Ankey ASAP

ГАЗИНФОРМ СЕРВИС

Advanced Security Analytics Platform

# Платформа расширенной аналитики безопасности

GIS ГАЗИНФОРМ СЕРВИС

**ООО «Газинформсервис»** — один из крупнейших в России системных интеграторов в области безопасности и разработчиков средств защиты информации.

Компания работает с 2004 года, реализует весь комплекс услуг, необходимых для создания систем информационной безопасности и комплексов инженерно-технических средств охраны любого масштаба.

## Наша миссия

Наша миссия — быть надежным партнером для бизнеса в построении комплексной безопасности будущего. Мы создаем и внедряем безопасные и доверенные решения на основе искусственного интеллекта, чтобы наши заказчики могли уверенно развиваться в цифровую эпоху. Основой нашего успеха являются высочайший профессионализм и преданность наших сотрудников.

# Партнеры

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

В рамках технологического сотрудничества компания Газинформсервис обеспечивает интеграцию собственных разработанных решений и продуктов наших партнеров, гарантируя **максимальную совместимость и высокую производительность**

pt

РЕДСОФТ

kaspersky

INFOWATCH® МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ASTRA LINUX®

Стахановец

АЙТИБАСТИОН

staffcop®

Ankey ASAP

ГАЗИНФОРМ СЕРВИС

Advanced Security Analytics Platform

# Платформа расширенной аналитики безопасности

# Ключевые вызовы современной информационной безопасности

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

## Лавина ложных срабатываний

Абсолютно все заказчики сталкиваются с высокой зашумленностью — сотнями тысяч алертов в сутки, многие из которых являются ложными срабатываниями.

## Острая нехватка квалифицированных кадров

Для ручного анализа даже части инцидентов требуются операторы первой линии SOC, которых критически не хватает на рынке.

## Время на реагирование сократилось до минут

С появлением ИИ у атакующих скорость реализации атак сократилась до десятков минут, что делает ручной анализ неэффективным даже при наличии операторов.

## Результат:

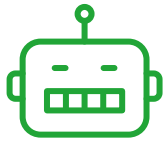
Ручной перебор алертов больше не справляется с современными угрозами, требуя принципиально новых подходов к анализу и реагированию.

**Первый ключ к решению проблемы False Positive** — в эффективном отсечении однотипных событий.

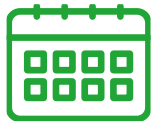
**Разработка интеллектуальных алгоритмов фильтрации** — сложный процесс, включающий анализ паттернов, создание базовых линий и адаптацию под специфику инфраструктуры.

Ankey ASAP **автоматически строит поведенческие базовые линии** и подсвечивает отклонения, избавляя от необходимости донастройки сигнатурных правил в SIEM-системах и в анализаторах трафика

