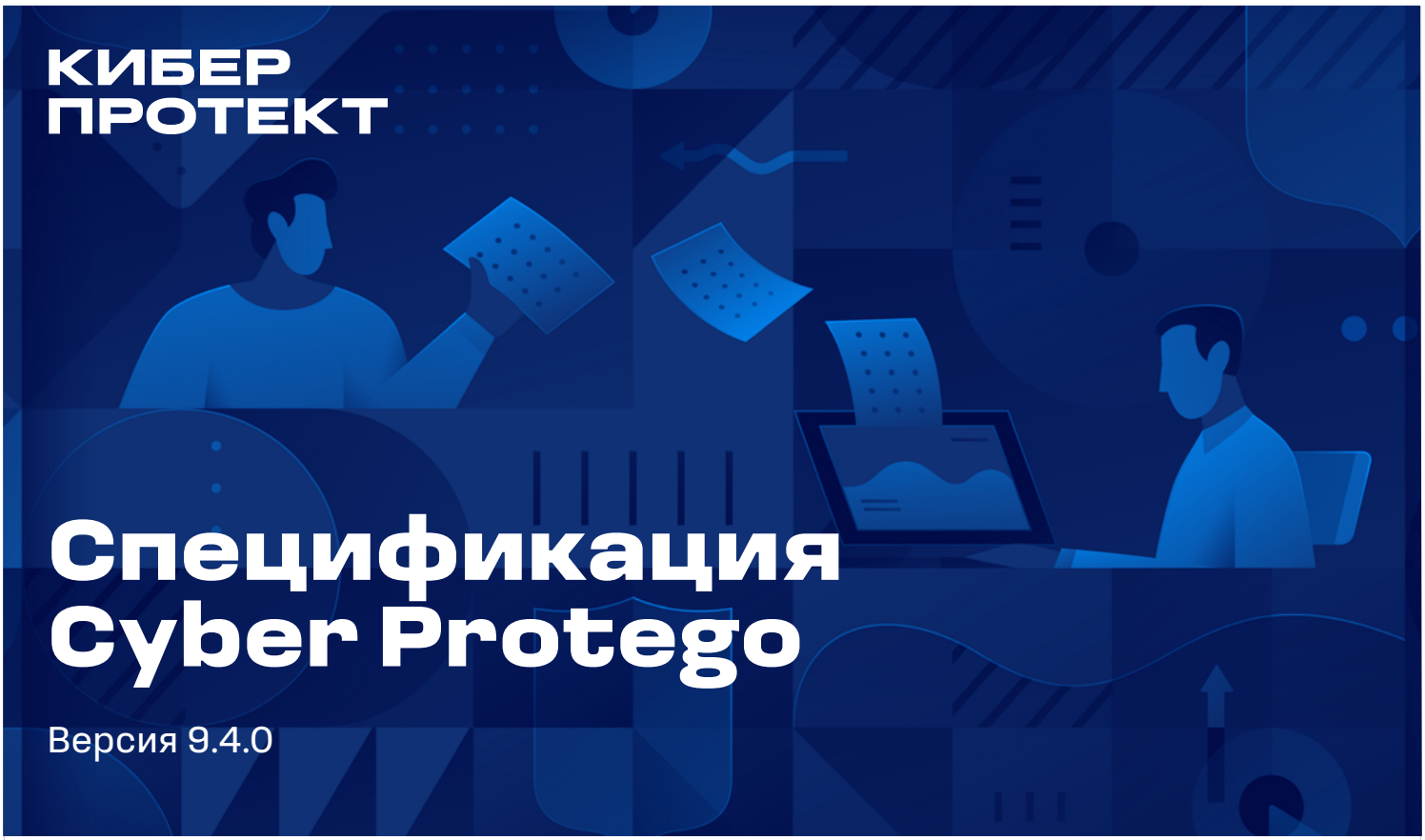
КИБЕР ПРОТЕКТ



Спецификация Cyber Protego

Версия 9.4.0

ИНФОРМАЦИЯ О ВЕРСИИ И СИСТЕМНЫЕ ТРЕБОВАНИЯ КОМПЛЕКСА CYBER PROTECO

Номер версии (сборки)
Русскоязычная версия:
9.4.0
Англоязычная версия:
9.4.0

Консоли управления
Поддерживаемые операционные системы:
- Windows 7/8/8.1/10/11 до 22H2 включительно (32/64-bit);
- Windows Server 2008R2-2019 (32/64-bit).

Минимальные требования
ЦПУ Pentium 4, ОЗУ 512Мб, Диск 1Гб.

Агенты
Поддерживаемые ОС:
- Windows 7/8/8.1/10/11 до 22H2 включительно (32/64-bit);
- Windows Server 2008R2-2019 (32/64-bit);
- macOS 10.15 -11.2.3 (32/64-bit).

