КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Минск, 2023

КИБЕРПРОТЕКТ

CYBERPROTECT.RU

Безопасный файловый обмен

Цифровизация бывает безопасной

СЕРГЕЙ ВАХОНИН

Директор направления систем ИБ
Киберпротект

КИБЕРПРОТЕКТ

>7 ЛЕТ

На рынке решений инфраструктурного ПО, резервного копирования и защиты данных

>1 400

Партнёров в России и Республике Беларусь

>300

Сотрудников

Призер премии #МЫВМЕСТЕ

2022

Призёр международной премии в номинации «Ответственный бизнес»

2022

В рейтинге ТОП-50 лучших работодателей страны по версии Headhunter

2023

Лауреат премии «Приоритет цифра» в номинации «Информационная безопасность» за СРК Кибер Бэкап

2023

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

2023

Победитель премии в номинации «Информационная безопасность» за СРК Кибер Бэкап

Ассоциации и партнёры

АРПП Отечественный софт

РУС СОФТ

АПКИТ

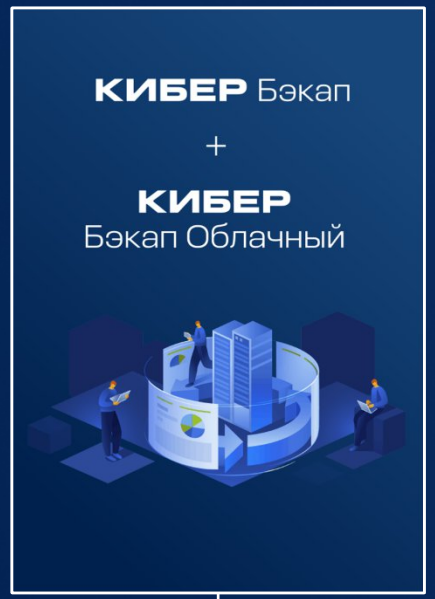
Sk Сколково

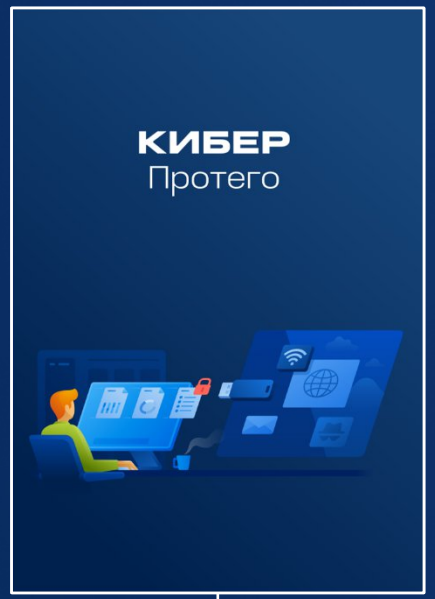
ОЭЗ Иннополис

МФТИ

РАЗРАБАТЫВАЕМ, ПРОДАЁМ И ВНЕДРЯЕМ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

КИБЕРПРОТЕКТ





СРК	HCI	DLP	EFSS/VDR	Утилита РК
Он-прем + BaaS в нашем ЦОД Для организаций + для поставщиков услуг	Он-прем Для организаций	Он-прем Для организаций	Он-прем Для организаций	Для домашних пользователей

КИБЕРПРОТЕКТ

Файловый обмен
vs
Безопасный файловый обмен

ИНФОРМАЦИОННЫЙ ОБМЕН В СОВРЕМЕННЫХ РАБОЧИХ ПРОЦЕССАХ

Внутри организации и с контрагентами, с использованием корпоративных и теневых решений, из любого места, с использованием всех возможных устройств

Преимущества более организованного информационного обмена над менее организованным

Для бизнеса

Повышение производительности

Снижение рисков ИБ, несоответствия требования регуляторов

Для ИТ

Контроль над процессами, интеграция в инфраструктуру, управление нагрузкой на инфраструктуру

