iRule

Технологии анализа информации

и визуализации знаний

ОБЩЕЕ ОПИСАНИЕ

1. Функциональные характеристики

iRule – функционально полная технологическая платформа, предназначенная для построения информационно-аналитических систем.

Созданные на базе **iRule** информационно-аналитические системы результативно применяются для обеспечения различных видов деятельности (проведение проверок и расследований, выявление и предотвращение мошенничества, противодействие отмыванию денежных средств и финансированию терроризма, оптимизация бизнес-процессов, управление рисками и не только).

Ключевые преимущества **iRule**:

- эффективная поддержка всех основных стадий аналитического процесса: от сбора информации до представления аналитических выводов для принятия решений;
- встроенные мощные инструменты анализа и представления информации (анализ связей, анализ потоков, временной анализ событий, анализ версий (гипотез), табличный и кросс-табличный анализ, картографический анализ и др.);
- прозрачный для пользователя поиск по всем доступным внутренним и внешним информационным ресурсам;
- создание выразительных аналитических материалов, интуитивно понятных как коллегам, так и руководителям, формирование отчётов в электронном и бумажном виде;
- открытость решения для интеграции с другими системами;
- лёгкость в использовании и быстрое освоение;
- соответствие требованиям и рекомендациям **Международной ассоциации аналитиков правоприменительных органов** (International Association of Law Enforcement Intelligence Analysts, IALEIA);
- кратчайшие сроки разработки и внедрения.

iRule не просто программное обеспечение для визуализации информации, это комплексное интеллектуальное решение для поддержки аналитической деятельности на любом уровне и в различных сферах.

iRule предоставляет пользователям мощные аналитические инструменты для детального и макростатистического анализа информации и построения точных обоснованных выводов.

Аналитический процесс или Intelligence Cycle

iRule обеспечивает эффективную поддержку пользователей на всех стадиях аналитического процесса, а именно:

Определение целей и планирование → Сбор информации → Проверка и оценка информации → Упорядочение и систематизация → Анализ информации → Представление результатов для принятия решений.

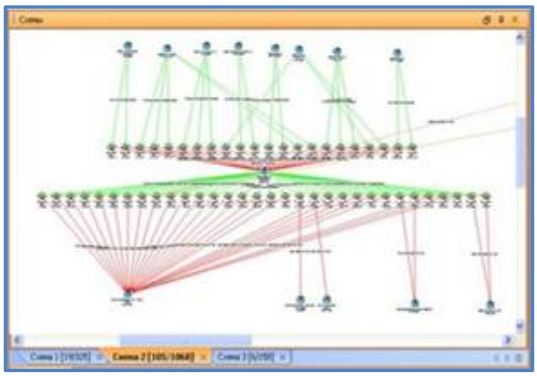
Эффективность работы, ускорение анализа данных

Использование решения **iRule** позволяет не только сократить время на решение стандартных задач, связанных со сбором информации из различных источников и ее предварительной оценкой, но и эффективно решать задачи детального анализа и построения точных обоснованных выводов.

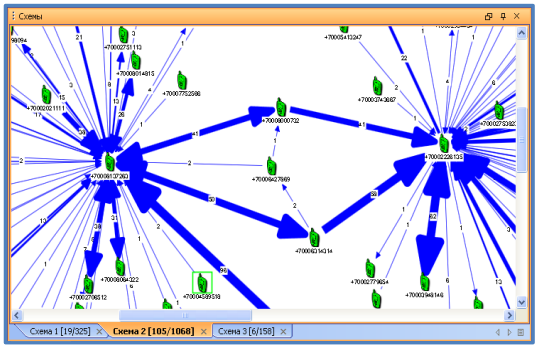
Мощные инструменты анализа и представления информации

Специальные форматы хранения аналитических материалов, доступ к результатам ранее проведенных исследований/расследований значительно сокращает время на поиск возможных пересечений по оперативно значимым объектам. **iRule** предоставляет широкий набор аналитических инструментов и методов для получения ответов на вопросы КТО? ЧТО? ГДЕ? КОГДА? КАК? ПОЧЕМУ? и др.

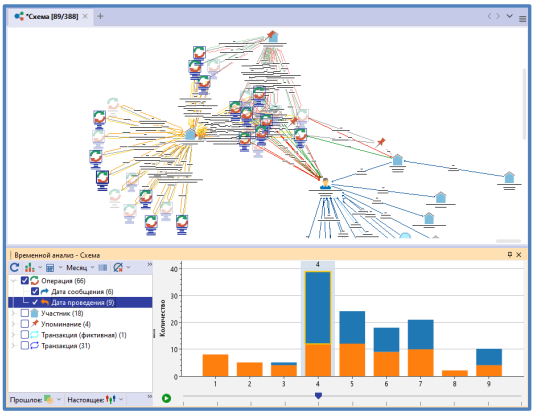
- **Анализ связей**. Метод позволяет выявить между различными объектами – лицами, организациями, событиями и т.д. – имеющиеся явные и неявные (скрытые) отношения и цепочки связей. Аналитические диаграммы связей представляют эту информацию в наиболее наглядном и понятном виде, что существенно помогает в подготовке выводов.



