеспечение
- ФЗ – федеральный закон

ЧТО МОЖНО ПОТЕРЯТЬ В СЛЕДСТВИИ КРАЖИ/УТЕЧКИ ИНФОРМАЦИИ И ПОТЕРИ ДОСТУПА

- ПДн
- Накопленный архив данных
- Доступ до камер
- Доступ до ПО, где проходит обработка/аналитика
- Прочая не доступность частей сети и серверных ресурсов

КАНАЛЫ УТЕЧЕК ИНФОРМАЦИИ. СРАВНЕНИЕ 2021 И 2022 ГОДА



Источник infowatch: Отчёт об утечках данных за 1 полугодие 2022 года

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

КАКИЕ ПРАВОВЫЕ НОРМЫ НУЖНО ОБЕСПЕЧИВАТЬ В ИБ

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

ОСНОВНЫЕ ЗАКОНЫ, КОТОРЫЕ ТРЕБУЕТСЯ УЧЕСТЬ ПРИ ПРОЕКТИРОВАНИИ ИТ СИСТЕМ ОБРАБОТКА ДАННЫХ С ВИДЕОКАМЕР

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

- Имеется описание категоричности Уровня Защищённости данных 1,2,3,4 исходя из типов ПДн. Соответственно, применяются разные инструменты защиты
- Требования к трансграничной передачи ПДн (обязанность оператора направить в Роскомнадзор уведомление о намерении осуществлять трансграничную передачу ПДн)
- И прочее

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

Почти все ИТ системы гос.компаний и компаний, которые обслуживают гос.компании стали со статусом КИИ или около КИИ

Минцифры готовит новую версию законопроекта об оборотных штрафах за утечку персональных данных.

Москва, 12 июля 2022 года — По итогам обсуждений с отраслью Минцифры готовит изменения в законопроект об оборотных штрафах за утечки персональных данных

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

ВИДЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В федеральном законе №152 обозначены виды персональных данных:

- **Общие.** К ним законодательство относит базовые личные данные: ФИО, место регистрации, информация об образовании, о месте работы, номер телефона, e-mail;
- **Специальные.** Информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях;
- **Биометрические.** Физиологические или биологические особенности человека, которые используют для установления его личности: фотографии, отпечатки пальцев, анализ ДНК, группа крови, рост, цвет глаз, вес и другие;
- **Иные.** К ним относят все данные, которые нельзя отнести к другим видам: принадлежность к определенной социальной группе, корпоративные данные и так далее.

Как только, вы понимаете, что можете идентифицировать человека в автоматизированной системе, то возникает требование: **«Обработка персональных данных»**

Обработка персональных данных должна осуществляться только с согласия субъекта

ВЫВОДЫ

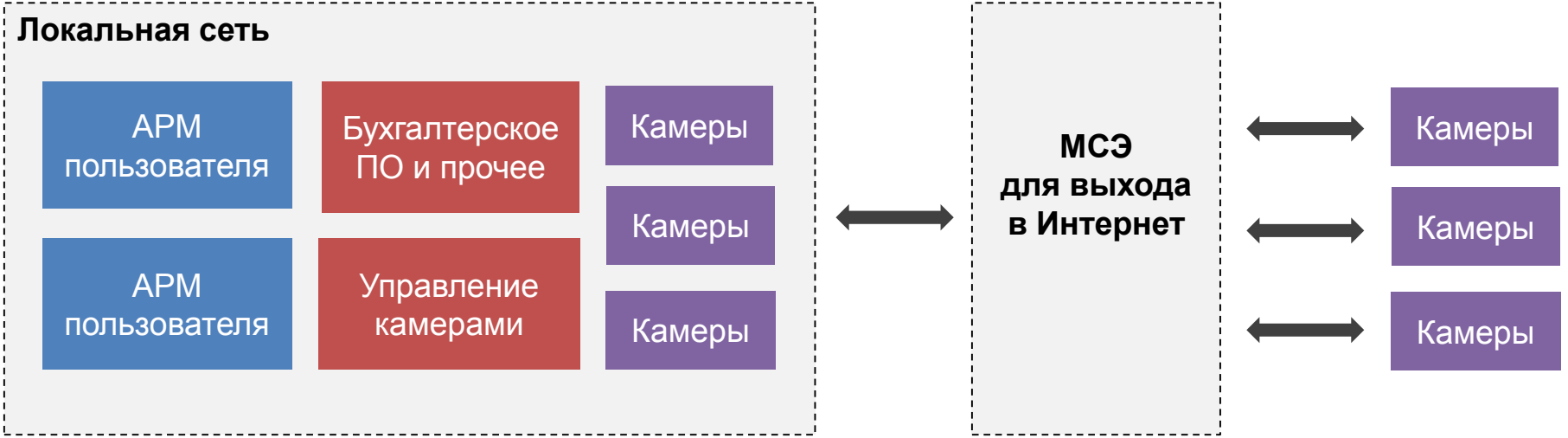
- Требования правовые основные перечислены в 152 ФЗ (про ПДн)
- При появлении модуля аналитики/идентификации пользователя – это идентифицируется как обработка ПДн с соответствующими требованиями
- Если гос.заказчик, то применяются требования 187 ФЗ (про КИИ)

