КИБЕРПРОТЕКТ

Безопасный файловый обмен

Цифровизация бывает безопасной

Ильшат Латыпов

Немного объективной статистики

83%

of organizations studied have had more than one data breach.

60%

of organizations' breaches led to increases in prices passed on to customers.

79%

of critical infrastructure organizations didn't deploy a zero trust architecture.

19%

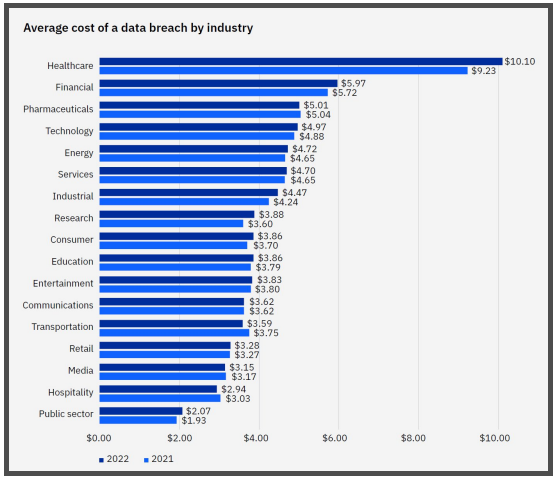
of breaches occurred because of a compromise at a business partner.

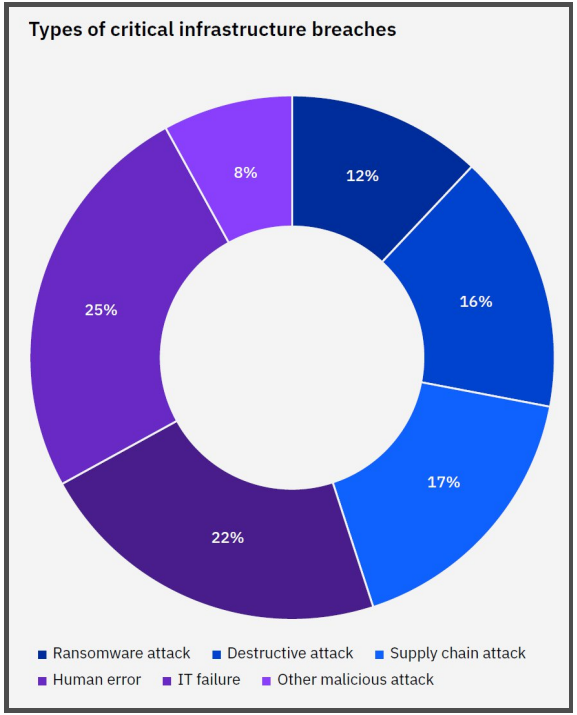
45%

of the breaches were cloud-based.

59%

Percentage of organizations that don't deploy zero trust





Ponemon: 3,600 separate interviews with individuals at 550 organizations that suffered a data breach between March 2021 and March 2022

Ponemon INSTITUTE

КИБЕРПРОТЕКТ

Источники: "Cost of a Data Breach", **Ponemon Institute & IBM Security, 2022** ; "Insider Threat Report", Cybersecurity Insiders, 2018; "Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017; CSO Online, 2017; "Insider Data Breach Survey", Opinion Matters, 2019; 2020 Cost of a Data Breach Report" Ponemon Institute LLC, July 2020; "2020 Cost of Insider Threats Global Report" Ponemon Institute LLC, February 2020; "Best Practices: Mitigating Insider Threats" Forrester Research, May 2019

Инсайдеры - основная причина утечки

90% организаций чувствуют себя уязвимыми перед лицом инсайдерских угроз - 53% сообщают, что подверглись атаке со стороны инсайдеров за последние 12 месяцев