Для ИБ

Гибкий контроль данных, пользователей, хранилищ

Обеспечение безопасности инструментами контроля доступа и защиты данных

ФАЙЛОВЫЙ ОБМЕН И СОВМЕСТНАЯ РАБОТА НАД ДОКУМЕНТАМИ

Существенная часть информационного обмена со своей спецификой

Технические аспекты

Электронная почта

Ограничения размера вложений

Общие сетевые папки и файловые серверы

Необходимость подключения к внутренней сети

Мессенджеры

Отсутствие механизмов совместной работы, версий документов

Серверы FTP

Низкая скорость передачи, ограниченные возможности разграничения доступа

Совместная работа

Гибридная или полностью удалённая работа

Доступ к файлам из любого места, с любого устройства

Отслеживание версий документов

Синхронизация, возможность совместного редактирования

Инфраструктура хранения

Управление нагрузкой

Сроком жизни, объёмом, числом версий

Сервисы публичного облака

Фактический современный стандарт

ПОТЕНЦИАЛЬНЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ СЕРВИСОВ ПУБЛИЧНОГО ОБЛАКА

Потеря или утечка данных, прекращение / приостановка доступа к сервису и данным

- Данные хранятся за пределами организации на серверах поставщика услуг
- Учётные данные доступа хранятся и обрабатываются на стороне поставщика услуг
- Функции обеспечения безопасности делегируются поставщику услуг
- Фокус на синхронизацию в реальном времени приводит к отправке в облако файлов, не предназначенных для общего доступа
- Поддержка мобильных устройств создает риски компрометации данных при их утере
- Изменяющиеся условия предоставления услуги и несвоевременная реакция на изменения со стороны пользователя могут привести к потере данных
- Поставщик услуг может приостановить / прекратить доступ к сервису и данным в любой момент по любым причинам

КИБЕРПРОТЕКТ

ПРЕЦЕДЕНТЫ ПО ФАКТУ ИСПОЛЬЗОВАНИЯ СЕРВИСОВ ПУБЛИЧНОГО ОБЛАКА

КИБЕРПРОТЕКТ

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

Наиболее вероятный сценарий утечки – самый простой
Пользователи не ищут сложных путей

Размытый периметр безопасности

Распределённость ИТ-процессов, гибридные и удалённые режимы работы, распространение моделей BYOD / GYOD / CYOD

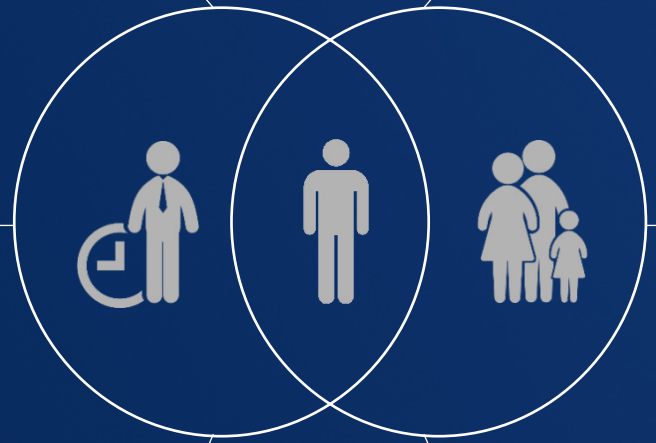
Рост скорости и удобства передачи данных по сетевым каналам

Рост пропускной способности проводных и беспроводных каналов, мессенджеры, веб-сервисы: облачные хранилища, социальные сети и другие

Рост размеров памяти внешних и встроенных в устройства носителей при снижении их стоимости

Снижение стоимости облачного хранения данных

Удешевление хранения данных



Консьюмеризация ИТ

Одни и те же устройства и сервисы используются для решения как личных, так и рабочих вопросов

Отсутствие фокуса на безопасности

Устройства, приложения и сервисы ориентированы на удобство использования в ущерб безопасности,

Все решения о способах и уровне авторизации, аутентификации и уровне доступа к данным принимает конечный пользователь

Рост числа уязвимостей аппаратного и программного обеспечения

По мере масштабирования и усложнения корпоративных и личных инфраструктур

КИБЕРПРОТЕКТ

КИБЕРПРОТЕКТ

Безопасный файловый обмен

Обеспечение защиты данных и безопасного файлового обмена: решения Киберпротект

КИБЕР Файлы

КОРПОРАТИВНЫЙ СЕРВИС ФАЙЛОВОГО ОБМЕНА И СОВМЕСТНОЙ РАБОТЫ

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 адми-нистрирования, шифрование хранимых данных