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

МОДЕЛИ НАРУШИТЕЛЕЙ

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

СХЕМА ТИПОВОЙ ИТ ИНФРАСТРУКТУРЫ



Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

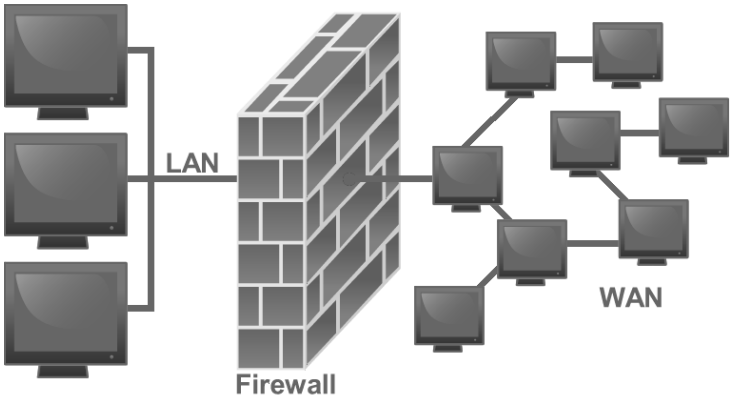
КАКИЕ СРЕДСТВА ИБ МЫ МОЖЕМ ЗАДЕЙСТВОВАТЬ

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

МЕЖСЕТЕВЫЕ ЭКРАНЫ



Межсетевой экран (МЭ, он же брандмауэр или фаервол) — программный или программно-аппаратный комплекс, предназначенный для фильтрации исходящего и входящего сетевого трафика.

Что делает МСЭ:

- Отделяет внутреннюю сеть от сети «Интернет»;
- Запрет на проникновения в сеть организации небезопасного трафика из недоверенных сетей;
- отслеживания состояния сессии;
- блокировки передачи трафика на основе протоколов, источников или приемников, портов отправки и назначения, а также иных параметров.
- Функционал VPN

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СОСТАВЕ NGFW

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СОСТАВЕ NGFW

IDS (Intrusion Detection System, система обнаружения вторжений) — программная или аппаратно-программная система сетевой безопасности, предназначенная для выявления сетевых атак и аномалий.

IDS отслеживает трафик, сравнивая его с собственной базой данных возможных сетевых атак и базовой сетевой активностью. Такой механизм работы позволяет обнаруживать:

- сетевые атаки;
- неавторизованный доступ к данным;
- действия вредоносных скриптов и программ;
- функционирование сканеров портов;
- нарушение политик безопасности;
- обращение к центрам управления бот-сетями и майнинг-пулам;
- аномальную активность.

*Важно заметить, что IDS-система не отражает атаки, а только обнаруживает их и уведомляет администратора, помогая найти причину и устранить ее.

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

ЧТО ТАКОЕ СИГНАТУРЫ?

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

ЧТО ТАКОЕ СИГНАТУРЫ?

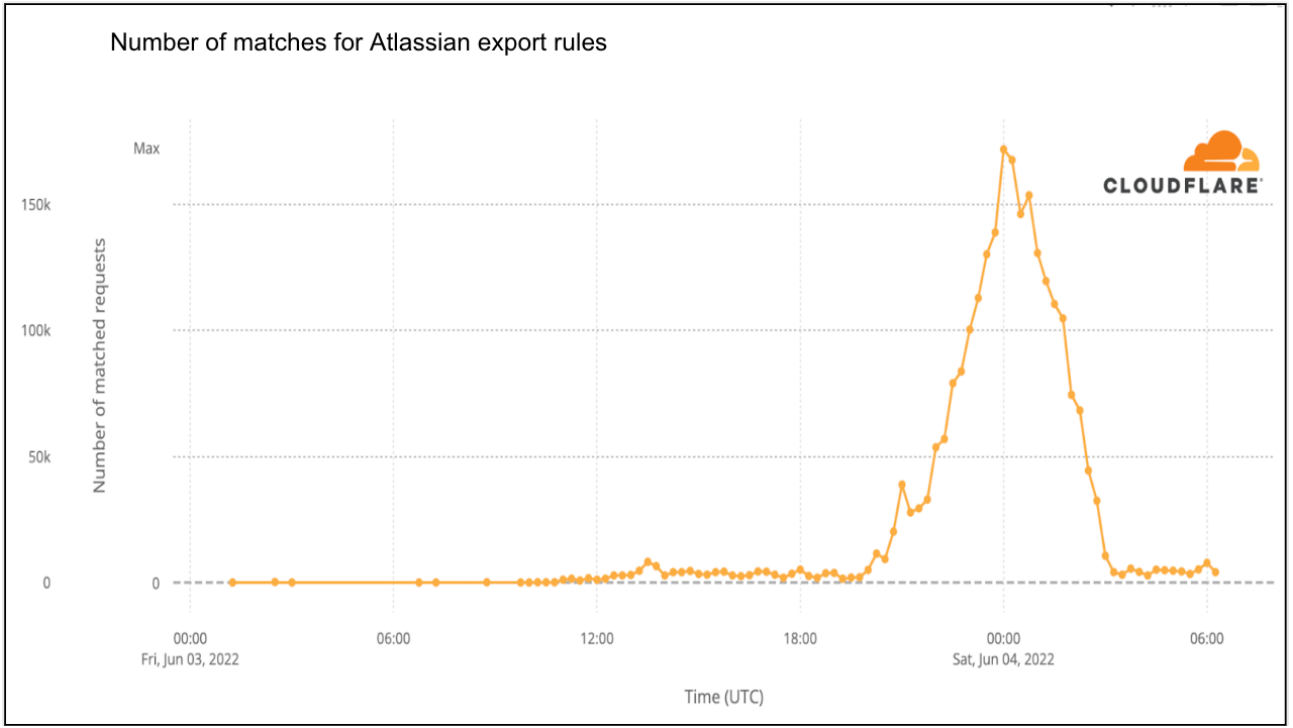
Сетевая IDS сигнатура – набор данных, которые мы хотим найти в трафике.

