Безопасность информационного обмена.

Цифровизация бывает безопасной

ИРИНА РОМАНОВА
Руководитель отдела продаж систем ИБ
КИБЕРПРОТЕКТ

ОТЕЧЕСТВЕННАЯ ТЕХНОЛОГИЧЕСКАЯ КОМПАНИЯ

> 7 ЛЕТ
на рынке решений для резервного копирования, защиты данных и инфраструктурного ПО

> 1 600
партнеров в России и Республике Беларусь

> 400
сотрудников

2023
Лауреат премии в номинации «Информационная безопасность» с решением Кибер Бэкап

2023
Победитель национальной премии «Наш вклад» с образовательным проектом Cyber Care

2023
Победитель премии в номинации «Информационная безопасность» с решением Кибер Бэкап

2024
Победитель в номинации «Информационные технологии» конкурса новых российских брендов

2024
В рейтинге топ-200 работодателей России по версии HeadHunter

Ассоциации и партнеры

АРПП Отечественный софт
RUS®SOFT
АПКИТ
Sk Сколково
ОЭЗ Иннополис
МФТИ

КИБЕРПРОТЕКТ
CYBERPROTECT.RU
КИБЕРПРОТЕКТ 2024

ЛИНЕЙКА ПРОДУКТОВ

КИБЕР Бэкап
+
КИБЕР
Бэкап Облачный

ИИ

Система резервного копирования

КИБЕР
Бэкап
Персональный

Резервное копирование на домашнем компьютере

КИБЕР
Инфраструктура

Программно-определяемая инфраструктура

КИБЕР
Протего

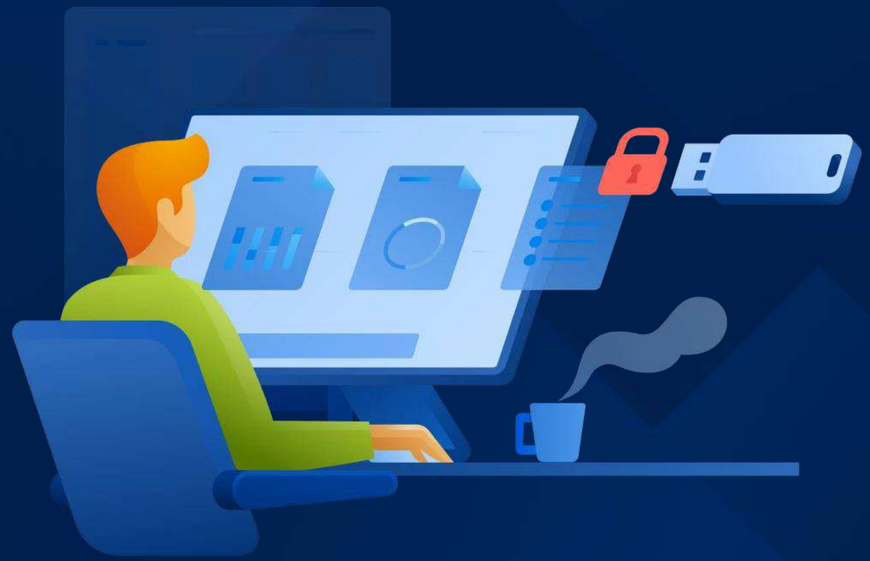
Система защиты от утечки данных

КИБЕР
Файлы

Система обмена файлами и синхронизации данных

ИИ Зарегистрировано как ПО, относящееся к сфере искусственного интеллекта

Проблематика файлового обмена для организаций



КИБЕРПРОТЕКТ

CYBERPROTECT.RU

КЛАССИЧЕСКИЕ СТАНДАРТЫ ФАЙЛОВОГО ОБМЕНА

Факторы организации современного файлового обмена

- Рост объёма рабочих данных и среднего размера файлов
  Рост требований к скорости передачи и снятию ограничений на максимальный размер файла
- Гибридная или полностью удалённая работа
  Доступ к файлам необходим из любого места, с любого устройства
- Оптимизация очистки хранилищ
  Необходимо автоматическое удаление ненужных файлов
- Отслеживание версий документов
  Нужны синхронизация с рабочими местами и возможность совместного редактирования документов

