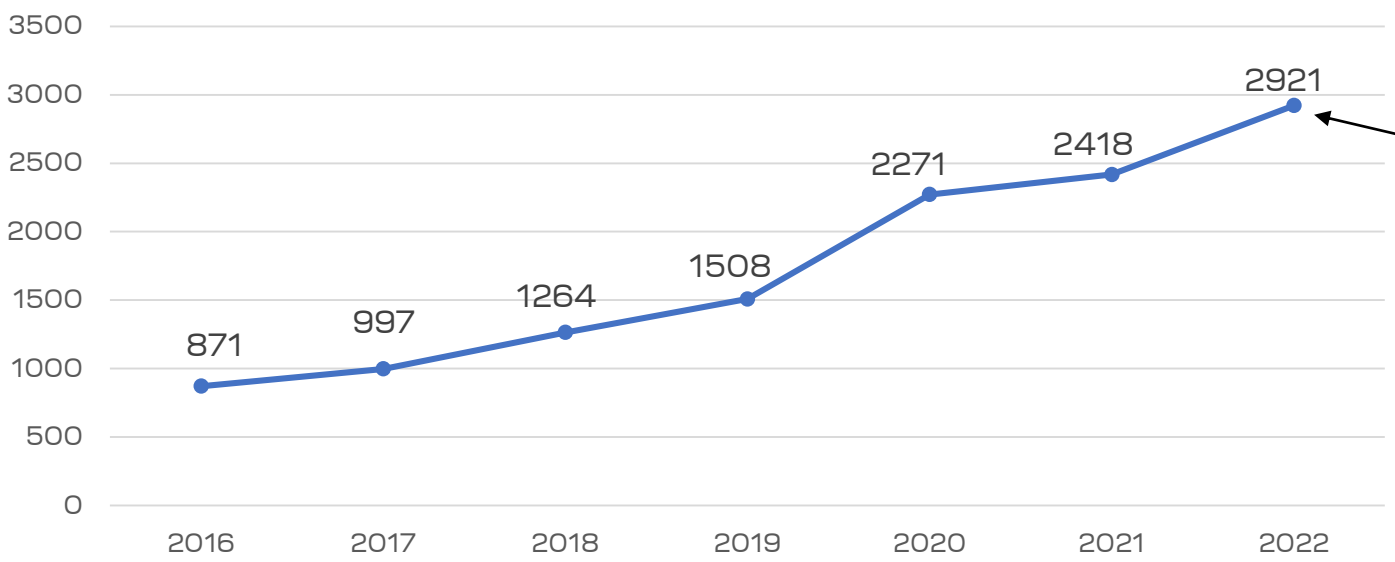
Автоматизация деятельности центров противодействия киберугрозам средствами платформы UDV ePlat4m SOAR

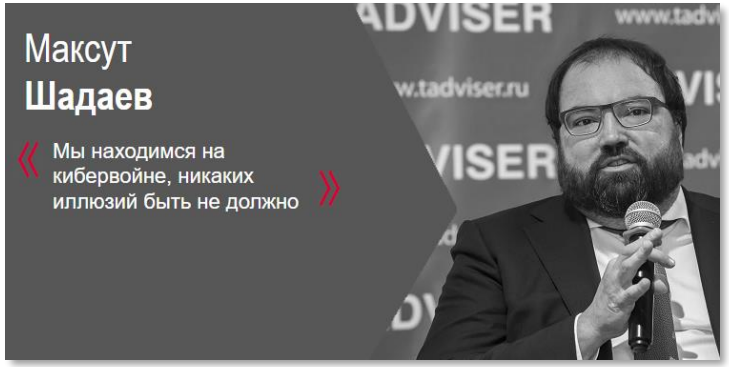
Современные тренды кибербезопасности

Рост количества кибератак по годам [1]



304 млн. рублей средний ущерб от инцидента ИБ в мире

277 дней средний срок выявления и локализации инцидента ИБ[2]



«Сбер» оценил число участвующих в кибервойне с Россией хакеров в 100 тыс.

Более 100 тыс. хакеров участвуют в кибервойне против России, считают в Сбербанке, указав, что ежедневно отражают DDoS-атаки.

