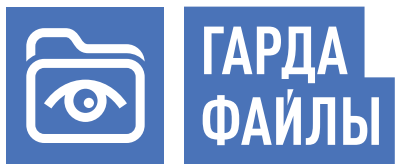




**ГАРДА**  
ТЕХНОЛОГИИ

# СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



## Аппаратно-программный комплекс класса DAG<sup>1</sup>

АПК «Гарда Файлы» предназначен для управления доступом к неструктурированным данным в компьютерах и сетевых хранилищах.

### Защита файловых хранилищ



Категоризация и классификация неструктурированных данных



Аудит прав доступа в реальном времени



Оптимизация сетевых хранилищ



Локализация конфиденциальной информации в общем массиве корпоративных данных



Управление правами доступа к корпоративной информации



### Преимущества решения

- Мгновенный поиск по всем хранилищам.
- Высокая производительность - обработка до 1 млрд событий за секунды.
- Раннее выявление нарушения прав доступа к данным.
- Интеграция с системами безопасности через Rest API.
- Распознавание графических изображений (паспорта, чертежи, данные карт, ИНН и пр.).



### Практическая безопасность

- Выявление конфиденциальных документов в общем доступе.
- Автоматизация управления правами доступа по категории данных.
- Выявление рисков от ранее выданных прав доступа.
- Построение профилей сотрудников и хранилищ для выявления аномалий.
- Активная реакция на инциденты безопасности — автоматическая блокировка аномальной активности (остановит вирус шифровальщика).



### Соответствие требованиям

Гарда Файлы обеспечивает соответствие требованиям регуляторов к хранению данных:

- ФЗ-152;
- Приказы ФСТЭК №176, 216, 239;
- PCI DSS;
- GDPR;
- HIPPA.



### ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ АПК «ГАРДА ФАЙЛЫ»

Аудит доступа выполняется с помощью агентов. Классификация, получение структуры хранилищ и прав доступа происходит удалённо.



Dell EMC



NetApp



Active Directory



Файловые хранилища Unix / Linux



Файловые хранилища MS Windows



Microsoft Exchange



Серверы Sharepoint



Коллекторы/Агрегаторы



Коллекторы/Агрегаторы



## ГАРДА МАСКИРОВАНИЕ

### Система для создания обезличенных копий баз данных

Обеспечивает безопасность передачи данных информационных систем.

### Маскировка баз данных



Возможность передачи данных тестирующим без риска утечки



Автоматическое выявление чувствительной информации в массиве данных



Маскирование данных «на лету» при передаче в среды тестирования и разработки



Подготовка данных для аналитики и выявления статистических закономерностей

### Широкие возможности маскирования СУБД



Репликация баз данных с полным сохранением структуры БД и её взаимосвязей, с заменой чувствительной информации по справочникам и в соответствии с алгоритмами



Автоматическое выявление и маскирование чувствительных данных: ФИО, номера банковских карт, паспортные данные, даты рождения, ИНН, ОГРН, СНИЛС, номера телефонов, e-mail, логины учетных записей.



Не требует внесения изменений в структуру защищаемых БД



### Принцип работы

1 ЭТАП

#### 1 ЭТАП — СКАНИРОВАНИЕ

- Автоматический анализ структуры БД
- Выявление персональных данных и других чувствительных данных
- Анализ взаимосвязей хранимых данных
- Формирование предварительного отчёта



Васильев Дмитрий Александрович

26.03.1996  
177-162-846-95  
52563008230000405  
+790835162816

2 ЭТАП

#### 2 ЭТАП — ПЕРЕНОС ДАННЫХ

- Создание копии БД
- Замена персональных данных и чувствительной информации (обезличивание)
- Сохранение взаимосвязей, форматов и структуры данных
- Формирование результирующего отчёта



Игнатьев Алексей Игоревич

16.08.1996  
162-177-476-32  
52561008960000465  
+79082814154

### Единый комплекс управления циклом безопасности данных



#### ЗАЩИТА НА УРОВНЕ ПОЛЬЗОВАТЕЛЕЙ СУБД

В информационных системах и бизнес-приложениях данные систематизированы и структурированы. Защита — DAM-система «Гарда БД».

