Meridian DB Patrol

ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В ЮРИДИЧЕСКОЙ КОМПАНИИ

Политика конфиденциальности персональной информации

Юридическая компания в соответствии с законодательством Российской Федерации обязана обеспечивать режим конфиденциальности в отношении всей информации, получаемой от клиентов.

Что подлежит защите?

Компания обязана обеспечивать конфиденциальность персональной информации, к которой относятся:

I. Персональная информация о клиенте

ФИО, место жительства, реквизиты паспортов, семейное положение, номер телефона, адрес электронной почты.

II. Информация, полученная от клиентов

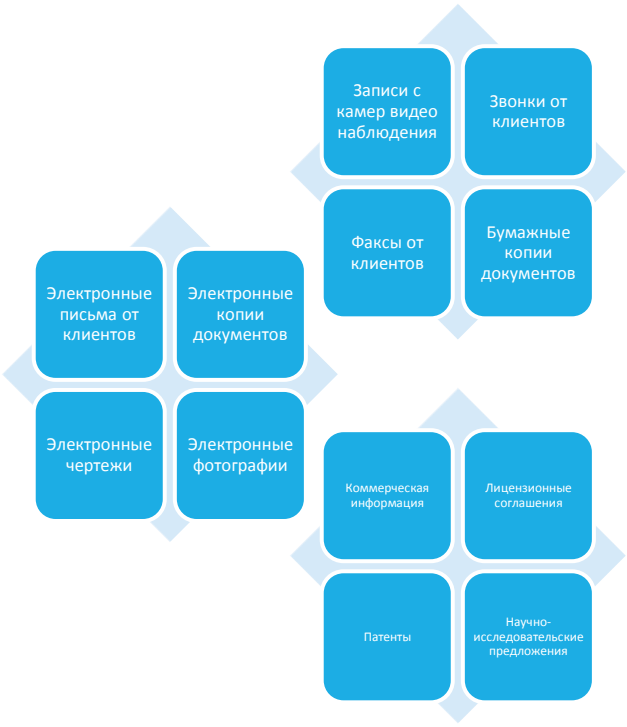
Бумажные документы, носители электронной информации, фотографии, чертежи.

III. Информация, представляющая потенциальный научный или коммерческий интерес

Лицензионные соглашения, патенты, договора, научно-исследовательские предложения.

IV. Факты обращения к услугам Компании

Обращения по телефону, через электронную почту, лично или иным способом.



Чем должна руководствоваться компания при защите персональных данных?

В соответствии с законодательством Российской Федерации юридическая компания ***обязана принимать необходимые и достаточные организационные и технические меры для защиты персональной информации клиента*** *от неправомерного или случайного доступа, уничтожения, копирования, распространения, а также от иных неправомерных действий с ней третьих лиц*

1. ФЗ РФ N152 от 27.07.2006г. (Закон "О персональных данных", статья 19. Меры по обеспечению безопасности персональных данных при их обработке)

2. ФЗ РФ N149 от 27.07.2006 г.(Закон "Об информации, информационных технологиях и о защите информации", статья 16. Защита информации)

3. ФЗ РФ N98 от 29.07.2004 г. (Закон "О коммерческой тайне", статья 10. Охрана конфиденциальности информации)

4. Постановление Правительства РФ от 01.11.2012г. №1119 "Об утверждении требования к защите персональных данных при их обработке в информационных системах"

Последствия утраты конфиденциальных (персональных) данных

I. Прямые потери

- Штрафы – 5 000 - 10 000 руб за 1 нарушение (ст. 13.11 КоАП РФ)
- Ответственность – гражданская, административная, вплоть до уголовной (ст. 137 УК РФ)
- Проверки – 1 801 плановая и 617 внеплановых проверок Роскомнадзора за 2013 год (http://rkn.gov.ru/personal-data/reports/)
- Убытки по NDA – утечка коммерческой тайны компании

II. Косвенные потери

- Репутационные потери – уход 1 клиента оборачивается потерей 40-80 клиентов (исследование http://soa.sys-con.com/node/2279242)
- Снижение конкурентоспособности – потеря клиентов, заинтересованных в защите персональной информации

Как защитить данные?

Организационные мероприятия

- Работа службы безопасности с персоналом;
- Организация внутриобъектового и пропускного режимов и охраны;
- Комплексное планирование мероприятий по защите информации.

Технические мероприятия

- Контроль прав доступа к конфиденциальной информации;
- Протоколирование действий пользователей;
- Предотвращение несанкционированного доступа и утечек данных.

Целесообразным решением является хранение персональной информации на выделенных серверах баз данных и перенос технических мероприятий защиты данных на уровень сервера баз данных.

