МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»

Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: "Обзор решений(продуктов) для обеспечения безопасности баз данных"

Студентка ИВТ 22-17
Филимонова Ангелина
Научный руководитель
к.ф.-м.н., доцент

Цель

рассмотрение специализированных средств защиты информации в базах данных, их эксплуатация

ЗАДАЧИ

- Собрать общую информацию о специализированных средствах защиты информации в базах данных;
- Проанализировать и систематизировать информацию о готовых решениях;
- Развернуть и проэксплуатировать решение
- Выяснить, чем готовые решения лучше штатных средств защиты.

ОБЪЕКТ

- готовые решения для обеспечения безопасности баз данных

ПРЕДМЕТ

- анализ готовыхрешений от отечественного производителя

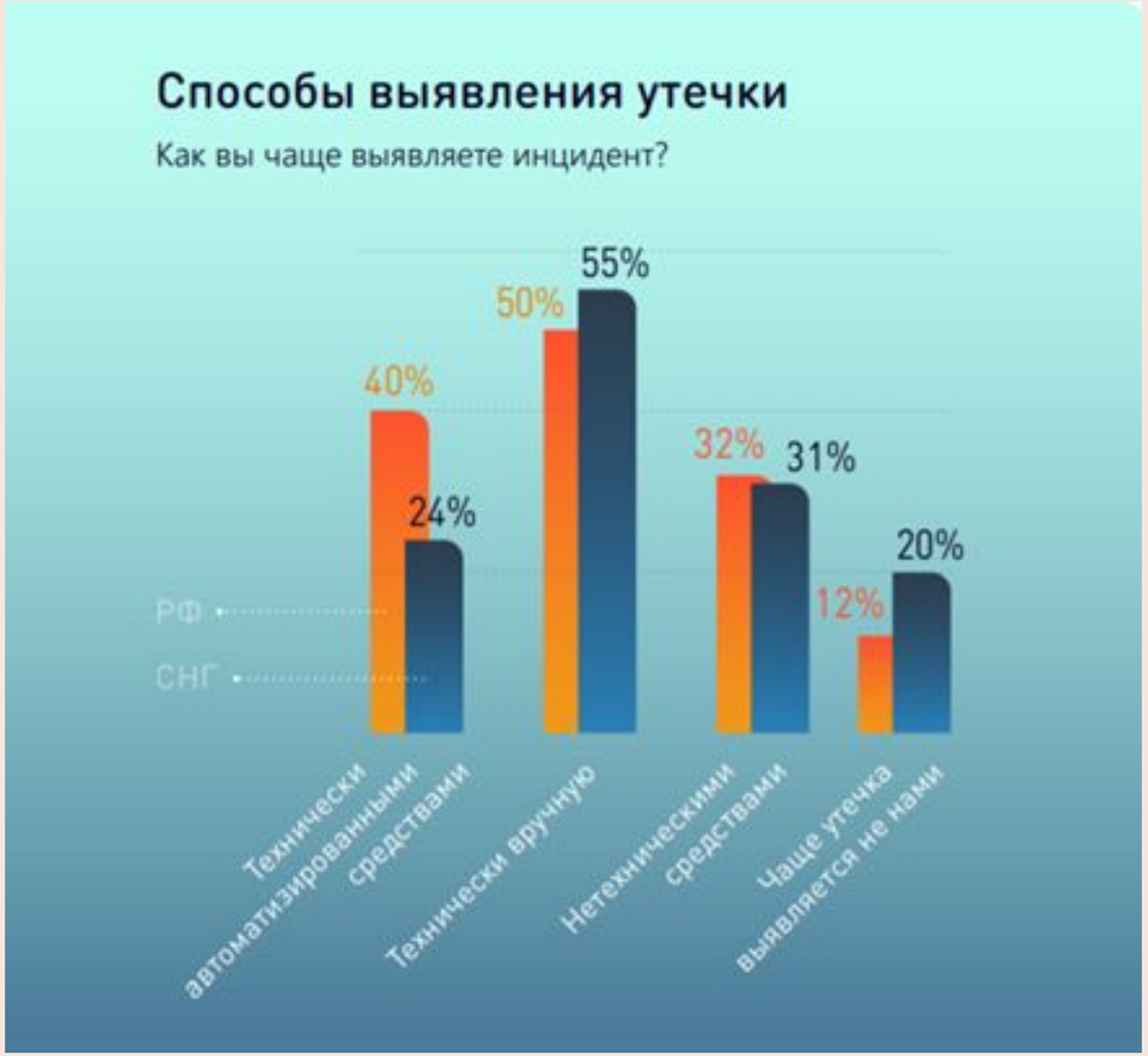
АКТУПЛЬНОСТЬ

обосновывается объемом фактов утечек важной информации, хранимой в базах данных и

