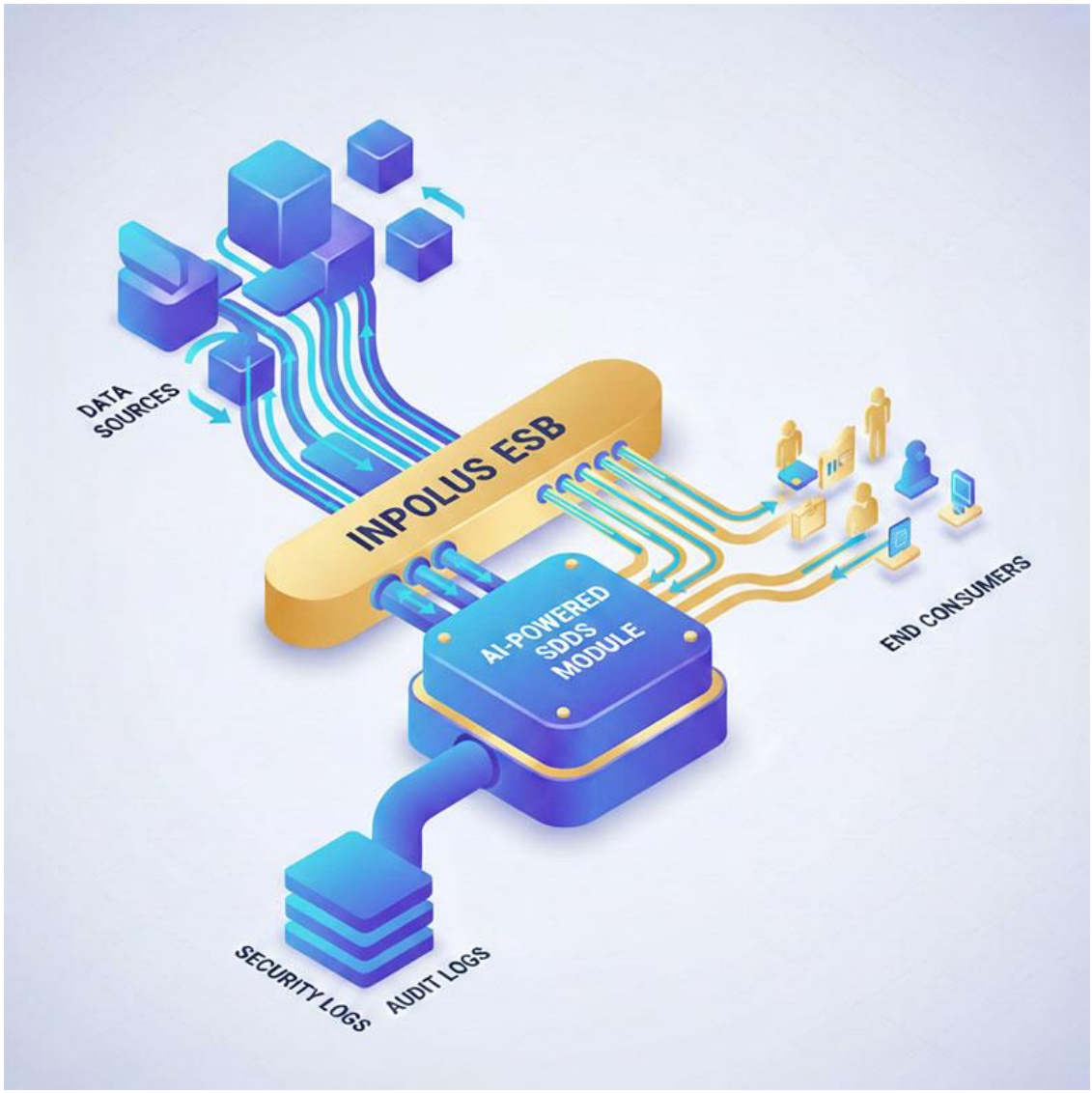
Inpolus SDDS: цифровой страж для ваших данных в потоке информации