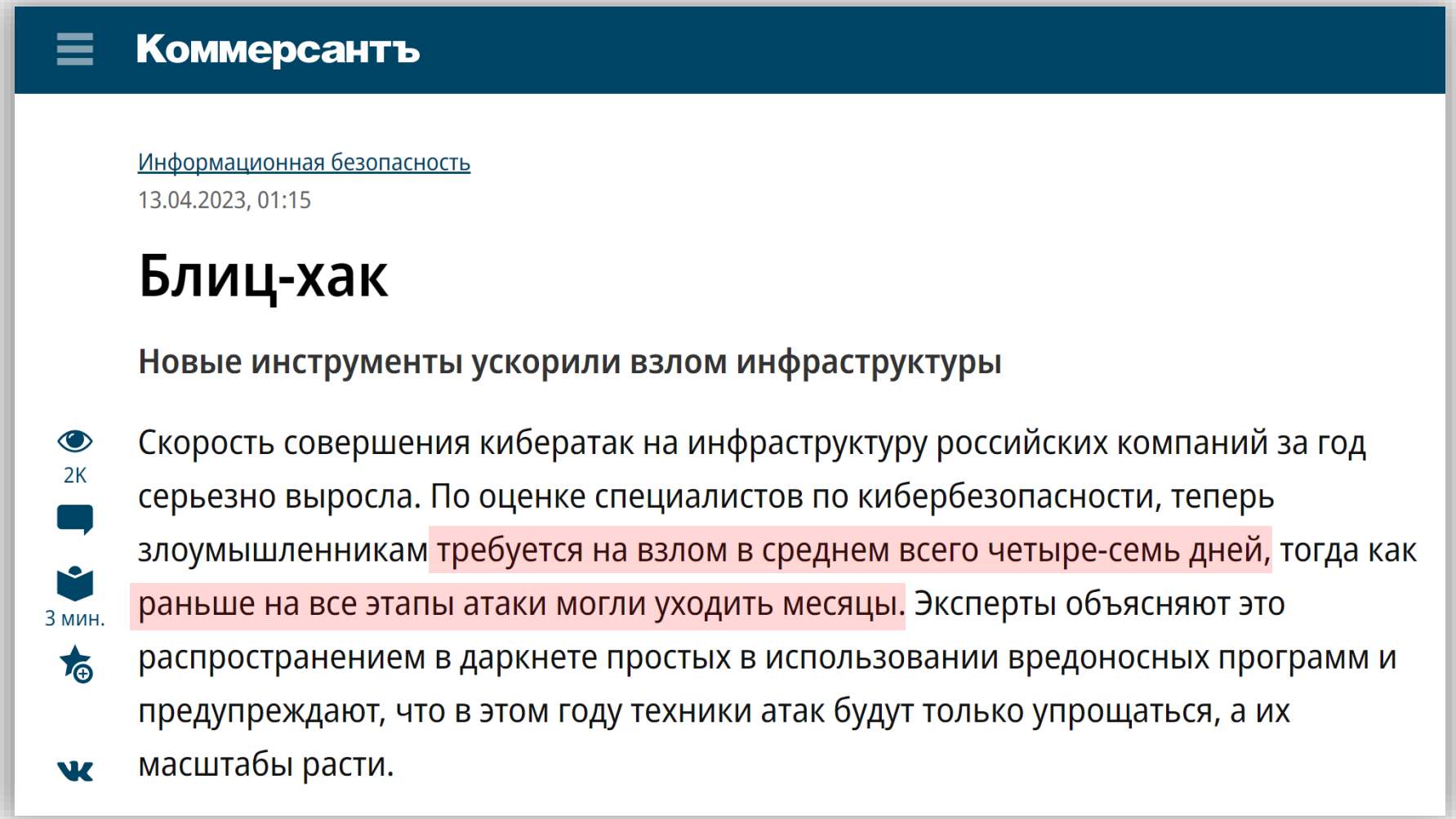
Участники рынка оценили дефицит специалистов по кибербезопасности в 30–50 тыс. человек

ИИ научился моментально взламывать каждый второй пароль

Home Security Heroes: ИИ-инструмент PassGAN научили моментально взламывать 51% паролей