Традиционные способы файлового обмена

Электронная почта

Общие сетевые папки

Файловые серверы

FTP-серверы

Проблемы

- **Ограничения** максимального **размера** файла
- Необходимость подключения к сети предприятия (напр., **VPN**)
- **Низкая скорость** передачи
- **Отсутствие возможностей** совместной работы (синхронизация, отслеживание версий файлов)

«Слепые зоны» за корпоративным периметром

Публичные облачные ресурсы не контролируются корпоративными ИБ-инструментами

- Данные хранятся **за пределами организации** на серверах поставщика услуг
- Функции обеспечения безопасности – на поставщике услуг
- Не всегда обеспечиваются безопасное хранение и передача данных
- Риски компрометации данных при утере устройства
- Автоматическая синхронизация файлов без DLP-контроля приводит к неконтролируемой отправке в облако файлов, не предназначенных для общего доступа
- Учётные данные доступа хранятся у поставщика услуг
- Интеграция с корпоративными ИБ-решениями невозможна

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%

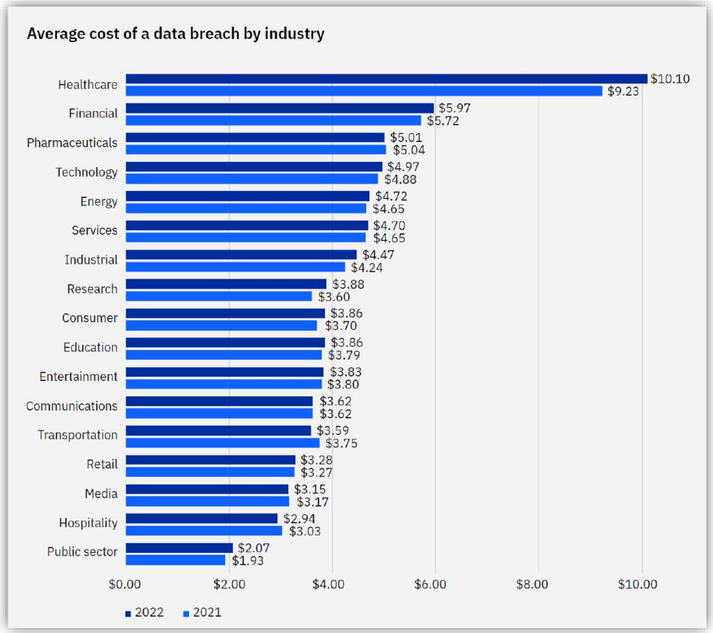
of breaches occurred because of a compromise at a business partner.

