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%

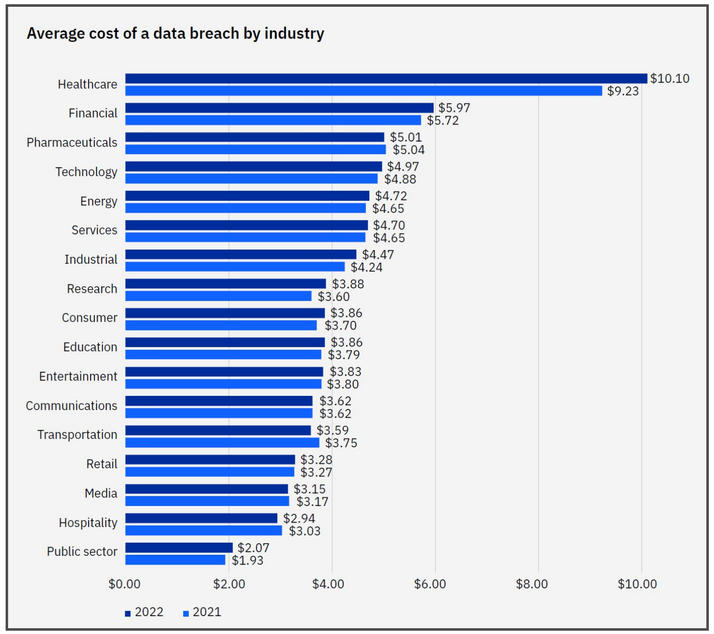
of breaches occurred because of a compromise at a business partner.