Ankey ASAP GIS ГАЗИНФОРМ СЕРВИС



**Только ИИ** способен эффективно анализировать тысячи алертов от различных СЗИ в режиме реального времени



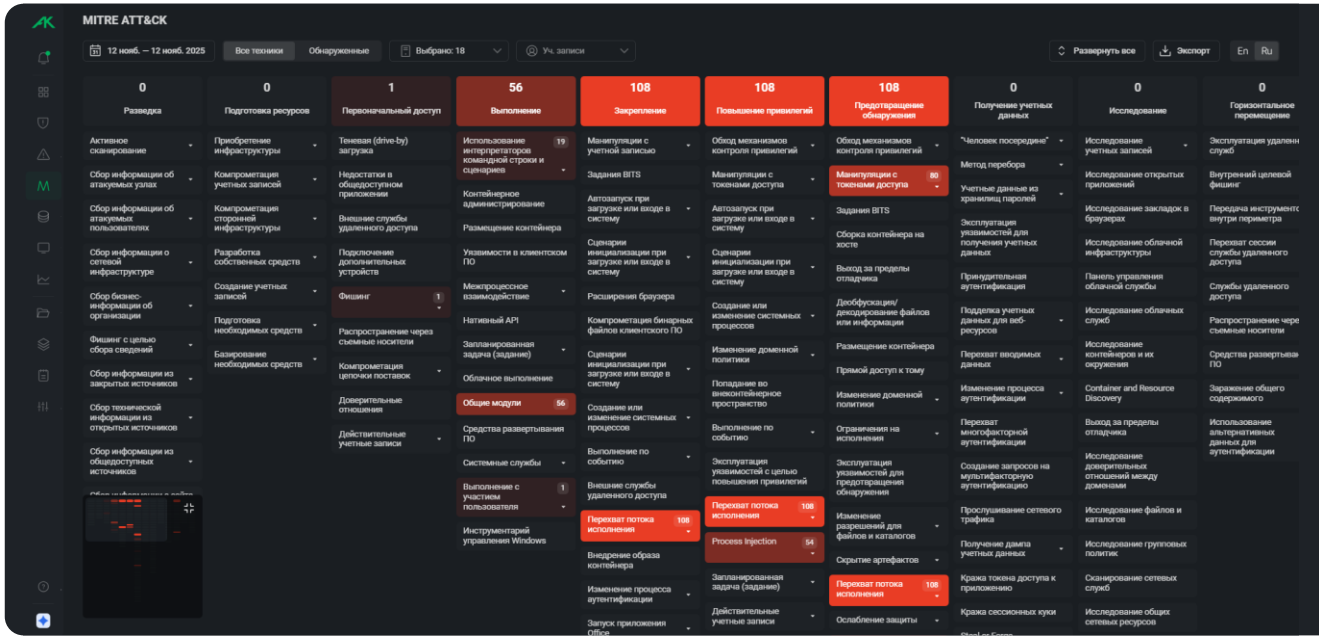
Создание таких систем требует **глубокой экспертизы** и занимает многие месяцы целенаправленной работы

Мы создаем решения с **повышенной объяснимостью** через интеграцию ИИ, графов атак и матрицы MITRE ATT&CK

# Поведенческая аналитика
UEBA

Профилирование базовых линий поведения объектов анализа (пользователей и устройств) и выявление отклонений методами статистического анализа и машинного обучения.

Обнаружение подозрений на инциденты на основе корреляции с паттернами атак.




# Инструменты расследования инцидентов

Формирование контекста для проведения аналитики операторами SOC:

- настраиваемые дашборды;
- визуализация инцидента в виде графа;
- визуализация действий объектов в виде таймлайна (ленты событий).