1 – Исследования компании Positive Technologies. 2 – Исследование компании IBM

Рост скорости совершения кибератак



Коммерсантъ

Информационная безопасность

13.04.2023, 01:15

Блиц-хак

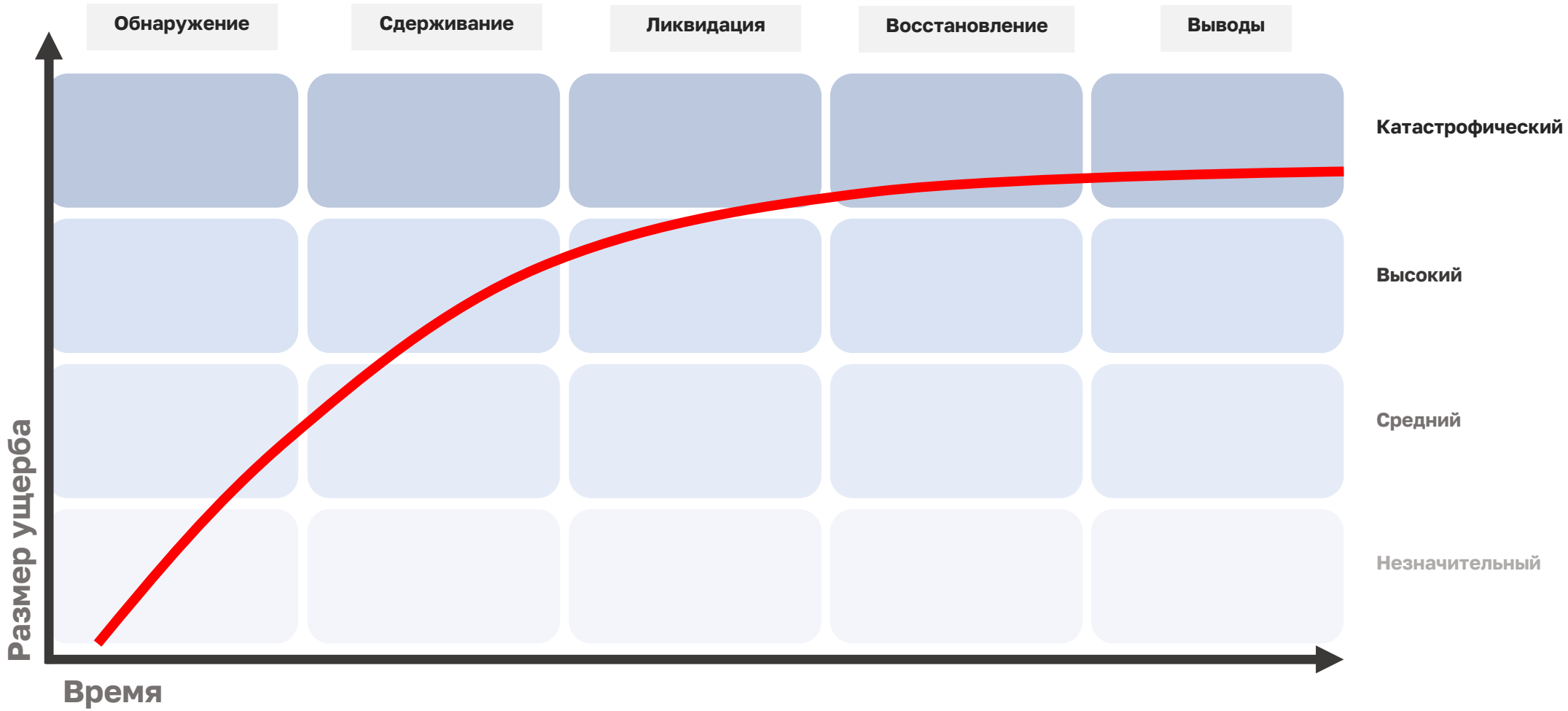
Новые инструменты ускорили взлом инфраструктуры

2K

3 мин.

Скорость совершения кибератак на инфраструктуру российских компаний за год серьезно выросла. По оценке специалистов по кибербезопасности, теперь злоумышленникам требуется на взлом в среднем всего четыре-семь дней, тогда как раньше на все этапы атаки могли уходить месяцы. Эксперты объясняют это распространением в даркнете простых в использовании вредоносных программ и предупреждают, что в этом году техники атак будут только упрощаться, а их масштабы расти.

Влияние времени выявления и реакции на инцидент ИБ на ущерб



Способы недопущения наступления критичных инцидентов ИБ

Автоматическое выполнение

- рутинных операций при реагировании на инциденты ИБ, выполняемых ранее специалистами в ручную
- сбора информации, необходимой для принятия решений об инцидентах ИБ
- исключения ложно-положительных подозрений

от 85% **сокращение времени реагирования на инциденты ИБ при использовании решений по автоматизации**

¾ **операций может быть автоматизировано**

Снижение влияния человеческого фактора

- Наличие типовых апробированных сценариев реагирования для всех типовых инцидентов ИБ
- Снижение вероятности возникновения ошибок из-за человеческого фактора

