CYBER FENCE
INTELLIGENCE SYSTEMS

RSS

Reports Security Suite

Платформа управления состоянием безопасности данных.

Видеть данные. Измерять защищенность.

Петр Вырупаев · архитектор RSS

ЧАСТЬ 1 · КОНТЕКСТ РЫНКА

Как российский рынок пришёл к защите данных

Шесть ступеней за тридцать лет

СТУПЕНЬ 1 · 1990-Е — 2000-Е

01

СЗИ НСД и режим секретности

Dallas Lock · SecretNet · «Кобра» — разграничение доступа, мандатный контроль

Сертификация ФСТЭК/ФСБ — жёсткий рыночный фильтр: без сертификата продукт фактически непродаваем госсектору и КИИ.

Итог — on-prem-менталитет на десятилетия: софт ставится на собственное железо, в собственный контур. С 2025 года 223-ФЗ закрепил эту модель окончательно.

СТУПЕНЬ 2 · 2003–2015

02

DLP: синхронно с миром

Триггер — инсайдерские утечки и персональные данные, а не облако. Российские вендоры вышли раньше западной волны или одновременно с ней.

2001	«Инфосистемы Джет» представляет систему «Дозор-Джет» — первую в России и одну из первых в мире систем защиты от утечек данных
2004	Основана компания InfoWatch как специализированный поставщик DLP-решений

РЫНОК DLP В РОССИИ · 2015

91 %

российского рынка DLP к 2015 году
принадлежало российским вендорам

Solar · InfoWatch · SearchInform · Zecurion · DeviceLock · МФИ Софт

Импортозамещение здесь случилось задолго до 2022 года

ОГРАНИЧЕНИЕ МЕТОДА

DLP контролирует каналы передачи — но не знает, что и где лежит в хранилищах

СТУПЕНЬ 3 · 2010-Е

03

DAM/DCAP для баз данных

InfoWatch Traffic Monitor DB · «Гарда БД» — аудит доступа к СУБД

Российский аналог западного DCAP/DAM развивался параллельно — под требования 152-ФЗ и отраслевых регуляторов.

Здесь рынок шёл в ногу с мировым, а не с опозданием — но в рамках on-prem баз данных, а не облачных хранилищ.

СТУПЕНЬ 4 · 2012–2020

04

SIEM: соответствие требованиям, а не обнаружение.

MaxPatrol · R-Vision · Kaspersky SIEM — централизованный сбор событий

Драйвер — регуляторный аудит в соответствии с приказами ФСТЭК и 187-ФЗ, а не реальный ландшафт угроз.

По форме соответствует западному SIEM, но смещено на «сдачу проверки», а не на обнаружение атак.

СТУПЕНЬ 5 · 2020–2025

05

Уход западных вендоров освободил нишу

В 2022 году из России ушли Varonis, Netwrix и Forcepoint — свободна ниша DCAP: доступы к файловым хранилищам и аудит прав.

5,4 млрд ₽

рынок PAM к концу 2025 года. Точка насыщения: крупный бизнес и госсектор завершили первичную модернизацию контуров.

СТУПЕНЬ 6 · 2024–2026 · МЫ ЗДЕСЬ

06

Data Discovery — точка схождения

Обзор Anti-Malware (апрель 2026): рынок Discovery-решений перешёл «от стадии зарождения к активному росту».

КОМПЛЕКСНЫЕ DCAP-ПЛАТФОРМЫ

Solar, «Гарда», InfoWatch Data Discovery

DISCOVERY-МОДУЛИ В DLP

Кибер Протего · Zecurion · Falcongaze

Драйверы: 152-ФЗ и приказы ФСТЭК · рост неструктурированных данных · кадровый голод в ИБ · импортозамещение DCAP

398+ млн

записей утекло в России за один месяц

22 инцидента утечек — за тот же январь 2026 года

Две траектории — одна точка схождения

	ЗАПАД	РОССИЯ
Триггер эволюции	миграция в облако и SaaS	регулятор и инсайдеры
Каналы передачи	DLP	DLP — своё, сильное
Доступ к SaaS	CASB	ступени нет
Позиция инфраструктуры	CSPM / CNAPP	сертифицированные СЗИ, PAM
Аудит доступа к данным	DCAP → вытеснен DSPM	DAM / DCAP → Data Discovery
Следующий шаг	DSPM for AI	**открытая ниша**

Облачных ступеней в России физически не было — миграции в SaaS не случилось.

