RUSIEM
Всё под контролем

АЛГОРИТМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАХ БЕЗОПАСНОСТИ

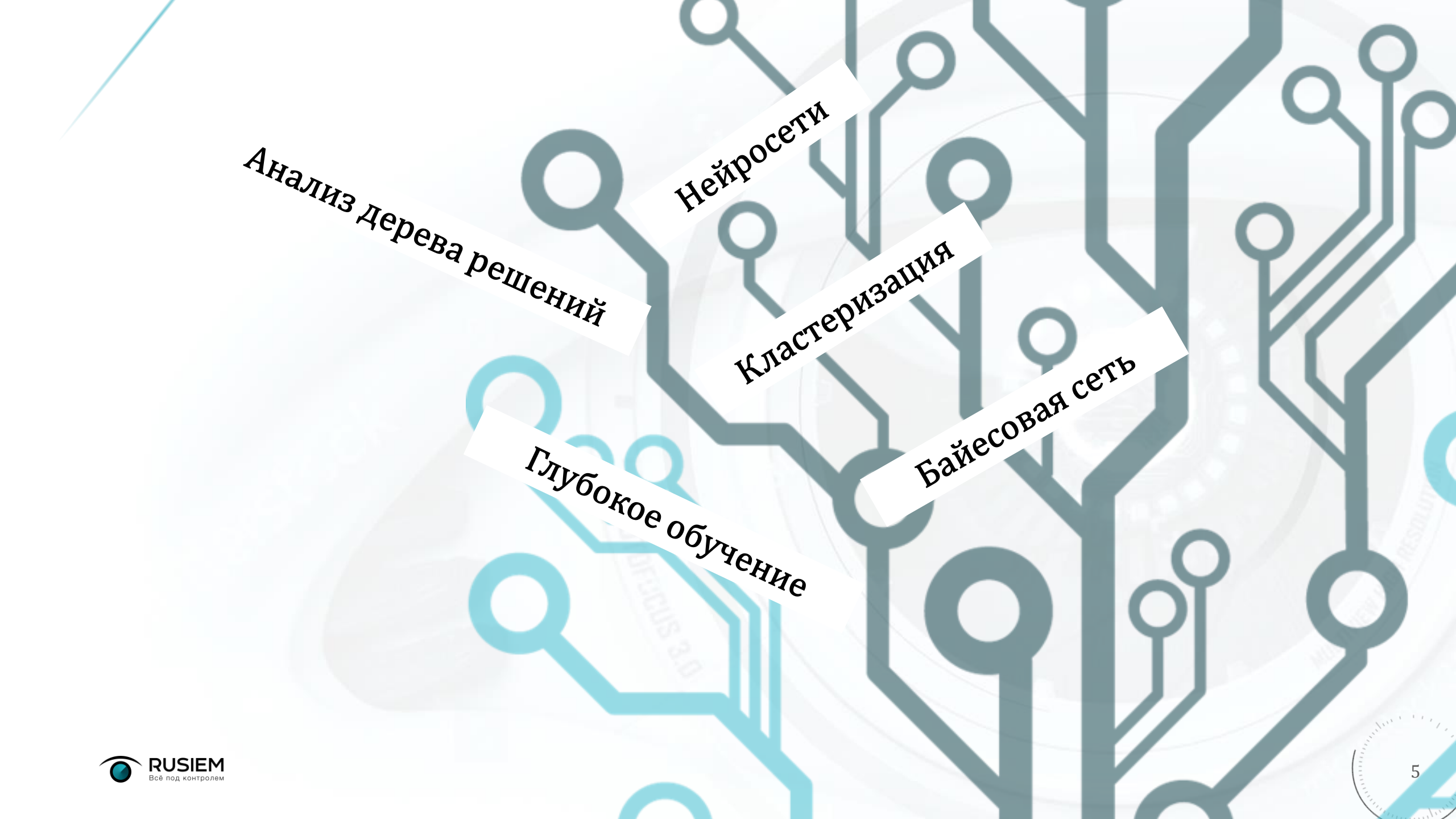
Антон Фишман, технический директор RuSIEM

ИИ - ЧТО ЭТО?