СЗИ, используемые в российских компаниях и странах СНГ на 2020 год
DLP-системы это программные и программно-аппаратные средства для решения задачи предотвращение утечек данных
Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба.Решения класса DCAP (data-centric audit and protection) предназначены для обнаружения, категоризации и защиты т.н. «данных в покое». Й
IPS/IDS (Intrusion Prevention/Detection System) предназначаются, соответственно, для

Database Activity Monitoring (DAM) - **это технология безопасности базы данных для мониторинга и анализа активности, которая работает независимо от системы управления базами данных и не зависит от какой-либо формы внутреннего аудита или собственных журналов**

Леонид Чуриков, ведущий аналитик «СёрчИнформ»: « Интересно, как в инфобезе приживаются современные трендовые технологии. В 2020 году большинству компаний было не до внедрения новых инструментов, но организации демонстрируют интерес к ним. Компании видят в технологиях возможность снизить затраты на безопасность: автоматизировать контроль и сократить трудозатраты. Но главное – принципиально меняется запрос компаний: выявлять инцидент по факту совершения поздно, нужно предотвращать и предсказывать его. Это позволяют делать поведенческие технологии.»



Способы выявления утечек информации в российских компаниях и компаниях СНГ за 2020 год

помогаЮТ 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 обеспечение ИБ банков РФ)
·GDPR (Европейский регламент по защите ПДн)
·PCI DSS (Международный стандарт безопасности данных платежных систем)

DAM-решения на российском рынке

«ГАРДА БД»
Компания "Гарда Технологии"

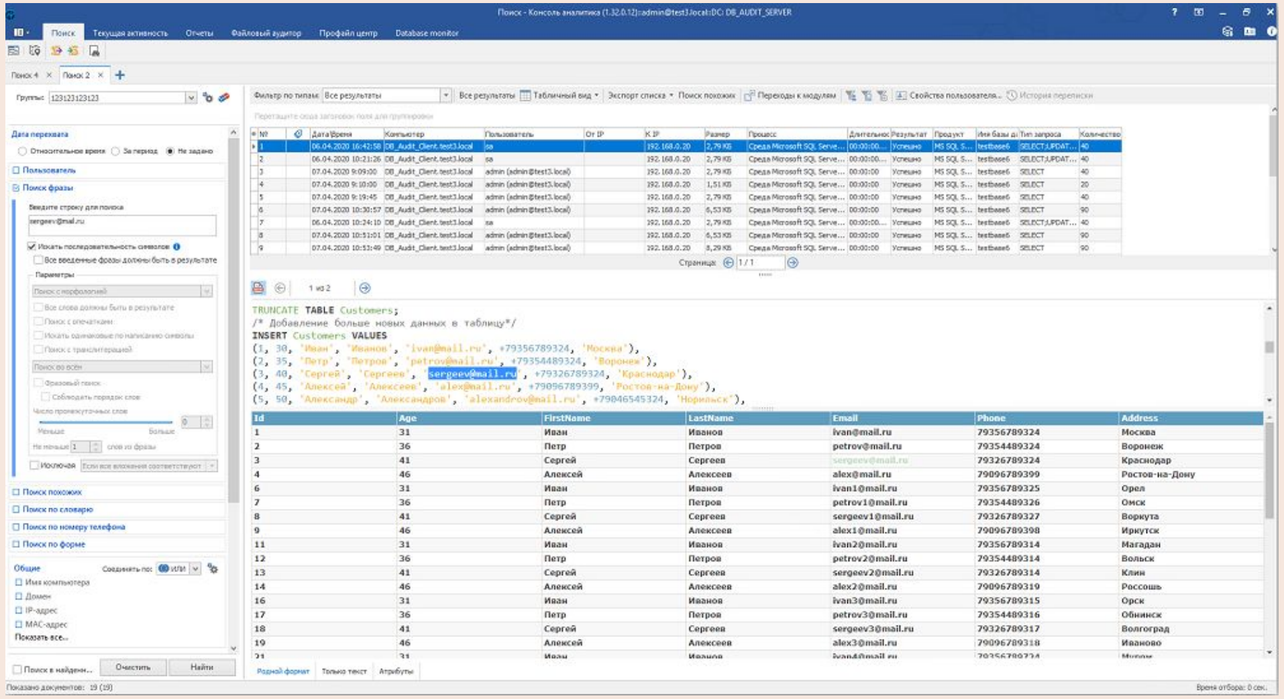
«КРИПТО БД»
Компания "Аладдин Р.Д."