Ankey ASAP

ГАЗИНФОРМ СЕРВИС

# АРХИТЕКТУРА ПЛАТФОРМЫ

# Вариант инсталляции Ankey ASAP


**Аппаратные требования:**

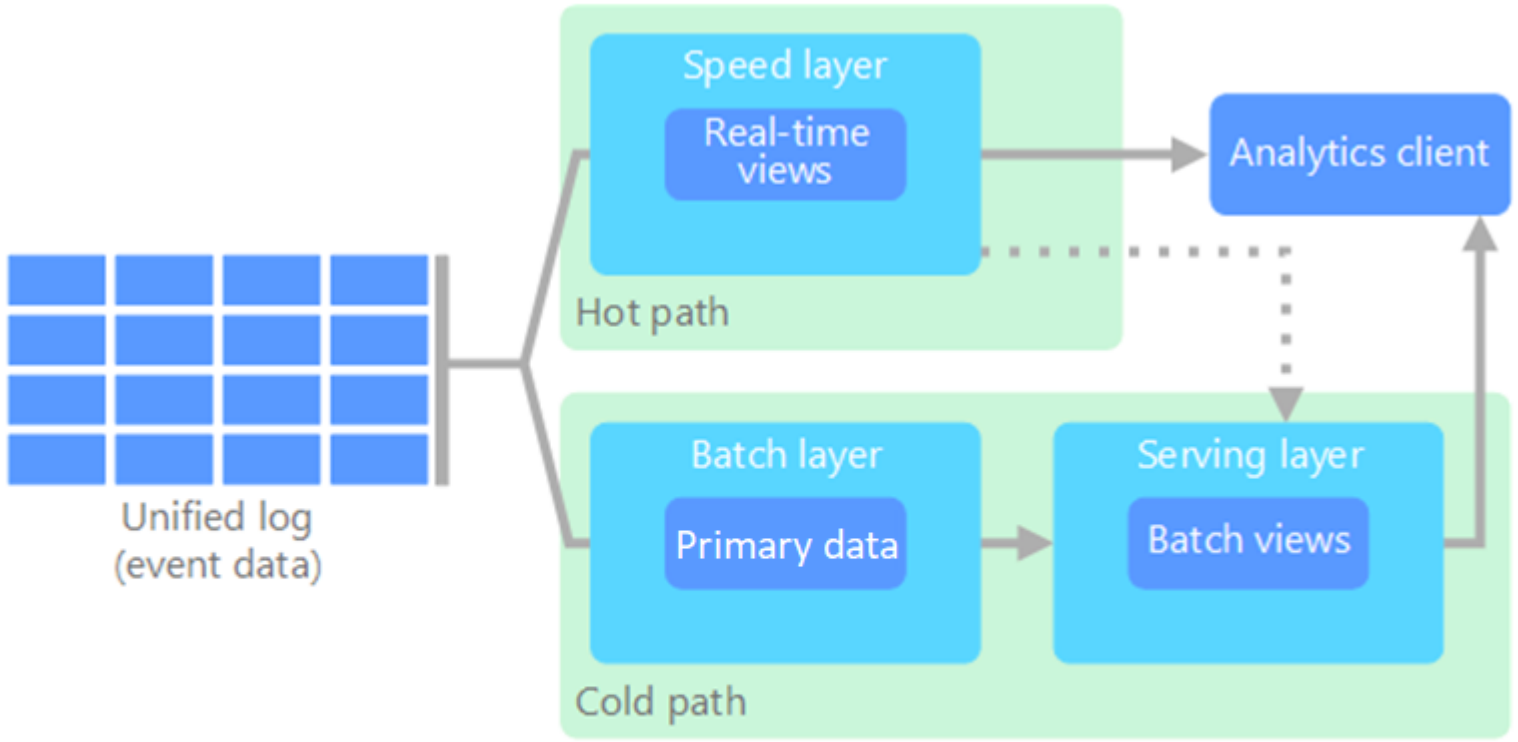
ОС: Astra Linux Special Edition 1.7.1 и выше, РЕД ОС 7.3 или 8

СУБД: Защищенная СУБД «Jatoba», сертификат соответствия № 4327 (выдан ФСТЭК России 19.11.2020 г.) (поддерживается версия ядра «4»)