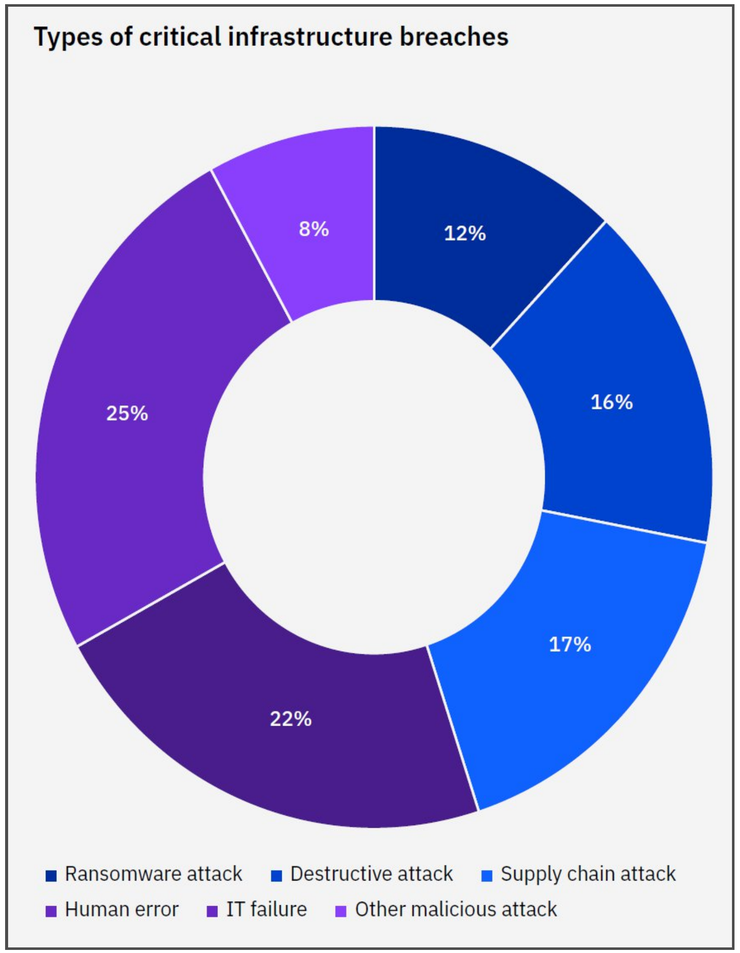
45%

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

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

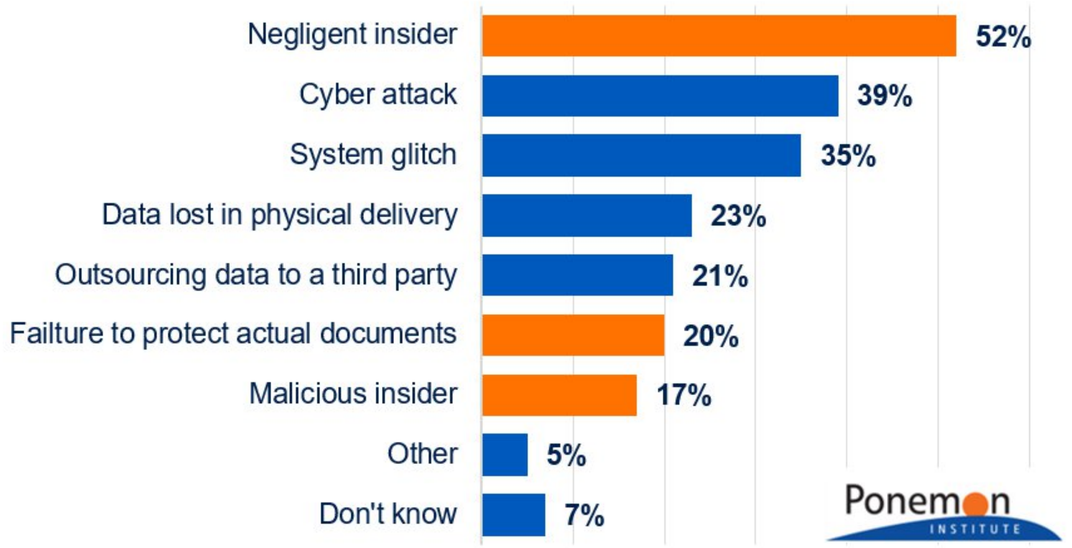
- **90% организаций** чувствуют себя уязвимыми перед лицом инсайдерских угроз - 53% сообщают, что подверглись атаке со стороны инсайдеров за последние 12 месяцев

- **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)
  - 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

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

КИБЕРПРОТЕКТ

КИБЕР Файлы 9.0

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 и МойОфис

Отсутствие ограничений
На размер файлов, количество пользователей и объём хранилищ

КИБЕРПРОТЕКТ

CYBERPROTECT.RU

СОЗДАНИЕ КИБЕР ПЕРИМЕТРА КАК СРЕДЫ КОНТРОЛИРУЕМОГО ФАЙЛОВОГО ОБМЕНА

«Можно» только в контролируемый сервис файлового обмена

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

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

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

Контроль данных, передаваемых при файловом обмене

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

Сводный анализ файлового обмена и других операций передачи данных

Унификация журналов

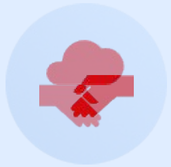
Журналы Кибер Файлов, содержащие события генерации ссылок, скачивания файлов и др, можно импортировать в единый журнал событий DLP-системы в целях сводного аудита событий