«СЁРЧИНФОРМ DATABASE MONITOR»
Компания "SearchInform"

СЕРТИФИЦИРОВАНЫ

ПОЛНОСТЬЮ ОТЕЧЕСТВЕННЫЕ РЕШЕНИЯ

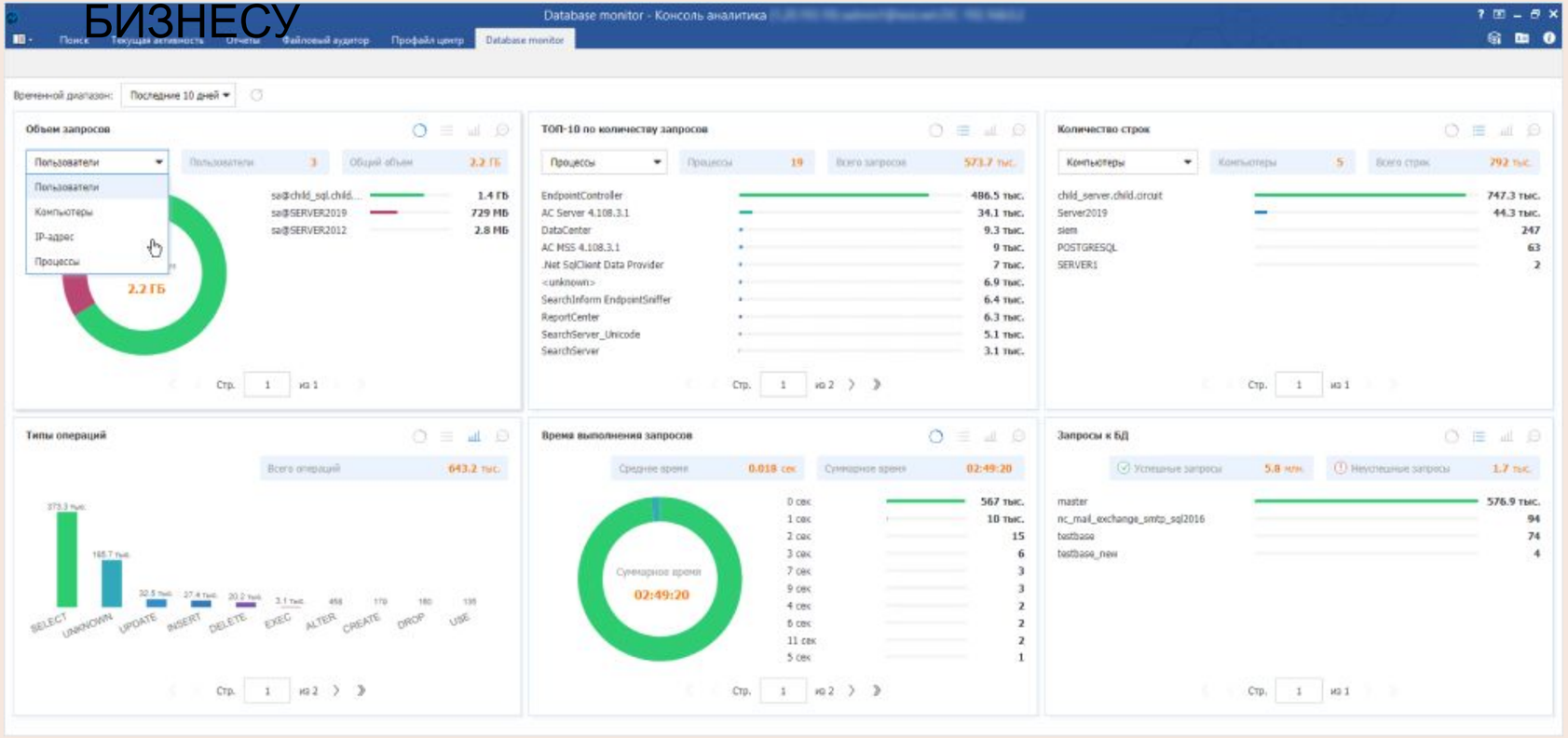
КАК DATABASE MONITOR ПОМОГАЕТ БИЗНЕСУ



Просмотр списка пользовательских запросов к БД и ответов системы

Программа логирует все запросы к БД и ответы на них и проверяет собранную информацию по установленным правилам – политикам безопасности. И в случае их нарушения отправляет автоматическое уведомление службе безопасности компании.