Среды виртуализации/VDI:
- Microsoft RDS, Citrix XenDesktop /Xen App, XenServer, VMware Horizon View;
- VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC.

Минимальные требования
ЦПУ Pentium 4, ОЗУ 512MB, Диск 400Мб.

Серверные компоненты
Сервер Управления, Сервер Поиска, Сервер Discovery:
- Windows Server 2008R2-2019 (32/64-bit), Microsoft RDS, Citrix XenServer, VMware vSphere Desktop;
- SQL Express / MS SQL Server 2005-2019 или PostgreSQL 9.5 (и более новые).

Минимальные требования
2xЦПУ Intel Xeon Quad-Core 2.33GHz, ОЗУ 8GB, диск 800GB (меньше, если не используется БД SQL).

КОНТРОЛИРУЕМЫЕ ТИПЫ УСТРОЙСТВ

Windows
Съемные накопители (флэш, карты памяти, eSATA и др.), приводы CD-ROM/DVD/BD, приводы Floppy, жесткие диски, ленточные накопители, адаптеры Wi-Fi и Bluetooth, устройства Apple iPhone/iPod touch/iPad, BlackBerry, Windows Mobile и Palm, MTP-устройства (телефоны на базе Android, Windows Phone и др.), принтеры (локальные, сетевые и виртуальные), модемы, цифровые камеры, сканнеры.

Mac
Съемные накопители, жесткие диски, приводы CDROM/DVD/BD, адаптеры Wi-Fi и Bluetooth.

Терминальные сессии
Перенаправленные диски (съемные, оптические, жесткие), USB-устройства, принтеры.

КОНТРОЛИРУЕМЫЕ ПОРТЫ

Windows
USB, FireWire, IR, COM, LPT.

Mac
USB, FireWire, COM.

Терминальные сессии
USB, COM.

КОНТРОЛЬ БУФЕРА ОБМЕНА

Контроль операций обмена данными между приложениями
Контроль операций обмена данными в пределах приложения.

Windows
Контроль передачи данных между рабочей станцией и буфером обмена сеанса удаленного рабочего стола/приложения.

Раздельный контроль типов данных
Файлы, текстовые данные, графические данные, аудио данные, неопределенные данные.

Снимки экрана
Контроль снимков экрана (для приложений и клавиши PrintScreen).

Терминальные сессии
Контроль операций обмена данными между гостевой и родительской ОС.

КОНТРОЛИРУЕМЫЕ КАНАЛЫ СЕТЕВЫХ КОММУНИКАЦИЙ

Сетевые протоколы
HTTP/HTTPS, FTP/SFTP/ FTPS, Telnet.

Электронная почта
SMTP/SMTPS, IMAP, Microsoft Outlook (MAPI), IBM Notes.

Веб-почта
AOL Mail, Gmail, Web.de, Hotmail/ Outlook.com, GMX.de, Mail.ru, T-online.de, freenet.de, Yahoo! Mail, Rambler Mail, Yandex Mail, Outlook Web App/Access (OWA), NAVER, ABV Mail, Zimbra Collaboration, Google Workspace Sync for Microsoft Outlook (G-Suite).

Веб-поиск
Google, Яндекс, Bing, Baidu, Yahoo, Поиск Mail.Ru, Ask.com, AOL Search, Рамблер, Wolfram Alpha, DuckDuckGo, Search.com, WebCrawler, Wayback Machine, Dogpile, StartPage, Excite, NAVER, Web.de.

Службы мгновенных сообщений (мессенджеры)
Skype/Skype for Web/Skype for Business/Microsoft Lync 2013, ICQ Messenger, Zoom, Viber, IRC, Jabber, Агент Mail.ru, WhatsApp, Telegram.

Сетевые сервисы файлового обмена и синхронизации
Яндекс.Диск, Облако Mail.Ru, Google Drive, Dropbox, OneDrive, Box, iCloud, Sendspace, Amazon S3, GMX.de, Web.de, MagentaCLOUD, freenet.de, MediaFire, WeTransfer, 4shared, GitHub, MEGA, AnonFile, dmca.gripe, Easyupload.io, Files.fm, Cofile.io, transfer.sh, TransFiles.ru, Uploadfiles.io, DropMeFiles.

Социальные сети (включая мобильные версии)
ВКонтакте, Одноклассники, LiveJournal, LiveInternet.ru, Facebook, Twitter, Pinterest, Instagram, Google+, LinkedIn, Tumblr, MySpace, XING.com, MeinVZ.de, StudiVZ.de, Disqus.