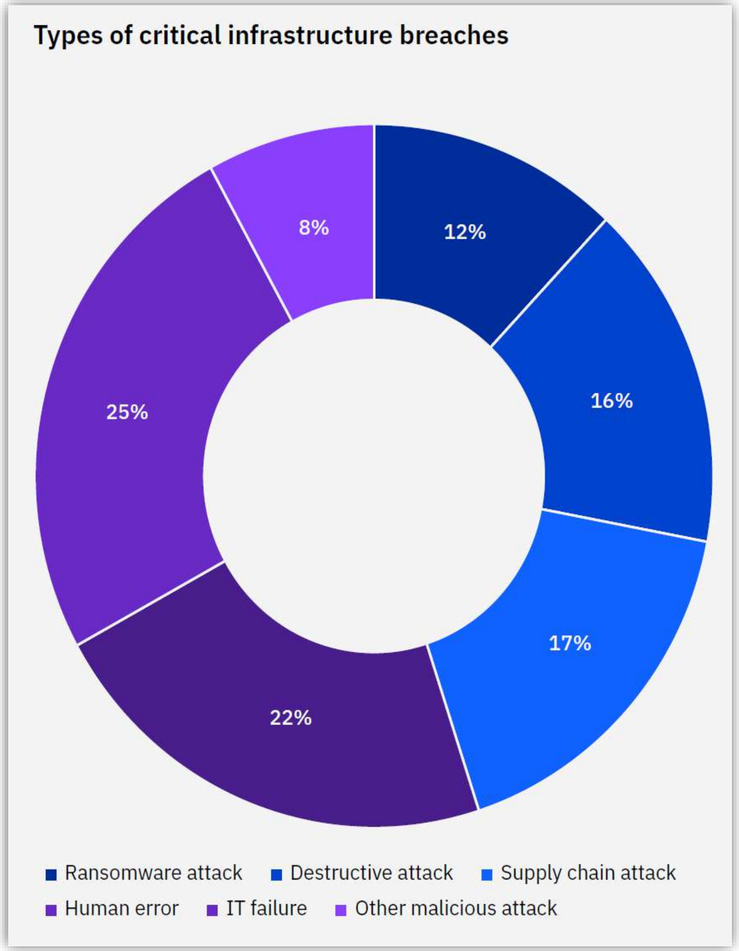
45%

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

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 ДАННЫХ

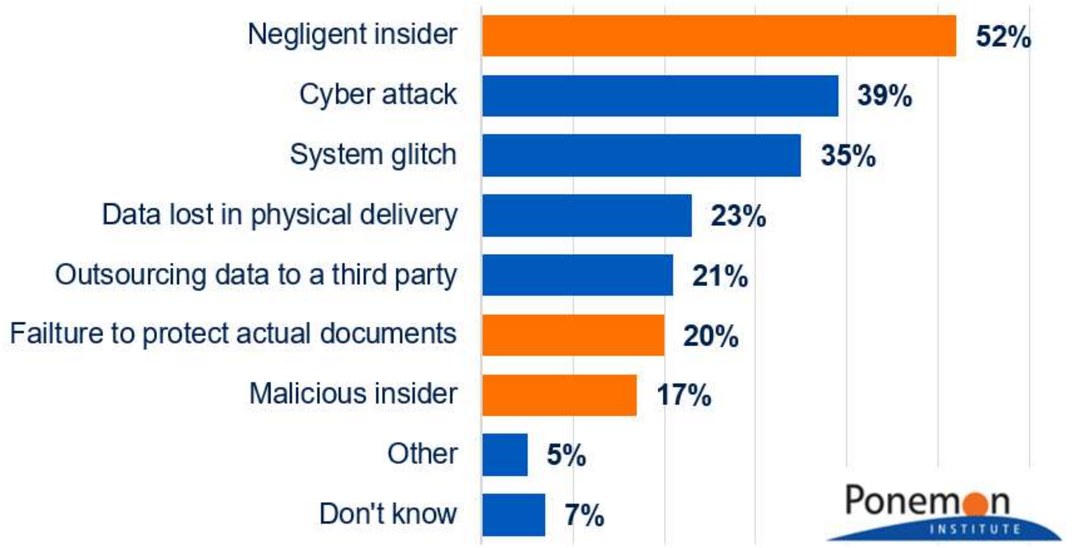
- **90% организаций** чувствуют себя уязвимыми перед лицом инсайдерских угроз - 53% сообщают, что подверглись атаке со стороны инсайдеров за последние 12 месяцев

- **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)
  - 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

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

ПРЕЦЕДЕНТЫ ПО ФАКТУ ИСПОЛЬЗОВАНИЯ СЕРВИСОВ ПУБЛИЧНОГО ОБЛАКА

Western Digital My Cloud

2023

Атака на сервис, доступ приостановлен на 10+ дней всем пользователям

Amazon Web Services
Google Cloud
Microsoft Azure

2022

Прекращен доступ новых пользователей из России и Республики Беларусь

2022-н.в.

Отключение существующих пользователей некоторыми сервисами

Яндекс.Диск

2021-н.в.