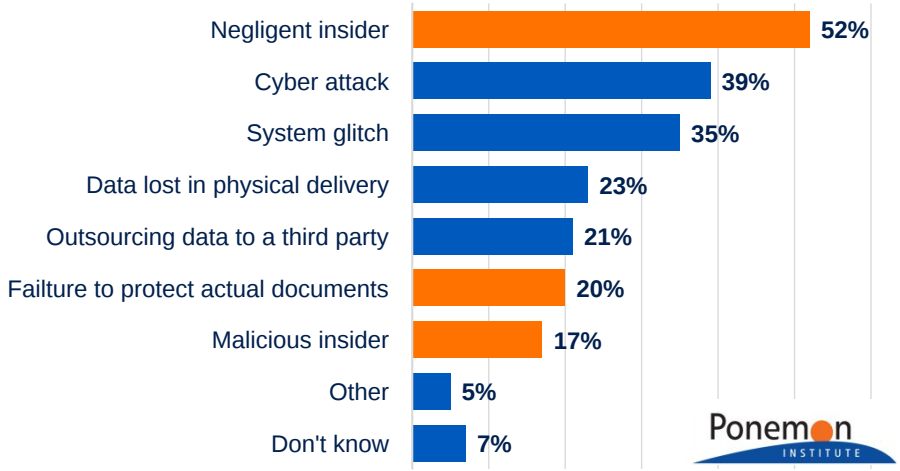
72% сотрудников делятся конфиденциальной или иной защищаемой информацией компании

35% сотрудников поделились информацией, **не подозревая,** что ей не следует делиться.

Годовой ущерб от утечек, связанных с инсайдерами (~ 45% всех нарушений)

- **31% увеличение** за последние 2 года
- Средний **по всему миру**: **$11,45 млн.**
- В среднем за **Малый и средний бизнес: $7,68**
- **89% от стоимости** связано с действиями после инцидента (реактивная защита)

Причины утечки данных



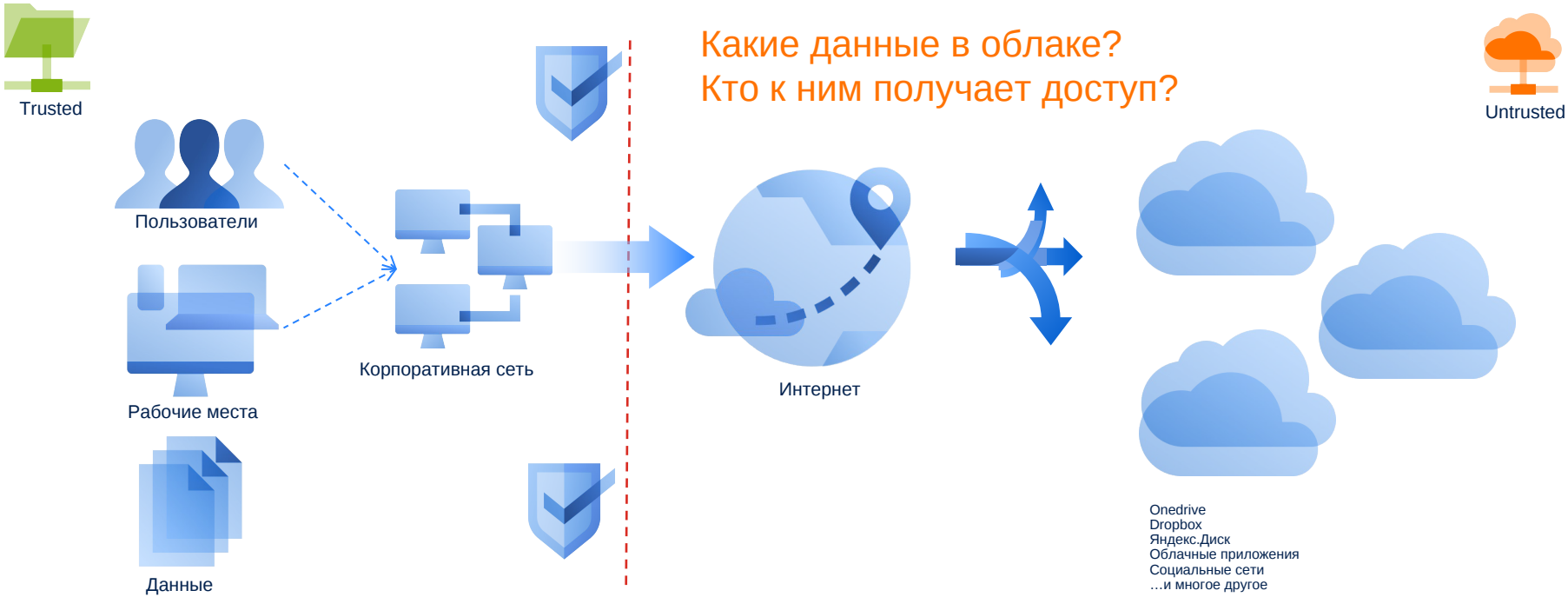
Традиционные антивирусы, брандмауэры, шифрование **и даже бэкапы** не защищают от внутренних утечек данных