# Лямбда-архитектура*

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС



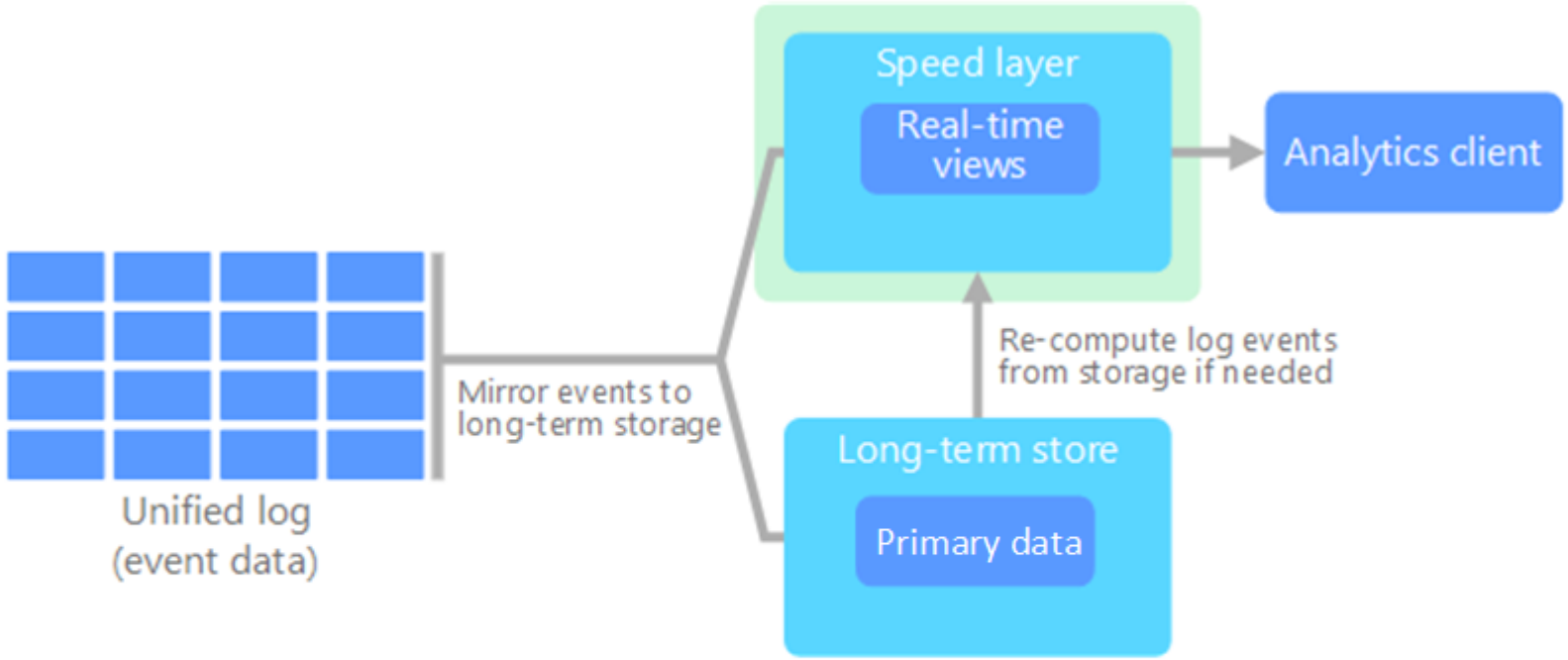

Microsoft Azure

*Немного на душном

# Каппа-архитектура*

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС




Microsoft Azure

*Немного на душном

# Интеграция с продуктами

Ankey ASAP | Ankey ASAP GIS ГАЗИНФОРМ СЕРВИС

Ankey ASAP имеет прямую интеграцию
со следующими продуктами:

- SIEM KUMA
- SIEM MAX Patrol
- SIEM ArcSight
- SIEM Саврус
- SIEM Ankey SIEM NG
- DLP Staffcop
- DLP Стахановец
- Efros CI