Совместная работа
Включая управление версиями и интеграцию с Office365 и Р-7 Офис

Отсутствие ограничений
на размер файлов, количество пользователей и объём хранилищ

БЕЗОПАСНОСТЬ

Шифрование

SSL-доступ к веб-консоли администрирования

HTTPS-транспорт для передачи файлов

Шифрование хранимых данных

- AES-128
- AES-256
- ГОСТ 28147-89

Пароль приложения

К вводу перед запуском мобильного клиента синхронизации, опционален

Конфигурируемая сложность пароля

Конфигурируемое число неудачных попыток ввода пароля с очисткой данных с устройства по его достижении

Удалённая очистка данных

Политики удалённой очистки мобильных устройств клиентов синхронизации

- При заданном числе неудачных попыток ввода пароля
- После заданного периода неудачных попыток связаться с сервером *Кибер Файлы*

Ручная удалённая очистка мобильных устройств клиентов синхронизации

При компрометации устройства

Локальное хранение

Включение или отключение возможности сохранять файлы на мобильном устройстве

ПРИМЕРЫ ОГРАНИЧЕНИЙ ДОСТУПА

КИБЕР Файлы

Доступ / Уровни	К системе	К источникам данных	К папкам	К файлам
Политики	▪ Белые и чёрные списки доступа к системе для групп LDAP и доменов электронной почты ▪ Запрет анонимного доступа ▪ Чёрный список файлов к загрузке в систему по расширениям	Управление источниками данных ▪ Добавление / удаление ▪ Назначение контура файлового обмена, синхронизации и совместной работы	▪ Запрет общего доступа к отдельным файлам ▪ Запрет публичных ссылок ▪ Срочный / одноразовый доступ	
Права	▪ Роли в ролевой модели администрирования ▪ Доступ только учётным записям службы каталогов Active Directory	▪ Доступ к заданным источникам внутреннего контура заданным пользователям / группам ▪ Гибкая настройка прав доступа на уровне хранилища*	▪ Срочный доступ ▪ Только чтение ▪ Запрет на приглашение участников	▪ Запрет анонимного доступа ▪ Доступ только по приглашениям ▪ Срочный / одноразовый доступ

* Например, на уровне SMB для соответствующих источников

КИБЕР Файлы

ЦЕНТРАЛИЗОВАННЫЙ АУДИТ СОБЫТИЙ

Все события

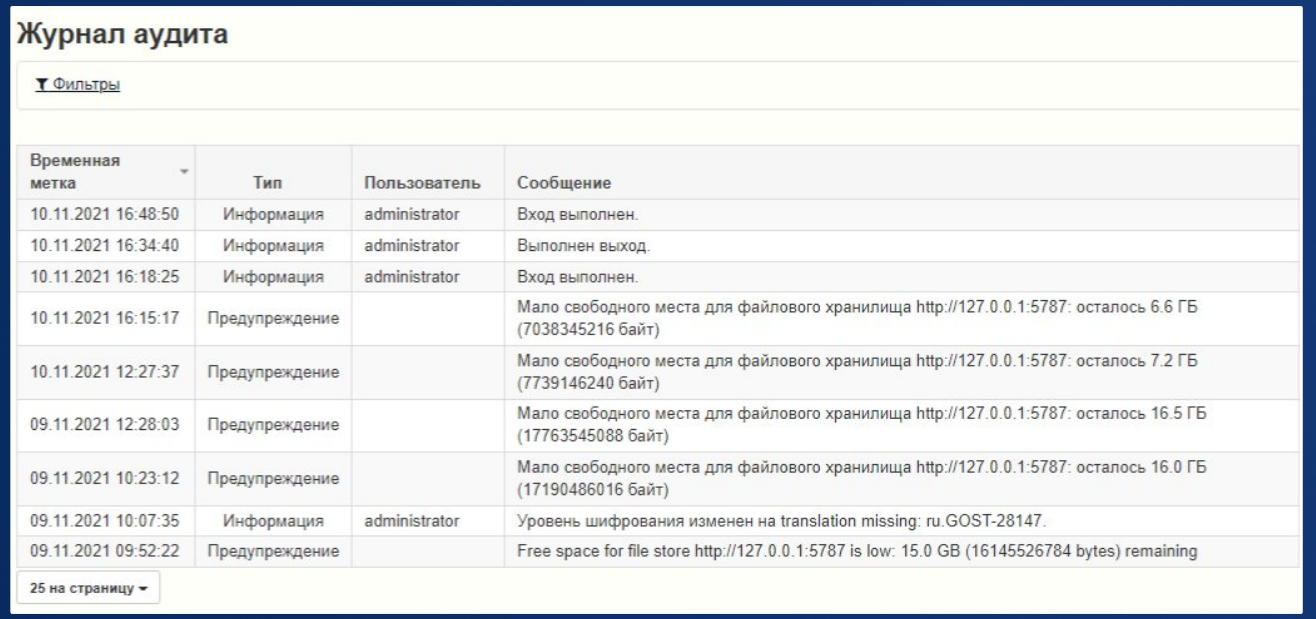
Доступ, синхронизация, обмен файлами, статус хранилищ и другие