КИБЕРПРОТЕКТ

Источники: “Global Cost of Insider Threats”, Ponemon Institute, 2020; “Insider Threat Report”, Cybersecurity Insiders, 2018; “Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017; CSO Online, 2017; “Insider Data Breach Survey”, Opinion Matters, 2019; 2020 Cost of a Data Breach Report” Ponemon Institute LLC, July 2020; “2020 Cost of Insider Threats Global Report” Ponemon Institute LLC, February 2020; “Best Practices: Mitigating Insider Threats” Forrester Research, May 2019

«Слепые зоны»

Облачные сетевые ресурсы не контролируются корпоративной ИБ



КИБЕРПРОТЕКТ

Кибер Файлы

Файловый обмен и синхронизация

Корпоративный сервис файлового обмена

Полный контроль
над данными на собственных серверах, в локальных ЦОДах и частных облаках

Подключение существующих хранилищ
Файловые серверы, SharePoint, EMC Documentum и CMIS

Безопасность
Централизованные политики доступа, ролевая модель администрирования, шифрование

Совместная работа
Управление версиями
Интеграция с Office365 и Р-7 Офис, *Мой Офис* *

* СКОРО

Файловое хранилище

Два раздела в разных моделях использования и администрирования

Сеть

Корпоративные источники данных

Доступ к **сетевым папкам, узлам и библиотекам SharePoint, OneDrive**

Sync & Share

Личные хранилища для файлового обмена и синхронизации.

Файловая система, **Swift S3**, **Ceph S3** или другое **S3-совместимое хранилище**

Опциональные ограничения доступа

Глобальные – на уровне системы

Белые и чёрные списки доступа к системе для групп LDAP и доменов электронной почты

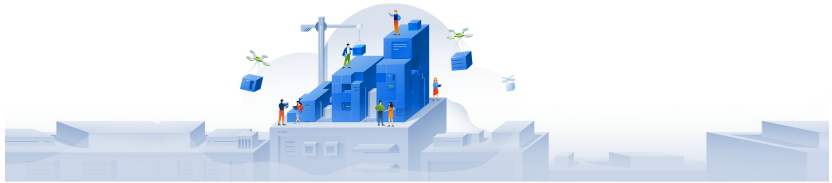
Запрет общего доступа к отдельным файлам