ВЫВОД 1 ИЗ 3

Российский DSPM — это не DSPM в западном смысле

Западный DSPM вырос из облачной слепой зоны и неразрывно связан с CSPM. Российский эквивалент — реинкарнация DCAP + Discovery: обнаружение и классификация в on-prem хранилищах и базах данных, с фокусом на соответствие требованиям, а не на непрерывную оценку состояния защищённости.

ВЫВОД 2 ИЗ 3

Развитие не отстало — оно пошло другим путем

DLP и DAM Россия прошла синхронно с миром. Пропущены только облачные ступени — CASB и CSPM, которых здесь физически не было. Зато есть ступень, которой на Западе нет как категории, — сертифицированные СЗИ.

ВЫВОД 3 ИЗ 3

Ниша российского DSPM-for-AI открыта

Локальные LLM уже разворачиваются в закрытых контурах. Первый, кто соединит Discovery + DCAP с контролем доступа LLM к корпоративным данным, создаст российский DSPM-for-AI. Ни один из шести вендоров обзора этого пока не заявляет.

ЧАСТЬ 2 · РЕШЕНИЕ

RSS — Reports Security Suite

Платформа управления состоянием безопасности данных: обнаружение, классификация и защита — на уровне данных, а не сетевых узлов.

152-ФЗ · On-premise · Автосканирование · Без агентов · Интеграция с DLP / SIEM

Существующие подходы не дают полной картины

01	Ручной труд не масштабируется	Инвентаризация и разметка данных требуют десятков человеко-дней и хронически отстают от роста систем и объёмов.
02	Теневые источники невидимы	Доля БД и файловых хранилищ не попадает в реестры. Нельзя защитить то, о существовании чего не знаешь.
03	Разрыв ИБ, ИТ и владельцев	ИБ не знает инфраструктуру данных, ИТ — классы информации в системах, у владельцев нет актуального реестра активов.
04	Регуляторное давление растёт	Оборотные штрафы, указы № 166 и № 250, обязательный расчёт УЗ ПДн — нужен постоянный контроль, а не разовый аудит.

По итогам 2025 года и первого полугодия 2026 года Россия стала **мировым лидером по числу публичных утечек** баз данных — 326 случаев

РЕШЕНИЕ · RSS

Управление рисками на уровне данных, а не сетевых узлов

RSS автоматически находит теневые базы данных и файловые хранилища, классифицирует чувствительную информацию — персональные и платёжные данные, коммерческую тайну, интеллектуальную собственность — и передаёт события в DLP, SIEM и IRP/SOAR.

152-ФЗ · On-premise · Автосканирование · Без агентов · REST API

Три шага — от источника к защите

01

Инвентаризация и классификация данных

Иерархические классификаторы, теги, ML и экспертная система. Автоматический расчёт УЗ ПДн — до уровня таблицы.

02

Автоматический расчет рисков и приоритетов защиты

Аналитические механизмы, отчеты, автоматический расчет УЗ ПДн, выявление наиболее насыщенных чувствительной информацией источников данных.

03

Применение политик и обогащение знаниями

Правила «условие — действие». События и уведомления в DLP, SIEM, IRP/SOAR. Модули проксирования информационных потоков к источникам данных.