Изменение условий подписки приводит к удалению данных пользователей

Dropbox

2012

Утечка учётных данных доступа к сервису 68+ миллионов пользователей

Цифры*

- Обеспечивать безопасность в облаке сложнее, чем вне облака, для 55% респондентов
- 75% респондентов хранят в облаке >40% данных, категорированных как защищаемые
- 46% опрошенных сталкивались с утечкой данных из облака

* 2023 Cloud Security Study, Thales Group

КИБЕРПРОТЕКТ

КИБЕР Файлы

Файловый обмен и синхронизация

КИБЕР Файлы

КОРПОРАТИВНОЕ РЕШЕНИЕ ДЛЯ БЕЗОПАСНОГО ФАЙЛОВОГО ОБМЕНА

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

Подключение собственных хранилищ
Вместо загрузки данных на серверы поставщика услуг

Безопасность
Политики и права доступа, ролевая модель администрирования, шифрование хранимых данных

Совместная работа
Включая управление версиями и интеграцию с серверами Office365, Р7-Офис, МойОфис и OnlyOffice

Отсутствие ограничений
На размер файлов, количество внешних (нелицензируемых) пользователей и объём хранилищ

КИБЕР Файлы

КОРПОРАТИВНОЕ РЕШЕНИЕ ДЛЯ БЕЗОПАСНОГО ФАЙЛОВОГО ОБМЕНА

Простой и надежный обмен информацией между сотрудниками и с контрагентами

Собственный сервер

- Физический, облачный или виртуальный сервер для обмена файлами через интернет или в рамках корпоративной сети без ежемесячной подписки на онлайн-сервисы.
- Возможность масштабирования решения.
- Брендирование и персонализация - собственные логотип, цветовая схема, пользовательские сообщения

Доступ к внутренним файловым ресурсам

- Веб-доступ и автоматическая синхронизация с файлами, размещенными на внутренних файловых серверах и SMB-ресурсах, NAS, в SharePoint и других информационных системах.
- Возможность выделения «закрытого контура» с веб-доступом только для сотрудников извне корпоративной сети

Совместная работа с документами

- Прозрачная интеграция с продуктами «Р7-Офис. Сервер документов», «Сервер совместного редактирования МойОфис», OnlyOffice и Microsoft Office Online – организация сама выбирает онлайн-редактор.
- Поддержка синхронизации файлов для Windows, macOS и Android.
- Одноразовые ссылки на файлы и папки, контроль срока и условий доступа к файлам, онлайн-просмотр без скачивания документа и многое другое.

КИБЕР Файлы

КОРПОРАТИВНОЕ РЕШЕНИЕ ДЛЯ БЕЗОПАСНОГО ФАЙЛОВОГО ОБМЕНА

Защищенный обмен информацией между сотрудниками и с контрагентами

Политики безопасности и защита от утери данных

- Централизованное управление правами доступа, ролевая модель администрирования, белые и черные списки.
- Защита данных от намеренного удаления и удаление файлов с личных устройств в случае увольнения сотрудника из компании, утери или кражи устройства пользователя.
- Ограничения срока доступа к файлам на уровнях организации (системы), папок и отдельных файлов

Мониторинг и аудит

- Регистрация всех действий пользователей в системе - что делают пользователи, к каким документам обращаются, с кем обмениваются файлами.
- Интеграция с DLP-сервером Кибер Протего для единого просмотра событий безопасности, возможность работы с событиями (статусы, комментарии)
- Открытая интеграция с SIEM-системами благодаря поддержке протокола Syslog

Интеграция с AD и СЗИ

- Поддержка Active Directory для аутентификации, управления учетными записями пользователей и регистрации устройств
- Проверка загружаемых файлов с помощью Kaspersky Scan Engine (на уровне сервера)
- Контроль контента загружаемых файлов с помощью Кибер Протего (на уровне агентов DLP-системы)
- Шифрование хранимых файлов