Запрет **общедоступных ссылок** на загрузку

Запрет доступа **незарегистрированным** пользователям

Ограничения **срока доступа** к общим файлам

Запрет **многоразовых ссылок** на загрузку файлов



Локальные – на уровне папок / файлов

Уровень папок

Запрет **изменения и удаления** содержимого

Запрет **на приглашение** участников

Запрет на просмотр **списка доступа** к папке

Истекающий срок доступа к папке

Уровень файлов

Доступ **только пользователям** Кибер Файлы

Доступ только пользователям, **получившим приглашение**

Истекающий срок **действия ссылки**

Одноразовые ссылки на загрузку

Контроль и аудит

Хранилищ, файлов, учётных записей

Политики безопасности и доступа к хранилищам и данным

Контроль операций учётных записей пользователей и групп

HTTPS транспорт **для передачи** файлов

Шифрование хранимых файлов

AES-128, AES-256, ГОСТ 28147-89

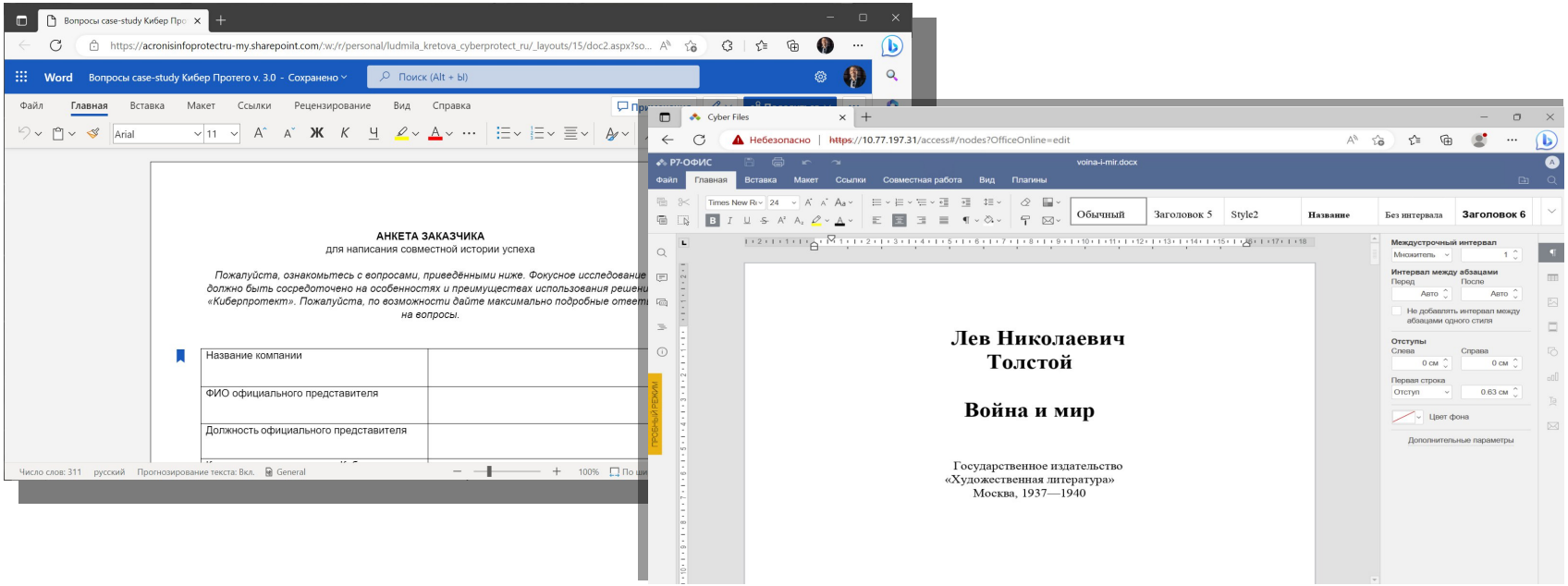
Протоколирование действий пользователей, **операций** синхронизации и предоставления доступа