Фильтрация

По заданным полям

Экспорт

В текстовый и табличные форматы



Журнал аудита

Фильтры

Временная метка	Тип	Пользователь	Сообщение
10.11.2021 16:48:50	Информация	administrator	Вход выполнен.
10.11.2021 16:34:40	Информация	administrator	Выполнен выход.
10.11.2021 16:18:25	Информация	administrator	Вход выполнен.
10.11.2021 16:15:17	Предупреждение		Мало свободного места для файлового хранилища http://127.0.0.1:5787: осталось 6.6 ГБ (7038345216 байт)
10.11.2021 12:27:37	Предупреждение		Мало свободного места для файлового хранилища http://127.0.0.1:5787: осталось 7.2 ГБ (7739146240 байт)
09.11.2021 12:28:03	Предупреждение		Мало свободного места для файлового хранилища http://127.0.0.1:5787: осталось 16.5 ГБ (17763545088 байт)
09.11.2021 10:23:12	Предупреждение		Мало свободного места для файлового хранилища http://127.0.0.1:5787: осталось 16.0 ГБ (17190486016 байт)
09.11.2021 10:07:35	Информация	administrator	Уровень шифрования изменен на translation missing: ru.GOST-28147.
09.11.2021 09:52:22	Предупреждение		Free space for file store http://127.0.0.1:5787 is low: 15.0 GB (16145526784 bytes) remaining

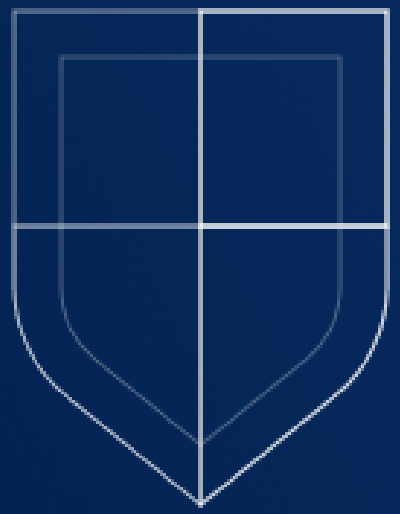
25 на страницу

ИНТЕГРАЦИЯ С DLP - КИБЕР ПРОТЕГО

Контроль передаваемых данных

КИБЕР Файлы

Кибер Протего



перехват

контроли

Распознавание веб-сервиса 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 операций с каналом