#### ЗАЩИТА НА УРОВНЕ РАЗРАБОТЧИКОВ ПО

Маскирование данных — необходимая защита информации при передаче разработчикам, тестирующим, аналитикам и другим лицам, для которых доступ к содержимому СУБД не обязателен. Защита — система «Гарда Маскирование».

<sup>1</sup> DAG (Data Access Governance) — средства защиты для управления доступом к разрозненным данным.



## Аппаратно-программный комплекс класса DAM/DBF<sup>2</sup>

Система аудита и блокировки сетевого доступа к базам данных для обеспечения безопасности СУБД и независимого аудита операций с базами данных и бизнес-приложениями. Ведет непрерывный мониторинг обращений к базам данных и выявляет подозрительные операции в режиме реального времени.



### Функциональные возможности

- Аудит всех операций с БД в режиме реального времени
- Контроль действий привилегированных пользователей
- Выявление и предотвращение попыток внешнего вторжения в СУБД
- Блокирование нежелательных запросов к БД и веб-приложениям
- Обнаружение существующих и новых БД в компании, их классификация и сканирование на уязвимости
- Контроль удаленного доступа сотрудников

Гарда БД защищает от преднамеренных или неумышленных действий инсайдеров, хакеров, привилегированных и рядовых пользователей.



### Примеры решаемых задач

- Предотвращение выгрузки и продажи критичных данных клиентов, в том числе персональных данных, данных кредитных карт и т.д.
- Контроль манипуляций с клиентскими базами, накрутки KPI менеджерами.
- Проверка БД на обезличенность при их клонировании для целей тестирования.
- Выявление не оптимально настроенных конфигураций СУБД с точки зрения стандартов и лучших практик по информационной безопасности.
- Применение для аттестации ГИС, ИСПДн, АС по требованиям ФСТЭК в случае использования несертифицированных СУБД и приложений.
- Предотвращение мошенничества и прямых хищений денежных средств с использованием БД и бизнес-приложений компании.
- Выявление несанкционированного разворачивания теневых, нелегитимных и неконтролируемых баз данных администраторами.
- И другие.



### Соответствует требованиям

Гарда БД обеспечивает выполнение требований следующих нормативно-правовых документов:

- СТО БР ИББС;
- PCI DSS;
- 152-ФЗ «О персональных данных»;
- 161-ФЗ «О Национальной платежной системе»;
- П-1119 «Об утверждении требований к защите ПДн»;
- 98-ФЗ «О коммерческой тайне»;
- 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положение Банка России о требованиях к обеспечению защиты информации 382-П;
- Basel II;
- SOX;
- Сертифицировано ФСТЭК на соответствие ТУ, является СЗИ класса НДВ-4;
- Входит в реестр отечественного ПО;
- И пр.

2) DAM (Database Activity Monitoring) — мониторинг и аудит активности пользователей в базах данных.

DBF (Database Firewall) — активный мониторинг и защита баз данных в режиме реального времени.



## Аппаратно-программный комплекс класса NTA<sup>3</sup> для выявления и расследования сетевых инцидентов.

Система обеспечивает прозрачность сетевых потоков данных с помощью тотального контроля и записи трафика сети компании, выявляет сетевые атаки и аномалии, помогает в расследовании инцидентов.



### Функциональные возможности

- Запись копии сетевого трафика
- Сигнатурный анализ трафика
- Обнаружение обращений к скомпрометированным ресурсам
- Выявление новых устройств и служб в заданном сегменте сети
- Выявление отклонений в поведении устройств
- Позволяет выполнять расследования сетевых инцидентов

+ При установке система уже содержит подключенные и обновляемые базы сигнатур и репутационные списки

Гарда Монитор повышает эффективность работы центров мониторинга (SOC), холдинговых структур, территориально-распределенных компаний и других секторов бизнеса.