на 61% **уменьшение затрат на устранение последствий инцидентов ИБ в организациях, разработавших и регулярно тестирующих планы реагирования на инциденты**

SOAR

Security Orchestration,
Automation and Response

ОРКЕСТРАЦИЯ

АВТОМАТИЗАЦИЯ

РЕАГИРОВАНИЕ

Основные задачи центра противодействия киберугрозам

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ

1

- мониторинг инфраструктуры и сбор инцидентов ИБ из различных источников;
- анализ подозрительных событий, регистрация инцидентов, определение их типов и критичности;
- реагирование на инциденты ИБ: локализация, расследование, ликвидация последствий;
- формирование отчетности, взаимодействие с регуляторами (ГосСОПКА)

УПРАВЛЕНИЕ ИТ-АКТИВАМИ

2

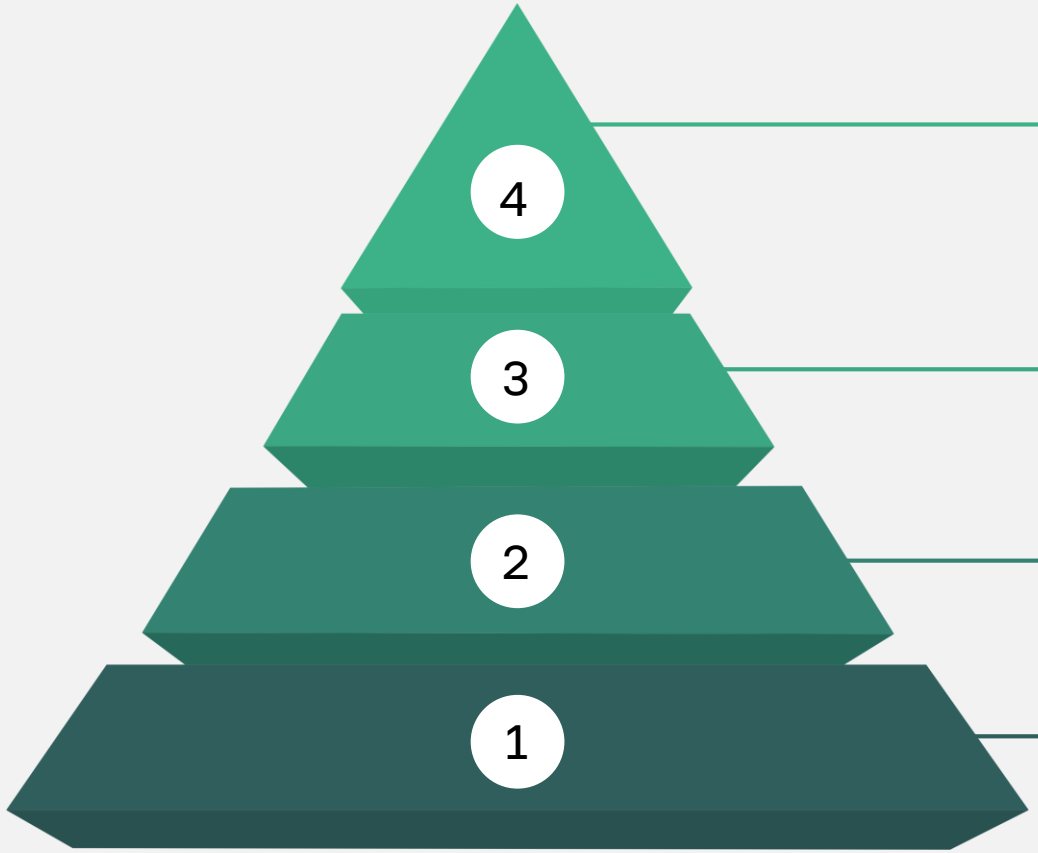
- ведение реестра ИТ-активов инфраструктуры;
- выявление активов, неохваченных системой обеспечения ИБ;
- определение влияния ИТ-активов на информационные системы, процессы и функции предприятия;
- выявление «узких мест» инфраструктуры

УПРАВЛЕНИЕ ВЕКТОРАМИ АТАК

3

- сопоставление инцидента ИБ с ИТ-активами, пораженными в ходе данного инцидента;
- выявление и устранение потенциальных векторов атак;
- минимизация поверхности атаки

