Уникальность – 100% (https://text.ru/antiplagiat/60ed6c5c1888a)

# Лучшие программы для обеспечения информационной безопасности в бизнесе

«Противостояние брони и снаряда» - выражение, когда-то введенное в обиход теоретиками войны и конструкторами оружия. Его суть – как только появляется новая, более прочная и надежная броня, сразу начинается разработка снаряда, способного ее пробить. И наоборот. Впрочем, это правило работает не только в оружейной среде, но и в других сферах. В том числе в секторе обеспечения информационной безопасности компаний и предприятий.

Базовый постулат обеспечения корпоративной цифровой безопасности в современных реалиях – [принцип «нулевого доверия»](https://www.kickidler.com/ru/info/zero-trust-pochemu-nulevoe-doverie-eto-tak-vazhno.html), Zero Trust. Он заключается в том, что киберзащита компании должна быть тотальной, и охватывать не только попытки взлома извне, но и потенциальные недружественные действия изнутри. Основывается такая система на использовании комбинации из разных программных решений.

В этой статье мы расскажем, какое ПО лучше использовать, чтобы создать «кибер-броню», способную защитить корпоративную информацию от «снарядов» преступников, мошенников, конкурентов и недоброжелателей. Рассмотрим комплекс из SIEM и DLP-систем, программ для защиты документооборота, антивирусов и СУРВ.

## SIEM-системы

SIEM (Security Information and Event Management) – системы сбора и управления информацией о безопасности, а также анализа событий информационной безопасности. Само это ПО не предназначено для защиты и предотвращения утечек данных и иных кибер-проблем. Его задача – собирать информацию от DLP, IDS, антивируса, маршрутизатора и проч., анализировать ее и сообщать об отклонениях, подозрительных действиях и т.п.

Подобных программ достаточно много, поэтому мы выбрали сразу несколько вариантов для рассмотрения.

### IBM QRadar Security Intelligence

IBM QRadar Security Intelligence – платформа, в рамках которой реализовано сразу несколько продуктов для обнаружения угроз сетевой безопасности, оценки и противодействия им. ПО обеспечивает возможность управления событиями, интеграции информации о безопасности, обнаружения аномальных ситуаций, управления журналами и реализации других задач. Именно комплексность и большое количество возможностей – главные достоинства данной системы.

### Основные возможности

* Единая архитектура анализа угроз, журналов, событий и других маркеров.
* Расчет корреляции, а также аномальных событий фактически в режиме реального времени.
* Обширные возможности анализа сетевой активности.
* Обширные возможности анализа действий пользователей и запущенных приложений.
* Определение инцидентов с высоким уровнем приоритетности.
* Автоматизированная система составления отчетов.
* Сбор и обобщение информации о зафиксированных угрозах.
* Масштабированный контроль активности в рамках предприятия.
* Проведение детального анализа на основании технологий больших данных.

### Недостатки

* Некоторым регистрируемым событиям не присваивается категория.
* Это масштабная система, что может повлечь некоторые сложности с интеграцией.

### Стоимость

Доступен 14-дневный пробный период, а также возможность бесплатного использования ПО с ограниченным функционалом. Стоимость лицензии – от 800$ в месяц.

### Splunk Enterprise Security

Splunk Enterprise Security – еще один мощный инструмент, предназначенный для аналитики событий информационной безопасности на предприятиях. Его основная отличительная черта – ориентированность в первую очередь на современные угрозы и адаптивность с новыми программно-аппаратными решениями. Благодаря этому ПО отличается высокой оперативностью обнаружения угроз и оповещения о них.

#### Основные возможности

* Мониторинг угроз в режиме реального времени.
* Проверка пользователей, программ и сетевых ресурсов.
* Обнаружение сложных угроз, в том числе определение взаимосвязей между разными событиями.
* Обнаружение внутренних угроз, в том числе касающихся злонамеренных действий со стороны сотрудников.
* Расследование инцидентов, в том числе установление их масштабов.
* Автоматизация управления и выгрузки данных.
* Обнаружение мошенничества на основании выявления аномалий в действиях.

#### Недостатки

* Корпоративная версия отличается определенной сложностью установки.
* Отсутствует русскоязычная локализация новых версий ПО.

#### Стоимость

Стоимость лицензии – от 1800$ в год в зависимости от конфигурации.

### McAfee Enterprise Security Manager

Разработчики McAfee Enterprise Security Manager называют свою систему одним из лидеров по скорости и полноте обработки информации. Это ПО доступно для развертывания, как в облачных, так и в локальных сетях. Хорошо подходит для предприятий и организаций, где требуется обработка больших объемов данных. Также продукт отличается высоким уровнем интеграции с ПО сторонних разработчиков без API, что позволяет создавать корпоративные системы информационной безопасности, используя наиболее подходящее с собственной точки зрения программное обеспечение.

