



**ГАРДА
БД**



ГАРДА
ТЕХНОЛОГИИ

ГАРДА БД

АУДИТ И ЗАЩИТА БАЗ ДАННЫХ И ВЕБ-ПРИЛОЖЕНИЙ

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

**«ГАРДА БД» ОБЕСПЕЧИВАЕТ БЕЗОПАСНОСТЬ СУБД
И НЕЗАВИСИМЫЙ АУДИТ ОПЕРАЦИЙ
С БАЗАМИ ДАННЫХ И БИЗНЕС-ПРИЛОЖЕНИЯМИ**



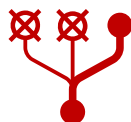
Защита от утечек информации,
хранящейся в БД.



Аудит всех операций с БД
в режиме реального времени.



Контроль действий
привилегированных пользователей



Контроль удаленного доступа
сотрудников



Выявление и предотвращение попыток
внешнего вторжения в СУБД



Блокирование нежелательных запросов
к БД и веб-приложениям



Обнаружение всех БД в компании,
их классификация и сканирование на уязвимости



ГАРДА
БД

ГАРДА
ТЕХНОЛОГИИ

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 передаче (например при их клонировании для целей тестирования)
- Разграничение доступа к СУБД для аттестации информационных систем
- Выявление не оптимально настроенных конфигураций СУБД с точки зрения стандартов и лучших практик по информационной безопасности
- Предотвращение мошенничества и прямых хищений денежных средств с использованием БД и бизнес-приложений компании
- Выявление несанкционированного разворачивания теневых, нелегитимных и неконтролируемых баз данных со стороны администраторов
- И другие



ГАРДА
БД

ГАРДА
ТЕХНОЛОГИИ

ОТ КОГО НУЖНО ЗАЩИЩАТЬСЯ?

БАЗЫ ДАННЫХ — ОСНОВНОЙ ИСТОЧНИК НАИБОЛЕЕ ЦЕННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИИ. КРОМЕ ВЛАДЕЛЬЦЕВ ДАННЫХ ЭТА ИНФОРМАЦИЯ ИНТЕРЕСУЕТ МНОЖЕСТВО ДРУГИХ ЛЮДЕЙ.

ИНСАЙДЕРЫ



Хищения информации сотрудниками с целью продажи конкурентам или использования на новом месте работы.

ХАКЕРЫ



Целенаправленные атаки на базы данных для получения доступа к ним.

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ



Контроль действий администраторов баз данных, контрагентов

ХАЛАТНОСТЬ



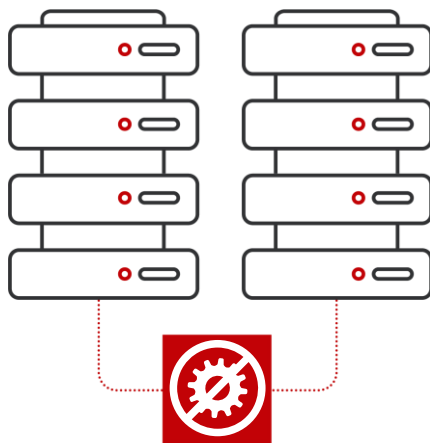
Случайные утечки данных, совершенные по неосторожности.



ПОМОГУТ ЛИ ШТАТНЫЕ СРЕДСТВА КОНТРОЛЯ?



**ИСПОЛЬЗОВАНИЕ ШТАТНЫХ СРЕДСТВ
АУДИТА БАЗ ДАННЫХ ВЛЕЧЁТ ЗА СОБОЙ
ДОПОЛНИТЕЛЬНЫЕ ЗАТРАТЫ
И НЕ ОБЕСПЕЧИВАЕТ
ПОЛНОГО КОНТРОЛЯ**



- ☒ Требуют постоянного ручного контроля и специфических знаний пользователя
- ☒ Существенно снижают производительность СУБД (10-40%)
- ☒ Отсутствие контроля привилегированных пользователей
- ☒ Невозможность блокировки действий пользователей
- ☒ Нет идентификации пользователя в трёхзвенной архитектуре
- ☒ Отсутствие механизмов реагирования при нарушении
- ☒ Невозможность расследования инцидента при нарушении работоспособности самой СУБД

ПРИНЦИП РАБОТЫ



Анализ сетевого трафика с возможностью мониторинга или блокировки нелегитимных запросов пользователей и получаемых данных из СУБД



Обработка данных и долгосрочное хранение всех запросов и ответов для ретроспективного анализа



Автоматический поиск новых СУБД, не стоящих на контроле, классификация их по типу хранимых данных



Сканирование баз данных, находящихся под контролем,



Аналитическая отчетность и поведенческий анализ (UBA), выявление нарушений политик безопасности



Система оповещения уведомляет о событиях по электронной почте, передает данные во внешние SIEM-системы, отображает отчеты на главном экране