Комплекс технологических решений, имитирующий когнитивные функции человека и позволяющий достигать результаты сопоставимые с результатами интеллектуальной деятельности человека

В 1959 году Артур Самуэль (Arthur Samuel), исследователь в области искусственного интеллекта и изобретатель первой самообучающейся компьютерной программы игры в шашки, **ввел в научный обиход термин «машинное обучение»**


Машинное обучение
Natural Language Processing
Deep Learning
Чат-боты
Компьютерное зрение
Когнитивистика


Анализ дерева решений
Нейросети
Кластеризация
Байесовая сеть
Глубокое обучение

1

система поддержки
принятия решений

2

система принятия решений
на основе входящей информации

Технологии машинного обучения давно используются в различных отраслях

Системы безопасности – это одна из малого количества современных, наукоемких отраслей, где технологии ИИ появились относительно поздно

ВОПРОС:

А ВЫ ЗНАЕТЕ В ЧЕМ ОТЛИЧИЕ
МЕЖДУ СИСТЕМОЙ Безопасности
и системой УПРАВЛЕНИЯ ПОГОДОЙ?

RUSIEM
Всё под контролем


— Ну что ж, Гидрометеоцентр передал осадки!

Киберпреступники и Защитники информации - вечная борьба добра и зла!

Кто окажется более оснащеным и технологичней!?

DGA Families

DGA Families

bamital	banjori	bigviktor	blackhole	ccleaner	chinad
conficker	cryptolocker	dircrypt	dyre	emotet	enviserv
feodo	fobber	gameover	gspy	locky	madmax
matsnu	mirai	murofet	mydoom	necurs	ngioweb
nymaim	omexo	padcrypt	proslikefan	pykspa	qadars
ramnit	ranbyus	rovnix	shifu	shiotob	simda
suppobox	symmi	tempedreve	tinba	tinynuke	tofsee
vawtrak	vidro	virut	xshellghost		

Распределение продуктов с технологией ИИ по сценариям использования*

- Обнаружение и реагирование на кибератаки
- Обнаружение мошенничества в бизнес-процессах
- Управление событиями безопасности
- Защита конечных точек
- Защита приложений и управление уязвимостями
- Управление доступом и аутентификацией
- Анализ поведения пользователей и устройств
- Обнаружение вредоносных программ
- Антифишинг

*Из публичных аналитических отчётов, упоминаний в прессе и открытых баз

RUSIEM
Всё под контролем

ПЕРЕЧЕНЬ СИСТЕМ, ИСПОЛЬЗУЮЩИХ UEBA

- DLP
- IAM
- EM
- EDR
- NTA
- Data-Centric Audit and Protection
- Cloud Access Security Broke
- PAM
- Application security testing

EDR

ENDPOINT DETECTION AND RESPONSE

Передает данные в центр управления, где с помощью технологий ИИ обнаруживает угрозы, классифицирует , расследует и реагирует на них, передавая команды на рабочую станцию. ИИ принимает решения на основе общей базы знаний, накопленной со множества устройств.

NDR

NETWORK DETECTION AND RESPONSE

С помощью технологий ИИ выявляет угрозы в сетевом трафике и автоматически реагирует, изменяя конфигурацию сетевых устройств. Часть продуктов данного типа специализируется на защите облачных провайдеров и их инфраструктуры.

TIP

THREAT INTELLIGENCE PLATFORM

Платформы кибербразведки. Действует на основе большого количества данных, получаемых из разных источников.. Применение ИИ позволяет повысить доверие IoC-ам из разных источников. Сценарий очень близок к работе с SIEM-системами, но нацелен на внешние источники данных и внешние угрозы.

SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

Мониторинг информационных систем, в режиме реального времени анализирует события безопасности, помогают обнаружить инциденты ИБ. Применение технологий ИИ помогает выявлять аномалии эвристическими методами и сокращать ложные срабатывания при изменении паттернов и моделей данных. Применение ИИ в SIEM-системах позволяет достигнуть очень высокого уровня автоматизации

SOAR

SECURITY ORCHESTRATION AND AUTOMATED RESPONSE

Системы управления и автоматизации реагирований на инциденты.