КАК DATABASE MONITOR ПОМОГАЕТ БИЗНЕСУ



Дашборд с виджетами, данные на которых обновляются в режиме реального времени

Программа автоматически индексирует обращения к БД и делает их доступными для поиска и анализа. В системе доступны различные виды поиска – по фразам, по атрибутам БД и пользователей, по типам запросов. Их можно комбинировать, уточняя условия поиска. На основе собранных данных Database Monitor генерирует отчеты в режиме реального времени.

Крипто БД

ФИО	№ карты	Дата рождения	Сумма
Иванов Иван Иванович	123456789012	**********	100 000,00
Петрова Мария Александровна	210987654321	**********	102 000,00
Глушко Сергей Викторович	345010102230	**********	95 000,00
Антонова Елизавета Петровна	310456789012	**********	110 000,00
Малинин Андрей Александрович	890121234567	**********	64 000,00
Сопкин Денис Владимирович	105010102230	**********	19 000,00

Данные о дате рождения на данном рисунке засекречены.

Администратор, имея доступ к БД, не может увидеть сами данные под маской.

Гарда БД

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

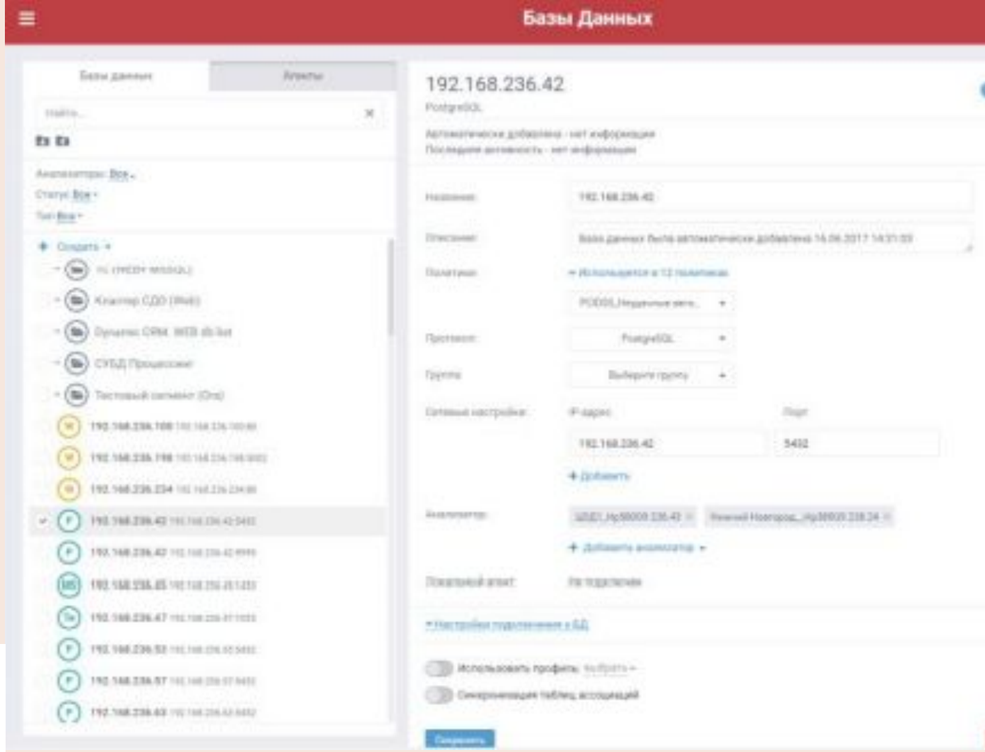
Сканирование баз данных, находящихся под контролем,