ГАРДА
БД

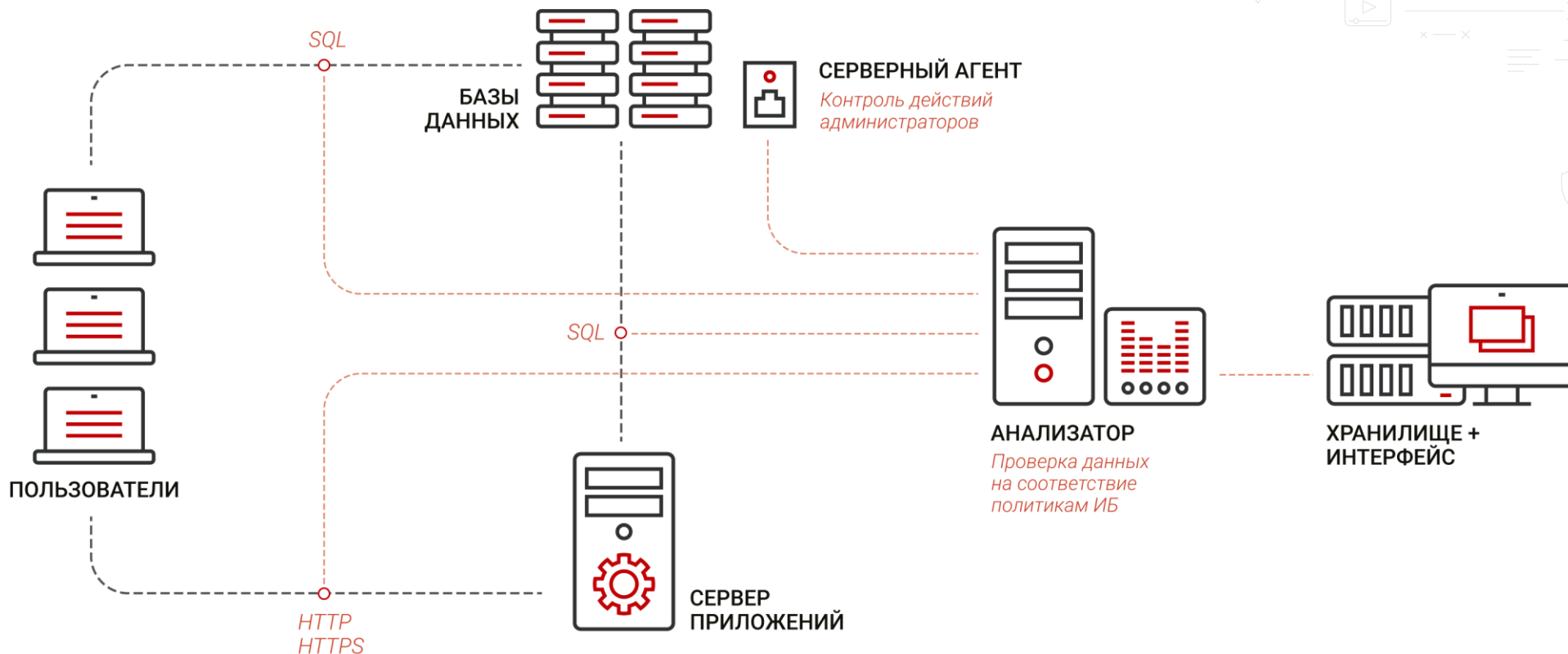
ГАРДА
ТЕХНОЛОГИИ

СХЕМА ИНТЕГРАЦИИ В СЕТЬ ЗАКАЗЧИКА



ГАРДА
БД

ГАРДА
ТЕХНОЛОГИИ



ОПЦИОНАЛЬНО

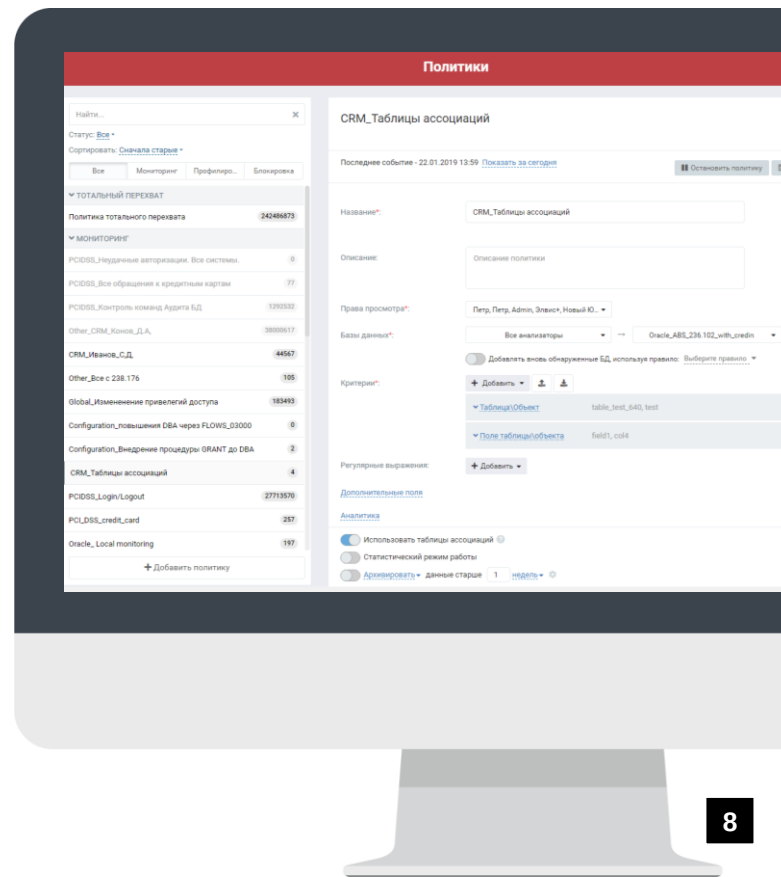
Агенты для контроля локальных подключений

ПОЛИТИКИ БЕЗОПАСНОСТИ

ПРАВИЛА РАБОТЫ СИСТЕМЫ ЗАДАЮТСЯ В КОНСТРУКТОРЕ ПОЛИТИК БЕЗОПАСНОСТИ

- ✓ Большой выбор критериев и их объединений.
- ✓ Предустановленные шаблоны регулярных выражений (персональные данные, банковские карты и т.д.).
- ✓ Синхронизация с LDAP – возможность обогащения перехваченной информации.
- ✓ Экспорт результатов работы политик в SIEM.
- ✓ Архивация перехваченных данных по конкретной политике.
- ✓ Политики блокировки позволяют предотвращать нежелательные операции с СУБД
- ✓ Список предустановленных политик ИБ:

- Помогают в регулярных задачах ИБ
- Закрывают требования регуляторов
- Эффективно защищают БД «из коробки»



КРИТЕРИИ ФОРМИРОВАНИЯ ПОЛИТИК

- ☒ IP-адрес клиента
- ☒ Имя пользователя в БД
- ☒ Имя пользователя в ОС
- ☒ Название клиентского ПО
- ☒ Результат аутентификации
- ☒ Дата/время запроса

- ☒ Запрашиваемые/передаваемые поля таблицы, синонимы, представления
- ☒ Объём данных ответа/запроса
- ☒ Имя объекта БД
- ☒ Ключевое слово
- ☒ Тип SQL-команды
- ☒ Количество записей в ответе



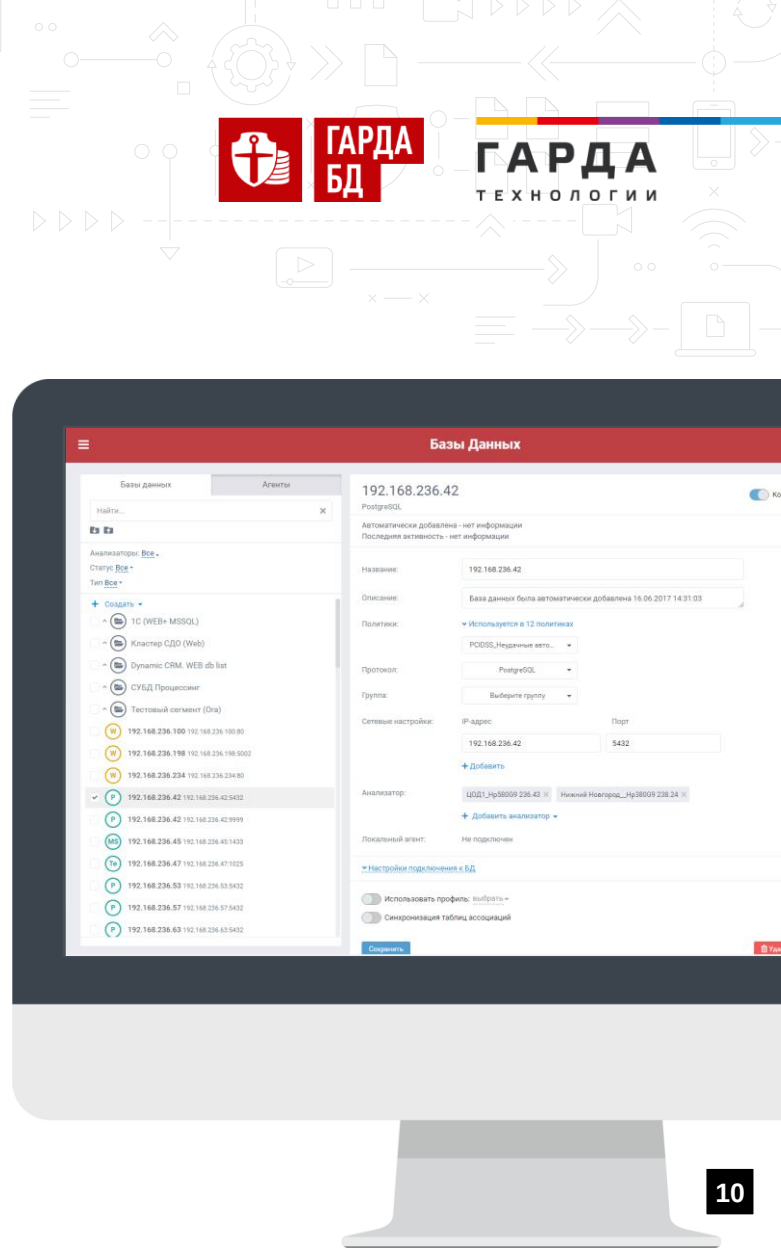
ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ БД

**СИСТЕМА АВТОМАТИЧЕСКИ НАХОДИТ НОВЫЕ БД,
НЕ СТОЯЩИЕ НА КОНТРОЛЕ,
И КЛАССИФИЦИРУЕТ ИХ ПО ТИПУ ХРАНИМЫХ ДАННЫХ
(НАПРИМЕР, ВЫЯВЛЯЕТ ПЕРСОНАЛЬНЫЕ ДАННЫЕ).**

На основе типа данных «Гарда БД» автоматически сформирует политики ИБ для новой базы данных.

Постановка на контроль также может осуществляться автоматически.

- Всегда актуальный перечень СУБД компании.
- Обнаружение новых БД (создание новых ИС/АС).
- Выявление открытия новых портов, изменения IP-адресов СУБД.
- Контроль обезличенности баз данных компании



СКАНИРОВАНИЕ БАЗ ДАННЫХ

**«ГАРДА БД» ПРОВОДИТ СКАНИРОВАНИЕ
КОНТРОЛИРУЕМЫХ БАЗ ДАННЫХ.**

**ЭТО ПОЗВОЛЯЕТ РЕШАТЬ ЗАДАЧИ, СВЯЗАННЫЕ
НЕ ТОЛЬКО С КОНТРОЛЕМ ДОСТУПА,
НО И С НЕКОРРЕКТНЫМИ НАСТРОЙКАМИ БЕЗОПАСНОСТИ**

КЛАССИФИКАЦИЯ



Поиск местонахождения
критичной информации

Создание политик по
результатам сканирования

Настройка уровня угроз

УЯЗВИМОСТИ



Неустановленные обновления

Проверка оптимальности
конфигурации СУБД

База проверок на уязвимости

МАТРИЦЫ ДОСТУПА



Построение карты доступа
вида «Пользователь – Объект
доступа (таблицы ,функции) –
Типа прав доступа»

Сравнение текущей картины
с эталонной



КОНТРОЛЬ И АНАЛИТИКА

ВСТРОЕННЫЕ СРЕДСТВА АНАЛИТИКИ ПОЗВОЛЯЮТ ВЫЯВЛЯТЬ ОТКЛОНЕНИЯ В ОБЫЧНЫХ СЦЕНАРИЯХ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ БД И ПРЕДОСТАВЛЯЮТ НАГЛЯДНЫЕ СТАТИСТИЧЕСКИЕ ОТЧЕТЫ.