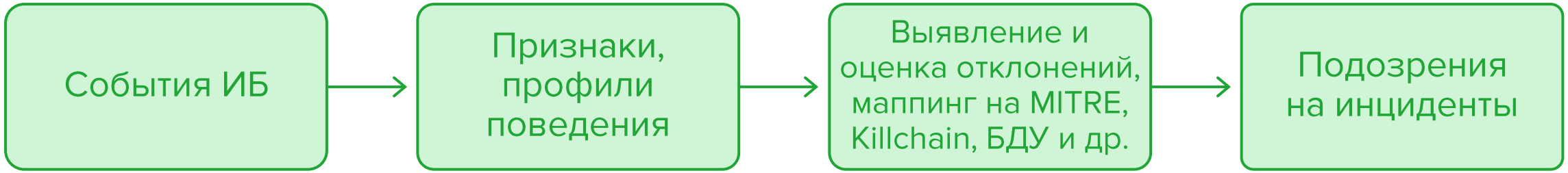
Ankey ASAP

ГАЗИНФОРМ СЕРВИС

# АНАЛИЗАТОРЫ

# Как Ankey ASAP «видит» атаки

Ankey ASAP | GIS ГАЗИНФОРМ СЕРВИС




1. **Профилирование «нормального» поведения:**
   Создание профилей нормального поведения для каждой учетной записи и устройства.
2. **Обнаружение отклонений:**
   Автоматическая генерация алертов об аномальном или подозрительном поведении.
3. **Разметка на классификаторы:**
   Каждый алерт автоматически сопоставляется с конкретной техникой и тактикой в матрице MITRE, этапом цепочки Killchan и техникой матрицы инсайдера.
4. **Построение цепочки атаки (корреляция):**
   Алерты не являются инцидентами, они служат контекстом для обнаружения потенциальных инцидентов.
   Система объединяет разрозненные алерты на основе классификаторов и оценки скоринга в единую цепочку, формируя для Оператора «готовый к расследованию» инцидент.

# Анализаторы Ankey ASAP

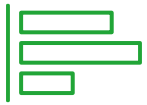
Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

## Редкие события

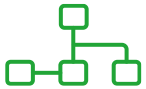
Выявление впервые происходящих действий

(новых или редких событий)



## Подозрительные терминальные команды

Выявление деструктивных терминальных команд при использовании легитимных или встроенных системных утилит (cmd, powershell, netcat и др.) алгоритмами обучения с учителем (ансамбль решающих деревьев, Random Forest и BLEU)



## Отклонение от базовой линии поведения

Выявление аномального количества или объема событий методами статистического анализа

## Нетипичное время

Выявление событий, происходящих в необычное время для объектов, статистическими методами оценки функции плотности вероятности

# Анализаторы в Ankey ASAP

Ankey ASAP | GIS ГАЗИНФОРМ СЕРВИС

| Наименование | Вид анализатора | Механизм | Модели\Правила | Решаемые задачи |
|---|---|---|---|---|
| Анализатор детектирования аномального количества | Обучение на данных Заказчика | Вычисление процентиля в распределении значений отслеживаемого признака | 45 | Выявление статистическим методом аномально большого количества событий |
| Анализатор терминальных команд | 2 режима работы:<br>• Предобученный<br>• Предобученные + первые действия (обучение на данных заказчика) | Алгоритм Random Forest + алгоритм выявления схожести команд | Модели для Windows и Linux | Выявление использования потенциально вредоносных терминальных команд |
| Анализатор детектирования редких или впервые совершаемых действий | Обучение на данных Заказчика | Хэширование признаков, правила + списки | > 1 300 правил | Выявление фактов выполнения редкого или впервые совершаемого действия объектом анализа |

# Анализатор детектирования аномального количества

Ankey ASAP | GIS ГАЗИНФОРМ СЕРВИС

Выявление статистическим методом аномально большого количество событий

Пакет контента состоит из 45 профилей

**Основные параметры**

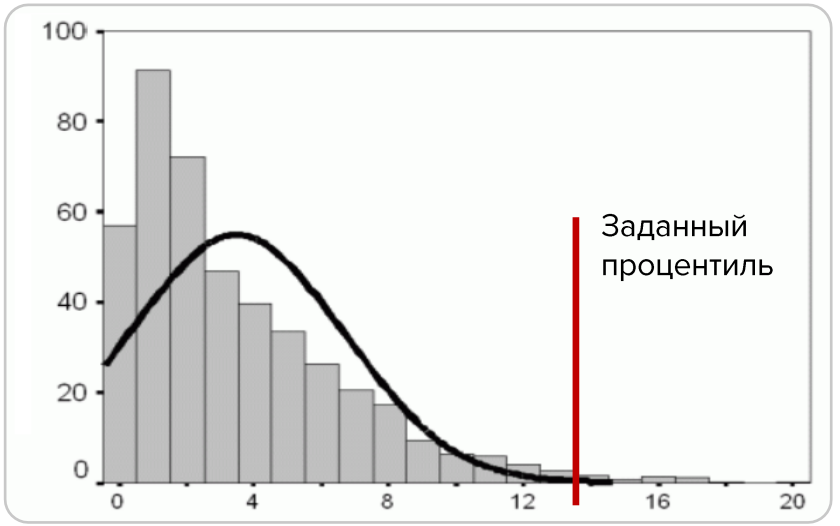
1. Значение процентиля. По умолчанию – 0,01.
2. Минимальное количество слотов для расчетов. По умолчанию – 10.
3. Максимальное количество слотов для расчетов. По умолчанию – 672.
4. Временной слот (период для агрегации событий). По умолчанию – 15 минут

**Алгоритм работы**

1. Соблюдение всех условий.
2. Построение распределения.
3. Получение нового значения, которое не учитывалось в расчетах.
4. Если расчетное значение количества определенных событий не будет укладываться в заданный процентиль, то будет формироваться алерт.