- **Анализ потоков**. Данный метод является важным расширением анализа связей, т.к. суть преступной деятельности и ее организации может быть раскрыта через анализ перемещения предметов, связанных с этой деятельностью. Анализ потоков позволит представить механизм преступления наиболее наглядно и таким образом поможет в подготовке вывода.

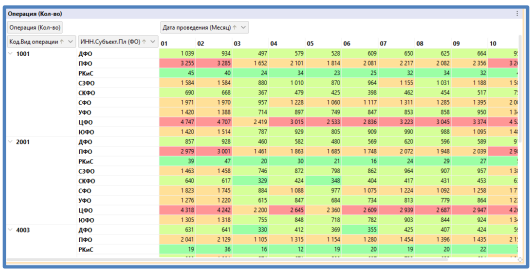


- **Временной анализ событий**. Метод позволяет более четко представить развитие сложных ситуаций по времени: установить последовательность событий, их хронологию, характер связи между событиями и роли основных участников.

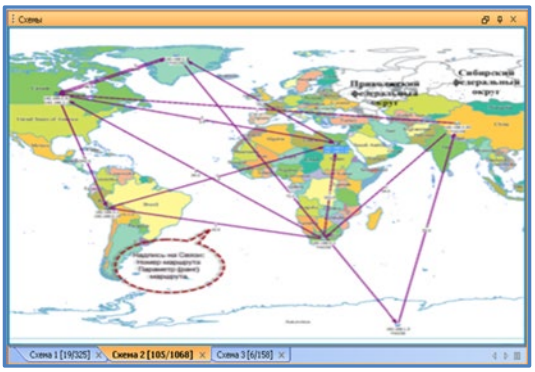


- **Анализ бизнес-процессов (процесса деятельности, в т.ч. преступной).** Метод используется для визуализации последовательности действий, направленных на достижение конкретной цели. Построенные схемы отражают принцип деятельности и устанавливают типичный способ совершения преступления.

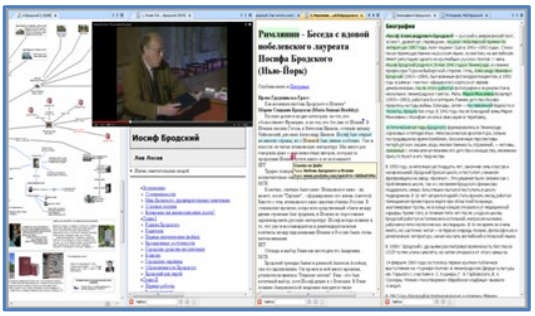
- **Табличный и кросс-табличный анализ.** Традиционный метод табличного анализа необходим для проверки и предварительной оценки данных (методы сортировки, фильтрации…), используется для выделения значимой информации в целях дальнейшего детального исследования. Кросс-табличный анализ в комплексе с методами визуализации детальных данных позволяет наиболее эффективно вести анализ статистики и готовить сложные отчеты для стратегического уровня управления.



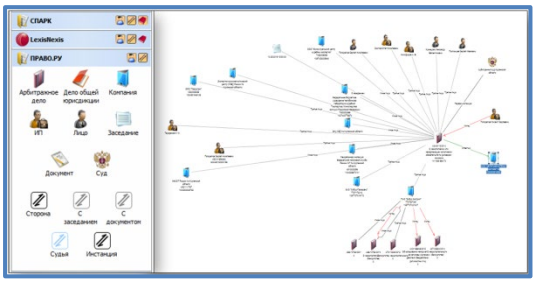
- **Картографический анализ.** Знание времени и места преступления/происшествия порой жизненно необходимо для принятия оперативных мер. Картографический анализ (маршруты, расстояния, геокоординаты объектов, пространственно-временной анализ событий, очаги преступной активности, тематические карты …) позволяет принимать решения на основе более точной и своевременной информации.



- **Анализ текстовых документов.** Позволяет выделить из текста все значимые элементы (авторы, темы, записи, адреса, события …), определить роли и характер связей между объектами. При этом аналитическая информация представляется на интерактивной карте в наиболее удобном для понимания виде (как известно, одна картина заменяет тысячи слов).



- **Извлечение данных из внешних информационных ресурсов.** Позволяет извлекать информацию из внешних информационных систем и сохранять полученные данные в БД системы. Подключение к конкретной информационной системе осуществляется с помощью соответствующего адаптера через предоставляемые системой веб-сервисы.



