

КАК ВЫБРАТЬСЯ ИЗ КАМЕННОГО ВЕКА DLP?

И какие из новейших технологий
взять на вооружение

Александр Федорчуков, руководитель отдела по работе
с партнёрами

Zecurion





ZECURION — КТО МЫ ТАКИЕ



- Один из старейших независимых DLP-вендоров — основана в 2001 года
- Входим в топ мировых DLP-вендоров. Единственный российский DLP-разработчик, признанный «Большой тройкой» аналитических агентств – Gartner, IDC, Forrester
- Zecurion стала учредителем технологической ассоциации Innovation Exchange совместно с IBM, Samsung, Intel и др.
- Алексей Раевский, генеральный директор Zecurion входит в Экспертный совет по цифровой трансформации при Генеральной прокуратуре РФ
- Защищаем информацию от утечек в отечественных госучреждениях, крупнейших российских и международных компаниях
- Zecurion возглавляет рабочую группу по блокчейн-технологиям и криптовалютам в рамках Комитета по информационной безопасности АРПП «Отечественный софт»

DLP-СИСТЕМЫ – КЛАССИЧЕСКОЕ ПОНИМАНИЕ

Задачи DLP – контроль информационных потоков на основе централизованных политик.

Защита данных:



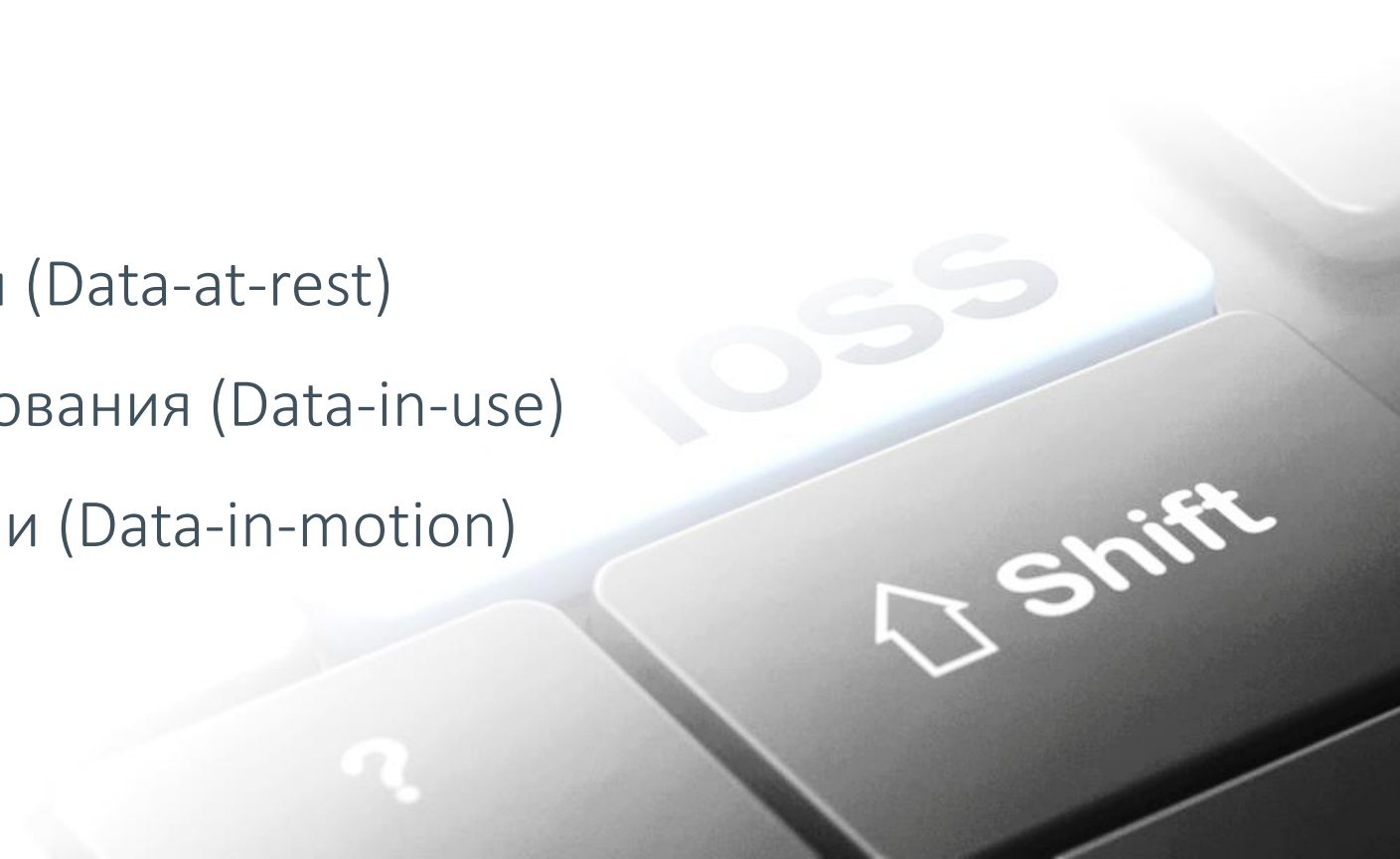
на этапе хранения (Data-at-rest)