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

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

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

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

КИБЕРПРОТЕКТ

CYBERPROTECT.RU

КИБЕРПРОТЕКТ 2024

КИБЕР Файлы 9.0 | ИНТЕГРАЦИЯ С КИБЕР ПРОТЕГО

Централизованный мониторинг операций с файлами и папками

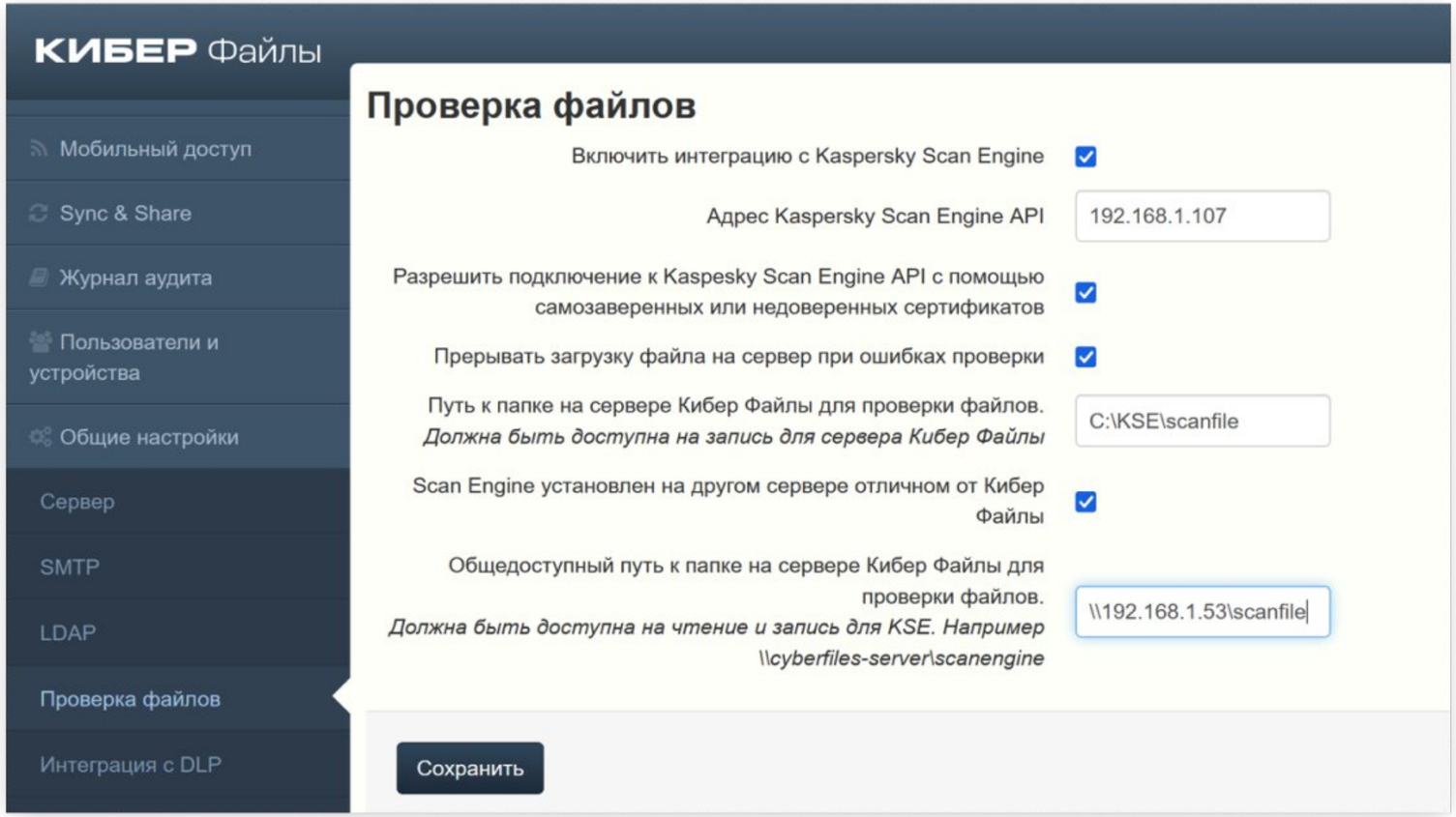
Интеграция через API позволяет отправлять с сервера Кибер Файлов на сервер Кибер Протего события из журнала аудита об отправке файлов и доступа к ним.