Подключение к сервису, POST-запросы, исходящие файлы

Контроль данных, передаваемых по каналу

POST-запросы, исходящие файлы

Блокировка или допуск операции

Тревожное оповещение, информационное оповещение

Протоколирование действий пользователя, теневое копирование

Запись экрана, клавиатурного ввода, сведений о процессах

КИБЕР Протего

DLP-контроль каналов утечки, данных, хранилищ, сотрудников

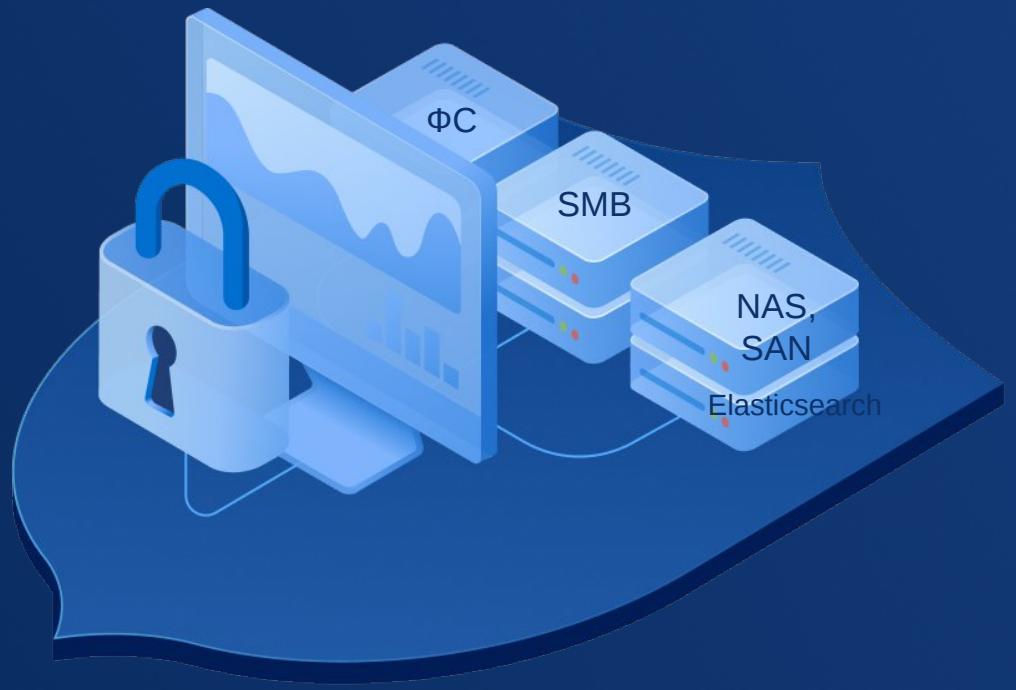
Контроль в реальном времени

При использовании и передаче данных

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

Превентивный контроль

При хранении данных

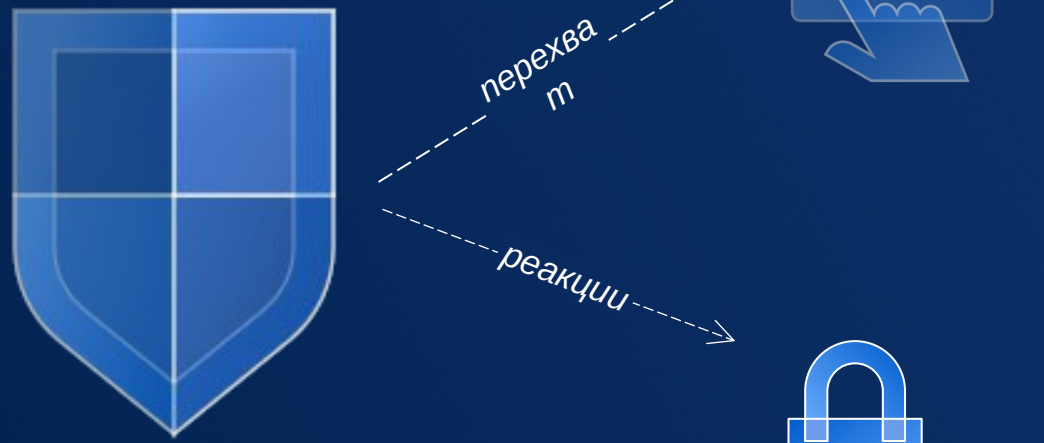


В хранилищах

На сервере – удалённое сканирование хранилищ

ЗАЩИТА В РЕАЛЬНОМ ВРЕМЕНИ

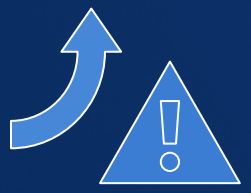
Контроль операций с каналами и данными непосредственно в точке передачи



Операции с каналами и данными

Запись, чтение, форматирование, извлечение, копирование/вставка, подключение к серверам, отправка и получение сообщений, отправка вложений, совершение звонков, публикация постов, синхронизация файлов и другие