Техническая инфраструктура SOC/ЦПК



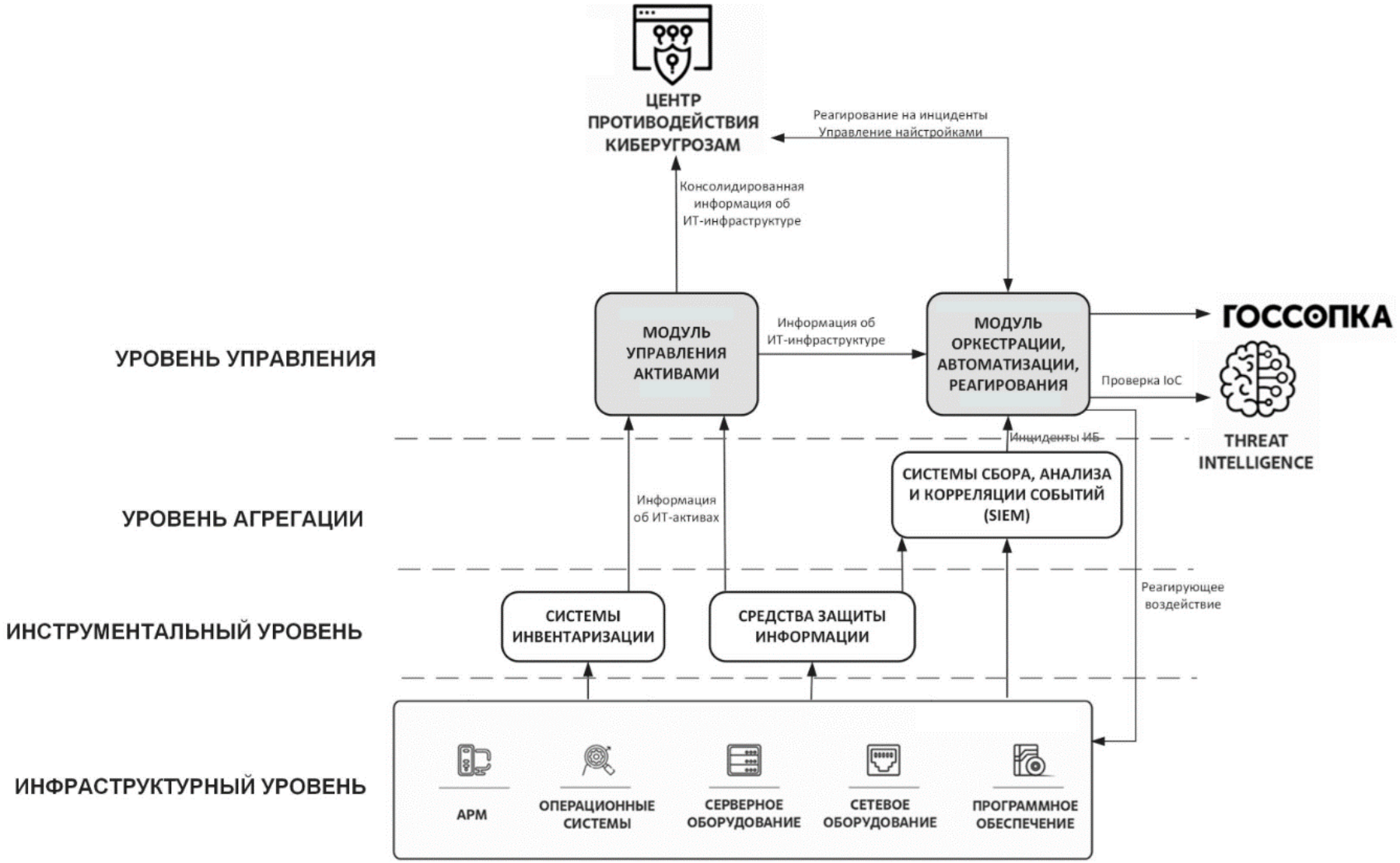
УРОВЕНЬ УПРАВЛЕНИЯ
UDV ePlat4m SOAR

УРОВЕНЬ АГРЕГАЦИИ
SIEM

ИНСТРУМЕНТАЛЬНЫЙ УРОВЕНЬ
Антивирусная защита, МЭ, WAF, СЗИ
от НСД, IDS/IPS, СКЗИ, DLP, anti-DDoS и т.д.