#### Основные возможности

* Наличие готовых конфигураций с предварительно настроенными сценариями.
* Встроенные пакеты материалов по базовым поведениям пользователей.
* Отдельный пакет функций для мониторинга внутренних служб ОС Windows.
* Обнаружение угроз в режиме реального времени.
* Система информирования об угрозах.
* Мониторинг данных в облачных и локальных сетях.
* Сбор и кластеризация событий.
* Формирование автоматических отчетов о событиях.

#### Недостатки

* Система требовательна к объему вычислительных ресурсов.
* Не всегда оперативное устранение обнаруженных багов.

#### Стоимость

Стоимость одной бессрочной лицензии – от 1400 рублей. Для всех новых пользователей доступен 14-дневный бесплатный тестовый период.

## DLP-системы

[DLP-система](https://www.kickidler.com/ru/info/obzor-i-sravnenie-luchshix-besplatnyix-open-source-dlp-sistem-2019-goda.html) (расшифровка аббревиатуры – Data Leak Prevention) – специализированное ПО, предназначенное для защиты от утечек и кражи конфиденциальной корпоративной информации. Такие программы используют технологии блокировки передачи информации через разные каналы, предлагают функционал для мониторинга поведения сотрудников и всех участников сети, предоставляют некоторые возможности отслеживания активностей персонала.

Рынок DLP-систем обширен, но на нем можно выделить два лидирующих продукта.

### InfoWatch Traffic Monitor

Система InfoWatch Traffic Monitor разработана для работы под большими нагрузками при необходимости обработки значительных объемов информации. Это масштабируемое ПО, которое одинаково хорошо подходит для крупных организаций и небольших офисов. Основные функции – мониторинг и блокировка данных. Особенность – способность обнаруживать документы и мультимедийные данные, блокировать их даже в случае их значительного видоизменения пользователем.

#### Основные возможности

* Обнаружение трафика конфиденциальной информации всех типов.
* Блокировка передачи конфиденциальной информации.
* Обнаружение недобросовестных сотрудников.
* Обнаружение мошеннических схем.
* Обнаружение неочевидных угроз.
* Контроль путей распространения информации внутри компании.

#### Недостатки

* Недостаточный функционал контроля активности пользователей.
* Отсутствие кейлоггера.
* Модульная инфраструктура с размещением модулей на отдельных серверах.

#### Стоимость

Продукт продается с годичной возобновляемой лицензией. Стоимость зависит от выбранной конфигурацией и предоставляется разработчиком по запросу.

### DeviceLock DLP

DeviceLock DLP – хостовая DLP-система, предназначенная для мониторинга информации и блокировки ее несанкционированного распространения. Предоставляет обширные возможности настройки сценарий и политик контроля, что позволяет интегрировать ее в организациях разных типов для решения большинства задач, связанных с защитой конфиденциальных данных.

#### Основные возможности

* Блокировка доступа пользователей к данным.
* Блокировка доступа пользователей к серверам и периферийным устройствам.
* Индивидуальная настройка параметров мониторинга и блокировки.
* Контроль доступа и взаимодействия пользователей с сетевыми сервисами.

#### Недостатки

* Ограниченные возможности мониторинга сотрудников.
* Необходимость точной настройки сценариев для корректного срабатывания блокировки.

#### Стоимость

Стоимость годичной лицензии – от 4 275 рублей. Точная цена зависит от выбранной версии и конфигурации.

## Решения для защиты документов

Еще одна категория полезных программ – ПО, позволяющее обнаружить человека, похитившего документы. В разных решениях реализованы различные методы достижения такого результата. Но действительно эффективной можно назвать только одну систему.

### EveryTag

EveryTag – программа, которая позволяет с очень высокой вероятностью обнаружить сотрудника, похитившего информацию. ПО особым образом маркирует документы, причем маркировка визуально незаметна. В случае утечки информации и появления несанкционированной копии, ее достаточно загрузить в систему чтобы узнать, кто из сотрудников совершил хищение. Подход простой, но эффективный.

#### Основные возможности

* Защита документов в электронном формате.
* Защита от несанкционированного фотографирования распечатанных документов.
* Защита от кражи методом несанкционированных снимков экрана.
* Защита от хищения распечатанных документов.

#### Недостатки

* Это целевое ПО, функционал которого позволяет только обнаруживать сотрудников, похищающих документы.

#### Стоимость

Стоимость зависит от приобретаемой конфигурации ПО. Прайс-лист разработчик предоставляет только по запросу клиента.

## Корпоративные антивирусы

Система информационной безопасности компании не будет полной без внедрения хорошего [корпоративного антивируса](https://www.kickidler.com/ru/info/rejting-luchshix-korporativnyix-antivirusov-dlya-malogo-i-srednego-biznesa-2020.html). Это ПО для защиты информации и оборудования от вредоносного программного обеспечения, вирусных угроз и кибер-атак. Рынок предлагает достаточно много хороших программ такого типа. Рассмотрим некоторые из них.