Поиск работы
hh.ru, Яндекс.Работа, Rabota.ru, SuperJob.ru, Авито, CareerBuilder, College Recruiter, craigslist, Dice, Glassdoor, GovernmentJobs, HeadHunter.com, Hired, Indeed, JobisJob, Mediabistro, Monster, Simply Hired, Ladders, us.jobs, USAJOBS, ZipRecruiter.

Прочее
Файловые ресурсы (SMB), частные беседы Skype, звонки Skype, Torrent, трафик Tor Browser.

КОНТРОЛЬ ХРАНИМЫХ ДАННЫХ

Объекты сканирования
- Рабочие станции и серверы Windows (файловая система, репозитории электронной почты, подключенные периферийные устройства);
- Общие сетевые ресурсы, сетевые хранилища;
- Локальные папки синхронизации облачных сервисов файлового обмена;
- Базы данных Elasticsearch.

Режимы сканирования
С использованием агента, удаленное (без агента), смешанное.

Корректирующие действия
Удаление, гарантированное удаление, удаление контейнера (если нарушение выявлено в файле внутри контейнера или архива), задание прав доступа (только для файловой системы NTFS), протоколирование, тревожное оповещение администратора, оповещение локального пользователя, шифрование (только с использованием EFS в файловой системе NTFS).

Операции сканирования
Ручной и автоматический (в соответствии с расписанием) запуск задач сканирования и обнаружения.

Прочие возможности
Статическое и динамическое формирование списка сканируемых компьютеров, отчеты, автоматическая установка и удаление агента.

ТЕХНОЛОГИИ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Контролируемые каналы
Съемные накопители, принтеры (локальные, сетевые, виртуальные), буфер обмена, перенаправленные диски и буфер обмена терминальной сессии, сетевые коммуникации (Электронная почта, Веб-почта, Мессенджеры, Социальные сети, Облачные хранилища, Веб-поиск, Поиск работы, HTTP/HTTPS, IMAP FTP/SFTP/FTPS, SMB).

Контролируемые виды данных
Текстовые данные, бинарные файлы, определение типа файла.

Контролируемые типы данных
Более 5300 типов файлов, свойства файлов и документов, объекты буфера обмена (файлы, текст, изображения, аудио, прочее), объекты протоколов синхронизации (Microsoft ActiveSync®, Palm® HotSync, iTunes®) с мобильными устройствами, контроль текста в графических изображениях (встроенных в документы Microsoft Office, AutoCAD и Adobe PDF или отдельных графических файлах), объекты данных с метками классификатора Boldon James.

Методы распознавания бинарных данных
Анализ по цифровым отпечаткам (с частичным или полным соответствием с заданным образцом) с поддержкой классификации образцов.

Возможности OCR
Оптическое распознавание символов (OCR) для более чем 30 языков, включая русский.

Распознаваемые форматы данных
- Более 100 форматов файлов, включая документы Microsoft Office, Adobe PDF, AutoCAD, OpenOffice, Lotus 1-2-3, WordPerfect, WordStar, Quattro Pro, архивы и репозитории электронной почты, CSV, DBF, XML, Unicode, др.;
- Более 40 форматов архивов с любой глубиной вложенности, включая GZIP, RAR, ZIP, др.

Контентная фильтрация для теневого копирования
Для всех контролируемых каналов и типов данных.

Методы определения текстовых данных
- Поиск по ключевым словам с применением морфологического анализа (для английского, французского, итальянского, немецкого, испанского/каталанского, русского, португальского и польского языков) по целым словам или частичному совпадению, поддержка транслитерации для русского языка;
- Поиск по встроенным шаблонам регулярных выражений (номера кредитных карт, адреса, паспортные данные и т.д., более 90);
- Встроенные отраслевые терминологические словари (более 160);
- Анализ расширенных свойств документов и файлов (имя, размер, наличие парольной защиты, наличие текста, дата и время последнего изменения, заголовок, тема, метки и категории документа, комментарии и авторы, метки классификатора Boldon James и др.).

МОНИТОРИНГ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ (UAM)

Запись по событию
Видеозапись экрана пользователя, запись всех нажатий клавиш, сохранение информации о процессах и приложениях, которые выполнялись и запускались во время записи.

Условия записи
Запись осуществляется в заданном интервале времени на основе параметров состояния системы, срабатывания DLP-политики или других заданных событий, включая запись до момента срабатывания.

Гибкая настройка
Настраиваемые частота, цветность и разрешение выходного видео, независимые настройки для онлайн/офлайн профиля, валидация синтаксиса правила UAM перед активацией, приостановка записи при бездействии, логирование паролей.

Централизованный архив
Автоматический сбор записей сеансов мониторинга с рабочих станций в центральную базу данных.