КИБЕР Файлы 9.0

ИНТЕГРАЦИЯ С KASPERSKY SCAN ENGINE

Проверка загружаемых на сервер файлов с помощью Kaspersky Scan Engine

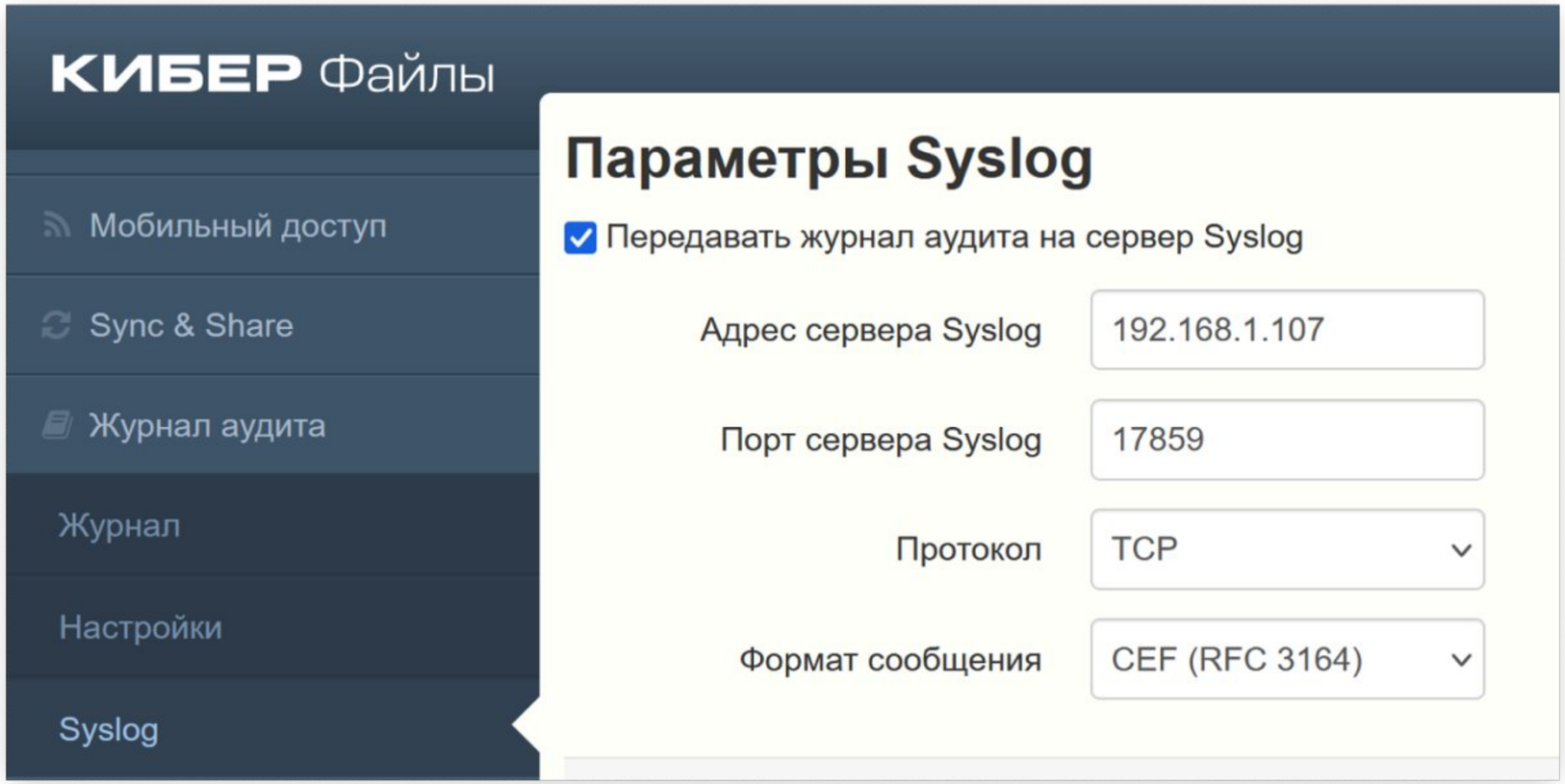
Позволяет проверять загружаемые на сервер файлы при помощи Kaspersky Scan Engine и при обнаружении угрозы блокировать отправку опасного содержимого.



КИБЕР Файлы 9.0 | SYSLOG

Отправка событий из журнала аудита в сторонние SIEM системы по протоколу Syslog

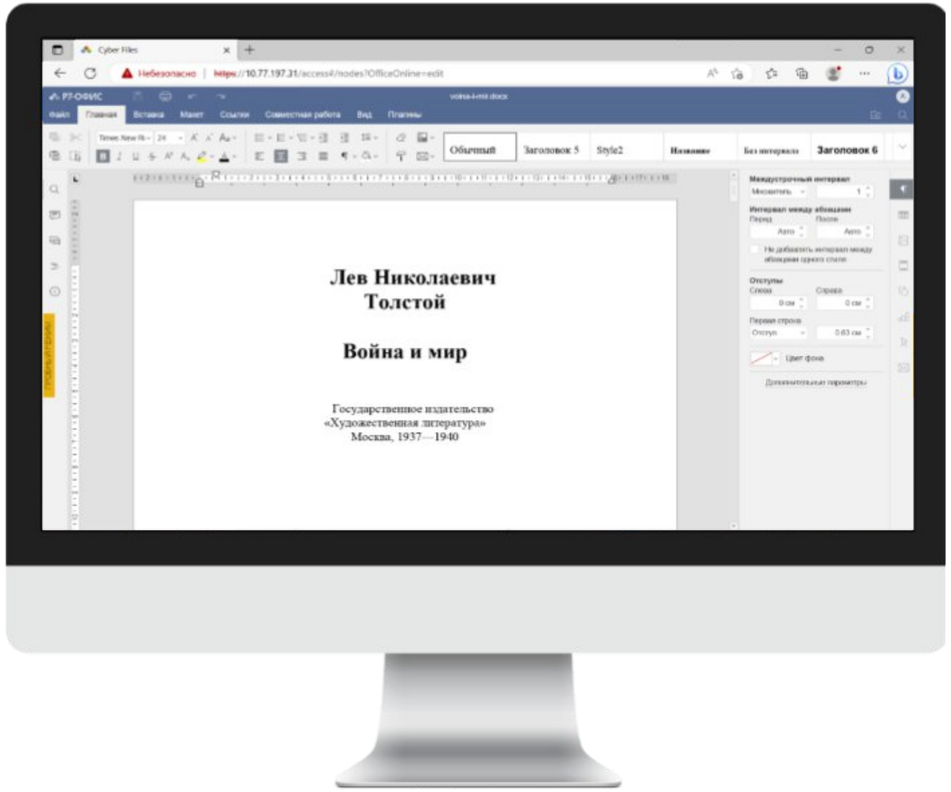
Добавлена функция отправки событий из журнала аудита на Syslog-сервер в форматах CEF (RFC 3164) и Syslog (RFC 5424) для возможности их обработки и анализа в различных SIEM-системах.