КИБЕР Файлы | КРОСС-ПЛАТФОРМЕННАЯ АРХИТЕКТУРА

Веб-сервер Кибер Файлов
- Windows Server 2012, 2016, 2019
- Альт Сервер 10
- РЕД ОС Сервер 7.3
- Astra Linux Server 1.7
- Поддержка сред виртуализации

Windows | base alt | ASTRALINUX | РЕДОС

Сервер шлюза
- Windows Server 2012, 2016, 2019
- *Linux – в разработке*
- Поддержка сред виртуализации

КИБЕР Файлы

ИНТЕГРАЦИЯ С КИБЕР ПРОТЕГО

Централизованный мониторинг операций с файлами и папками

Интеграция через API позволяет отправлять с сервера Кибер Файлов на сервер Кибер Протего события из журнала аудита об отправке файлов и доступа к ним.

КИБЕРПРОТЕКТ

КИБЕР Протего

Полнофункциональное DLP-решение корпоративного класса

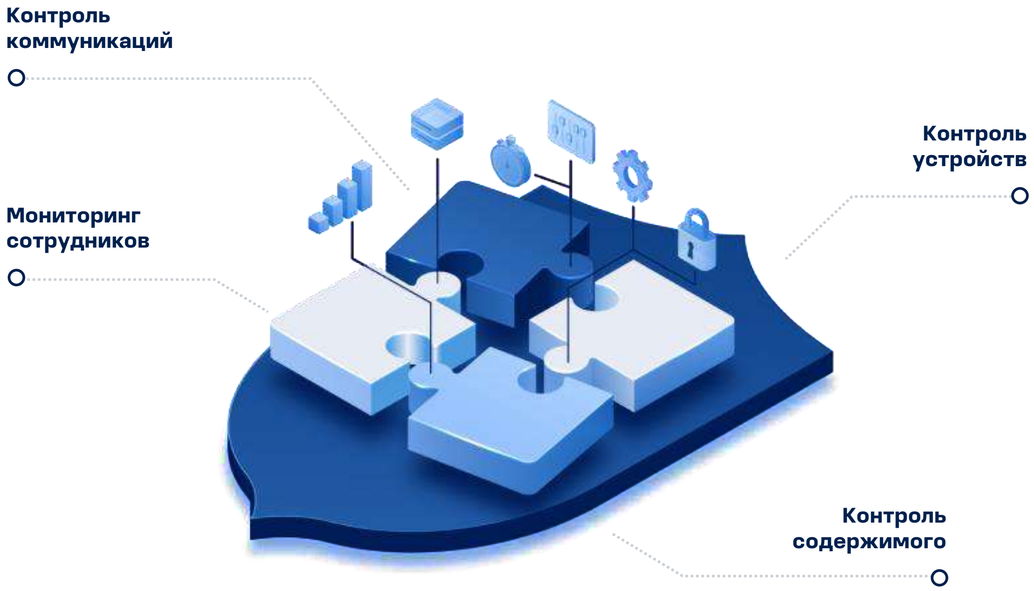
КИБЕР Протего

ПОЛНОФУНКЦИОНАЛЬНАЯ DLP-СИСТЕМА

Контроль каналов утечки, данных, хранилищ, сотрудников

Контроль в реальном времени

При использовании и передаче данных



На физических рабочих станциях и серверах, виртуальных и **терминальных средах**

Превентивный контроль

При хранении данных

В локальных и сетевых хранилищах

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

Возможности КИБЕР Протего

Контроль устройств, сетевых коммуникаций, данных, мониторинг активности пользователей

Возможности КИБЕР Протего

Контроль устройств и интерфейсов

+ Уникальная технология Cyber Protego TS для контроля терминальных сессий

Windows

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 терминальной сессии

Linux

- USB
- Съемные устройства
- Канал печати
- Белый список
- Теневое копирование
- Журналирование, алерты
- Буфер обмена в терминальной сессии

Возможности КИБЕР Протего

Контролируемые сетевые каналы

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
Jabber	IRC	TamTam	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