2. Архитектура

iRule представляет собой совокупность функциональных элементов, установленных на технических средствах из состава комплекса технических средств и обеспечивающих автоматизацию деятельности пользователей.

Типовая структура комплекса технических средств

Программный продукт **iRule** построен по трёхзвенной архитектуре: клиент – сервер приложений – сервер БД, функционирует на базе серверов и персональных компьютеров и содержит следующие компоненты:

1. **Рабочая станция пользователя** предназначена для решения задач анализа и формирования схем, выявления и мониторинга типологий. Для извлечения объектов и связей запрос в понятиях предметной области направляется на сервер приложения. От сервера приложения ответ приходит в виде объектов и связей. Взаимодействие с сервером приложения осуществляется по протоколам HTTP/HTTPS и JMS.
2. **Рабочая станция администратор** предназначена для изменения параметров сервера приложения, управления пользователями и их правами, подключения источников данных. Взаимодействие с сервером приложения осуществляется по протоколам HTTP/HTTPS и JMS.

3. **Сервер приложения** предназначен для выполнения прикладных процессов. Сервер приложений, с одной стороны, взаимодействует с клиентами, получая задания, с другой стороны, взаимодействует с источниками данных (реляционными или многомерными БД, веб-сервисами), извлекая данные, необходимые для обработки. Взаимодействие с сервером БД осуществляется с помощью **JDBC**-драйвера соответствующей СУБД. Взаимодействие с внешними и внутренними информационными ресурсами осуществляется по поддерживаемым ими протоколам.
4. **Сервер метаобласти**. Данный элемент входит в структуру функционально, на нём развёрнута метаобласть сервера приложения. На сервере должна быть установлена любая свободная или проприетарная реляционная СУБД, предоставляющая **JDBC**-драйвер.
5. **Внутренние и внешние информационные ресурсы**. Данные элементы входят в структуру функционально, выступают в качестве источников данных для проведения анализа. Данные могут: размещаться под управлением свободной или проприетарной СУБД (должна предоставить **JDBC**-драйвер, например, **Arenadata DB, Arenadata QuickMarts, ClickHouse, Greenplum, Postgres Pro, Oracle Database, MS SQL Server, PostgreSQL, MySQL, Sybase, DB2, SAP HANA, MariaDB, TeraData** и т.п.), выставлены в виде веб-сервисов (SOAP или REST) или доступны по специализированному API. Возможность аналитической обработки больших массивов информации из множества различных источников существенно повышает качество аналитических результатов

Необходимость выделения отдельных функциональных элементов является следствием модульности структуры программного обеспечения **iRule** и вызвана требованиями обеспечения независимости функций накопления и анализа данных, а также необходимостью обработки и продолжительного хранения больших объёмов данных.

Допускается размещение нескольких компонент совместно на одном сервере (например, для формирования тестовой среды). Возможно обеспечить терминальный доступ пользователей и администраторов.

Данная архитектура позволяет минимизировать администрирование: не требуется установка и обновление ПО пользователя и администратора на каждой рабочей станции, этот процесс происходит автоматически с сервера приложения.

Рекомендуемые характеристики технических средств

Рабочая станция пользователя и администратора

- процессор с тактовой частотой 3,0 ГГц
- оперативная память - 8 Гбайт
- дисковая подсистема HDD - 80 Гбайт
- монитор - 1920*1080
- сетевой адаптер - 1 Гбит/с Ethernet
- операционная система - Windows, Linux

Сервер приложения

- 2 процессора Intel Xeon с тактовой частотой каждого ядра 3,0 ГГц
- оперативная память - 16 Гбайт
- дисковая подсистема HDD - 100 Гбайт
- сетевой адаптер - 1 Гбит/с Ethernet
- операционная система - Windows, Linux, Solaris

В качестве операционной системы поддерживаются и отечественные решения.

3. Подготовка и поддержка пользователей

Разработчиком **iRule** является российская компания **ООО «Институт проблем безопасности и анализа информации»**. При разработке **iRule** был учтён опыт работы аналитических подразделений правоохранительных органов России.

Институт проблем безопасности и анализа информации обеспечивает всестороннее сопровождение и поддержку пользователей iRule, предоставляя услуги по обучению и технической поддержке:

- базовый учебный курс «Системный анализ информации. Специальные аналитические методы и технологии» (Intelligence Analysis)
- специализированный учебный курс «iRule. Технологии анализа информации, визуализации и передачи знаний»
- консультации службы технической поддержки, обновление версий программного обеспечения

Решения на основе технологий **iRule** используют важнейшие государственные структуры и крупные коммерческие организации: Росфинмониторинг, ФСБ России, ФТС России, Счётная палата, Росатом, Роснефть, Банк России, Газпромбанк, Сибур и другие.