во время использования (Data-in-use)



в момент передачи (Data-in-motion)



ЭТАПЫ РАЗВИТИЯ КЛАССИЧЕСКИХ DLP

1

этап

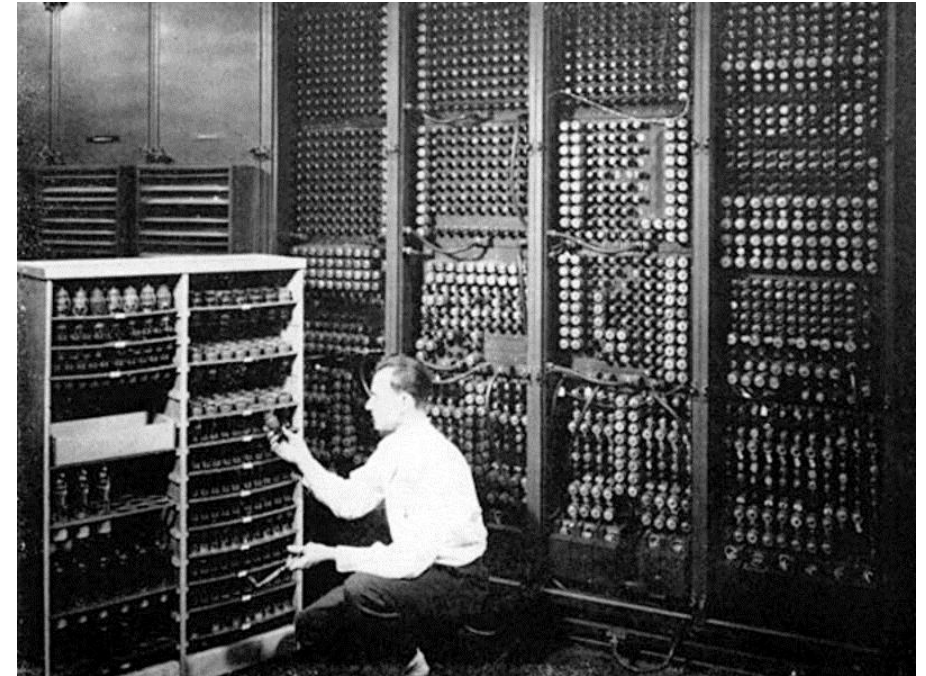
- Контекстный анализ (формальные признаки)
- Отдельные технологии контентного анализа
- Заимствование технологий («антиспам наоборот»)
- Преимущественно шлюзовые решения