Примеры и методы, которые позволяют их идентифицировать:

- Попытки подключения с IP-адреса. Могут быть легко обнаружены простой проверкой поля адреса в IP-заголовке.
- Пакеты с недопустимыми комбинациями TCP-флажков. Могут быть найдены сравнением набора флажков в TCP заголовке с известными допустимыми или недопустимыми комбинациями флажков.
- Электронные сообщения, содержащие определенные вирусы. IDS может сравнить имя поля объекта или вложения с известными именами, связанными с известными вирусами.
- Переполнение буфера в DNS при использовании недопустимого запроса. Анализ DNS полей и проверка длины каждого из них помогает идентифицировать попытку переполнения буфера.
- DoS против POP3 сервера путем вызова одной и той же команды тысячи раз. Сигнатура для этого типа нападения должна хранить информацию о том, сколько раз была вызвана команда и предупреждение, когда это число превысит некоторый порог.
- Попытка запроса файла на FTP сервере без предварительной регистрации. Сигнатура должна предупреждать в случае, когда произошла попытка вызова команды без подтверждения подлинности.

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

ЧТО ТАКОЕ СИГНАТУРЫ?



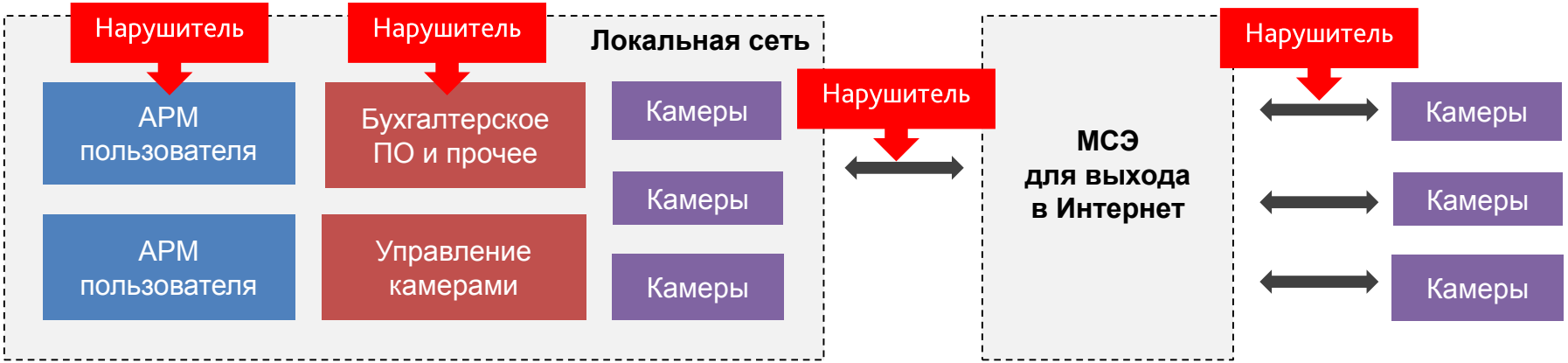
Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

ЗАЧЕМ НУЖНЫ ВСЕ ЭТИ СРЕДСТВА ИБ

Погоржельский Станислав Игоревич, Технический пресейл, ПАО МегаФон

КАК МОГУТ НАРУШИТЕЛИ ПОПАСТЬ В ИТ СИСТЕМУ ЗАКАЗЧИКА

- Сканировать порты с целью поиска открытых и дальнейшее проникновение в ИТ Инфраструктуру
- Найти уязвимость в ПО Заказчика, которое «смотрит» в Интернет
- Подключится физически к сети через Патч-корд Ethernet камеры, т.к. в основном используется UTP кабеля и канал без шифрования
- Через пользователя, получив у него логин и пароль



В ЗАПИСНУЮ КНИЖКУ ПРОЕКТИРОВЩИКА

1. Сети, где находятся камеры нужно отделять от основных
2. Учитывать требования, если появляются ПДн
3. Использовать VPN при необходимости
4. Желательно, использовать МСЭ или NGFW для защиты сервера управления
5. Соблюдайте парольную политику и учитывайте уровень ответственность оператора (пользователя)