конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

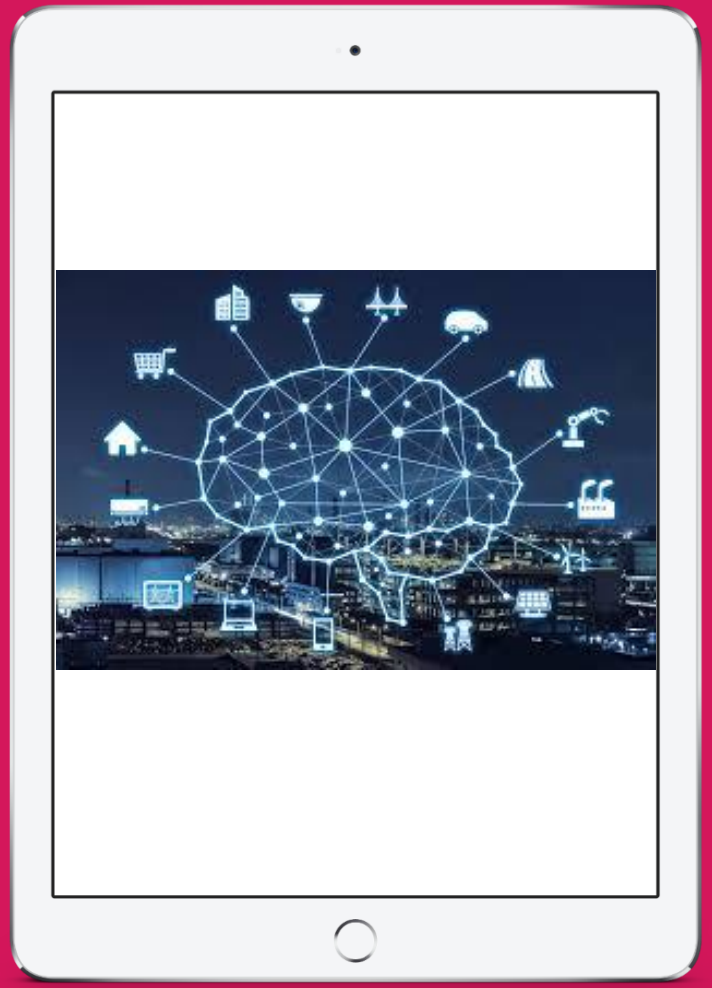
Применение технологий ИИ в ИБ

Айк Татевосян,
Заместитель генерального директора, CrossTech Solutions Group

ИИ в ИБ, миф или реальность?

- Мировой рынок ИИ в 2021 году 3 трлн. долларов;
- Более 20 различных классов решений в ИБ уже сегодня используют ИИ;
- Насколько в действительности ИИ повышает уровень ИБ?

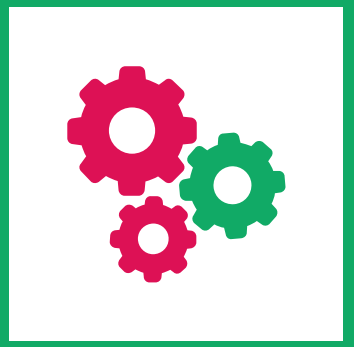
Немного терминологии



- **Большие данные** – данные, обработка которых в заданных условиях/ограничениях требует применения новых технических подходов;
- **Искусственный интеллект** – способность компьютера анализировать данные для решения различного рода задач
- **Модель машинного обучения** – способность компьютера самостоятельно обучаться на наборе данных для принятия решения в конкретной задаче