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

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

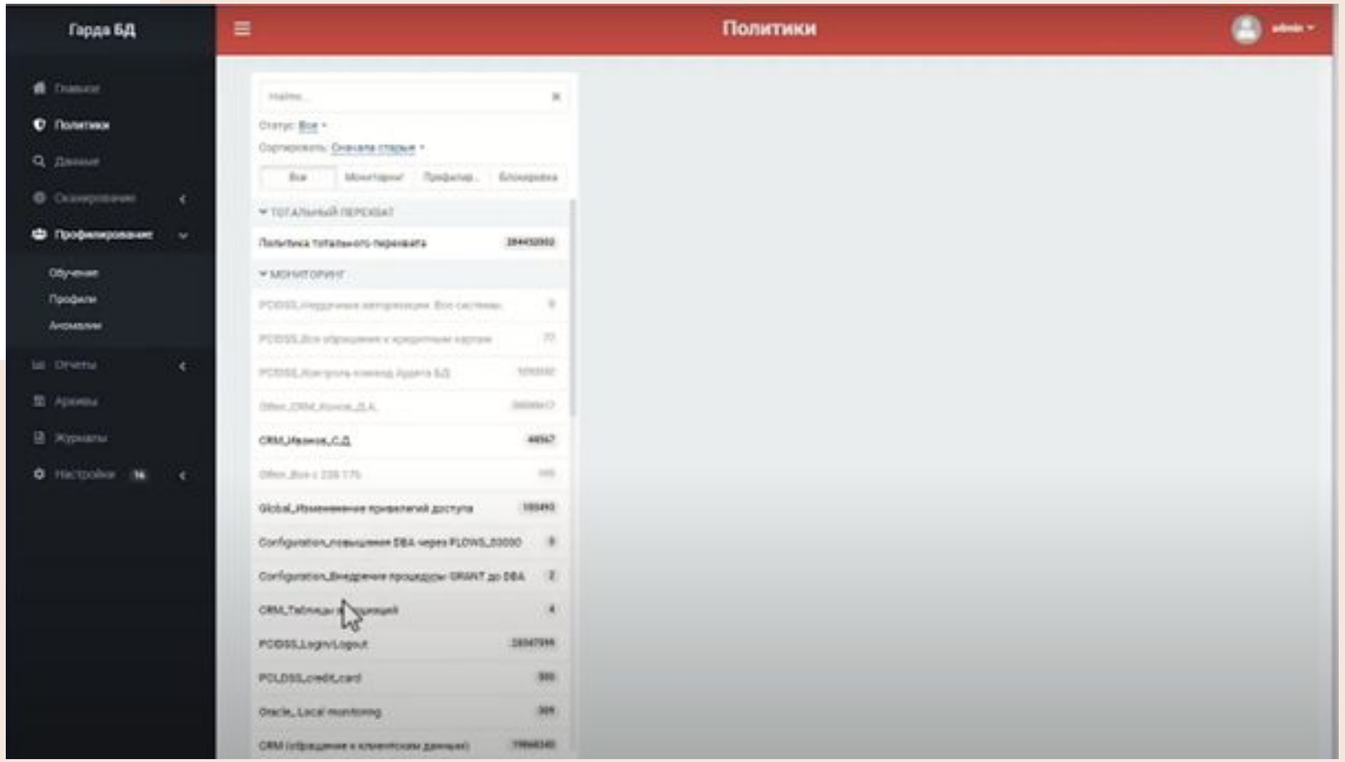
Автоматический поиск новых СУБД, не стоящих на контроле, классификация их по типу хранимых данных