Интерактивная отчётность



Конструктор отчётов с возможностью анализа любого объёма данных за любой промежуток времени



Возможность создания индивидуального дашборда



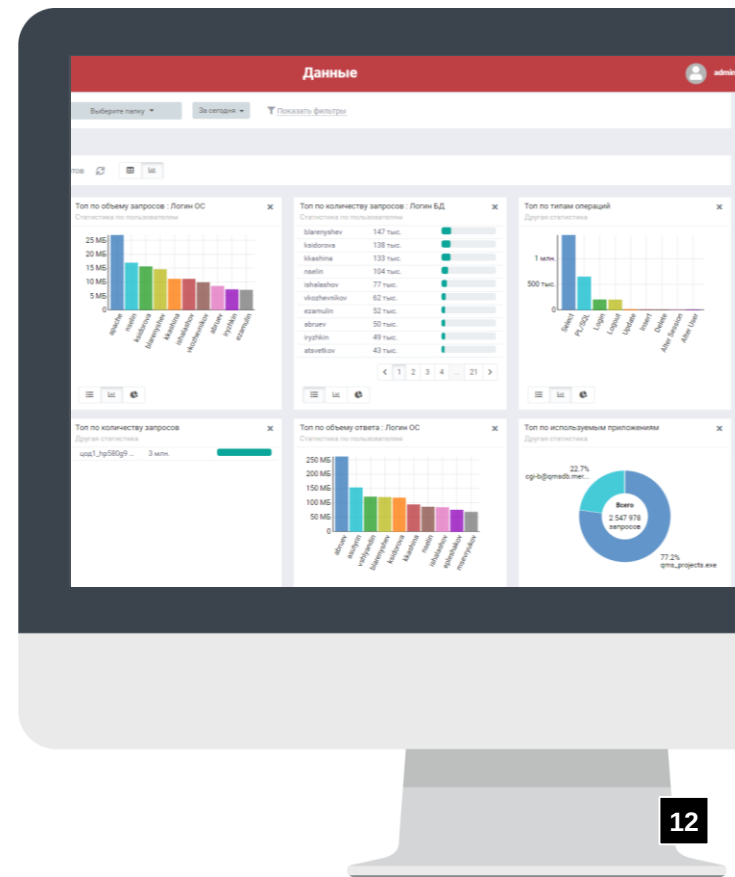
Поведенческий анализ пользователей БД (UEBA)



Уведомление о нарушениях по электронной почте



Уведомление о выявленных аномалиях в SIEM



СЕТЕВОЙ ЭКРАН

БЛОКИРУЕТ НЕЖЕЛАТЕЛЬНЫЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ, ПРОТИВОРЕЧАЩИЕ ПОЛИТИКАМ БЕЗОПАСНОСТИ.

Умная система самообучения анализирует деятельность операторов БД для предотвращения ложных срабатываний. Для гарантирования доступности защищаемых баз данных сетевой экран ставится в режиме отказоустойчивого кластера.

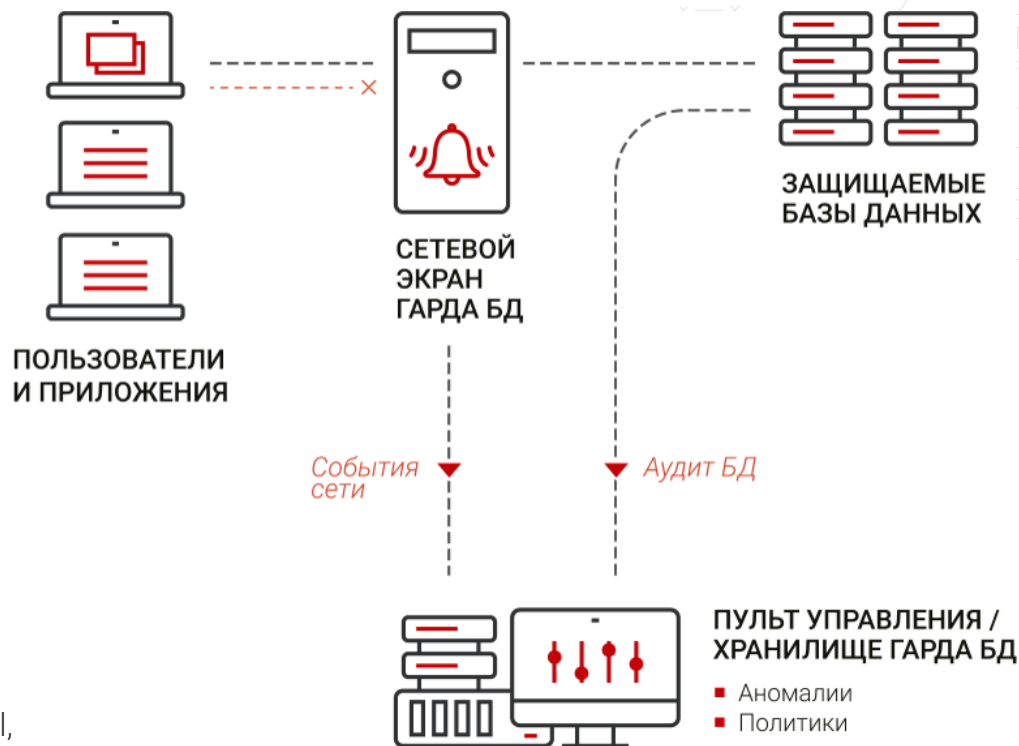
- ☒ Возможность дешифрации HTTPS-трафика по принципу Man In the middle (MITM)
- ☒ Возможность реализации системы разграничения прав доступа к СУБД для аттестации ИС, использующих несертифицированные СУБД



Блокировка реализуется по принципу L3 Reverse Proxy Firewall, обеспечивается повышенная отказоустойчивость.