В отличие от SIEM-систем, ИИ помогает не столько проводить анализ, скорее обогащать, расследовать и автоматически реагировать надлежащим образом на выявленные угрозы

Application Security

Средства защиты приложений

Основной сценарий применения технологий ИИ — автоматический сбор информации об уязвимостях, атаках и заражениях, доступной в открытых источниках, автоматизация защитных действий: сканирования на уязвимости, изменения правил защиты для веб-приложений, выявления угроз и изменения рисковой модели

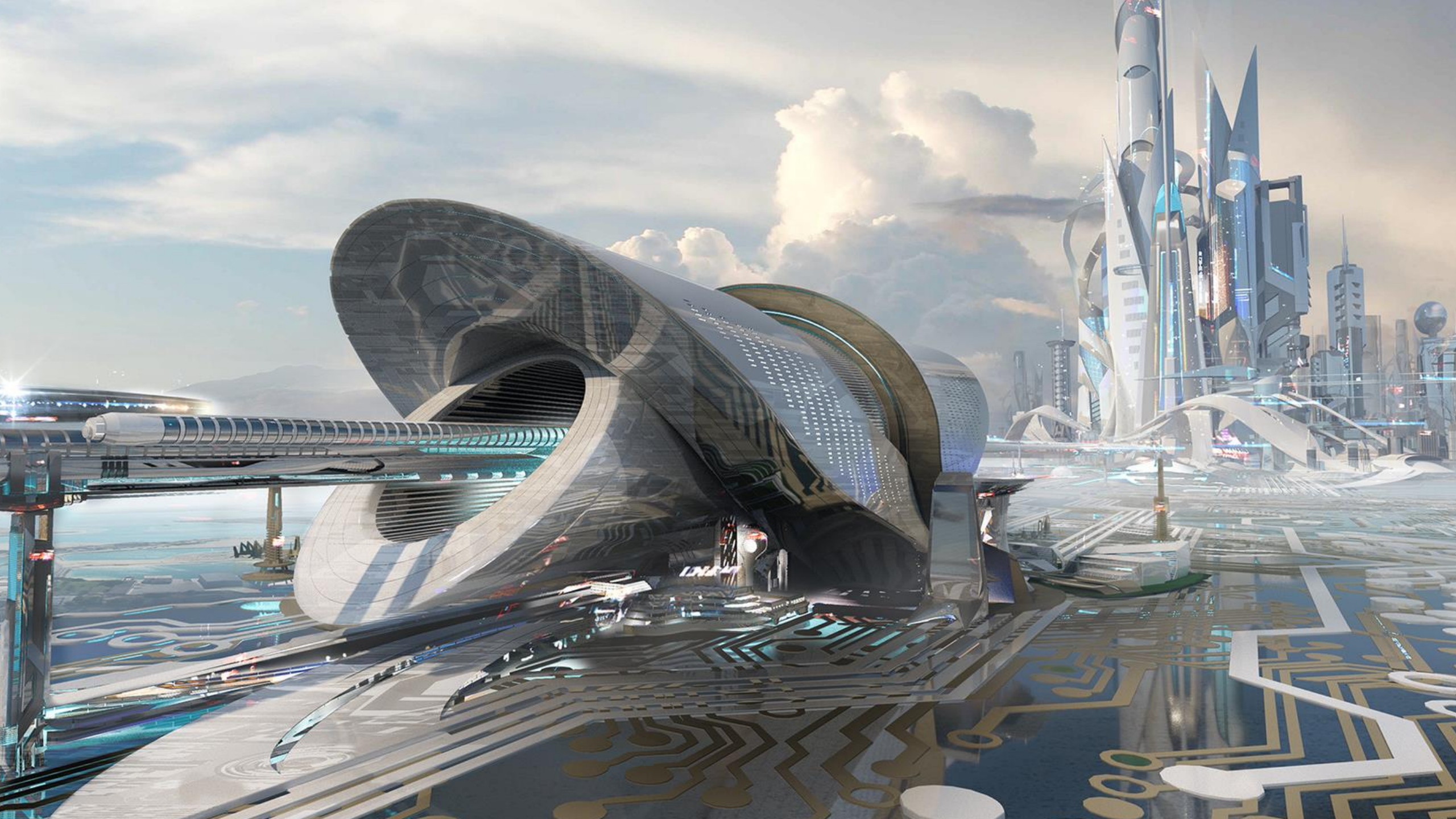
Antifraud

Системы по выявлению угроз в бизнес-процессах

Здесь технологии ИИ применяются для определения отклонений от установленных бизнес-процессов, помогая быстро реагировать на возможное финансовое преступление или уязвимость процессов. Применение ИИ в таких системах особенно актуально, так как позволяет быстро адаптироваться к изменению логики и различных метрик бизнес-процессов, а также использовать лучшие практики в индустрии