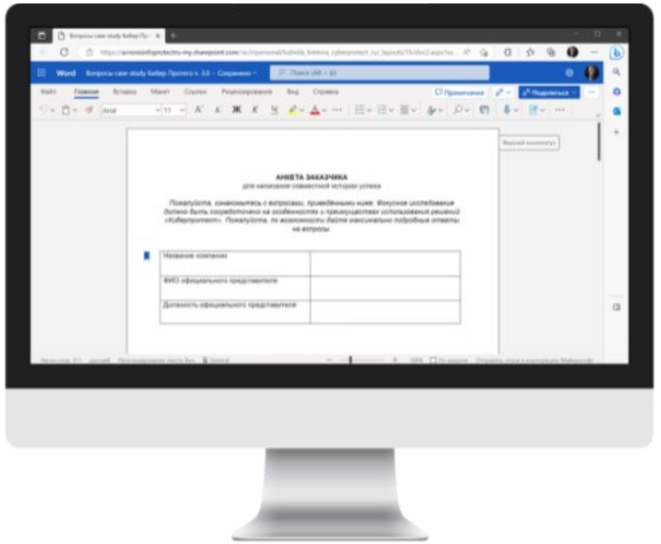


КИБЕР Файлы 9.0 | ИНТЕГРАЦИЯ С МОЙОФИС ССР

Microsoft Office Online, «Р7-Офис. Сервер документов» + МойОфис ССР

Возможность подключения к корпоративному серверу совместного редактирования по протоколу WOPI предоставляет доступ к фирменным технологиям компании МойОфис для редактирования документов.