Гибкий конструктор политик и блокировки по правилам на агенте предотвращают утечку данных с уведомлениями о заблокированных сессиях в интерфейсе системы.



ГАРДА
БД

ГАРДА
ТЕХНОЛОГИИ

ЗЕРКАЛИРОВАНИЕ ТРАФИКА

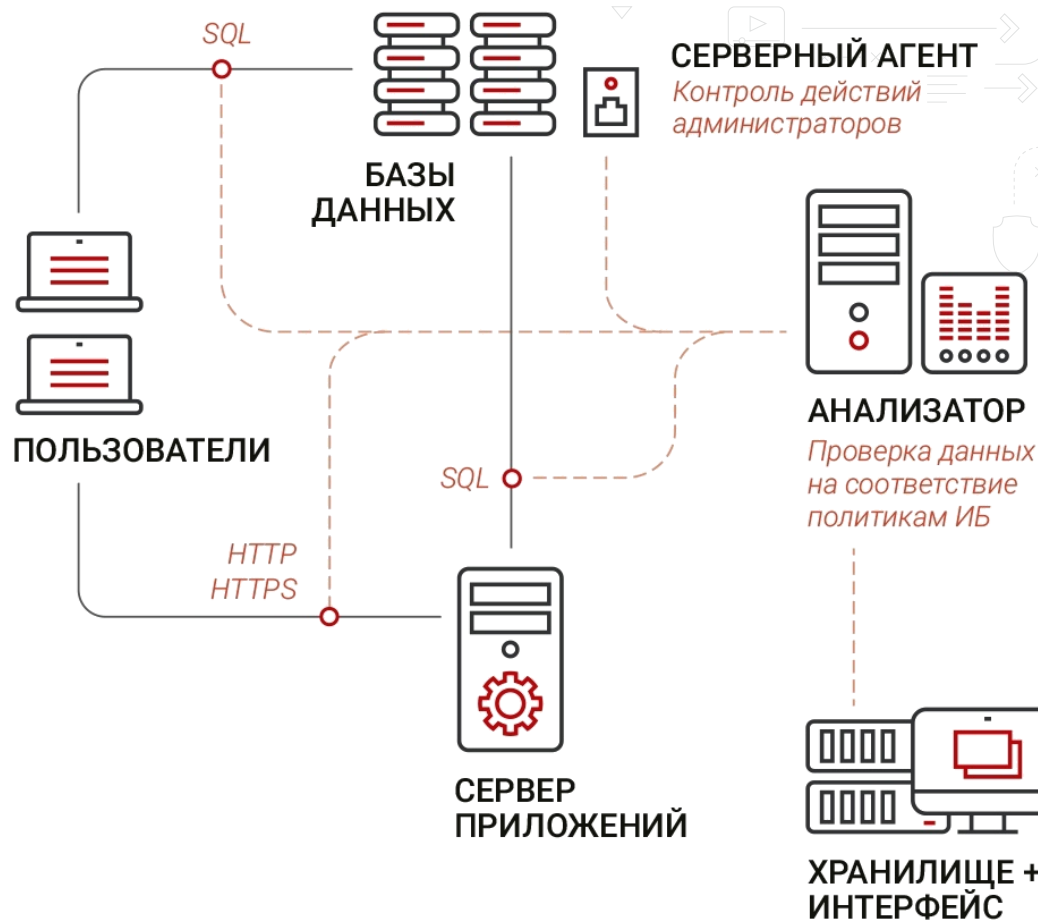
**ПРИМЕНЯЕТСЯ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ,
КОТОРЫЕ ОБРАЩАЮТСЯ К БД НАПРЯМУЮ
ИЛИ ЧЕРЕЗ ТРЕХЗВЕННЫЕ ПРИЛОЖЕНИЯ.**

**ИСПОЛЬЗУЮТСЯ АГЕНТЫ ДЛЯ КОНТРОЛЯ
ЛОКАЛЬНЫХ ПОДКЛЮЧЕНИЙ
ЛИБО ПЕРЕНАПРАВЛЕНИЯ ВСЕГО
СЕТЕВОГО ТРАФИКА К БАЗАМ ДАННЫХ.**



ГОРИЗОНТАЛЬНОЕ МАСШТАБИРОВАНИЕ

Позволяет защищать высоконагруженные,
в том числе территориально-
распределенные системы
любого масштаба
из единого интерфейса



ГАРДА БД: ЗАЩИТА «БОЛЬШИХ ДАННЫХ»

ГАРДА БД ОБЕСПЕЧИВАЕТ ЗАЩИТУ **BIG DATA**:
РЕЛЯЦИОННЫХ (ХРАНЯТСЯ В ТАБЛИЦАХ),

НЕ РЕЛЯЦИОННЫХ (ХРАНЯТСЯ В СПЕЦИАЛЬНЫХ КЛАСТЕРНЫХ
ХРАНИЛИЩАХ С ВОЗМОЖНОСТЬЮ РАСПРЕДЕЛЕННОЙ ОБРАБОТКИ).