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



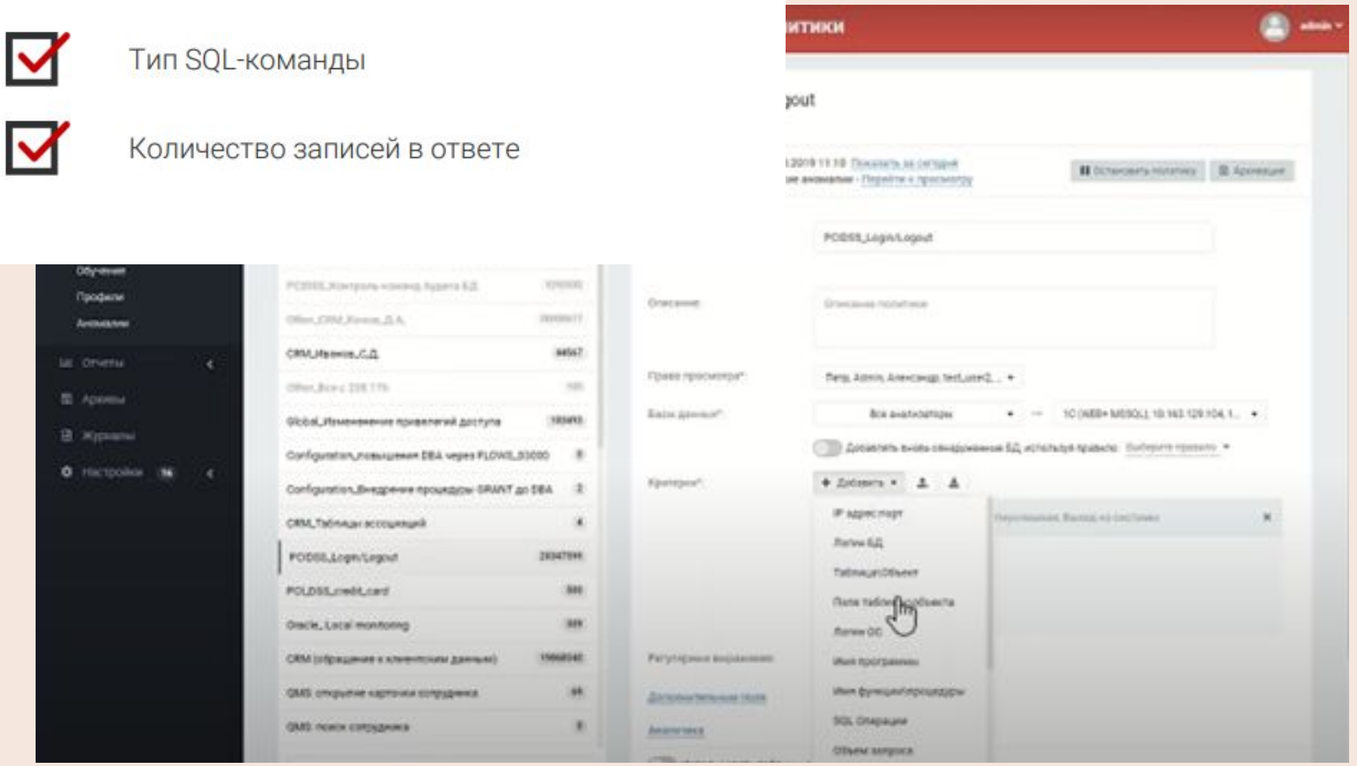
ПРАВИЛА РАБОТЫ СИСТЕМЫ ЗАДАЮТСЯ В КОНСТРУКТОРЕ ПОЛИТИК БЕЗОПАСНОСТИ

- 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:



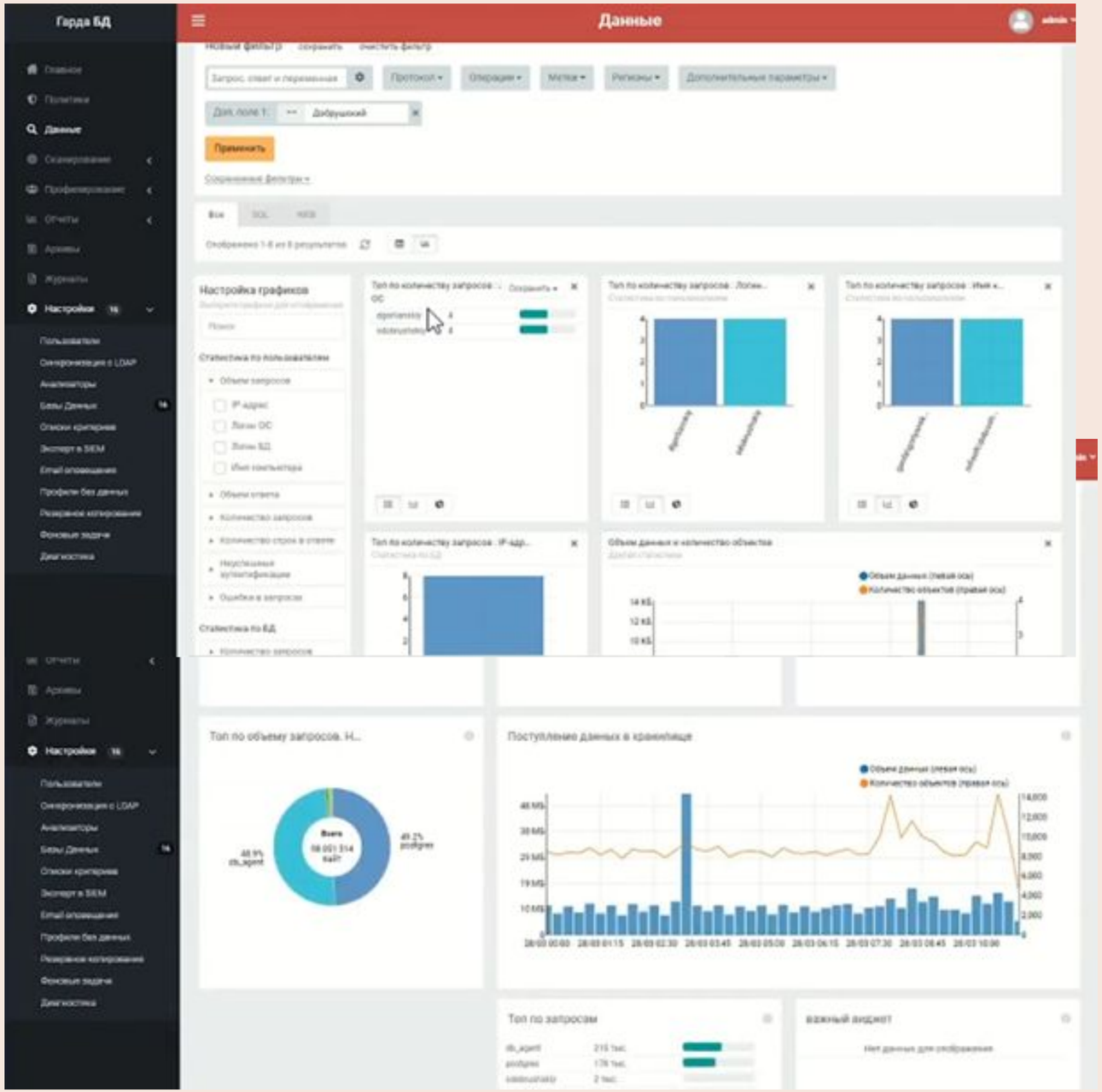
Критерии для формировнаия политик

- 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

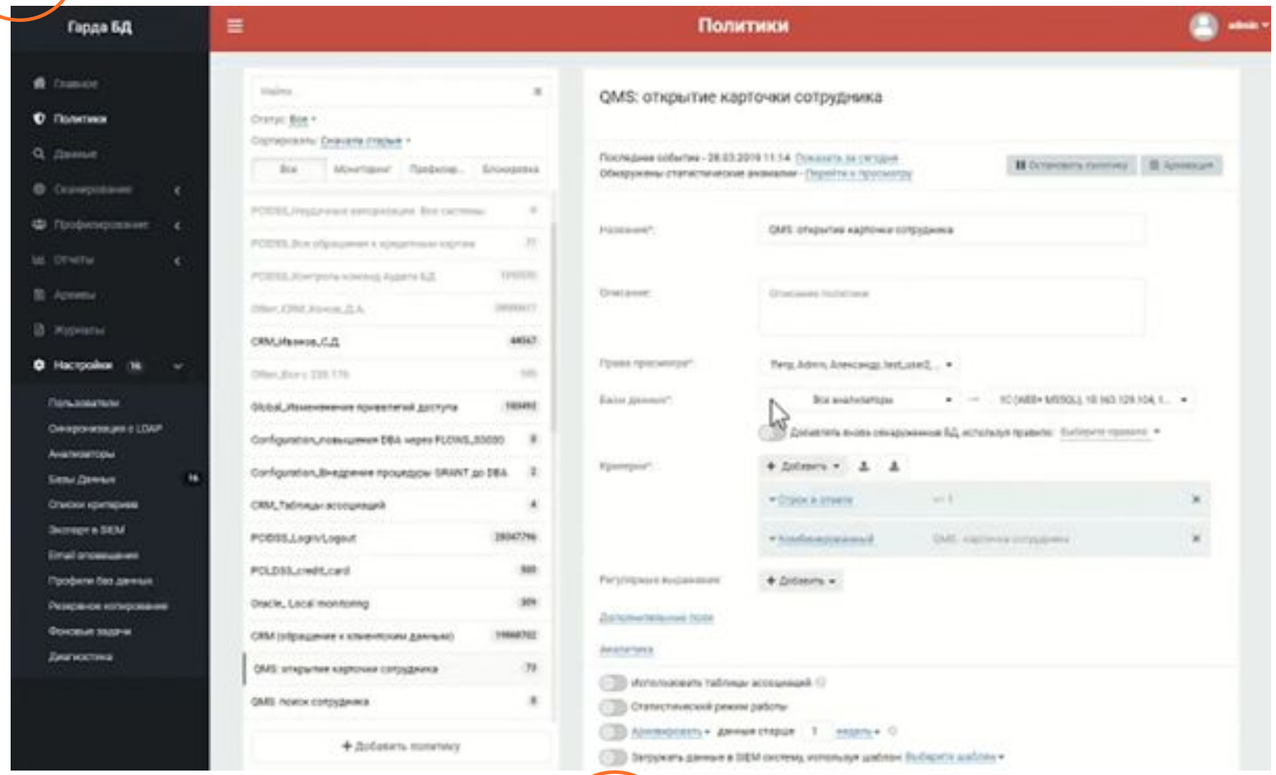


Аналитика

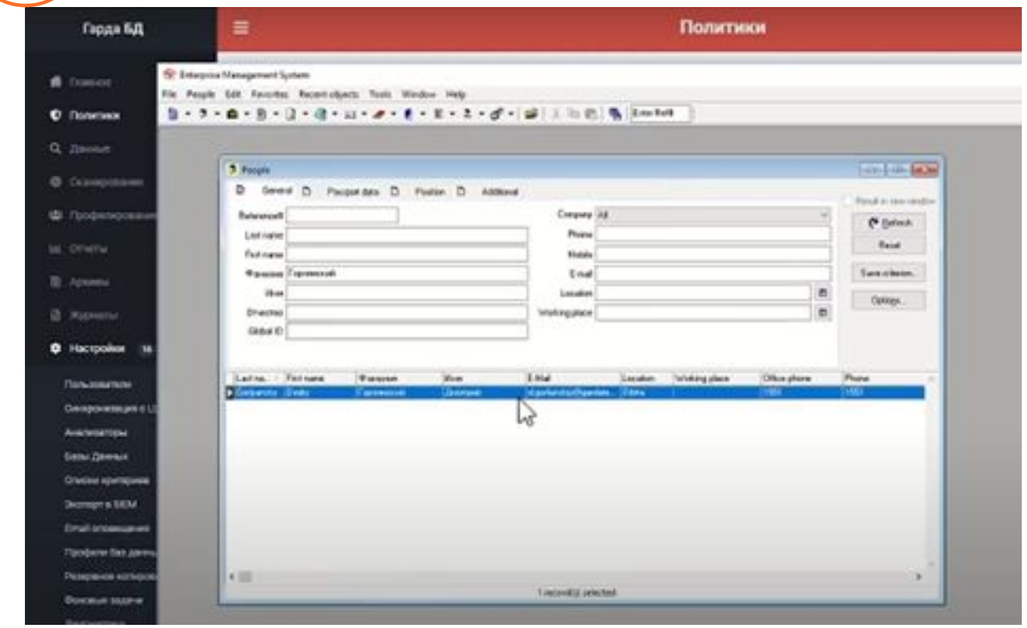
- [x] Интерактивная отчётность
- [x] Конструктор отчётов с возможностью анализа любого объёма данных за любой промежуток времени