Анализ журнала сеансов мониторинга
Просмотрщик локального и центрального журнала сеанса мониторинга, фильтрация записей по более чем 20 параметрам.

Просмотр записанных сеансов
Встроенный проигрыватель видеозаписей экрана, журнал списка запущенных приложений и нажатий клавиш.

ИНТЕГРАЦИЯ С КРИПТОГРАФИЧЕСКИМИ ПРОДУКТАМИ

Windows
Windows BitLocker To Go, Sophos® SafeGuard Easy®, SecurStar® DriveCrypt®, TrueCrypt®, PGP® Whole Disk Encryption, Infotecs SafeDisk®, SafeToGo, Рутокен Диск.

Mac
Apple® OS X FileVault.

КОНТРОЛЬ ВИРТУАЛЬНЫХ И ТЕРМИНАЛЬНЫХ СРЕД (CYBER PROTEGO TS)

Cyber Protego TS
Контролирует устройства хранения данных, сетевые ресурсы, USB-устройства, принтеры, буфер обмена данными, последовательные порты, перенаправленные в терминальную сессию по протоколам RDP, ICA, PCoIP, HTML5/WebSockets, равно как и сетевые коммуникации виртуальных рабочих столов и клиентов терминальных сессий.

Поддерживаемые среды
Microsoft RDS, Citrix XenDesktop/ XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC.

ПОЛЬЗОВАТЕЛЬСКИЕ ДОСЬЕ

Карточка пользователя
Отображается условный индикатор лояльности пользователя, диаграмма активности для локальных и сетевых каналов, сведения о действиях пользователей, интерактивный отчет Граф Связей.

Оптимизация отчета
Настраиваемый период отчета, сворачивание однотипных событий, автоматическое обновление статистики и отчетов.

ПОЛНОТЕКСТОВЫЙ ПОИСК ПО АРХИВУ СОБЫТИЙ И ТЕНЕВЫХ КОПИЙ

Индексируемые данные
- Задания на печать в форматах PCL, Postscript и другие;
- Все поддерживаемые механизмами контентной фильтрации форматы файлов.

Логика поиска
Возможность составления поисковых запросов на базе комбинации слов и фраз в булевой логике, релевантность, весовые коэффициенты терминов и полей документов.

Индексирование и поиск по параметрам
- комбинация слов, фраз, регулярных выражений, специальных символов, численных диапазонов, полей документов, записей журналов аудита;
- Морфологический поиск и фильтрация «стоп-слов» для языков: русский, английский, французский, немецкий, итальянский, японский, испанский;
- Синонимический поиск для английского и русского языков.

Текст в изображениях
Встроенный модуль OCR позволяет извлекать текст из графических файлов для его дальнейшего индексирования.

Поиск по расписанию
Запуск поисковых запросов по расписанию с автоматической отправкой результатов поиска (полных или инкрементальных по сравнению с аналогичным предыдущим запросом) по электронной почте.

ЛИЦЕНЗИРУЕМЫЕ КОМПОНЕНТЫ

Device Control **Базовый компонент**	Обеспечивает контекстный контроль доступа пользователей к локальным каналам передачи данных, включая все виды устройств и интерфейсов.
Device Control Mac **Базовый компонент для macOS**	Обеспечивает контекстный контроль доступа пользователей к локальным каналам передачи данных, включая все виды устройств и интерфейсов.
Web Control **Опциональный компонент**	Обеспечивает контекстный контроль доступа пользователей к каналам сетевых коммуникаций.
Content Control **Опциональный компонент**	Осуществляет контентный анализ и фильтрацию данных, передаваемых как через локальные каналы, так и по каналам сетевых коммуникаций.
User Activity Monitor **Опциональный компонент**	Осуществляет видеозапись экрана пользователя, запись нажатий клавиш и регистрацию запущенных процессов на контролируемой системе при наступлении заданных событий.
Search Server **Опциональный компонент**	Обеспечивает полнотекстовый поиск по базе данных теневого копирования и событийного протоколирования.
Discovery **Самостоятельный компонент**	Позволяет выполнять сканирование рабочих станций и корпоративных сетевых ресурсов с целью обнаружения хранимых конфиденциальных данных с автоматическим устранением выявленных нарушений.

ЛИЦЕНЗИРОВАНИЕ ДЛЯ ТЕРМИНАЛЬНЫХ СЕССИЙ / VDI

Лицензирование Cyber Protego для DLP-контроля в терминальных сессиях осуществляется аналогично лицензированию рабочих станций, на основе количества активных терминальных сессий. Лицензируемые компоненты - Device Control TS, Web Control TS, Content Control TS, User Activity Monitor TS.

КИБЕР ПРОТЕКТ

Больше информации
www.cyberprotect.ru