Журнал данных. Возможность группировки данных по времени – логинам - приложениям и другим свойствам



Контролируем доступ к любым Big Data системам через Rest API



Полностью поддерживаем протокол HTTP до уровня данных



Поддержка Hortonworks Data Platform



Унифицируем подходы к защите реляционных и NoSQL баз данных

ЗАЩИТА BIG DATA

- Контроль доступа к Big Data системам через Rest API
- Поддержка протокола http/https
- Поддержка Hortonworks Data Platform
- Унификация подходов к защите реляционных и NoSQL баз данных
- Профиль учитывает особенности работы каждого сотрудника

ДАННЫЕ ВАШЕЙ КОМПАНИИ ЯВЛЯЮТСЯ BIG DATA, ЕСЛИ ОНИ:

- ✓ Занимают большой объём >100 Тб
- ✓ Слабо структурированы
- ✓ Приходят из множества источников
- ✓ Должны обрабатываться в режиме реального времени
- ✓ Растут в размере хранения более чем на 50% в год



ДИНАМИЧЕСКОЕ ПРОФИЛИРОВАНИЕ (UEBA)



ГАРДА
ТЕХНОЛОГИИ



Встроенные средства аналитики позволяют выявлять отклонения от обычных сценариев работы пользователей БД и формируют наглядные отчёты по инцидентам.

АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ ПРОФИЛЕЙ В РЕЖИМЕ ОБУЧЕНИЯ



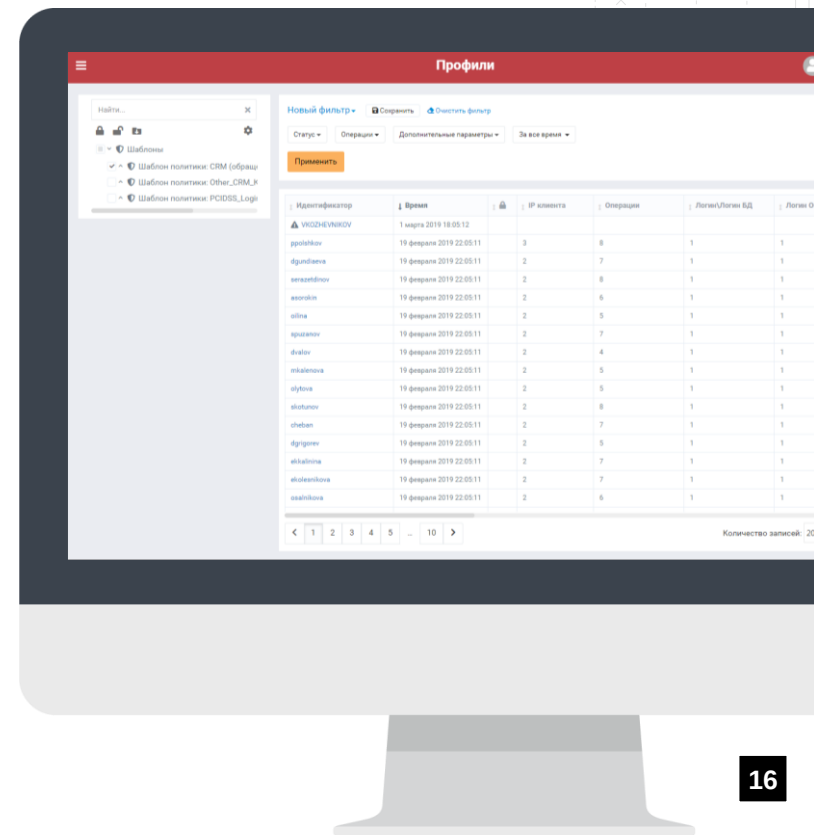
Учитываются:

- Логины, приложения, IP-адреса, названия таблиц и полей
- Особенности работы каждого сотрудника
- Информация о регионе

ВЫЯВЛЕНИЕ ОТКЛОНЕНИЙ ОТ ПРОФИЛЕЙ



- Нетипичное поведение для данного пользователя
- (Чужие IP-адреса, ранее не используемые таблицы, приложения и рабочие места);
- Статистические аномалии
 - Большое количество запросов
 - Большие выгрузки
 - Много неуспешных авторизаций



КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ И 1С

КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ

- Детальный разбор HTTP/HTTPS-трафика с выделением данных из веб-форм
- Возможность дешифрации HTTPS-трафика как в пассивном, так и в режимах работы «вразрыв»
- Персонализация пользователей с возможностью выделения учетных записей
- По протоколам передачи данных HTTP/HTTPS
- По протоколам аутентификации Kerberos, NTLM
- Аутентификация (web form authentication)
- Детальный разбор http/https-трафика с выделением данных из веб-форм

МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ 1С

Служба информационной безопасности в интерфейсе системы видит не только обращения к СУБД, но и все **пользовательские действия**, позволяющие понимать, какая информация, находящаяся в системе 1С, была модифицирована, а к какой были обращения со стороны пользователей, с привязкой к учётным записям.