- [x] Возможность создания индивидуального дашборда
- [x] Поведенческий анализ пользователей БД (UEBA)
- [x] Уведомление о нарушениях по электронной почте
- [x] Уведомление о выявленных аномалиях в SIEM



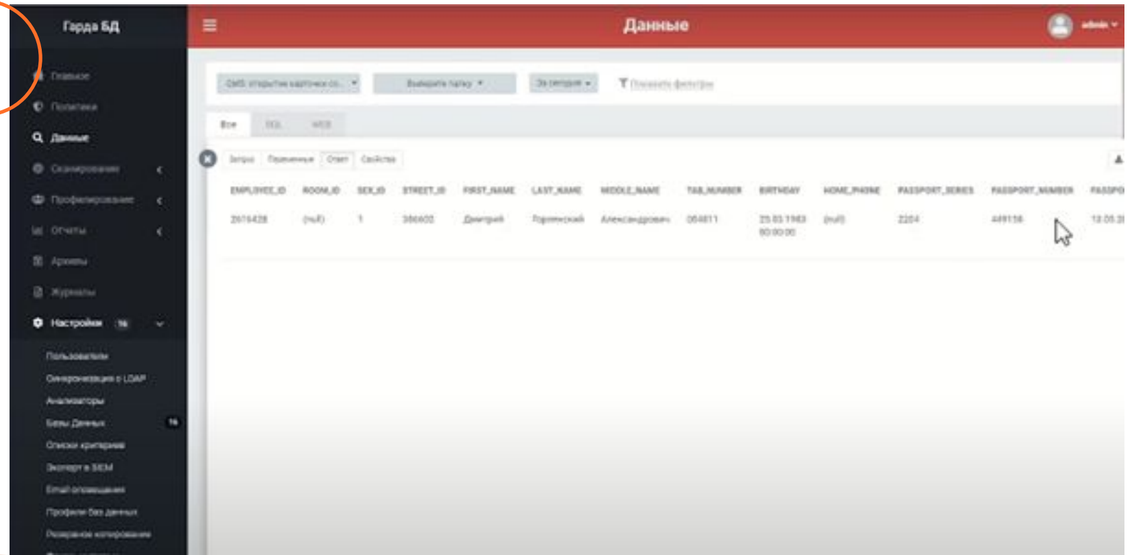
1


Гарда БД
Политики
QMS: открытие карточки сотрудника

2


Гарда БД
Политики

3


Гарда БД
Данные

Спасибо за внимание!