Фильтрация и экспорт журналов

Интеграция с онлайн-редакторами

Microsoft Office Online

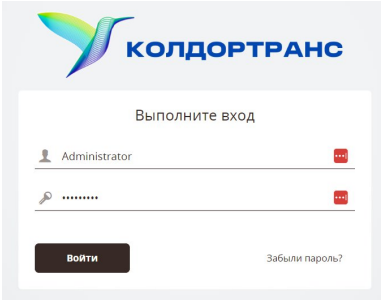
P7-Офис

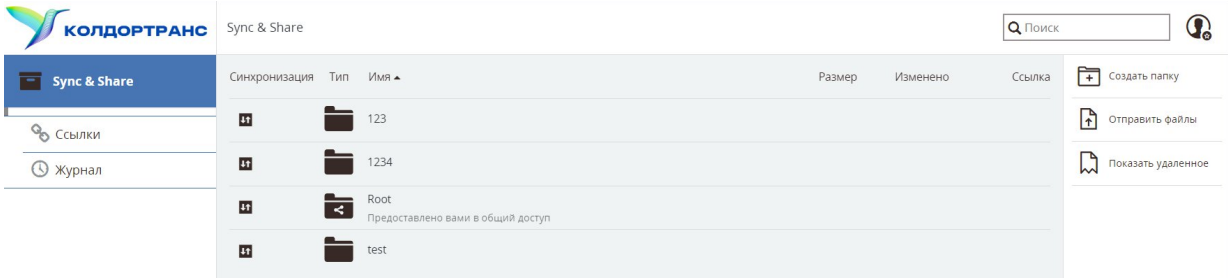


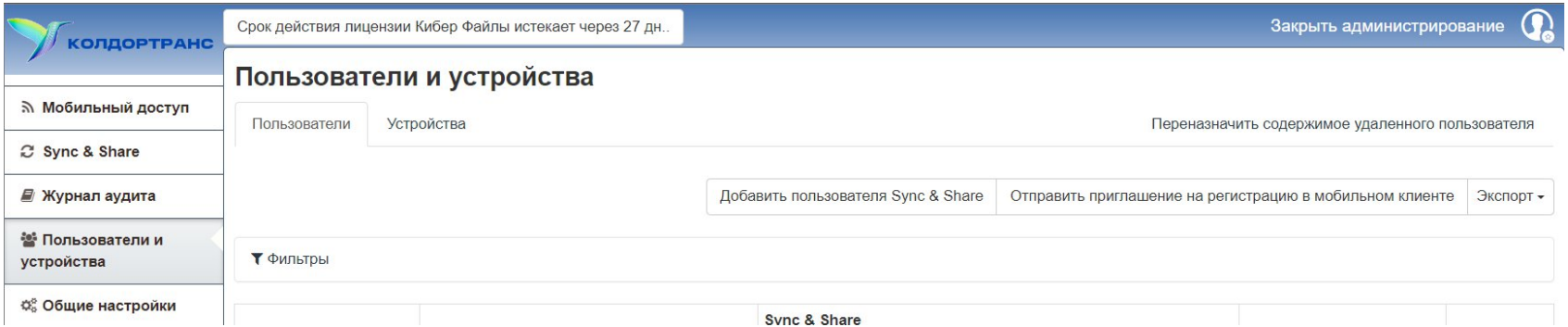
КИБЕРПРОТЕКТ

Брендирование и персонализация

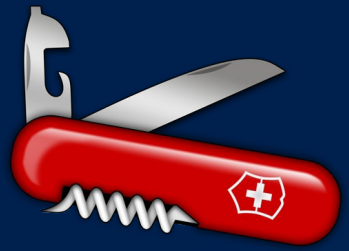
Собственные логотип, цветовая схема, пользовательские сообщения







КИБЕРПРОТЕКТ



Кибер Протего

Универсальный инструмент для любой концепции безопасности

Системы предотвращения утечек данных

Что должна уметь полнофункциональная DLP система

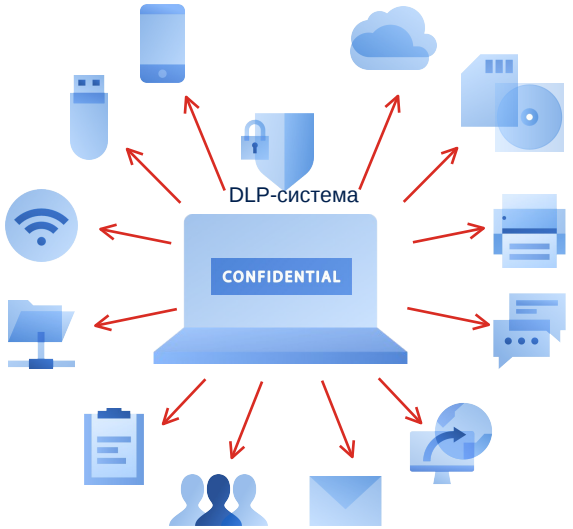
Ключевая задача любой DLP-системы – автоматическое принятие решения о возможности передачи/печати/сохранения данных

Отслеживание перемещения данных

Защита от утечки по сети и через устройства

Обнаружение данных в хранилищах

Мониторинг активности пользователя, расследование инцидентов, анализ лояльности и пр.



DLP-система (Data Loss Prevention) – ИТ-решение, обеспечивающее выявление, отслеживание и предотвращение неавторизованного использования, хранения и перемещения данных ограниченного доступа и др., используемых в организации

Кибер Протего

Программный комплекс на базе полнофункциональных агентов

Источники утечки данных

Рабочие станции

Серверы

Терминальные / виртуальные среды

Хранилища данных

- **Контроль каналов утечки**
  Устройств и сетевых коммуникаций
- **Контроль содержимого данных**
  Передаваемых по таким каналам
- **Контроль хранилищ**
  На предмет данных, которых в них храниться не должно

Контроль передаваемых данных

Возможности Cyber Protego

Контроль устройств, сетевых коммуникаций, данных, мониторинг активности пользователей