ЗАЩИТА ОТ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ

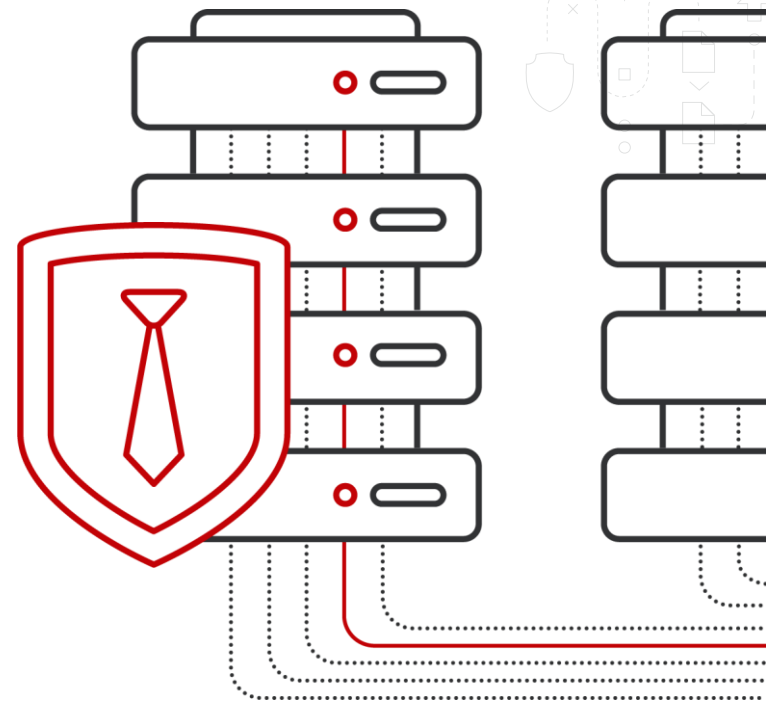
МОДУЛЬ «СЕРВЕРНЫЙ АГЕНТ»

- Позволяет протоколировать и/или блокировать действия на сервере БД
- Не оказывает существенного влияния на серверы баз данных
- Позволяет контролировать изменение конфигурационных файлов СУБД



Инновационные технологии «Гарда Технологии» позволили минимизировать влияние серверного агента на сервер.

Поддерживаются ОС семейства
Redhat, AIX, Windows Server, Solaris, Suse



ОСОБЕННОСТИ РЕШЕНИЯ



Возможность ретроспективного анализа по сохраненным данным объемом свыше 100 ТБ



Аудит доступа к БД всех филиалов компании из единого центра



Интеграция со всеми популярными SIEM



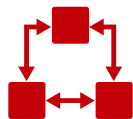
Интерактивные отчеты и понятная аналитика на основе всех запросов и ответов БД, статистика инцидентов



Встроенная система выявления аномалий и поведенческого анализа действий пользователей



Возможность анализа трафика на скорости более 10 Гбит/с



Полноценная работа с трёхзвенной архитектурой взаимодействия с БД



Минимальное влияние на производительность сети и серверов СУБД



Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени



Отсутствие стороннего лицензирования



ГАРДА
БД

ГАРДА
ТЕХНОЛОГИИ

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Более 30 поддерживаемых российских и зарубежных СУБД, в том числе на технологиях BigData
- Поддержка распределённой кластерной инсталляции и централизованного управления из единого интерфейса
- Множество способов подачи трафика (агенты, подача данных с TAP-устройств/SPAN, GRE, ERSPAN)
- Высокая производительность (обработка 10ГБит/с и выше), неограниченная возможность кластеризации
- Сетевой экран с функцией блокировки и динамической балансировки трафика
- Возможность дешифрации HTTPS-трафика как в пассивном режиме, так и при инсталляции «вразрыв»
- Персонализация пользователей с возможностью выделения учетных записей
- Контроль привилегированных пользователей
- Гибко настраиваемые фильтры, автоматическое формирование списков критериев для использования в политиках
- Инцидент-менеджмент
- Сводные отчёты (в том числе отчёт по уязвимостям)
- Встроенный модуль контроля Web-приложений, не требующий отдельных лицензий
- Контроль неявных обращений к СУБД
- Динамическое профилирование (UEBA) с уведомлениями и отчётами
- Доменная авторизация



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ (ИТОГО)



АГЕНТСКИЕ РЕШЕНИЯ ПОД ПОПУЛЯРНЫЕ СУБД

- Агенты с функцией перенаправления трафика, контроля локальных подключений и блокировки доступа к СУБД под операционные системы Linux, Windows, AIX, Solaris и пр.

ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ БАЗ ДАННЫХ

- Автоматическое обнаружение новых баз данных. Реагирование на изменения настроек имеющихся баз
- Сканирование баз данных на наличие конфиденциальной информации, номеров кредитных карт, ИНН и пр.
- Проверка БД на обезличенность

СКАНИРОВАНИЕ НА УЯЗВИМОСТИ

- Активные предустановленные учетные записи
- Неустановленные патчи
- Учетные записи с простыми паролями
- Расширенные привилегии доступа к системным объектам СУБД

МОНИТОРИНГ В РЕАЛЬНОМ ВРЕМЕНИ

- Гибкий конструктор политик безопасности помогает осуществлять контроль и выявление потенциальных инцидентов в режиме реального времени
- Большой список предустановленных политик для часто решаемых задач безопасности

СИСТЕМА ОТЧЁТНОСТИ

- Детализированная отчетность по всем событиям безопасности и операциям пользователей СУБД
- Наличие базы предустановленных отчетов

УВЕДОМЛЕНИЕ О СОБЫТИИ

- SIEM
- Электронная почта
- Отчёт на главном экранеК

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ (ИТОГО)

УМНЫЙ ПОИСК

- Контентный — по запросам, ответам, переменным и регулярным выражениям (ИНН, номера карт и пр.).
- Атрибутивный — по IP-адресам, учетным записям, текстам ошибок и пр.