Выборочный контроль множества операций

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

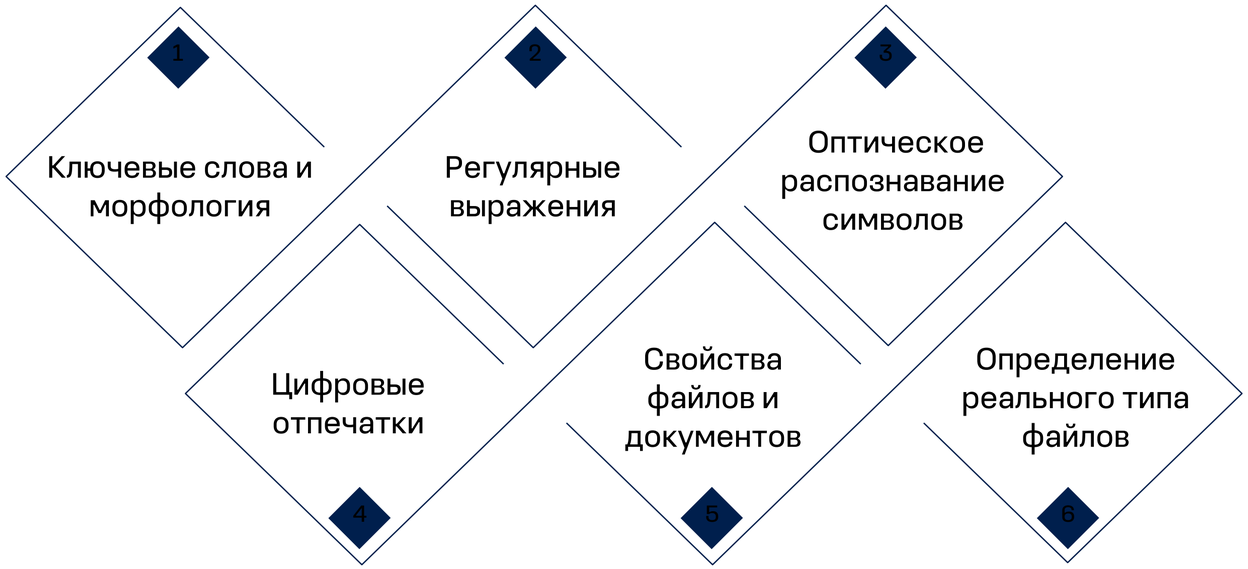
Белые списки

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

Возможности КИБЕР Протего

Контроль содержимого

Автономные технологии контентного анализа



- Словари и шаблоны регулярных выражений в комплекте поставки
- Составные правила, пороговые значения срабатывания
- Применимо в контроле терминальных сессий!

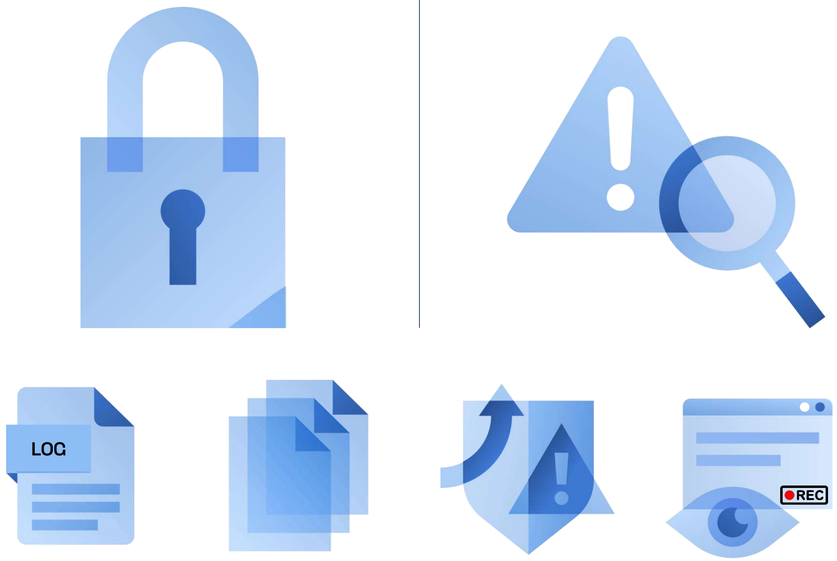
Типы правил

«В разрыв»