ЭТАПЫ РАЗВИТИЯ КЛАССИЧЕСКИХ DLP

2 этап

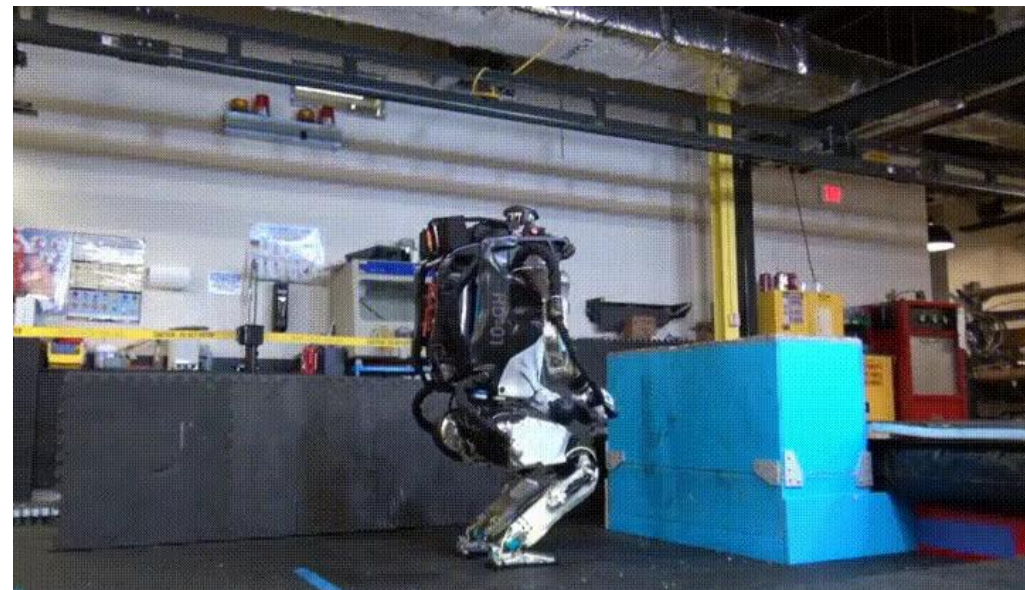
- Базовые методы контентного анализа (морфология, цифровые отпечатки)
- Контроль ограниченного объёма документов
- Поиск и категорирование данных в корпоративной среде
- Появление функциональных агентов



ЭТАПЫ РАЗВИТИЯ КЛАССИЧЕСКИХ DLP

3 этап

- Большое количество технологий анализа, внедрение OCR, самообучаемых технологий и др.
- Минимизация ложных срабатываний
- Контроль большинства корпоративных каналов, локальных и сетевых
- Шифрование данных



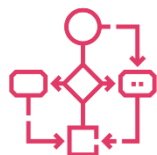
НОВЕЙШИЕ ТЕХНОЛОГИИ В DLP-СИСТЕМАХ



Поведенческий анализ (User Behavior Analytics)



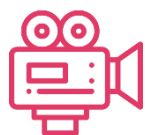
Гибридный анализ конфиденциальной информации



Рабочая среда офицера ИБ (workflow), реализованная в современном web-интерфейсе



Принудительное шифрование при записи данных на носители (криптопериметр)



Защита от внешней съёмки (Camera Detector)



Контроль голосовых каналов

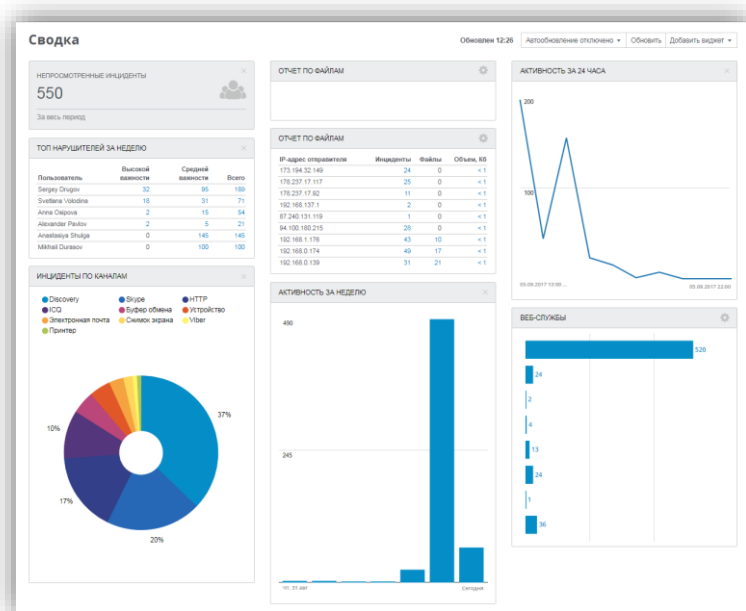
ГИБРИДНЫЙ АНАЛИЗ



Комбинирование контентного и контекстного анализа со сложными составными условиями



СОВРЕМЕННЫЙ WEB-ИНТЕРФЕЙС



- Единая консоль управления
- Кастомизируемая сводная информация
- Ролевая модель доступа к консоли
- Подключение из любой точки
- Автоматические ежедневные отчёты
- Возможность детально расследовать инциденты

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ (UBA)



Расчёт среднестатистических показателей различных параметров и событий, которые определяют поведенческий профиль сотрудников