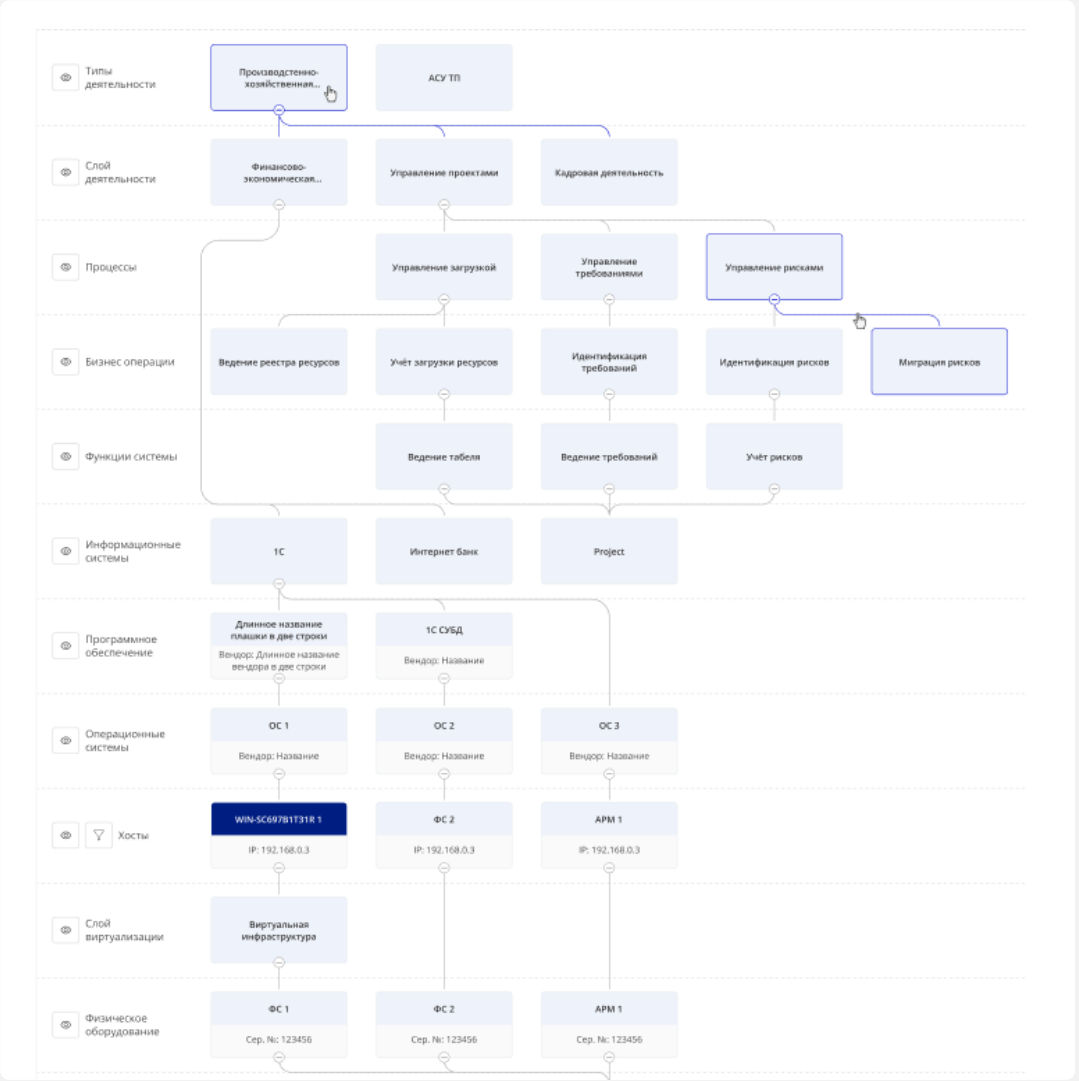
ИНФРАСТРУКТУРНЫЙ УРОВЕНЬ
Серверное оборудование, сетевое
оборудование, АРМ, ОС, СПО, ППО и т.д.