Представьте себе современное предприятие как огромный живой организм. Его кровеносная система – это бесконечные потоки информации: данные бегут между программами, уходят в облака, к искусственному интеллекту, возвращаются обратно. Но что, если в этом потоке «уплывут» паспортные данные клиента, коммерческая тайна или банковские реквизиты? Раньше защита напоминала охрану склада: проверили диски и файлы на полках – и порядок. Но сегодня данные не лежат, а движутся, и старые методы тут бессильны.



Здесь на сцену выходит Inpolus SDDS (Sensitive Data Detection System). Простыми словами, это умный фильтр, который следит за данными прямо в пути. Его главная задача – найти и обезвредить «чувствительную» информацию там, где она течёт потоком, например, через корпоративную шину данных Inpolus ESB, которая соединяет все системы компании.

Сегодня данные – это цифровая нервная система современного предприятия. Они непрерывно циркулируют между десятками сервисов через шины данных, поступают из внешних API, передаются в облачные сервисы и анализируются системами ИИ. В этом динамичном магистральном потоке традиционные средства защиты, ориентированные на контроль статичных данных и периметра системы, теряют свою эффективность. Утечка происходит не через USB-носитель, а через Kafka-топик, не через Email, а через ответ REST API.

Решение Inpolus SDDS (компонент детектирования чувствительных данных) создано для защиты данных именно в движении. Его ключевая и наиболее мощная роль – стать встроенным слоем безопасности корпоративной шины данных, обеспечивающим сквозной контроль на всех этапах жизненного цикла сообщения.

Inpolus SDDS как встроенный слой безопасности шины данных Inpolus ESB

Шина данных Inpolus ESB – основной канал межсервисного/межсистемного взаимодействия. Inpolus SDDS интегрируется в неё не как внешний сканер, а как нативный security-модуль, размещённый в критических точках маршрутизации данных. Это реализуется через систему гибкой интеграции точек входа и выхода сервиса Inpolus ESB для контроля утечек в ключевых местах потоков обработки данных.

Inpolus SDDS – это централизованный движок анализа, работающий через модульную систему адаптеров. Это позволяет также подключать любые источники данных на входе и направлять результаты обработки в любые целевые системы на выходе.

Точки входа (Ingress Points): откуда поступают данные на проверку

Любой поток данных может быть направлен в Inpolus SDDS через соответствующий адаптер:

- Встроенная интеграция с Inpolus ESB
- HTTP/S-адаптер – внешние REST-вызовы с JSON/XML или текстом передаются в Inpolus SDDS через HTTPS. Это позволяет контролировать данные в запросах к публичным API и предотвращать утечки конфиденциальной информации.
- Kafka-адаптер – подписывается на заданные топики и перенаправляет сообщения в Inpolus SDDS. Анализ данных выполняется без изменения логики продюсеров. Подход особенно эффективен в event-driven архитектурах.
- gRPC – для высокопроизводительных внутренних взаимодействий между микросервисами используется gRPC-адаптер, обеспечивающий

низкую задержку, высокую пропускную способность и строгую типизацию данных.
- Прочие источники – через кастомизированные адаптеры возможна интеграция с RabbitMQ, ActiveMQ, файловыми системами, CI/CD-пайплайнами или даже интерактивными консолями – любой источник, где есть риск утечки чувствительных и персональных данных.