Блокировка или допуск операции



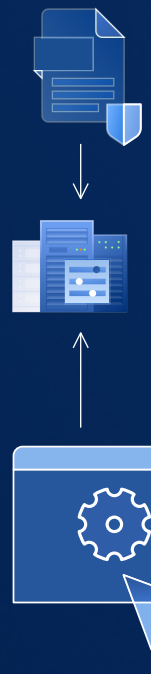
Тревожное оповещение, информационное оповещение

Протоколирование действий пользователя, теневое копирование

Запись экрана, клавиатурного ввода, сведений о процессах

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ И РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

КИБЕР Протего



Агенты Кибер Протего

Собирают журналы событий, теневые копии, видеозаписи экрана, записи нажатий клавиш и сведений о запущенных процессах

Передают их на *Сервер управления*

Консоль управления и веб-консоль

Предоставляют инструментарий работы с данными, хранящимися на *Сервере управления*

Досье | Фильтры журналов | Отчёты | Граф связей

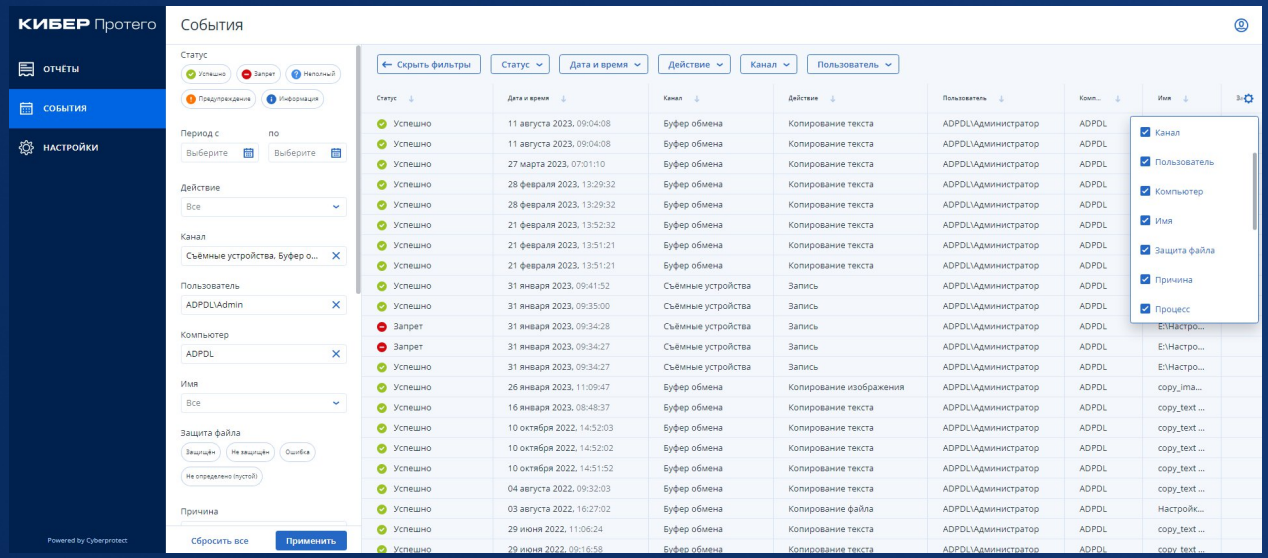
Фильтры журналов

Все собираемые данные хранятся в соответствующих журналах

Каждая запись содержит множество полей

По всем можно фильтровать

Один из основных инструментов расследования инцидентов, сбора доказательной базы, ретроспективного анализа



КОНТРОЛЬ ФАЙЛОВОГО ОБМЕНА С ПОМОЩЬЮ DLP-системы КИБЕР ПРОТЕГО

Предотвращение загрузки в *Кибер Файлы данных,* не предназначенных и совместной работы и последующего распространения третьим лицам