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

- Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени.
- Маскирование платёжных данных в хранилище

КОНТРОЛЬ БИЗНЕС-ПРИЛОЖЕНИЙ

- SAP Business Object
- Microsoft Dynamics CRM
- 1C
- Веб-формы
- Гибкие настройки для работы с любыми бизнес-приложениями на основе HTTP(s)-протоколов

КОНТРОЛИРУЕМЫЕ СУБД

- | | | |
|-----------------|---------------|-------------------|
| • Oracle | • IBM Netezza | • Interbase |
| • Microsoft SQL | • IBM DB2 | • Tarantool |
| • MySQL | • Линтер | • MongoDB |
| • SAP HANA | • Apache | • Kafka5 |
| • PostgreSQL | • Cassandra | • Hive5 |
| • Teradata | • Sun MySQL | • Ред База Данных |
| • Sybase ASE | • Firebird | • SPARK |

ПОДДЕРЖИВАЕМЫЕ ОС

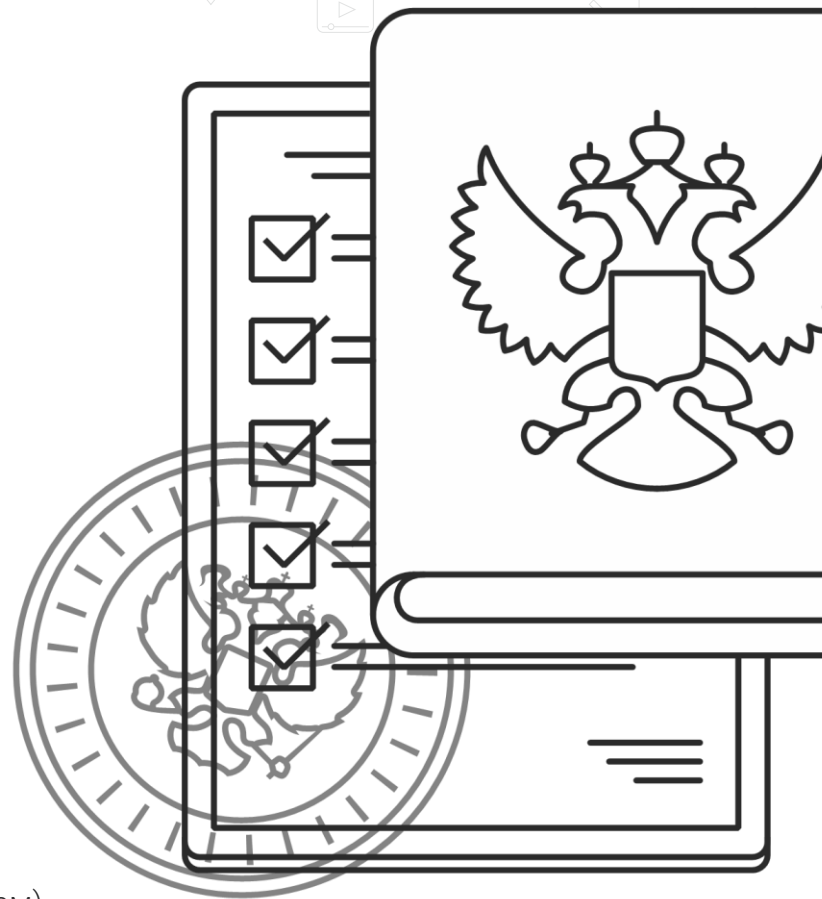
- | | |
|----------------------------|----------------------------|
| • OC Solaris | • OC Windows Server |
| • OC Ubuntu | • OC SUSE Enterprise Linux |
| • Red Hat Enterprise Linux | • AIX |
| • Oracle Enterprise Linux | |



СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

СИСТЕМА ПОМОГАЕТ ВЫПОЛНИТЬ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

- ☒ 8-ФЗ (Обеспечение доступа к информации гос. органов)
- ☒ 152-ФЗ (О персональных данных)
- ☒ 187-ФЗ (Безопасность объектов КИИ РФ)
- ☒ Приказ ФСТЭК №17 (Требования к защите информации в ГИС)
- ☒ Приказ ФСТЭК №21 (Обеспечение безопасности обработки ПДн)
- ☒ Приказ ФСТЭК №239 (Меры безопасности для значимых объектов КИИ)
- ☒ Приказ МинКомСвязи РФ №104 (Обеспечение безопасности для информационных систем общего пользования)
- ☒ ГОСТ Р 57580.1-2017 (Безопасность финансовых операций)
- ☒ СТО БР ИББС (Стандарт по обеспечению ИБ банков РФ)
- ☒ GDPR (Европейский регламент по защите ПДн)
- ☒ PCI DSS (Международный стандарт безопасности данных платежных систем)



ПОЛНОСТЬЮ РОССИЙСКОЕ РЕШЕНИЕ

СИСТЕМА КОНТРОЛЯ ВЕБ-ПРИЛОЖЕНИЙ И ДОСТУПА К БАЗАМ ДАННЫХ



- Разработка отечественного производителя
- Сертифицировано ФСТЭК на Соответствие ТУ, является СЗИ класса НДВ-4*
- Входит в реестр отечественного ПО
- Собственный исследовательский центр
- Квалифицированная русскоязычная техподдержка
- Запущена процедура ресертификации по новым требованиям доверия по уровню УД4



ГАРДА
ТЕХНОЛОГИИ



О РАЗРАБОТЧИКЕ



ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания обладает многолетним опытом в сфере информационных технологий и разрабатывает решения для различных задач безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.



100 +

Внедрений на территории России



180 +

Высококвалифицированных сотрудников



12 лет

Опыт разработки систем высокой сложности



5

запатентованных технологий собственного исследовательского центра



ПОЛНОСТЬЮ РОССИЙСКИЕ РЕШЕНИЯ

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий.
- Решения сертифицированы ФСТЭК.
- Включены в реестр отечественного программного обеспечения.



СПАСИБО ЗА ВНИМАНИЕ!



**ГАРДА
БД**



ГАРДА
ТЕХНОЛОГИИ

+7 (495) 540-05-27
+7 (831) 422 12-21
info @ gardatech.ru