Блокировка, мониторинг, алерты

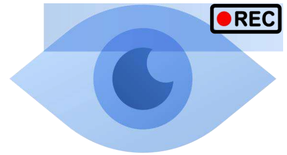
Пост-обработка

Мониторинг и алерты без блокировки



Возможности КИБЕР Протего

Мониторинг активности пользователей



Запись при реализации политики DLP другими модулями агента

Напр., срабатывание контентного правила

Запись при выполнении заданных системных условий

Напр., VPN подключение, заданное окно в фокусе

Запись до или после наступления заданного события

Видео может содержать до 5 предшествующих событию минут

Детализация условий начала записи

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

Балансировка длительности и размера записей

- Цветная или ч/б запись
- Запись в настраиваемом разрешении
- Запись с настраиваемой частотой кадров
- Остановка записи при отсутствии активности

Неотъемлемая часть контроля с прозрачной интеграцией в DLP-политики

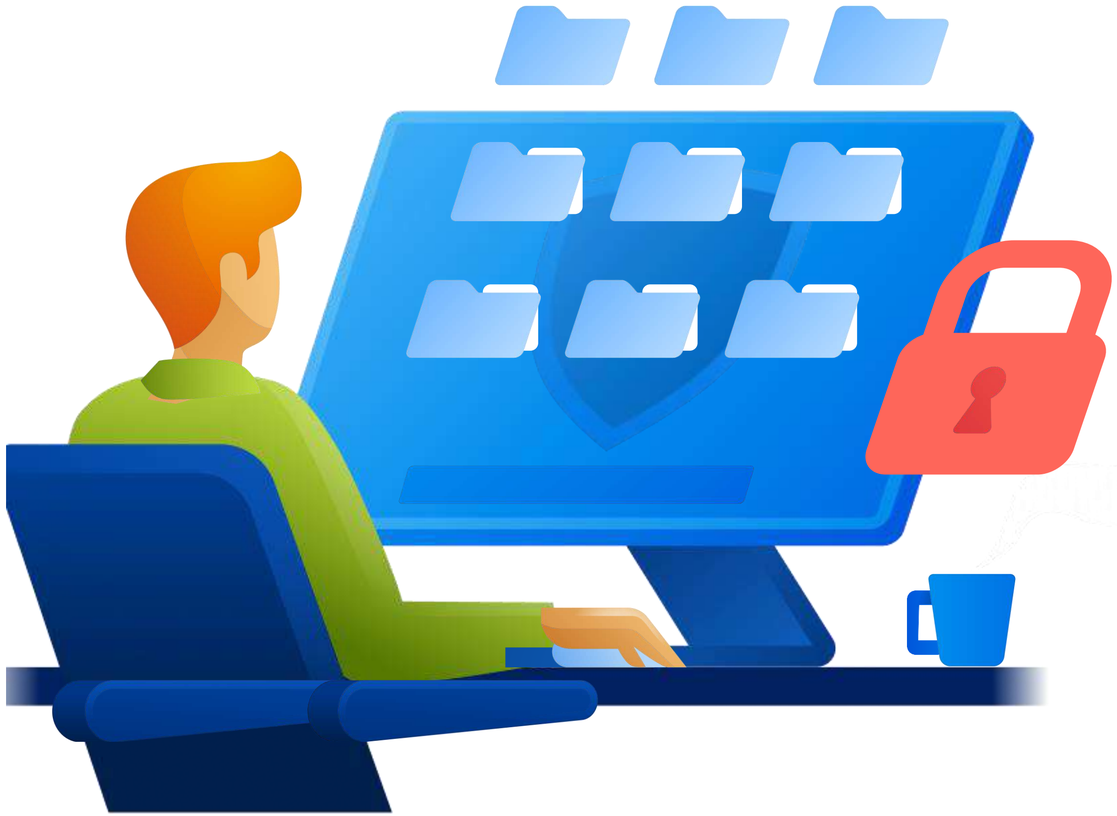
КИБЕР Протего | ИНТЕГРАЦИЯ С КИБЕР ФАЙЛАМИ