Splunk

1	id	title	inventor/author	priority da	filing/creation da	p
288	US-2018091528-A1	Configuring modular alert actions and reporting action performance information	Banipal Shahbaz, Siri Atma Oaklander De Licori, John Rob	26.09.2016	26.09.2016	
289	US-2018314601-A1	Intelligent captain selection for disaster recovery of search head cluster	Ankit Jain, Manu Jose, JR., Bharath Aleti, Amritpal Singh I	28.04.2017	28.04.2017	
290	US-2018293327-A1	Locating and categorizing data using inverted indexes	Jesse Miller, Jason Szeto, Jose Solis, Jindrich DINGA, Davi	05.04.2017	05.04.2017	
291	US-10725616-B1	Display of aggregation and category selection options based on field name selections	Michael Porath, Finlay Cannon, Thomas Allan Haggie	26.09.2016	31.10.2016	
292	US-2018218050-A1	Generating visualizations for search results data containing multiple data dimensions	Michael Porath, Marshall C. Agnew, Ho Lun Ng, Brian Rey	31.01.2017	31.01.2017	
293	US-2019236210-A1	Metric forecasting interface with alert prediction	Iman MAKAREMI, Gyanendra Rana, Iryna Vogler-Ivashcha	30.01.2018	30.01.2018	
294	US-2018196864-A1	Clustered search head configuration synchronization with bloom filter	Yuan Xu	09.01.2017	09.01.2017	
295	US-2018314745-A1	Dynamically-generated files for visualization sharing	Nicholas J. Filippi, Siegfried Puchbauer, Ruyuan Ge	28.04.2017	28.04.2017	
296	US-2018293304-A1	Sampling data using inverted indexes in response to grouping selection	Jesse Miller, Jason Szeto, Jose Solis, Jindrich DINGA, Davi	05.04.2017	05.04.2017	
297	US-10534791-B1	Analysis of tokenized HTTP event collector	Glenn Block, Patrick Lane Ogdin	31.01.2016	31.01.2016	
298	US-10747816-B1	Control interface for asset tree monitoring	Erick Anthony Dean, Brian Matthew Gilmore	31.07.2016	31.01.2019	
299	US-10564622-B1	Control interface for metric definition specification for assets and asset groups driven by search-derived asset tree hierarchy	Erick Anthony Dean, Jindrich DINGA, Marvin Herville Gre	31.07.2016	28.09.2018	
300	US-2019303373-A1	Using an electron process to determine a primary indexer for responding to search queries including generation identifiers	Vishal Patel, Mitchell Neuman Blank, JR., Sundar Renegar	15.05.2012	18.06.2019	
301	US-2018307727-A1	Skewing of scheduled search queries	Paul J. Lucas, Eric Woo	21.04.2017	21.04.2017	
302	US-2019098032-A1	Systems and methods for detecting network security threat event patterns	Lucas Murphey, Francis Gerard, Richard Barger, Bhavin Pa	25.09.2017	25.09.2017	
303	US-2020044927-A1	Behavioral based device clustering system and method	George Apostolopoulos, Zhuxuan Jin	31.07.2018	31.07.2018	
304	US-2020065303-A1	Addressing memory limits for partition tracking among worker nodes	Arindam Bhattacharjee, Sourav Pal, Srinivas Bobba	31.07.2017	18.10.2019	
305	US-2019034555-A1	Translating a natural language request to a domain specific language request based on multiple interpretation algorithms	Dipock Das, Aungon Nag Radon, Dayanand Pochugari, Ac	31.07.2017	31.07.2017	
306	US-2020050607-A1	Reassigning processing tasks to an external storage system	Sourav Pal, Arindam Bhattacharjee, Wayne Patterson	31.07.2017	18.10.2019	
307	US-10067876-B2	Pre-fetching data from buckets in remote storage for a cache	Ledion Bitincka, Alexandros Batsakis, Paul J. Lucas, Nicho	09.01.2017	09.01.2017	
308	US-2020257680-A1	Analyzing tags associated with high-latency and error spans for instrumented software	Gergely DANYI, Steve FLANDERS, Joseph Ari Ross, Justin S	26.10.2018	24.04.2020	
309	WO-2020087082-A1	Trace and span sampling and analysis for instrumented software	Joseph Ari Ross, Matthew William POUND	26.10.2018	28.10.2019	
310	US-2019034247-A1	Creating alerts associated with a data storage system based on natural language requests	Dipock Das, Aungon Nag Radon, Dayanand Pochugari, Ac	31.07.2017	31.07.2017	
311	US-2019294598-A1	Generating event streams including aggregated values from monitored netwrok data	Fang I. Hsiao, Clayton S. Ching, Michael R. Dickey, Vladim	15.04.2014	10.06.2019	
312	US-2015295796-A1	Adjusting network data storage based on event stream statistics	Fang I. Hsiao, Wei Jiang, Vladimir A. Shcherbakov, Ramku	15.04.2014	29.04.2015	
313	US-2019303385-A1	Bidirectional linking of ephemeral event streams to creators of the ephemeral event streams	Clayton S. Ching, Michael R. Dickey, Vladimir A. Shcherba	15.04.2014	14.06.2019	
314	US-2018217874-A1	Resegmenting chunks of data for efficient load balancing across indexers	Jag Kerai, Anish Shrigondekar, Mitchell Blank, Jr., Hasan A	31.01.2017	31.01.2017	
315	US-2019155803-A1	Selective query loading across query interfaces	Jesse Miller, Marc V. ROBICHAUD, Cory Burke, Alexander	30.01.2015	29.01.2019	
316	US-2019155804-A1	Selective filtered summary graph	Jesse Miller, Marc V. ROBICHAUD, Cory Burke, Jeffrey Thc	30.01.2015	29.01.2019	
317	US-2020050612-A1	Supporting additional query languages through distributed execution of query engines	Arindam Bhattacharjee, Sourav Pal, Timothy Tully	31.07.2017	18.10.2019	
318	US-2020050586-A1	Query execution at a remote heterogeneous data store of a data fabric service	Sourav Pal, Arindam Bhattacharjee, Timothy Tully	31.07.2017	18.10.2019	
319	US-2017031981-A1	Facilitating execution of external search commands during query processing	Jacob B. Leverich, Itay A. Neeman, David R. Marquardt	31.07.2015	31.07.2015	
320	US-2019155802-A1	Supplementing events displayed in a table format	Jesse Miller, Marc V. ROBICHAUD, Cory Burke, Alexander	30.01.2015	29.01.2019	