Схема функционирования UDV ePlat4m SOAR



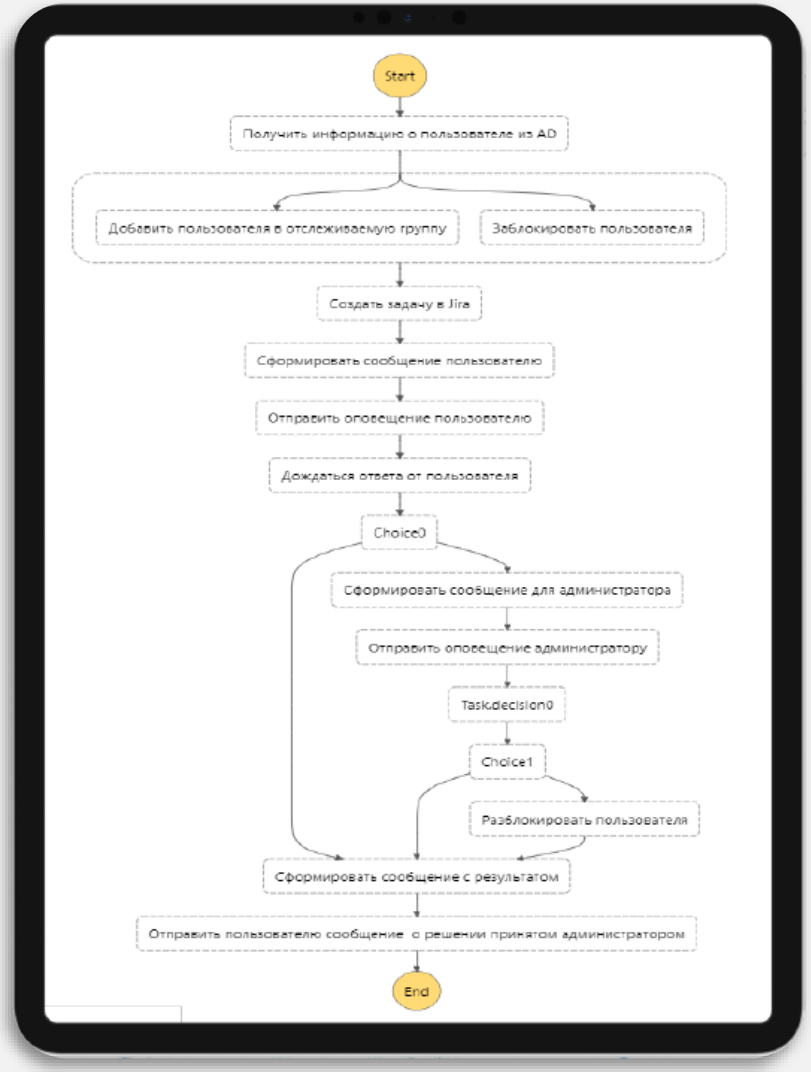
Модуль управления активами

- сбор из различных информационных систем сведений об активах ИТ-инфраструктуры и объединение их по гибко настраиваемым правилам
- ручной ввод информации, которую невозможно собрать в автоматическом режиме
- возможность индивидуальной настройки классификатора и атрибутного состава активов
- визуализация активов и связей между ними с поддержкой ресурсно-сервисной модели
- предоставление REST API для других систем как источник мастер-данных об активах
- возможность ретроспективного анализа состояния активов
- механизм тегирования активов для визуального разделения



Модуль оркестрации, автоматизации и реагирования

- сбор инцидентов ИБ из внешних систем, формирование и ведение карточки инцидента ИБ
- автоматизация workflow алгоритма реагирования на инцидент ИБ
- разграничение прав доступа к инцидентам ИБ согласно ролевой модели, контроль выполнения SLA по инцидентам ИБ
- обмен сведениями с ГосСОПКА
- обогащение инцидентов ИБ информацией из внутренних систем;
- проверка атрибутов инцидента ИБ во внешних сервисах
- реализация реагирующего воздействия на инциденты ИБ в автоматическом режиме путем выполнения скриптов
- возможность самостоятельной разработки и отладки новых наборов скриптов автоматизации