Специализированная защита баз данных с помощью системы Meridian DB Patrol

Система **Meridian DB Patrol** предназначена для дополнительной защиты конфиденциальной информации поверх штатных средств разграничения доступа данных СУБД. Система **Meridian DB Patrol** обеспечивает:

I. Аудит работы с данными с клиентских рабочих мест в режиме реального времени
Система протоколирует все обращения пользователей к БД с рабочих мест

II. Контроль работы привилегированных пользователей
Система независима от IT департамента и может полностью контролироваться службой безопасности. В состав решения входит локальный агент, который отслеживает все локальные обращения к базе данных. Это не дает скрыть свою активность даже администратору БД.

III. Предотвращение утечки данных
За счет комплексного контроля сетевых и локальных интерфейсов утечка данных исключена.

VI. Формирование отчетности для обеспечения соблюдения требований
Система имеет в своем составе рабочее место офицера безопасности, которое позволяет в удобном графическом интерфейсе осуществлять настройку правил и политик и формировать отчеты.

V. Контроль прав доступа
Система позволяет обнаруживать факты изменения прав доступа на объекты базы данных.

IV. Обнаружение тематической активности при обращении к конфиденциальным данным
Система позволяет настроить шаблоны аудита по ключевым словам в целях обнаружения активности по определенной тематике в общей массе конфиденциальной информации. Например, можно выявить активность запросов по определенному лицу, организации, номерам телефонов и иным атрибутам конфиденциальной информации, которые хранятся в базе данных.

Схема подключения комплекса Meridian DB Patrol

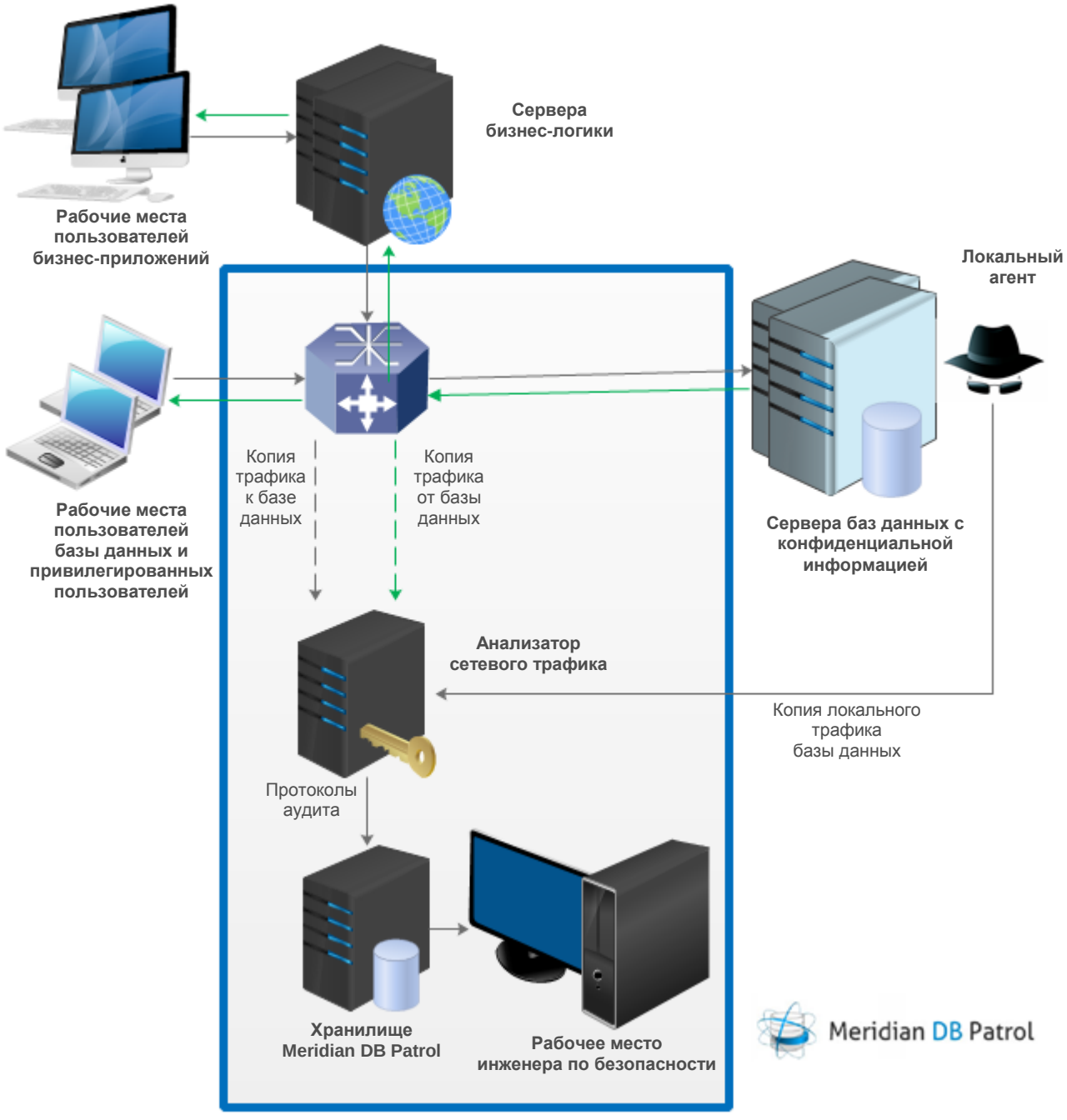
Система **Meridian DB Patrol** состоит из двух основных элементов:

I. Анализатор сетевого трафика (съемник)

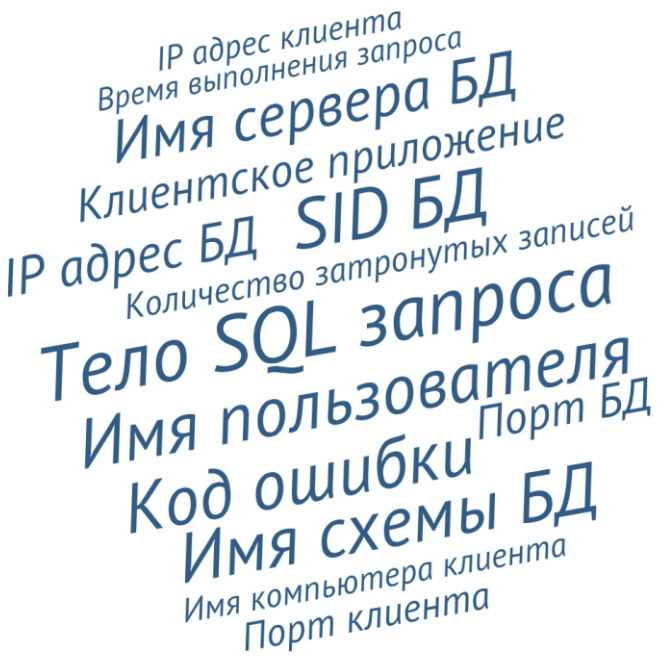
Съемник обеспечивает разбор и приведение к единому формату событий из протокола доступа к СУБД. Трафик копируется с точек концентрации на съемник с помощью программных (Cisco SPAN) или аппаратных (Network TAP) технологий.

II. Система хранения данных аудита

Система хранения и обработки данных включает в себя СУБД для хранения результатов анализа трафика и приложение, которое обрабатывает результаты и предоставляет инженеру по безопасности Web интерфейс для работы с системой.



Состав информации, накапливаемой в системе Meridian DB Patrol и доступной для анализа из web-интерфейса