RUSIEM
Всё под контролем

Релевантность искусственного интеллекта в информационной безопасности

Результат внедрение технологий искусственного интеллекта (поведенческий анализ и предиктивная аналитика):

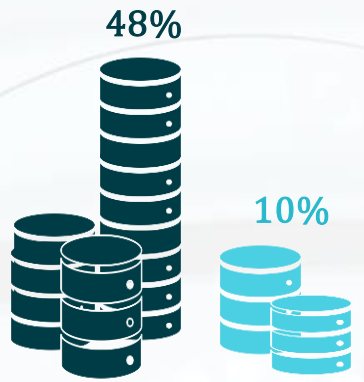
- повышение эффективности обнаружения атак
- сокращение времени реагирования
- сокращение затрат на организацию безопасности

СОКРАЩЕНИЕ ЗАТРАТ

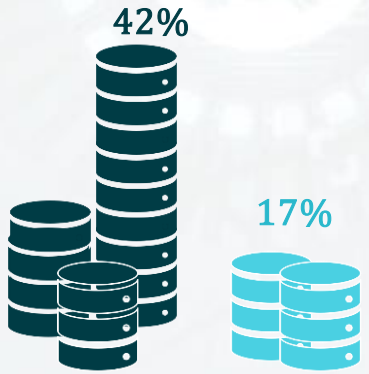
Статистика* сокращения расходов на детектирование и реагирование на инциденты при использовании технологий ИИ

- снижение на 1-15%
- снижение более, чем на 15%

*По данным Capgemini Research Institute



затраты на обнаружение нарушения



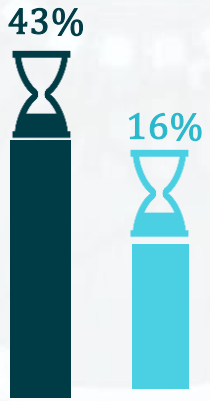
затраты на восстановление после нарушения с точки зрения ИТ-систем

СОКРАЩЕНИЕ ВРЕМЕНИ

Статистика* сокращения времени обнаружения угроз при использовании технологий ИИ

- снижение на 1-15%
- снижение более, чем на 15%

Время, затраченное на обнаружение нарушения



Время, затраченное на устранение нарушения

*По данным Capgemini Research Institute

SIEM – оперативное обнаружение угроз информационной безопасности

ПРИМЕРЫ СОБЫТИЙ

- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не администраторами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учетной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Выполнение требований Законодательства и регуляторов (PCI DSS, СТО БР, ISO 27xx)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

RUSIEM
Всё под контролем

Спасибо за внимание!

www.rusiem.com
info@rusiem.com
+7(495)748-83-11