Контроль передачи

«Можно» только в контролируемый сервис файлового обмена

Сканирование локальных папок синхронизации

Анализ

Автоматическое принятие решения системой

Блокировка или разрешение попытки передачи файла

Оперативное уведомление, журналирование

Удаление данных, шифрование данных

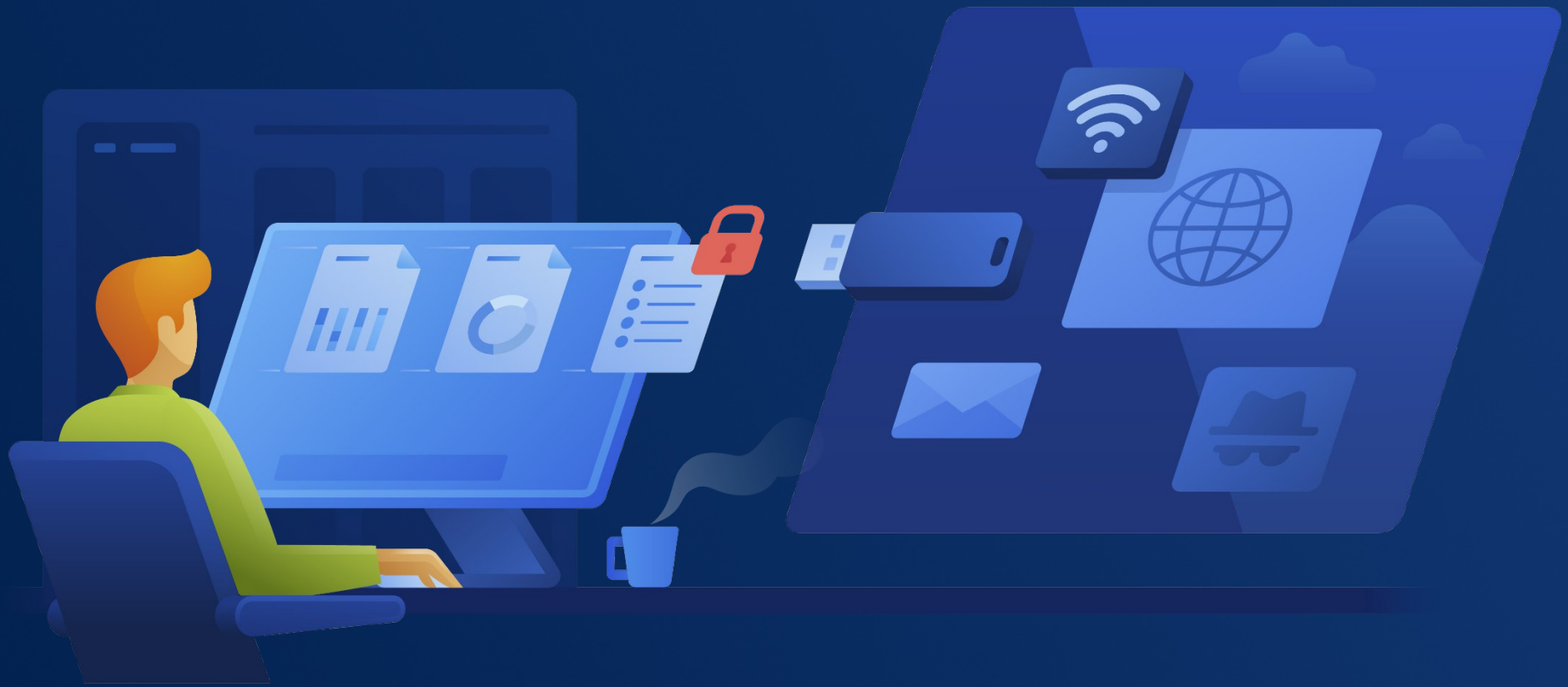
Смена прав доступа на уровне файловой системы

Отчёты, журналы, оповещения

- Что просканировано
- Что найдено
- Что сделано
- Что заблокировано, что разрешено

ЭКОСИСТЕМА БЕЗОПАСНОГО ОБМЕНА ФАЙЛАМИ

КИБЕР Протего **КИБЕР** Файлы



КИБЕРПРОТЕКТ

Серия вебинаров о резервном копировании
и защите данных

ВСТРЕТИМСЯ В РЕЗЕРВНЫЙ ЧЕТВЕРГ

Приглашаем вас на бесплатный вебинар
каждый четверг в 11:00!