Точки выхода (Egress Points): куда направляется результат

После анализа данных и применения соответствующих политик (передача без изменений с полным протоколированием, обезличивание данных или блокировка контента) результат доставляется через соответствующий канал:

- Встроенная интеграция с Inpolus ESB.
- HTTP/S ответ - финальный ответ внешнему потребителю формируется адаптером на основе результата, полученного при анализе данных с использованием локальных ИИ-моделей, обученных на русскоязычных данных. Если политика предписывает маскирование, клиент получает обезличенные данные без чувствительной информации.
- Kafka-producer – результат направляется в выходной Kafka-топик, который может быть интегрирован в существующий бизнес-поток (обеспечивая прозрачность для потребителей) или использоваться как отдельный безопасный канал.
- gRPC ответ – результат ИИ-анализа доставляется вызывающему микросервису, клиент получает проверенную и безопасную (обезличенную при необходиости) версию данных.
- Системы мониторинга и аудита – параллельно с ответом, в соответствии с политиками, генерируется стандартизированное событие безопасности, которое направляется в централизованный канал событий (например, выделенный Kafka-топик) для последующего потребления SIEM-системами, лог-агрегаторами, встроенной и/или внешними платформами управления инцидентами.

Гибкое управление политиками: от мониторинга к активной защите

Inpolus SDDS позволяет внедрять защиту данных постепенно – от пассивного наблюдения до полного контроля, в зависимости от зрелости процессов и требований безопасности.

На начальном этапе система может анализировать потоки без вмешательства: все данные передаются в неизменном виде, но фиксируется наличие конфиденциальной информации. Это даёт возможность оценить объёмы рисков, выявить критичные каналы и настроить правила без влияния на бизнес-процессы.

По мере готовности политики могут быть усилены:

- система начинает автоматически обезличивать персональные и другие чувствительные данные (например, заменяя ФИО или номер паспорта на структурированные маски);
- в самых строгих сценариях - полностью блокировать передачу сообщений, содержащих критичную информацию, и инициировать расследование инцидента.

Политики применяются динамически на основе контекста: источника данных, канала передачи, времени суток, окружения (тест/пром) и других атрибутов.

Такой подход обеспечивает плавное внедрение, минимизирует риски для стабильности системы и позволяет адаптировать уровень защиты под конкретные бизнес-требования.

Универсальность Inpolus SDDS: защита за пределами шины

Благодаря модульной архитектуре и поддержке различных протоколов, Inpolus SDDS легко интегрируется не только в современные event-driven системы, но и в другие критически важные контуры:

- безопасное взаимодействие с внешними ИИ-сервисами и SaaS-платформами – все исходящие запросы к внешним API проходят через Inpolus SDDS, где автоматически выявляются и обезличиваются персональные данные. Это позволяет использовать облачные ИИ-решения без риска нарушения требований ФЗ-152 или GDPR;
- поиск чувствительных данных в процессе разработки – в CI/CD-пайплайнах Inpolus SDDS сканирует исходный код и конфигурации на наличие учётных данных, API-ключей и других секретов, предотвращая их попадание в промышленную среду;
- подготовка протоколов к анализу – перед отправкой в системы мониторинга протоколы очищаются от персональных данных и другой чувствительной информации, что обеспечивает безопасность при централизованном сборе данных;
- защита унаследованных систем – для legacy-приложений, не подключённых к единой шине, достаточно направить их данные через HTTP-интерфейс Inpolus SDDS – и получить тот же уровень контроля, что и в современных микросервисах.

Полный аудит и работа с инцидентами

Независимо от способа интеграции Inpolus SDDS обеспечивает единый формат регистрации всех операций:

- по каждому запросу формируется структурированное событие, содержащее: тип применённого действия (пропуск, обезличивание или блокировка), источник данных (канал, сервис, окружение), криптографический хеш исходного сообщения для однозначной

идентификации, перечень выявленных категорий конфиденциальной информации.

- все события безопасности публикуются в выделенный Kafka-топик, откуда они могут быть автоматически потреблены SIEM-системами, платформами мониторинга или средствами управления инцидентами.
- полный журнал операций сохраняется в зашифрованном виде и доступен для внутренних расследований, аудита и формирования отчётности перед регуляторами.