3 кита искусственного интеллекта

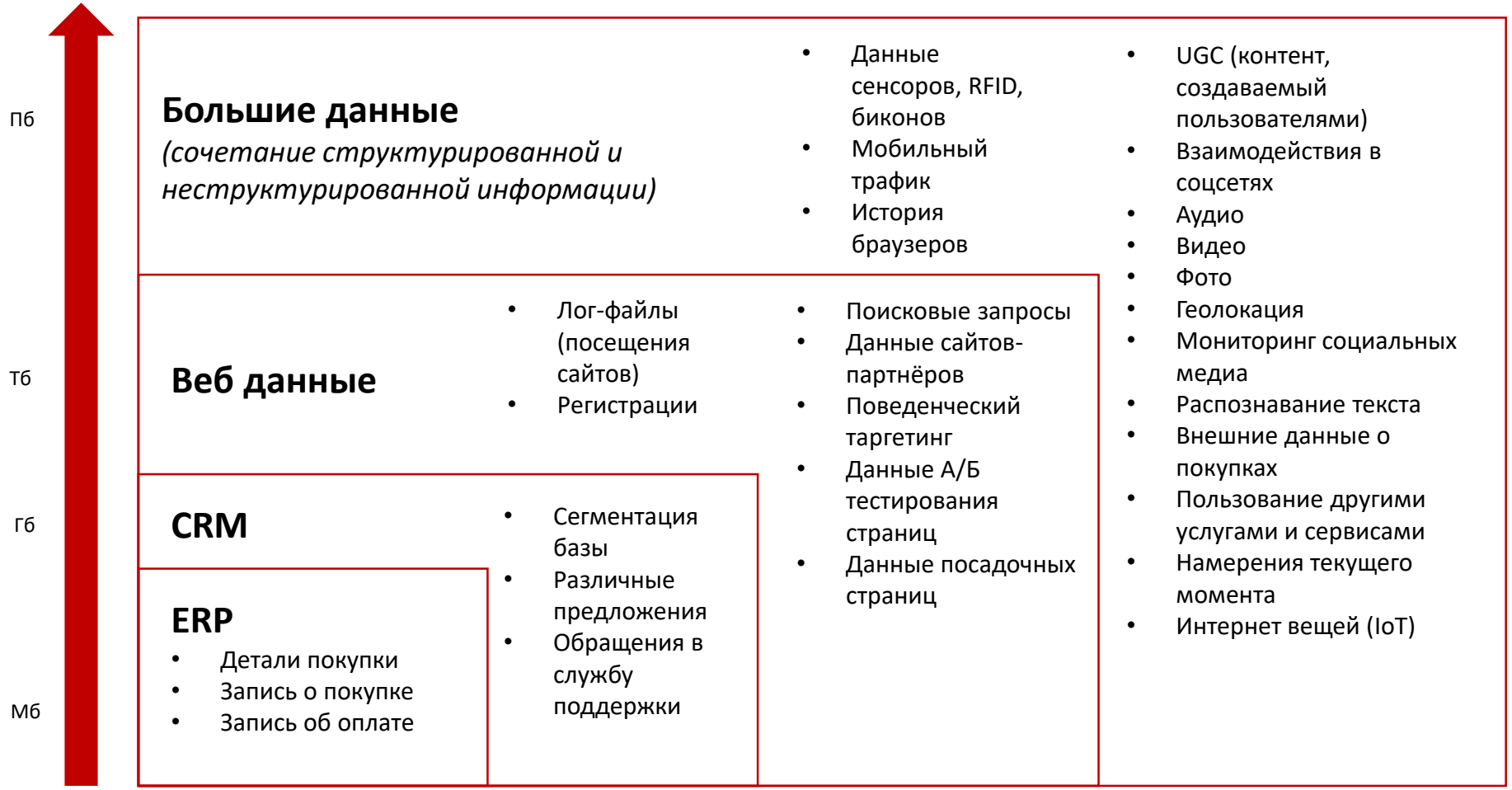
Аналитика и машинное обучение, дающие новые знания



Распределенные хранение и обработка этих данных

Большие массивы данных, в том числе неструктурированные

Что такое BigData?



DataGrain ESO

- **DataGrain ESO –** отечественное решение, позволяющее собирать, фильтровать и профилировать входящие события ИБ, осуществлять централизованное хранение данных в хранилище в сжатом формате и передавать только необходимые данные на сторонние решения.

Интеграция с целевыми источниками данных по различным протоколам и интерфейсам

Реализация наиболее эффективной структуры по долгосрочному хранению данных

Настройка передачи отфильтрованных данных на **SIEM**-платформу в поддерживаемом формате

Настройка механизмов по профилированию входящего потока данных и «умной» фильтрации

DataGrain ESO – описание решения

- Отечественное ПО;
- Многоступенчатая фильтрация событий ИБ;
- Профилирование входящего потока событий ИБ в **SIEM;**
- Централизованное хранение всех исходных данных в сжатом формате;
- Сокращение финансовых затрат на лицензирование **SIEM.**

DataGrain ESO – импортозамещение

- Полностью отечественный технологический стек;
- Умная фильтрация;
- Гибкие возможности по поиску информации в собираемых данных;
- Поддержка всех крупных вендоров SIEM;
- Поддержка широкого перечня целевых источников данных;

MICRO FOCUS ArcSight

splunk>

LogRhythm®

DataGrain RUMA

- **DataGrain RUMA –** решение, позволяющее осуществлять поведенческий анализ пользователей и иных сущностей, осуществлять продвинутый мониторинг, выявлять аномалии в различных разрезах и визуализировать результаты аналитики.