**Тематики**

1. ACCESS
2. AD
3. FILEOP
4. ADM
5. AUTH
6. CONNECT
7. EMAIL
8. MESSENGER
9. PRINT
10. PRIV
11. PROCESS




**Особенности работы**

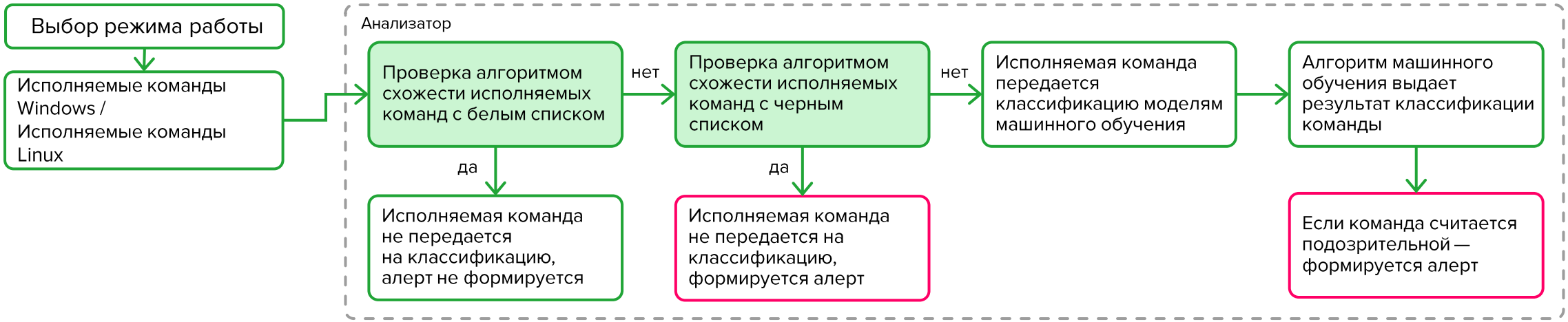
- Используется один анализируемый признак
- Легко интерпретируемые результаты
- Используются ненулевые значения

# Анализатор терминальных команд

Ankey ASAP

ГАЗИНФОРМ СЕРВИС

## Предназначен для выявления использования потенциально вредоносных терминальных команд




**Алгоритм работы:**

У анализатора существует 2 режима работы:

1. анализ всего потока;
2. анализ редких или впервые совершаемых действий.

Пользователю необходимо выбрать наиболее подходящий

**Алгоритм классификации:**

Random Forest для Windows

Random Forest для Linux

**Набор данных для обучения модели Windows:**

490 «плохих» команд

700 тыс. «хороших» команд

**Набор данных для обучения модели Linux:**

1 600 «плохих» команд

8 млн «хороших» команд

# Анализатор детектирования редких или впервые совершаемых действий

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

**Выявление фактов выполнения редкого или впервые совершаемого действия объектом анализа**

**В пакете контента более 1 300 правил**

## Тематики:

1. ACCESS
2. AD
3. ADM
4. AUTH
5. CONNECT
6. EMAIL
7. FILEOP
8. INSTALL
9. MESSENGER
10. POLICY
11. PRINT
12. PRIV
13. PROCESS
14. SHARE
15. USB
16. WEB
17. WIRELESS
18. WMI

## Основные параметры:

1. Анализатор является обучаемым.
2. Рекомендованный период для обучения – от 14 дней.
3. Присутствует функционал забывания совершенных действий. Параметр по умолчанию – 90 дней.