### Kaspersky Small Office Security

Kaspersky Small Office Security – надежный антивирус с быстрым обновлением баз данных и хорошим уровнем защиты от угроз. ПО оптимально подходит для небольших компаний, но может использоваться и в крупных организациях. Несомненное достоинство – расширенный функционал, охватывающий практически все аспекты цифрового взаимодействия компании с внешними сетями.

#### Основные возможности

* Файловый антивирус.
* Веб-антивирус.
* Защита от сбора данных.
* Контроль обновления программ.
* Защита веб-камер.
* Фильтрация активности пользователей.
* Контроль установленных программ.
* Защита финансовой информации.
* Блокировка рекламы.
* Шифрование информации.

#### Недостатки

* ПО в большей степени ориентировано на малые офисы.
* Ограниченный функционал управления в веб-панели.

#### Стоимость

Стоимость годичной лицензии – от 3900 рублей для конфигурации с защитой до 5 ПК.

### McAfee Endpoint Protection Essential

McAfee Endpoint Protection Essential – еще один популярный корпоративный антивирус. Также отличается хорошим набором инструментов для защиты от сетевых и программных угроз. Оптимизирован для решения задач компаний и организаций, отличается простотой настройки и управления, а также высокой частотой обновления баз данных. Ключевые достоинства – высокая эффективность обнаружения угроз и противодействия им, обширные возможности настройки отчетов.

#### Основные возможности

* Брандмауэр.
* Мониторинг в режиме реального времени.
* Защита от вирусов-вымогателей.
* Сетевая защита ПК.
* Контроль веб-трафика.
* Автоматическая реакция на вероятные угрозы.

#### Недостатки

* Усложненная установка и настройка.
* Требовательность к ресурсам оборудования при полном сканировании системы.

#### Стоимость

Стоимость годичной лицензии – от 6000 рублей. Точная цена зависит от выбранной конфигурации.

## Системы учета рабочего времени (Kickidler)

Системы учета рабочего времени (СУРВ) – еще одна категория ПО, без которого не обойтись, налаживая комплексную защиту корпоративных данных. Правда, здесь следует рассматривать только СУРВ, функционал которых дополнен инструментами контроля сотрудников, работающих за ПК. И здесь вне конкуренции программа Kickidler, поскольку среди всего доступного на рынке ПО именно у нее наиболее обширный набор инструментов для мониторинга работников и их действий.

Изобретательность недобросовестных сотрудников в стремлении к совершению корпоративных преступлений нельзя недооценивать. Они регулярно изобретают новые методы обхода внимания ПО для контроля и блокировки движения информации. Но возможные бреши в защите можно закрыть, контролируя не только движение корпоративных данных, но и действия самого работника.

Kickidler с его функциями записи видео с мониторов сотрудников, кейлоггера, онлайн-мониторинга и контроля времени пребывания за ПК в этом отношении очень хорош. К слову, у компании есть реальный [кейс по обнаружению инсайдера, ворующего клиентскую базу](https://www.kickidler.com/ru/info/kak-byil-obnaruzhen-insajder-voruyushhij-klientskuyu-bazu-realnyij-kejs.html), подтверждающий эффективность такого контроля.

К слову, сотрудник, зная, что каждое его действие регистрируется и сохраняется, с гораздо меньшей вероятностью попытается похитить данные или совершить другое корпоративное преступление. Особенно с учетом того, что противоречивые или спорные моменты можно уточнить на основании показателей сразу нескольких инструментов (например, проверив данные кейлоггера и запись видео с экрана).

#### Основные возможности

* Онлайн-мониторинг ПК работников – возможность смотреть экраны сотрудников в реальном времени.
* Кейлоггер – запись всех нажатий на клавиатуру.
* Запись видео – в непрерывном режиме записывается видеосигнал с экрана сотрудника.
* Регистрация времени начала и завершения работы, а также пауз и простоев.
* Удаленный доступ к ПК сотрудников.
* Автоуведомления о нарушениях на рабочем месте – напоминания о постоянном контроле для предупреждения серьезных проступков.

#### Недостатки

* Отсутствие мобильных версий.
* Отсутствие интеграции с облачными сервисами.

#### Стоимость

ПО доступно в бесплатной версии (подключение до 6 ПК). Доступен 2-недельный бесплатный тестовый период для полной версии. Стоимость лицензии – 220 рублей в месяц за каждый подключенный ПК.

## Выводы

SIEM-система контролирует информацию, ищет угрозы и предупреждает о них. DLP-система контролирует обмен данными и препятствует их краже. ПО для защиты документов исключает вероятность их кражи любым способом. Корпоративный антивирус противодействует вредоносному ПО. СУРВ контролирует поведение и действия сотрудников. А вместе все эти системы составляют надежный контур кибер-безопасности, который в такой конфигурации пробить практически невозможно.