Контроль устройств // Device Control

Проводные, беспроводные и программные интерфейсы, приводы, устройства, канал печати, терминальные сессии и виртуальные среды

Контроль коммуникаций // Web Control

Протоколы, почта, веб-сервисы, мессенджеры, поисковые запросы и карьерные ресурсы

Контроль данных // Content Control

Анализ и фильтрация содержимого данных, передаваемых на устройства и через каналы сетевых коммуникаций

Мониторинг активности // UAM

Видеозапись экрана, запись сведений о запущенных процессах, кейлоггер

Контроль данных в хранилищах, устранение нарушений

1 — **Сканирование** хранилищ

Локальные файловые системы, съёмные устройства, сетевые хранилища, Elasticsearch

2 — **Обнаружение** данных

На базе анализа их содержимого

3 — **Устранение** нарушений

Удаление данных, их шифрование, смена прав доступа к ним

4 — Оповещения и **отчёты**

По результатам сканирования

КИБЕРПРОТЕКТ *Применимо к агенту для ОС Windows

Контроль устройств и интерфейсов

USB	LPT	Оптический привод	Жёсткий диск
FireWire	COM	iPhone	MTP
Wi-Fi	IrDA	USB-камеры	USB-аудио
Bluetooth	Съёмные устройства	Сетевые карты	Буфер обмена
Гибкие диски	Ленточные накопители	Канал печати	Устройства в терм.сессии

- Альт Рабочая станция
- USB
- Съемные устройства
- Белый список
- Журналирование

Контроль сетевых коммуникаций

Контролируемые каналы коммуникаций

SFTP	HTTP(S)	FTP(S)	Telnet	SMTP(S)
IMAP	MAPI	IBM Notes	POP3	Соц. сети
Облачные хранилища		Веб-поиск	Поиск работы	Веб-почта
Telegram	Zoom	Skype	WhatsApp	Кибер Файлы NEW
Jabber	IRC	TamTam NEW	ICQ	SMB

Технологии контроля, в т.ч. VPN, P2P, прокси-трафика

Независимый от приложений контроль трафика

- Глубокая инспекция пакетов агентом **(DPI)**
- **MITM-контроль** SSL-трафика, в т.ч. своими сертификатами*
- Контроль **E2EE коммуникаций**

Встроенный **IP Firewall**

- Контроль **TCP и UDP** трафика
- **Независимо** от основных политик контроля **или в режиме наследования**
- Контроль сетевой активности приложений NEW

Выборочный контроль множества **операций**

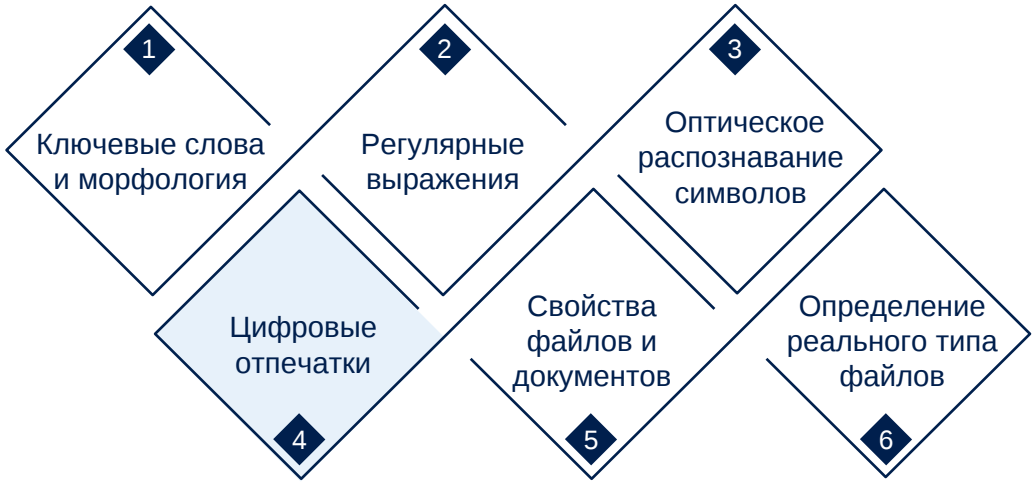
Подключения к серверам, отправки сообщений, вложений, POST- и поисковых запросов, публикации постов, других операций