- Автоматический анализ действий сотрудников
- Более 10 психологических индексов сотрудника
- Контроль лояльности сотрудников

КОНТРОЛЬ ПРИЛОЖЕНИЙ

- Контроль использования офисных, графических и др. приложений
- Выявление бездельников (подключение к онлайн-играм)
- Контроль использования популярных мессенджеров (web и desktop)



КРИПТОПЕРИМЕТР



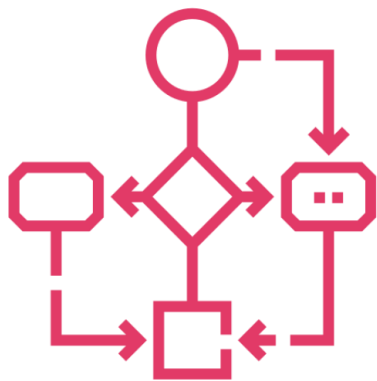
Принудительное шифрование
при записи данных на носители
в зависимости от их
содержимого

КОНТРОЛЬ ОБЛАЧНЫХ СЕРВИСОВ



- Сканирование файлов
- Поддержка клиентов и веб-версий

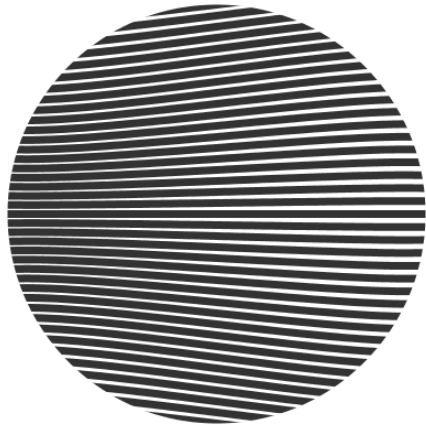
WORKFLOW



- Расследование в ручном режиме и автоматическое
- Продвинутая рабочая область с удобной визуализацией
- Ролевая модель работы с данными
- Встроенные шаблоны расследования (подсказки)



КОНТРОЛЬ ГОЛОСОВЫХ УТЕЧЕК



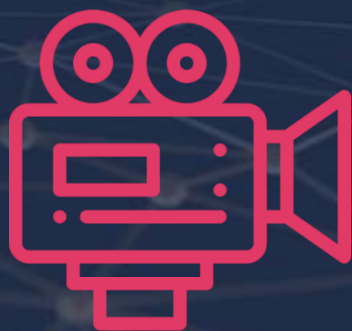
- Голосовой трафик мессенджеров
- Встроенные и подключаемые микрофоны
- Преобразование речи в текст

ВНИМАНИЕ, ВОПРОС!

ZECURION



КОНТРОЛЬ ВНЕШНЕЙ СЪЁМКИ



- Распознавание камер/телефонов/вспышки
- Проверка присутствия пользователя
- Распознавание лиц пользователя
- Старт записи видео с экрана
- Включение записи с микрофона
- Блокировка логина в момент обнаружения



TRAFFIC CONTROL

Анализирует и блокирует любую информацию, пересылаемую за пределы локальной сети через почту, форумы или мессенджеры




DEVICE CONTROL

Контролирует файлы, которые сотрудники распечатывают или копируют на USB, смартфоны и другие съёмные устройства



DISCOVERY

Сканирует сервера и компьютеры, обнаруживает места хранения конфиденциальных данных



ЧТО ДЕЛАТЬ ДЛЯ БОЛЕЕ ЭФФЕКТИВНОЙ РАБОТЫ DLP-СИСТЕМЫ

- 1** Используйте UBA, анализируйте поведение и выявляйте нелояльных сотрудников на ранней стадии
- 2** Защищайте от внешней съёмки (Camera Detector)
- 3** Принудительно шифруйте файлы при записи на носители (криптопериметр)
- 4** Используйте DLP в связке с PAM и SWG для комплексной защиты
- 5** Используйте современный web-интерфейс для детального расследования и ежедневных отчётов
- 6** Если актуально, контролируйте голосовые каналы утечки
- 7** Используйте DLP-систему с гибридным анализом для более точного выявления конфиденциальных данных
- 8** Используйте workflow для поэтапного и более детального процесса обработки инцидентов

———— #CODEIB ————

СПАСИБО ЗА ВНИМАНИЕ

 **ZECURION**

www.zecurion.ru

+7 495 221-21-60

info@zecurion.com