Автоматизация формирования управленческой и прикладной отчетности

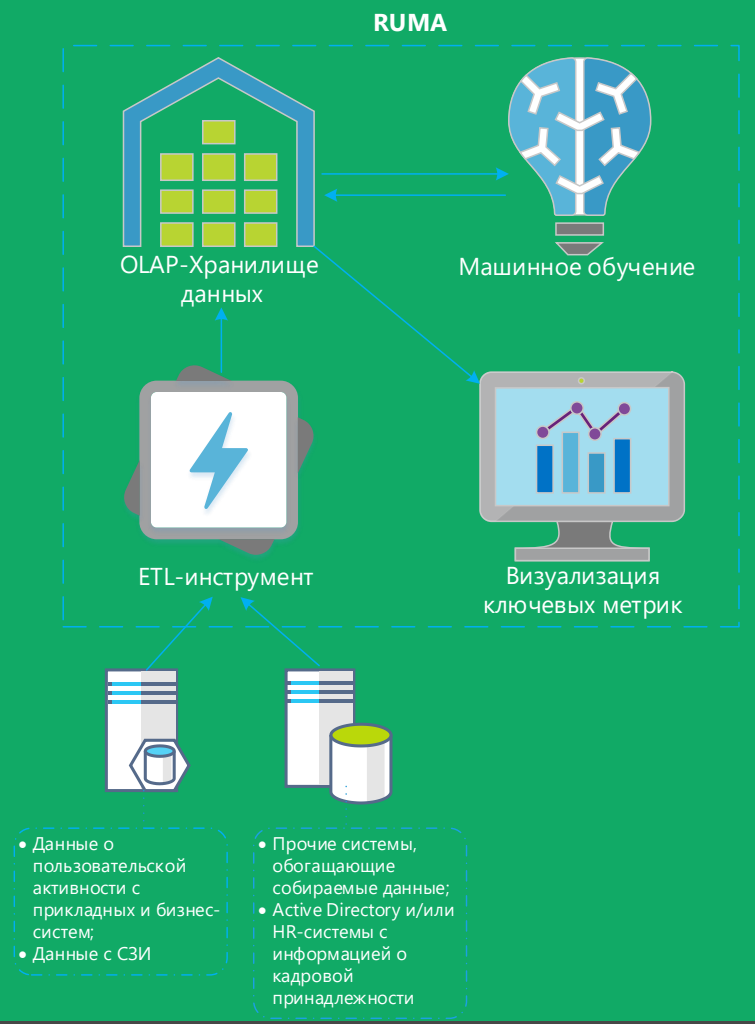
Интеграция с **HR**-системами/**AD** для обогащения информацией о кадровой принадлежности

Реализация логики выявления аномальной активности с помощью алгоритмов машинного обучения и статистического анализа

Интеграция с целевыми источниками данных или со смежными системами (например, **SIEM**)

DataGrain RUMA – описание решения

- Отечественное ПО;
- Продвинутый поведенческий анализ данных, использующий различных алгоритмы машинного обучения;
- Выявление нетипичного и аномального поведения с последующей пиритизацией полученных результатов;
- Обогащение данных и построения новых взаимосвязей;
- Возможность настройки и тюнинга поведенческих аналитических моделей и правил по выявлению аномалий



DataGrain RUMA – импортозамещение

- Широкий спектр поддерживаемых источников данных;
- Использование продвинутых алгоритмов статистического анализа и машинного обучения;
- Гибкие механизмы по доработке моделей и логики детектирования аномалий в зависимости от специфики Заказчика;
- Профилирование пользователей и иных сущностей, решение задач предиктивного анализа;

exabeam

SECURONIX

FORCEPOINT

splunk>

DataGrain Analyzer

- **DataGrain Analyzer –** решение, позволяющее проводить анализ логического содержимого БД и таблиц различных СУБД, выявлять коллизии и несоответствия в данных, названиях и типах полей, структуре хранения данных.