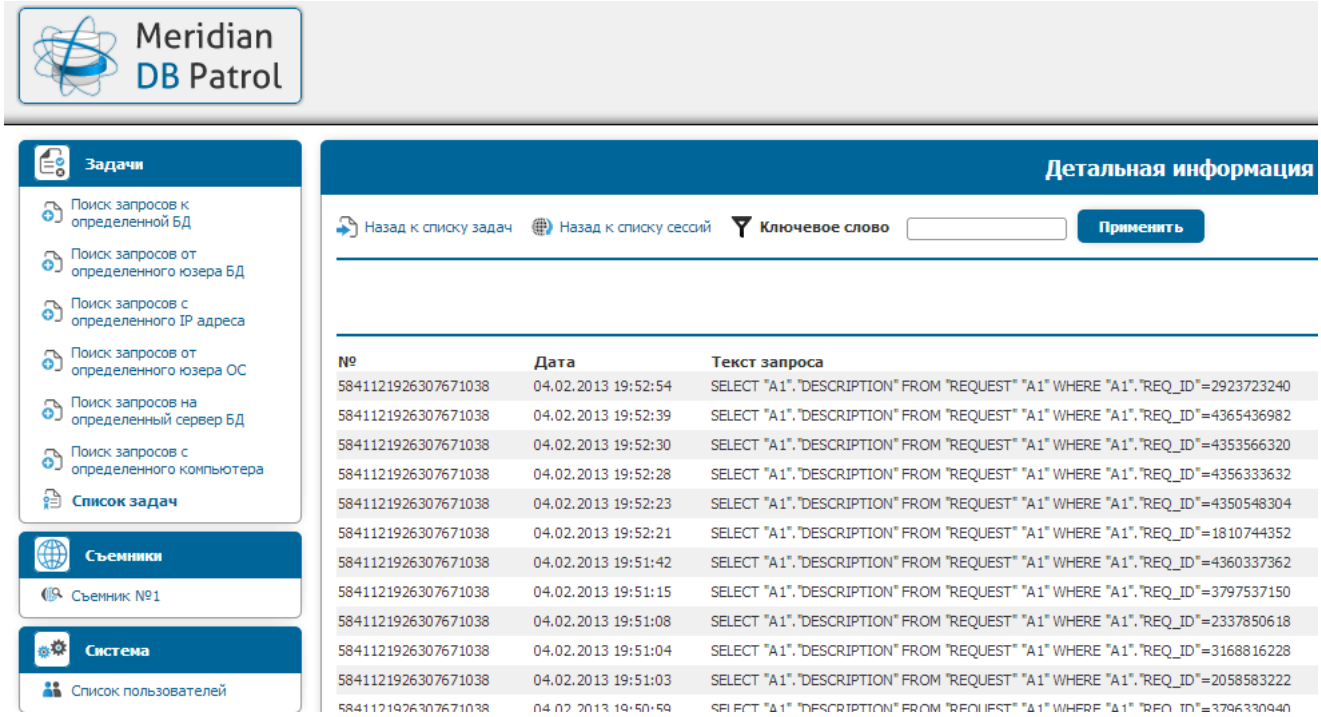


*Система **Meridian DB Patrol** обеспечивает протоколирование всех типов обращений к базе данных в режиме реального времени.*

*Система **Meridian DB Patrol** обладает гибкой настройкой критериев анализа для проведения аудита и разбора инцидентов по*

Пользовательский интерфейс системы Meridian DB Patrol

Система **Meridian DB Patrol** предоставляет пользователю удобный браузерный интерфейс, позволяющий создавать заявки на получение данных, выгружать отчеты в сертифицированном виде, просматривать результаты, управлять пользователями и многое другое.



Использование Meridian DB Patrol облегчает исполнение законодательства

ФЗ РФ N152 от 27.07.2006г.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

принятие необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении таких данных;

обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

установление правил доступа к персональным данным, обрабатываемых в информационной системе, а также обеспечение регистрации и учета всех действий, совершаемых с ними.

ФЗ РФ N149 от 27.07.2006 г.

Статья 16. Защита информации

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа;

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

своевременное обнаружение фактов несанкционированного доступа к информации.

ФЗ РФ N98 от 29.07.2004 г.

Статья 10. Охрана конфиденциальности информации

ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

Постановление Правительства РФ от 01.11.2012г. №1119

16. а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

Преимущества системы Meridian DB Patrol

Полнофункциональный аудит

- отслеживание обращений к базам данных с использованием SQL-запросов, хранимых процедур и функций, представлений, синонимов, заданий планировщика задач СУБД
- контроль всех обращений и операций с базой данных вплоть до полей данных, независимо от привилегий пользователя и вида приложения

Защита от привилегированных пользователей

- доступ к контролю действий привилегированных пользователей с базой данных, имеющих возможность локального доступа к серверу СУБД или доступа через службу удаленных рабочих столов
- запрет вмешательство в работу аудита со стороны администратора при удаленном доступе к базе данных

Производительность

- **высокая производительность съёма трафика:**
  - обработка трафика в секунду - 2 ГБ (2 * Ethernet 1000BaseT)
  - запросов в секунду на один съемник - 3000
  - одновременных сессий на один съемник - 20000
- **высокая производительность системы хранения**
  - объем загружаемых данных в сутки - до 100 Гб
  - общий объем хранения - до 2 Тб
  - возможность одновременной работы с системой нескольких инженеров по безопасности
- **отсутствие влияния на производительность защищаемой системы;**

Полнофункциональное рабочее место инженера по безопасности

- предоставление статистической информации по каждому обращению к БД (дата\время обращения, объем передаваемых данных, логин, IP-адрес и порт источника\приемника, название приложения и т.д.)
- построение статистических отчетов, ведение журналов событий

Клиентоориентированность

- возможность настройки комплекса под требования клиента
- комплексная техническая поддержка
- приемлемая стоимость

Свяжитесь с нами

Позвоните нам для получения дополнительной информации о наших услугах и продуктах.

Наш адрес:

123104, Москва, Трёхпрудный переулок 4, стр.1
+7 (495) 989-45-48
info@concerteza.ru
http://www.concerteza.ru/