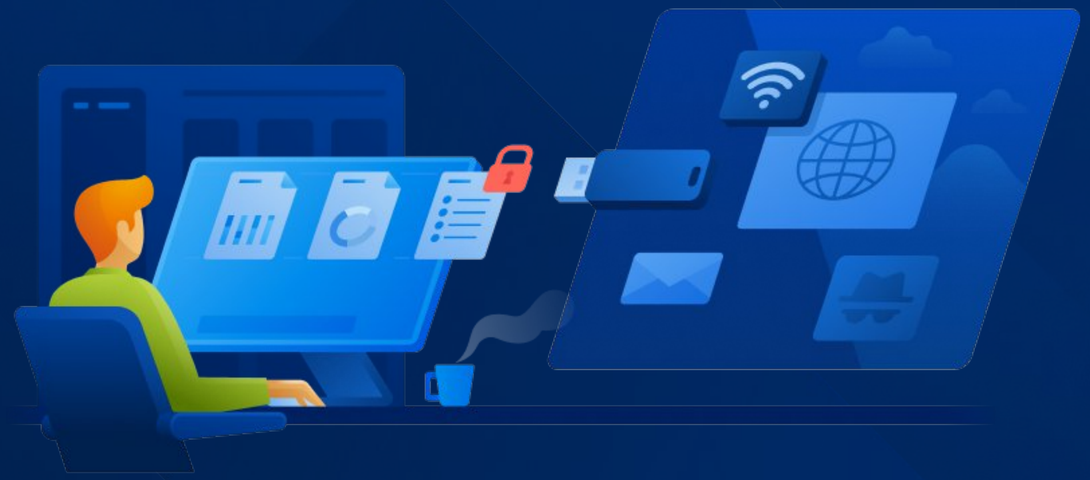




КИБЕРПРОТЕКТ

КИБЕР Протего 10.2

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 хранилищах различных типов

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

Блокировка, мониторинг, перехват

Возможности КИБЕР Протего

Контроль устройств и интерфейсов

+ Уникальная технология Cyber Protego TS
для контроля терминальных сессий

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

- USB
- Съемные устройства
- Канал печати
- Белый список
- Теневое копирование
- Журналирование, алерты

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 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 NEW

- 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

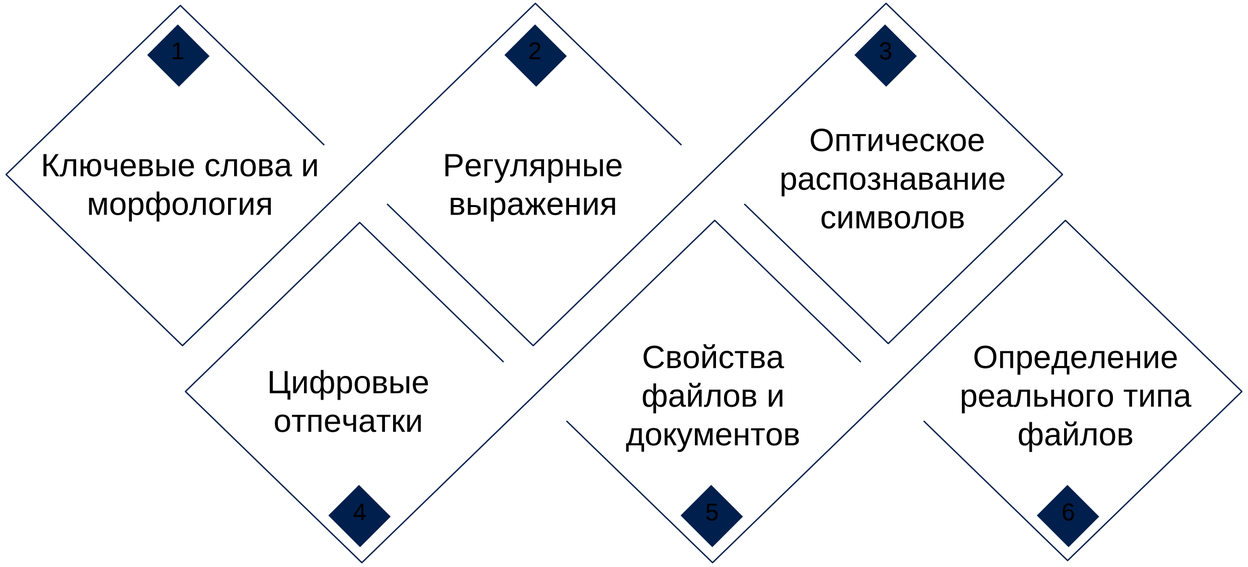
Белые списки

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



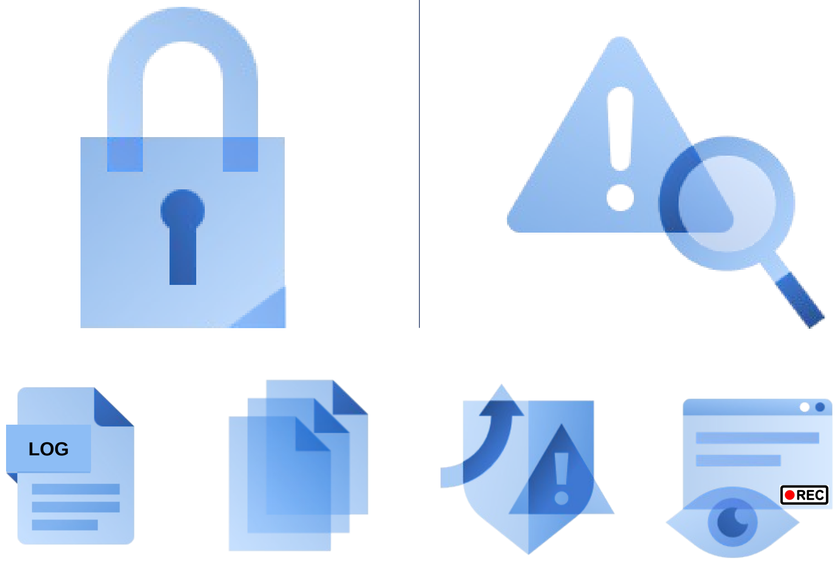
Типы правил

«В разрыв»