Пять модулей — одна платформа

01	Классификация	Агенты классификации, брокер сообщений, балансировщик, БД исключений, визуальный редактор классов данных.
02	Аналитика	Аномалии расположения данных: несочетаемые классы в таблице, новые классы, ошибки ввода, изменения структуры БД.
03	Расчет рисков	Визуализация классов информации: базы данных, файловые хранилища, шины данных. Risk Radar с собственной методологической базой. Автоматический расчет УЗ ПДн.
04	Интеграция	Работа по запросу и через модуль проксирования информационных потоков. Применение политик безопасности, шифрование информации.
05	API для ИБ-систем	Обогащение внешних политик безопасности классами данных для систем защиты.

Атомарные понятия выявляет ИИ

Малые ML-модели

Автоматическое отнесение данных к критичным категориям

BERT

Понимание смысла неструктурированного текста

Скрипты поиска

Точные шаблоны для формализованных данных

Экспертные системы

Правила отнесения в визуальном редакторе классов

Плюс инфраструктура модуля: иерархические классификаторы, теги и метки, БД исключений, система логирования.

ПРЕИМУЩЕСТВА

Защита от ценности данных

а не от топологии сети — пять причин выбрать RSS

01	Data Centric Security	Анализ содержимого и классов данных, а не адресов и протоколов.
02	Без агентов	Работа через существующие сетевые протоколы и анализ трафика — ничего не ставится на устройства.
03	Минимум ручного труда	Сканирование, классификация и расчёт УЗ ПДн выполняются автоматически.
04	Сильнее DLP и SIEM	Классы данных обогащают политики и правила корреляции — меньше ложных срабатываний.
05	Единый каталог и модель угроз	Risk Radar показывает наиболее уязвимые источники и помогает расставить приоритеты.

Для всех, кто отвечает за данные

CISO / руководитель ИБ	Единый центр контроля защищённости данных, объективная оценка рисков, соблюдение требований регуляторов.
Data Governance / CDO	Понимание, какие данные где хранятся, как классифицированы и используются в процессах.
SOC / расследования	К какому классу относился скомпрометированный файл, где он находился, каким политикам подчинялся.
Владельцы систем и ИТ	Прозрачный реестр информационных активов и ответственных — без разрыва между эксплуатацией и ИБ.

РЫНОК И МОДЕЛЬ

1,6 → 9,7 млрд ₽

объём рынка DCSP / DCAP / DAM / DBF
в России: оценка 2025 → 2030

МОДЕЛЬ

B2B-лицензии и консалтинг

ЦЕНА

от 20 000 ₽ за базу данных

КЛИЕНТЫ

Enterprise · Россия

MVP, пилоты, реестр ПО

Стадия	MVP и пилотные внедрения; разработка ведётся со II квартала 2025 года.
Реестр ПО	Свидетельство о государственной регистрации программы для ЭВМ № 2025687978 от 16 октября 2025 года. Подана заявка на внесение в реестр российского ПО.
Команда	13 человек: разработка — 8, продажи, менеджмент и маркетинг — 5.
Финансирование	Частная компания, развитие продукта на собственные средства.

ЦЕЛЬ

40 % рынка DCSP России

Дальше — рынки дружественных государств и новая категория: системы, управляющие данными внутри информационных систем компаний. Следующий шаг предсказуем — первый российский DSPM-for-AI.

Ищем партнёров для пилотных проектов

Проблема	Локальные LLM получают доступ к корпоративным данным, но неизвестно, какие это данные, где они лежат и насколько критичны.
Решение	Обнаружить, классифицировать и оценить риски данных, к которым обращается LLM, и подсветить, что защищать в первую очередь.
Что получаете	Проверим на вашем контуре: on-premise, без агентов, 152-ФЗ. Поможем настроить политики доступа LLM к данным.
Партнёрам	Приоритетный доступ к RSS, влияние на roadmap, первый кейс в открытой нише российского DSPM-for-AI.

RSS · REPORTS SECURITY SUITE

Рады ответить на ваши вопросы

CYBER FENCE
INTELLIGENCE SYSTEMS

rss-plus.ru

info@rss-plus.ru

+7 926 701-83-84