Такой подход обеспечивает:

- сквозную трассировку по уникальному корреляционному идентификатору;
- автоматизированное реагирование на потенциальные утечки;
- полную прозрачность для подтверждения соответствия требованиям ФЗ-152, GDPR, PCI DSS и другим стандартам информационной безопасности.

Эволюция защиты: от базового ядра к интеллектуальному анализу

Внедрение Inpolus SDDS начинается с минимально жизнеспособного набора функций, обеспечивающего быстрый старт без рисков для стабильности бизнес-процессов:

- надёжное ядро детекции – более 40 проверенных шаблонов на основе регулярных выражений позволяют точно выявлять структурированные данные: номера паспортов, банковских карт, телефонов, ИНН, СНИЛС и другие стандартные категории;
- простая интеграция - поддержка REST API и Kafka обеспечивает подключение к большинству современных систем уже на первом этапе - без необходимости изменения архитектуры;
- безопасный запуск - на начальном этапе система работает в режиме мониторинга и обезличивания: данные передаются дальше, но чувствительная информация либо фиксируется для анализа, либо заменяется на безопасные аналоги без остановки потоков.

На этом фундаменте постепенно развивается более продвинутая защита:

- подключаются NLP-модели, обученные на русскоязычных данных, для распознавания имён, адресов, названий организаций и других сущностей в неструктурированном тексте;
- расширяется поддержка различных протоколов, что позволяет охватить все ключевые точки обмена данными;
- вводятся строгие политики контроля, включая возможность полной блокировки передачи при обнаружении критичных данных.

Интеграция Open Source LLM с целевым дообучением

Ключевым преимуществом Inpolus SDDS является использование открытых больших языковых моделей (Open Source LLM), специально дообученных для задач обнаружения конфиденциальной информации. В отличие от универсальных моделей, наши NLP-компоненты проходят целевое обучение на русскоязычных корпусах данных, что позволяет с высокой точностью распознавать имена, адреса, реквизиты и другие сущности даже в неструктурированном тексте. Это обеспечивает глубокий контекстный анализ, недоступный для систем, основанных только на правилах и регулярных выражениях.

Архитектура Inpolus SDDS позволяет проводить специфическое дообучение моделей в рамках внедрения под уникальные потребности бизнеса. Мы адаптируем модели под отраслевую терминологию, внутренние форматы документов и конкретные типы защищаемой информации. Все модели развертываются локально в инфраструктуре заказчика, что гарантирует полный контроль над данными и соответствие требованиям ФЗ-152 и нормативов ФСТЭК России. Такой подход сочетает преимущества современных AI-технологий с необходимым уровнем безопасности и возможностей кастомизации.

Такой эволюционный подход позволяет начать с минимальных усилий и постепенно наращивать уровень защиты - от базовых шаблонов до интеллектуального LLM-анализа – по мере роста зрелости процессов безопасности.

Inpolus SDDS – это встроенный слой безопасности с AI-компонентами, предназначенный для защиты чувствительной информации в условиях современной распределённой инфраструктуры. Его ключевое преимущество – сочетание гибкой интеграции в любую точку обмена данными с интеллектуальными возможностями локально развернутых LLM.

Решение полностью разворачивается внутри доверенного периметра Заказчика, что обеспечивает:

- AI-анализ без компромиссов в безопасности – все LLM-модели работают локально, данные никогда не передаются во внешние системы;
- соответствие строгим требованиям регуляторов, включая ФЗ-152 и нормативные документы ФСТЭК России;
- адаптивную защиту – возможность дообучения моделей под специфику бизнеса и отраслевые требования;
- полный контроль над жизненным циклом информации и AI-компонентами.

В результате...

Вы получаете сквозную интеллектуальную защиту данных в движении – от микросервисов и API до CI/CD-пайплайнов и внешних интеграций. Это создаёт надёжную основу для цифровой трансформации, минимизирует

риски утечек через сложные каналы и укрепляет доверие со стороны клиентов и регуляторов в эпоху AI.