Белые списки

Сетевых протоколов и веб-сервисов, SSL-коммуникаций, диапазонов IP адресов, портов, веб-ресурсов по URL, адресов и ID отправителя / получателя

Контроль содержимого

Автономные* технологии контентного анализа



Словари и шаблоны регулярных выражений **в комплекте поставки**

Составные правила, пороговые значения срабатывания

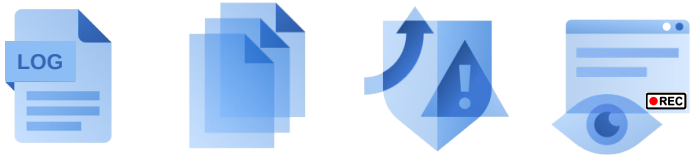
Типы правил

В разрыв

Блокировка, мониторинг, алерты

Пост-обработка

Мониторинг и алерты **без блокировки**

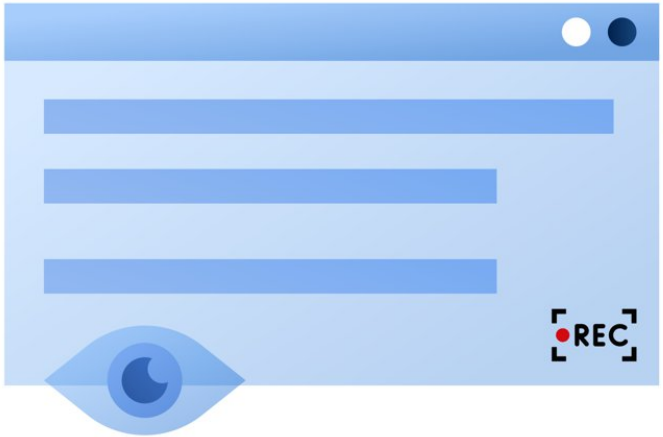


КИБЕРПРОТЕКТ

*За исключением правил поиска по цифровым отпечаткам

Мониторинг активности пользователей

Видеозапись экрана, запись сведений о запущенных процессах, кейлоггер



Неотъемлемая часть контроля с прозрачной интеграцией в политики предотвращения утечек

Запись **при реализации политики DLP** другими модулями агента

Запись **при выполнении** заданных **системных условий**

Запись **до или после** наступления заданного **события**

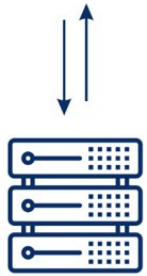
Глубокая **детализация условий** начала записи

Видео может содержать до 5 предшествующих событию минут

Составные правила с условиями, объединёнными операторами И/ИЛИ/НЕ

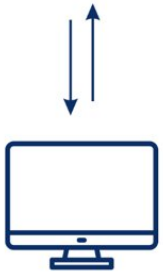
Контроль сеансов удаленного доступа

Терминальные сессии



КАНАЛЫ УТЕЧКИ ДАННЫХ

Виртуальные среды



Буфер обмена

Различные типы данных

- Файлы
- Текст
- Изображения
- Аудио
- Другие данные

Устройства

Проброшенные внутрь терминальной сессии

- Диски (съёмные, жесткие)
- Оптический привод
- Последовательный порт
- Принтеры

Векторы развития: DLP+EFSS

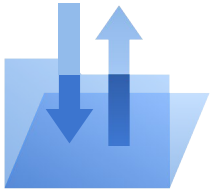
Кросс-платформенное решение, объединяющее возможности продуктов

Защита от утечки данных

- Добавление функционала на Linux
- Анализ трафика на шлюзе
- Поддержка отечественных систем
- Полный переход на Web-интерфейс

Единая платформа безопасности

- Интеграция с DLP для контроля обмена конфиденциальной информацией
- Централизованная статистика и объединенные отчеты DLP и EFSS
- Контроль хранения данных в соответствии с политикой компании



Безопасный файловый обмен

- Открытые и закрытые контуры файлового обмена в рамках одного сервера
- Возможность автоматической генерации ссылок в почте, вместо отправки самих фалов
- Интеграция с ИБ решениями

КИБЕРПРОТЕКТ

СПАСИБО!

Ильшат Латыпов

Менеджер продукта

Ilshat.Latypov@cyberprotect.ru

cyberprotect.ru