**Например:** подключение пользователем на новый для себя хост; получение письма с вложением от нового адресата для пользователя; впервые создание задачи в планировщике задач Windows; и т. д.

Ankey ASAP

ГАЗИНФОРМ СЕРВИС

# МЕСТО И РОЛЬ В ИБ

# Область применения продукта

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

1 SOC-центры, операторы первой линии

2 Enterprise-сегмент с большим штатом сотрудников и оборудования

3 Организации с развитой ИТ-инфраструктурой и большим количеством разных систем защиты информации

4 Компании, где четкое следование правилам корреляции (SIEM) невозможно в силу нестандартного процесса работы, необходимости подстройки под процесс

# Выгоды от использования

Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

## Для руководства

Снижение капитальных расходов на ИБ

Сокращение риска возможности кибератак

Поддержание репутации компании за счёт устойчивости перед атаками

## Для SOC

Аналитические дашборды — как инструмент для оперативного выявления признаков инцидентов ИБ

Сокращение потока срабатываний за счёт комплексной работы анализаторов

Выполнение требований регуляторов
(Приказы №17, 21: ИНЦ.2, ИНЦ.3, ИНЦ.4, АУД.4, АУД.6, АУД.7, АУД.9; Приказы №239, 31: ИНЦ.1, ИНЦ.2, ИНЦ.3 (совместно с орг.мерами), ИНЦ.6, АУД.4, АУД.6, АУД.7, АУД.9)

## Для ИБ

Обнаружение аномалий  и атак за счёт расширенной поведенческой аналитики

Раннее обнаружение действий атакующего в инфраструктуре

# Преимущества использования Ankey ASAP с SIEM и DLP

Актуален, когда часто изменяется ландшафт инфраструктуры и нужны частые перенастройки правил

Выявляет атаки, для которых не реализованы правила корреляции или сигнатуры

Подсвечивает риски ИБ, которые ещё не сработали

Не требует чёткой последовательности событий или чётко установленных порогов

Выявляет атаки на более ранних стадиях Kill-chain (подтверждённый опыт в ходе участия в theStandoff365)

# Сведения о продукте

Ankey ASAP | Ankey ASAP GIS ГАЗИНФОРМ СЕРВИС

## Ankey ASAP соответствует требованиям регуляторов

1. Внесен в Единый реестр российских программ для ЭВМ и Баз данных под регистрационным номером ПО 6651 приказом Минцифры России от 23.04.2020 г. №191
2. Сертифицирован ФСТЭК России по уровню доверия 4

## Меры защиты по Приказу ФСТЭК России № 239

Инц.1 Выявление компьютерных инцидентов

Инц.2 Информирование о компьютерных инцидентах

Инц.3 Анализ компьютерных инцидентов

Инц.6 Хранение и защита информации о компьютерных инцидентах

Ауд.4 Регистрация событий безопасности Ауд.6 Защита информации о событиях безопасности

Ауд.7 Мониторинг безопасности

Ауд.9 Анализ действия отдельных пользователей

# Лицензирование Ankey ASAP

Ankey ASAP | GIS ГАЗИНФОРМ СЕРВИС

**Программный комплекс  Ankey ASAP предусматривает следующие виды лицензий:**

### Демо

Бесплатная с ограниченным сроком лицензия, предназначенная для ознакомления с программой