### Расследование сетевых инцидентов

- Гибкие настройки параметров записи:
  - запись с сохранением «сырых» данных;
  - запись только статистики по всем потокам;
  - индексация и быстрый поиск по всему объему поступающих данных благодаря высокопроизводительной системе хранения.
- Библиотека предустановленных политик для выявления инцидентов сразу после внедрения.
- Возможность настроить свои политики для оперативного контроля трафика в режиме реального времени.
- Интерактивные отчеты и понятная аналитика входящего и исходящего трафика, статистика инцидентов.



### Контроль и анализ трафика

- Мониторинг IP-трафика локальных сетей и выявление сетевых инцидентов безопасности.
- Анализ информационных потоков по всем актуальным протоколам.
- Гибкий многокритериальный поиск.
- Возможность реагирования на события, удовлетворяющие пользовательским фильтрам, в режиме близком к реальному времени.
- Экспорт событий во внешние системы.
- Единый центр управления — агрегированная статистика с каждой точки подключения.

Гарда Монитор обеспечивает полный контроль сетевых потоков данных и позволяет выявлять угрозы, в том числе в случае проникновения из открытой сети за выстроенный периметр безопасности.



### Примеры решаемых задач

- Детектирование загрузки файлов с внешних неизвестных хостов.
- Обнаружение попыток удаленного выполнения кода.
- Выявление использования слабой парольной политики в компании.
- Контроль использования средств удаленного управления (TeamViewer, Radmin, VNC и т.д.).
- Обнаружение использования протоколов анонимных сетей DarkNet (Tor, I2P).
- Контроль использования некорпоративного DNS.
- Выявление использования программного обеспечения, предназначенного для загрузки пиратского контента (Torrent).
- Обнаружение сетевых протоколов на нестандартных портах.
- Выявление майнинга.
- И прочие.

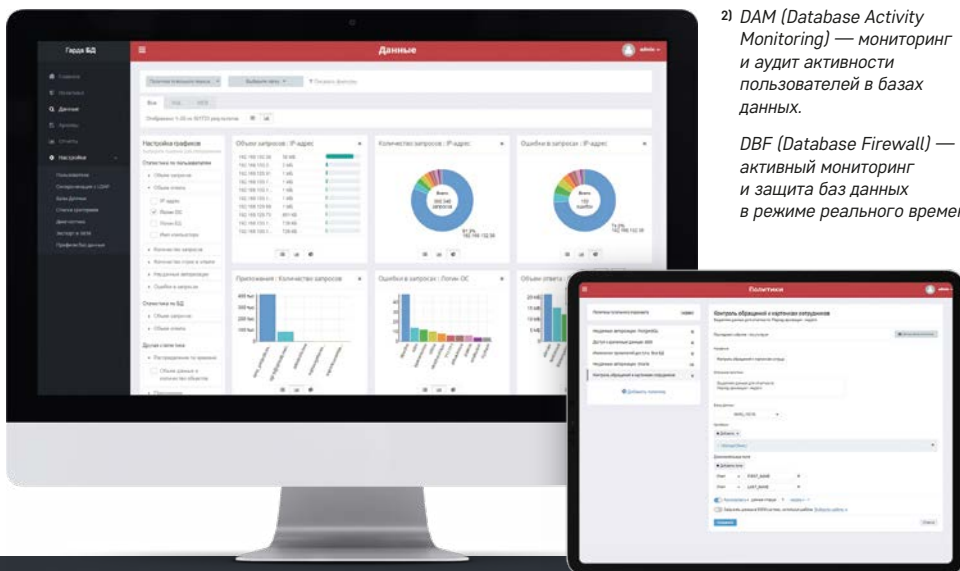
3) NTA (Network Traffic Analysis) — анализ сетевого трафика)

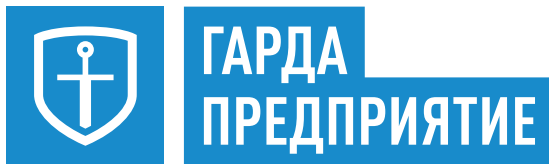


### Соответствует требованиям

Гарда Монитор обеспечивает выполнение требований следующих нормативно-правовых документов:

- 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;
- 152-ФЗ «О персональных данных»;
- 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».
- Входит в реестр отечественного ПО.