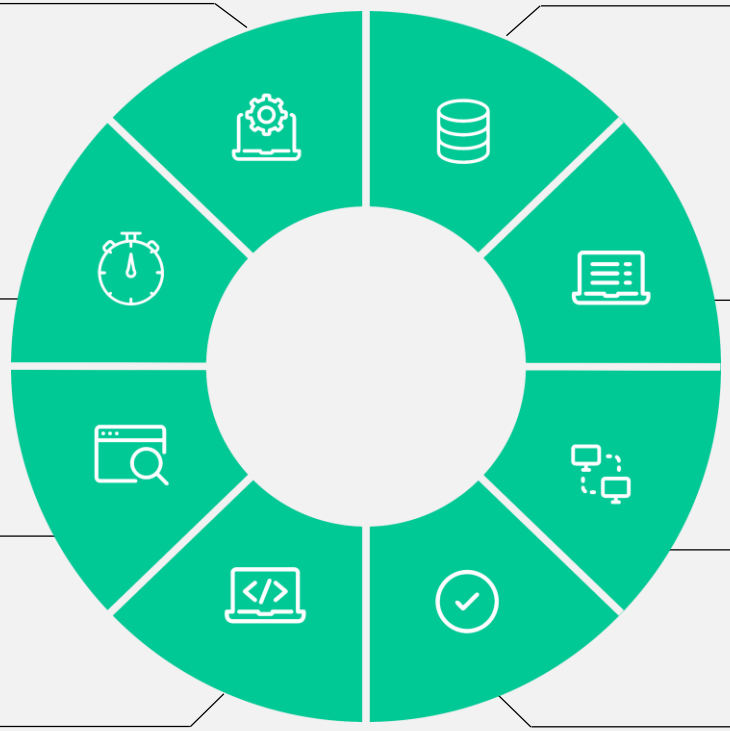


Преимущества SOAR-платформа UDV ePlat4m SOAR

Принцип **low-code**, позволяющий без программистов дорабатывать систему

Иерархичная инфраструктура, мультитенантность

Набор планов **мероприятий** по реагированию и **сценариев** реагирования из **«коробки»**



Гетерогенность, **кроссплатформенность**, поддержка **различных** скриптовых **языков**

Отслеживание **пораженных ИТ-активов**

Интеграции «из коробки» с наиболее распространенными ИТ и ИБ решениями

Инфраструктура разработки и отладки **сценариев реагирования**

Поддержка ресурсно-сервисной модели

Российское производство: № 3733 в реестре отечественного ПО сертификат соответствия ФСТЭК России № 4433

Эффект от внедрения

Автоматизация процесса управления Инцидентами	Уменьшение времени реагирования на инциденты и минимизация ущерба от них
Готовые сценарии реагирования на инциденты и сбор дополнительной Информации	Повышение качества реагирования на инциденты
Автоматическое выполнение операций и проверка на ложно-положительные Сработки	Уменьшение вероятности возникновения рисков, связанных с человеческим фактором
Уменьшение количества ручных операций	Снижение нагрузки на аналитиков ИБ

Выполнение требований нормативно-правовых документов в области ИБ

Номера закрываемых мер в соответствии с Приказом ФСТЭК России №17: РСБ.1-РСБ.8, АНЗ.2, Приказом ФСТЭК России №21: РСБ.1-РСБ.7, АНЗ.2, ИНЦ.1-ИНЦ.6, Приказом ФСТЭК России №31: ИНЦ.1-ИНЦ.6, УКФ.3, АУД.3, АУД.4, АУД.6-АУД.10, Приказом ФСТЭК России №239: ИНЦ.1-ИНЦ.6, УКФ.3, АУД.3, АУД.4, АУД.6-АУД.10, требования по организации взаимодействия с ГосСОПКА

Сокращение времени реагирования при использовании SOAR-платформы

Действие	До SOAR-платформы	С SOAR-платформы	Пример
Эскалация инцидента из одного из источников событий	5 мин	10 сек	Эскалация инцидента из SIEM – вредоносная активность на рабочей станции
Классификация и приоритизация инцидента	5 мин	10 сек	Отнесение инцидента к типу «Заражение ВПО», определение SLA и приоритета
Определение пораженных в рамках инцидента активов	5-10 мин	10 сек	Запросы в Security CMDB по рабочей станции и в Active Directory по пользователю
Проверка IOC в Threat Intelligence базах	5 мин	10 сек	В инциденте есть hash связанный с вредоносным ПО
Историческая корреляция инцидентов	10-20 мин	10 сек	2 других инцидента за последний месяц имеют тот же hash и исходящий трафик
Ручное обогащение сведений об инциденте из различных внутренних информационных систем и реализация реагирующего воздействия	30-60 мин	30 сек	Получение с рабочей станции всех необходимых сведений путем локального выполнения скриптов, изоляция рабочей станции. Инициация полного сканирования. Получение сведений из Active Directory сведений о группах, в которых состоит пользователь, блокировка учетной записи
Записи, постановка и ведение задач по инциденту на протяжении всего жизненного цикла	20-40 мин	20 сек	Система автоматически сохраняет все выполненные задачи и действия по реагированию
Отчет по статусу инцидента и визуализация для руководства	15-60 мин	20 сек	Встроенные дашборды и генерация отчетов предоставляют всю информацию в режиме реального времени без лишней работы
Итого:	**от 95 минут**	**2 минуты**	

udv|group

СПАСИБО ЗА ВНИМАНИЕ!

Закажите пилотный проект или персональную демонстрацию наших решений

commercial@udv.group

8-800-511-6551

udv.group