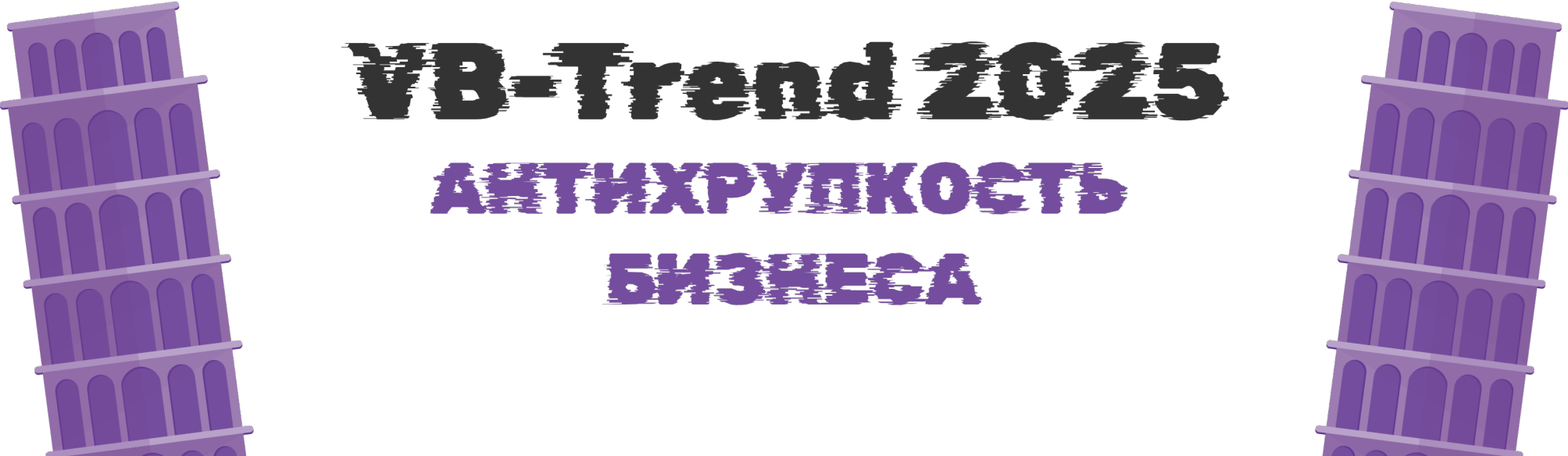




VB-Trend 2025

АНТИХРУПКОСТЬ

БИЗНЕСА

Smart Monitor

в Банке России



Митричева Наталия
ЛИНС-М

Smart Monitor в Банке России

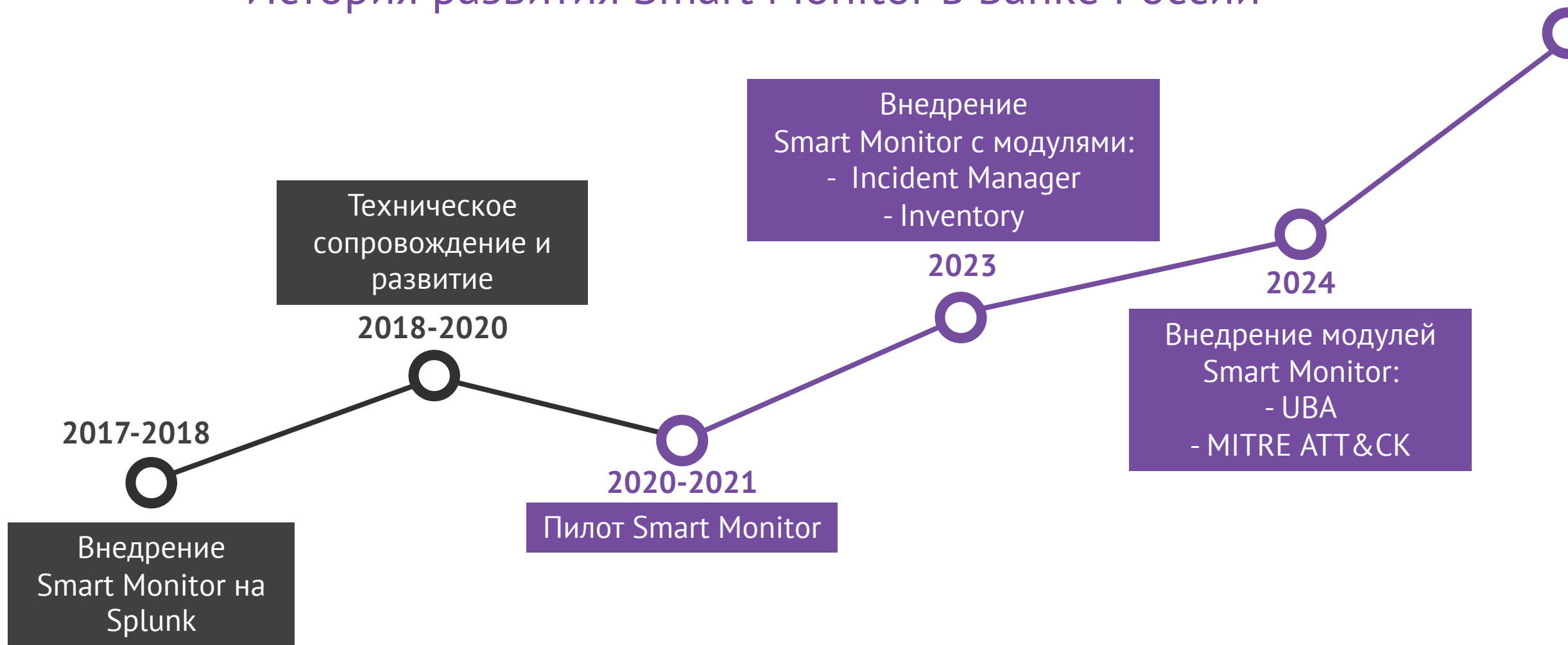


На базе платформы **Smart Monitor** реализован **комплексная платформа мониторинга данных** информационной безопасности

Ключевые функции:

- Централизованный **сбор, индексация и хранение** событий ИБ с узлов и телекоммуникационной инфраструктуры, узлов прикладных платформ и других компонентов комплекса технических средств
- **Аналитическую обработку** (в том числе с применением корреляционных правил) собранных событий ИБ
- **Визуализацию** состояния информационной безопасности
- **Оповещение** ответственных из подразделения информационной безопасности об обнаруженных инцидентах

История развития Smart Monitor в Банке России



Smart Monitor сейчас

Инсталляции
Smart Monitor
в нескольких сегментах

Кластеры в
отказоустойчивой
конфигурации на ресурсах
геораспределённого ЦОД

Модули Smart Monitor:

Incident Manager
Inventory
MITRE ATT&CK
UBA

Служба реагирования
работает в
Менеджере
Инцидентов

>50
типов источников

>13K
агентов

~300 БД
подключено

>200
контроллеров
домена
подключено

Особенности проекта

Требования к гибкости и адаптивности

- **любой** источник событий
- интеграция и **взаимодействие со сторонними системами**
- **создание интерактивных витрин**
- использование **не только для задач ИБ**

Сложность вписаться в ИТ ландшафт с учётом требований к системам и внутренним процессам

- **множество** сегментов
- **территориально-распределенный** ИТ-ландшафт
- автоматизация **имеющихся** процессов

Единое окно для работы с данным

- разные **роли** пользователей, разные **задачи**
- пользователи из разных **регионов и часовых поясов**

Развитие системы

Использование Smart Monitor для сценариев из смежных областей

- Единое озеро данных на Smart Monitor (ИБ, ИТ и ВІ)
- Сервис предоставления отчетов о доступах к ИС

Масштабирование
~ в 2 раза

Анализ метрик состояния системы обеспечения ИБ

Организация взаимодействия инсталляций из разных сегментов

Использование гибридного хранилища

SSO-аутентификация



Спасибо за внимание!