## Система обеспечения информационной безопасности и защиты от утечек конфиденциальных данных. Решение совмещает в себе классические инструменты DLP<sup>4</sup> и мощные аналитические возможности.

Система контролирует выполнение политик безопасности, прогнозирует потенциальные каналы утечки информации и выявляет отклонения от типовых шаблонов поведения сотрудников.

### Функциональные возможности

- Контроль сетевых каналов коммуникаций
- Автоматическая блокировка инцидентов
- Централизованное управление сетью из отдельно стоящих DLP-систем, распределенных по филиалам компании
- Контроль рабочих мест сотрудников (интернета, печати, съемных носителей, VoIP-телефонии, Skype, Viber и др.)
- Контроль рабочего времени сотрудников

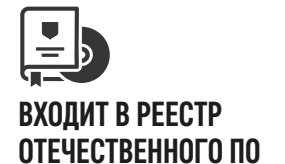
### Примеры решаемых задач

- Выявление фактов хищения и несанкционированного распространения данных.
- Обнаружение фактов несанкционированной отправки информации, относящейся к коммерческой тайне.
- Выявление сговоров сотрудников, с целью осуществления каких-либо противоправных либо мошеннических действий.
- Выявление фактов нецелевого использования сотрудниками рабочих ресурсов компании (поиск работы, посещение развлекательных сайтов, онлайн-игр и т.п.).
- Выявление фактов использования сотрудниками различного программного обеспечения, не относящегося к выполнению служебных обязанностей (торрент клиенты, VPN клиенты, программы удаленного доступа, игры и т.п.).
- Выявление фактов использования сотрудниками различных облачных хранилищ и файлообменных сервисов для хранения и передачи служебной информации.
- Контроль либо блокировка использования сотрудниками съемных устройств для хранения и передачи служебной информации.
- Выявление фактов переписки сотрудников с конкурентами (через почту, социальные сети, мессенджеры).

### Соответствует требованиям следующих нормативно-правовых документов:

- 152-ФЗ «О персональных данных»;
- 98-ФЗ «О коммерческой тайне»;
- ФСТЭК России принял решение о сертификации системы «Гарда Предприятие»;
- Входит в реестр отечественного ПО.

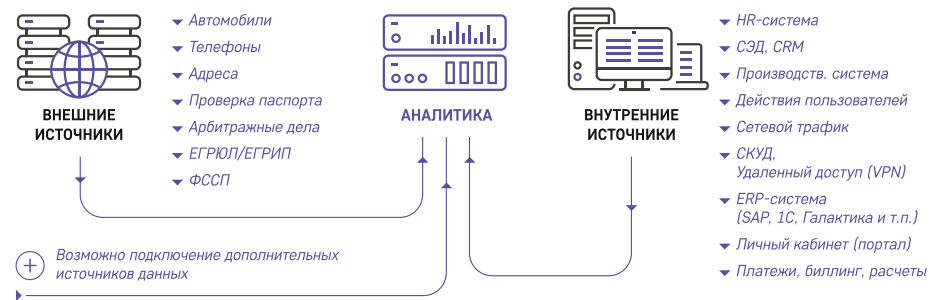
<sup>4</sup> DLP (Data Loss Prevention) — защита от утечки информации)



## Платформа информационной и экономической безопасности, обеспечивает глобальную видимость информации и открывает новые возможности для построения комплексных систем безопасности.