Автоматизация формирования и отправки отчетности

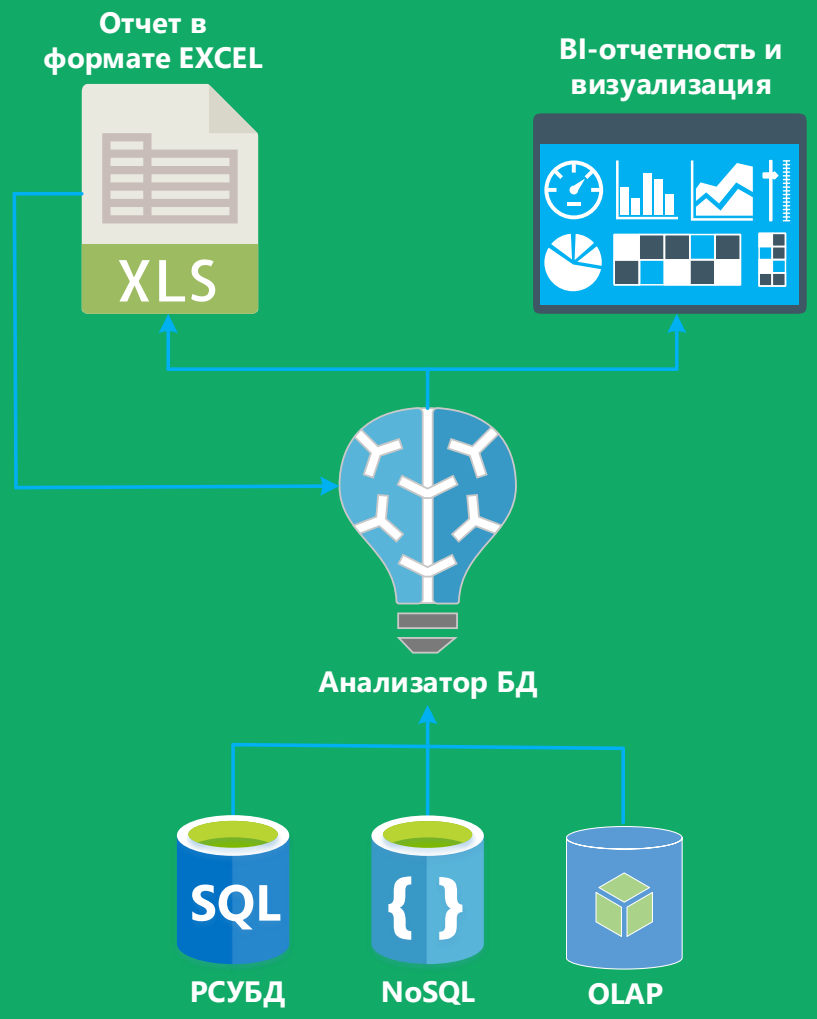
Обогащение аналитики пользовательскими справочниками и регулярными выражениями

Реализация логики анализа и логического соответствия типа БД-таблица-поле-содержимое поля

Реализация коннекторов к различным реляционным и **NoSQL** СУБД

DataGrain Analyzer – описание решения

- Статистический анализ по содержимому таблиц, в частности подсчет количества полей, их названий и типа, количества строк и уникальных строк в каждом из полей;
- Просмотр семплов таблицы и значений полей, а также поиска конкретных значений, путем наложения фильтра;
- Смысловой и контекстный анализ содержимого каждого из полей, выявление смыслового домена для каждого из полей;
- Создание пользовательских семантических доменов с помощью написания регулярных выражений.



DataGrain Analyzer – импортозамещение

- Широкий спектр поддерживаемых хранилищ данных;
- Огромная база регулярных выражений и справочников, отвечающий за смысловой анализ;
- Поддержка механизмов разработки пользовательских коннекторов к СУБД и регулярных выражений для поиска чувствительных данных;
- Возможность статического и динамического маскирования (обфускации) данных;

Infognito

Informatica™

Вопросы

???

Контактная информация

Электронная почта:
info@ct-sg.ru

Телефон:

+7 (495) 741-88-64

Сайт:

www.ct-sg.ru