Реализация концепции Кибер Периметра:
Контроль загружаемых файлов, контроль большинства облачных файлообменников, сводный анализ событий

Получение единой картины информационных потоков внутри организации

- Передача событий с сервера Кибер Файлов на сервер Кибер Протего через RestAPI
- Возможность получать все события в едином журнале
- Возможность работы с событиями (статусы рассмотрения и комментарии)

Контролируемый файловый обмен с использованием собственного сервиса файлового обмена

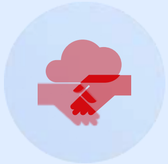


КИБЕР ПЕРИМЕТР: ОБЛАЧНЫЙ ФАЙЛОВЫЙ ОБМЕН VS КОНТРОЛИРУЕМЫЙ ФАЙЛОВЫЙ ОБМЕН

Облачный файловый обмен

Данные хранятся за пределами организации на серверах поставщика услуг

Поставщик услуг может приостановить/прекратить доступ к сервису и данным в любой момент по любым причинам



Функции обеспечения безопасности делегируются поставщику услуг

Контролируемый файловый обмен

«Можно» только в контролируемый сервис файлового обмена

4shared, Amazon S3, AnonFile, Box, Cloud Mail.ru, dmca.gripe, Dropbox, DropMeFiles, Easyupload.io, Files.fm, Freenet.de, GitHub, Gmx,de, Gofile.io, Google Docs / Google Drive, iCloud, Idrive, MagentaCLOUD, MediaFire, MEGA, OneDrive, Sendspace, transfer.sh, TransFiles.ru, Uploadfiles.io, Web.de, WeTransfer, Yandex.Disk

КИБЕР Файлы

Контроль большинства веб-сервисов файлового обмена с возможностью оставить только необходимые для работы

Начать хотелось бы с небольшого рассказа о том кто мы такие. Компания полностью российская, офис в Москве и в Татарстане, около 400 сотрудников, 70% из них это разработчики. Аккредитованная ИТ компания. Продукты находятся в реестре российского ПО.

«Можно» только те данные, что предназначены для совместной работы и последующего распространения

- Блокировка или разрешение отправки файла по результатам проверки его содержимого
- Протоколирование действий пользователя, теневое копирование
- Тревожное оповещение, информационное оповещение
- Запись экрана, клавиатурного ввода, сведений о процессах

Контроль данных, передаваемых при файловом обмене

Можно совместно анализировать данные по файловому обмену от EFSS и события передачи данных от DLP

События Кибер Файлов по генерации ссылок, скачиванию файлов и др, можно импортировать в единый журнал событий DLP-системы в целях сводного аудита событий

Унификация журналов

ВЕКТОРЫ РАЗВИТИЯ: DLP+EFSS

Кросс-платформенное решение, объединяющее возможности продуктов в концепции Кибер Периметра

ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ

- Расширение функционала на Linux
- Равноценные серверы управления для разных ОС Linux, поддержка разных СУБД
- Расширение аналитических возможностей

ЕДИНАЯ ПЛАТФОРМА БЕЗОПАСНОСТИ

- Дальнейшая интеграция EFSS и DLP решений для детектирования и контроля конфиденциальных данных
- 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
- Интеграция с почтовыми системами / клиентами, адресными книгами
- Интеграция с ИБ решениями
- Клиенты для Linux

Спасибо!

Ирина Романова

Руководитель отдела продаж систем
Информационной безопасноти

Irina.romanova@cyberprotect.ru

cyberprotect.ru