### Функциональные возможности

- Динамическое обогащение данных
- Выявление отклонений в поведении людей или устройств
- Построение явных и скрытых связей
- Объединение различных технологий анализа данных в одном инструменте



### Глобальная видимость информации

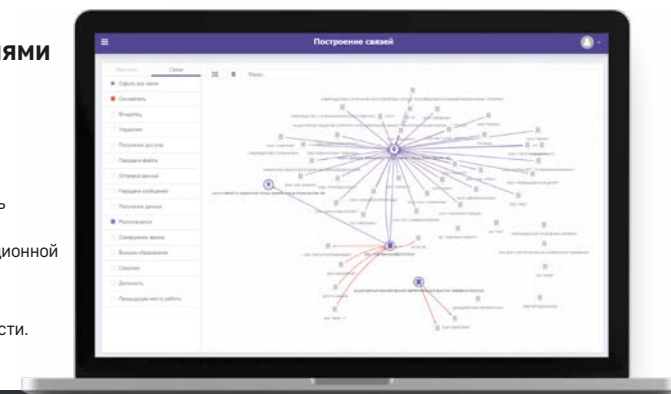
- Контролирует индикаторы риска и угрозы безопасности.
- Предупреждает о риске наступления инцидентов.
- Позволяет создавать библиотеки инцидентов и пополнять их новыми факторами рисков.
- Обогащает данные информацией из внешних и внутренних источников.
- Предоставляет инструментарий для расследования инцидентов.
- Анализирует данные, наполняет их смысловой информацией.
- Выявляет отклонения в бизнес-процессах организации.
- Сохраняет все факты коммуникаций организации.

### Примеры решаемых задач

- Оперативная оценка клиента, сотрудника, контрагента, создание информационной базы/досье.
- Поиск связи между группой подозреваемых через промежуточные «узлы» в почте/мессенджерах/соц.сетях и др.
- Транзакционный и телекоммуникационный фрод.
- Анализ финансовых операций.
- Контроль платежей и переводов, выявление фактов отмывания денег.
- Контроль закупочной деятельности (выявление конфликта интересов, родственных связей).
- Мошенничество при производстве и сбыте.
- Контроль целостности и защита критичных данных в информационных системах.
- Построение профилей устройств и пользователей, выявление аномалий.
- Обнаружение атак, заражений и теневых информационных технологий в сети.
- Контроль действий привилегированных пользователей в информационных системах.

### Гарда Аналитика совместима с решениями информационной безопасности линейки Гарда

- Позволяет оперативно создавать всесторонний комплекс защиты организации от угроз информационной и экономической безопасности.
- Минимизирует затраты на внедрение систем безопасности.





# ГАРДА ТЕХНОЛОГИИ

[gardatech.ru](http://gardatech.ru)

[info@gardatech.ru](mailto:info@gardatech.ru)

«Гарда Технологии» — российский разработчик систем информационной безопасности. Команда разработчиков обладает многолетним опытом в сфере информационных технологий и создает решения для различных задач безопасности.

Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.

«Гарда Технологии» осуществляет комплексное внедрение и последующую поддержку систем информационной безопасности:

- аудит информационных ресурсов компании;
- адаптация системы под потребности бизнеса;
- техническая поддержка;
- обучение персонала;
- послегарантийное обслуживание.



Опыт разработки систем высокой сложности с 2005 года.



Решения по информационной безопасности внесены в реестр отечественного ПО и соответствуют требованиям регуляторов.



Более 180 высококвалифицированных специалистов.



Собственная технологическая платформа.

**СВЯЖИТЕСЬ С НАМИ, ЧТОБЫ ЗАПРОСИТЬ  
ДЕМОНСТРАЦИЮ ИЛИ ЗАКАЗАТЬ БЕСПЛАТНЫЙ  
ПИЛОТНЫЙ ПРОЕКТ ПРОДУКТОВ «ГАРДА ТЕХНОЛОГИИ»**

## Нижний Новгород

проспект Гагарина, д. 50, корп. 9  
8 (831) 422 12 21

## Москва

Мичуринский проспект, дом 27, корп.5  
8 (495) 540 05 27