### Коммерческая

Платная лицензия, предоставляемая при приобретении программы

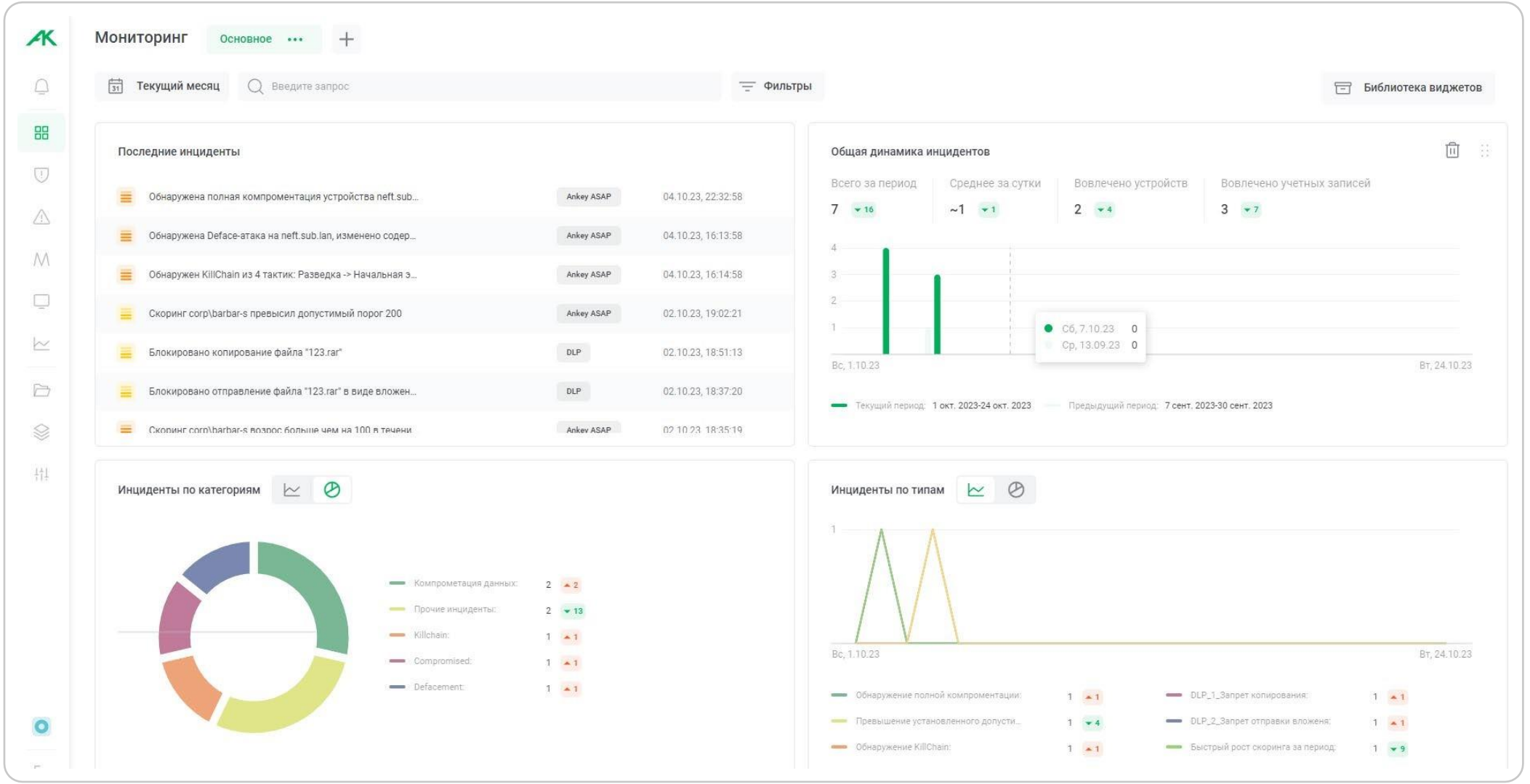
## Основные метрики лицензирования ASAP UEBA

- **Количество анализируемых объектов**
  Число учетных записей и хостов, подлежащих анализу поведения
- **Коннекторы интеграции**
  Источники событий безопасности, не поддерживаемые «из коробки»
- **Масштаб инсталляции**
  Многоузловая установка

# Демонстрация Ankey ASAP

Ankey ASAP

ГАЗИНФОРМ СЕРВИС



Ankey ASAP

GIS ГАЗИНФОРМ СЕРВИС

# Повысьте устойчивость вашей компании к атакам в два шага:

**1** Пилот ⟶ **2** Внедрение продукта

Отдел продаж:
+7 (812) 677-20-53
sales@gaz-is.ru