Блокировка, мониторинг, алерты

Пост-обработка

Мониторинг и алерты без блокировки



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

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 политики предотвращения утечек

КИБЕР Протего 10.2 | ЧТО НОВОГО?

Web-интерфейс, полный контроль устройств для Linux, интеграция с Кибер Файлами и многое другое

- Новый сервер с web-интерфейсом
- Интеграция с Кибер Файлами
- Графические интерактивные отчеты
- Дашборды
- Просмотр событий

- Контроль печати
- Теневое копирование для печати и съемных устройств
- Тревожные оповещения и передача по протоколу Syslog

- Поддержка Кибер Файлов
- Контроль TamTam
- Контроль Mailion
- Возможность блокировки сетевой активности для процессов

КИБЕР Протего

10.2

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

КИБЕРПРОТЕКТ

ВЕКТОРЫ РАЗВИТИЯ: DLP+EFSS

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

ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ

- Расширение функционала на Linux
- Полный переход на Web-интерфейс
- Функции контроля рабочего времени

ЕДИНАЯ ПЛАТФОРМА БЕЗОПАСНОСТИ

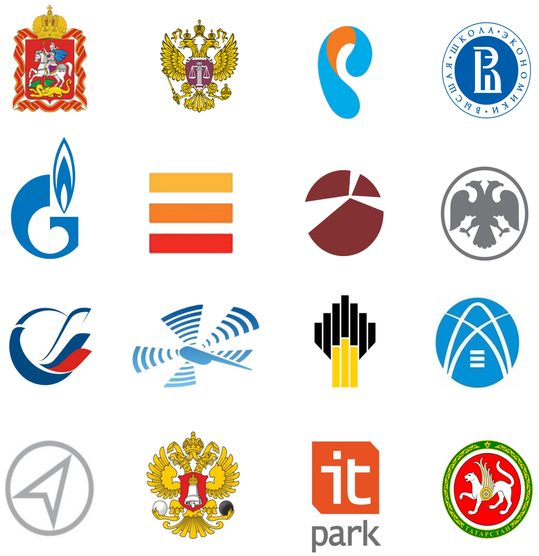
- Дальнейшая интеграция EFSS и DLP решений для детектирования и контроля конфиденциальных данных
- Централизованная статистика и объединенные отчеты DLP и EFSS
- Контроль хранения данных в соответствии с политикой компании

БЕЗОПАСНЫЙ ФАЙЛОВЫЙ ОБМЕН

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

ОТЕЧЕСТВЕННЫЙ ПРОИЗВОДИТЕЛЬ

Полный цикл разработки, развития, поддержки ПО



ПРОДУКТЫ И РЕШЕНИЯ

КИБЕР Бэкап

Резервное копирование
ИТ-систем любой сложности
с централизованным управлением
и оптимизацией хранения

КИБЕР Бэкап Облачный

Резервное копирование данных в физических, виртуальных и облачных средах для поставщиков услуг

Часть экосистемы отечественного ПО с постоянно расширяющейся сетью технологических партнёрств

ROSA, CommuniGate Pro, alt linux, МойОфис, AccentOS®, ASTRA LINUX®, ICL ТЕХНО, РЕДОС, HOSTVM, Postgres PROFESSIONAL, Р7-ОФИС

Единый реестр Минцифры

Сертификация ФСТЭК

КИБЕР Протего

Программный комплекс предотвращения утечек используемых, передаваемых и хранимых данных

КИБЕР Инфраструктура

Масштабируемое, экономичное и универсальное программно-определяемое решение: виртуализация, хранилище и сеть

КИБЕР Файлы

Корпоративное решение для синхронизации и безопасного обмена файлами

КИБЕРПРОТЕКТ

CYBERPROTECT.RU

Спасибо!

Ильшат Латыпов

Менеджер продукта
Ilshat.Latypov@cyberprotect.ru
cyberprotect.ru