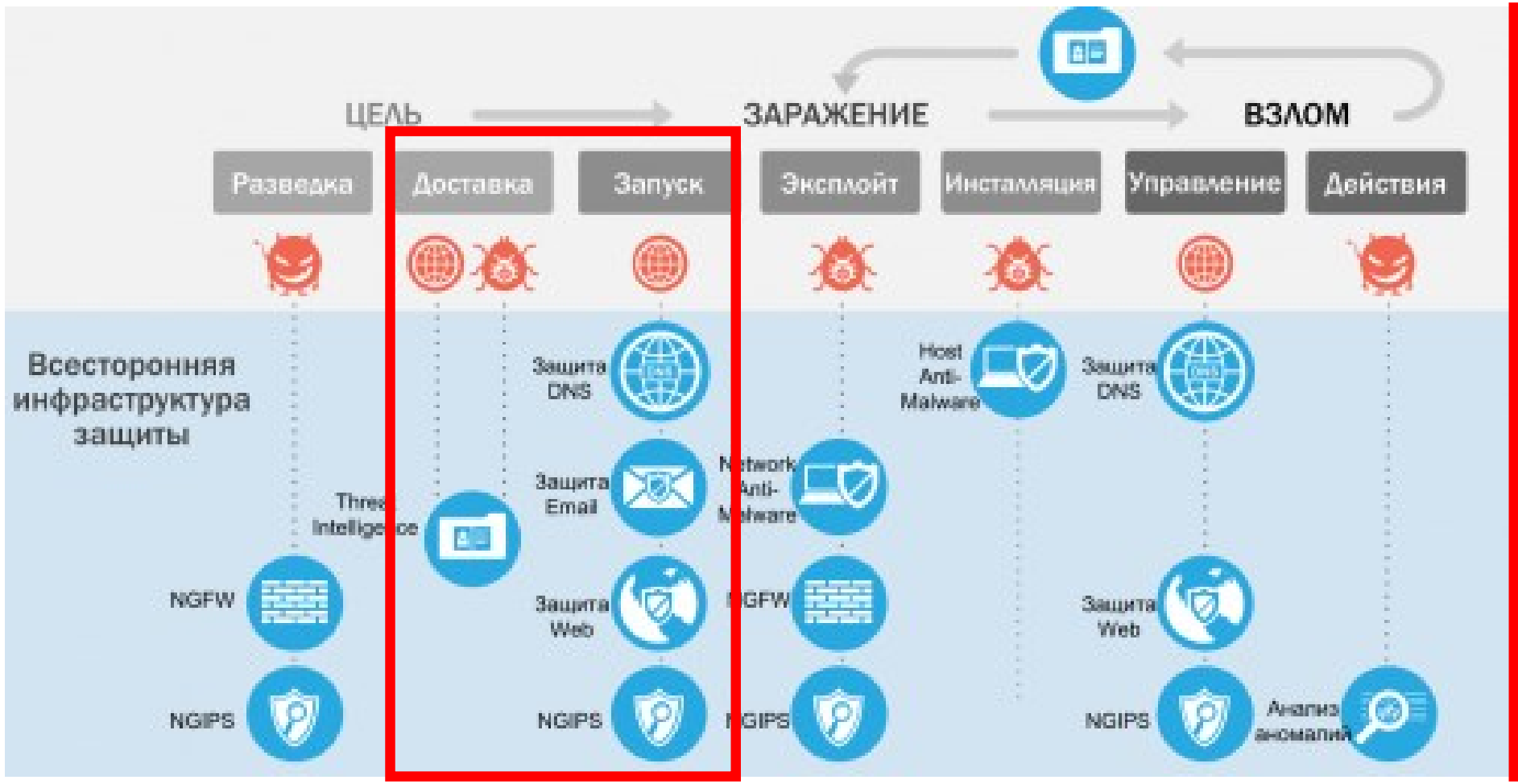
SURLPU

(Save URL PopUp)

РАЗРАБОТКА ФУНКЦИОНАЛЬНО-ОРИЕНТИРОВАННОГО ИНСТРУМЕНТАРИЯ ВЫЯВЛЕНИЯ ВРЕДОНОСНЫХ САЙТОВ НА ОСНОВЕ ОБРАБОТКИ КОМПЛЕКСНЫХ ДАННЫХ URL-АДРЕСОВ И УСРЕДНЕННОГО АНСАМБЛЯ МОДЕЛЕЙ

Менисов Артем Бакытжанович / GAUN

Актуальность (необходимость)



Факторы:

- *Изменение вектора атаки;*
- *Передача URL-адреса через любой мессенджер;*
- *Генерация URL;*
- *Сервисы сокращения ссылок;*
- *Обфускация.*
- *и т.д.*

Source: https://gblogs.cisco.com/ru/ransomware/

Актуальность (несовершенство)

Изменение вектора атаки

CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

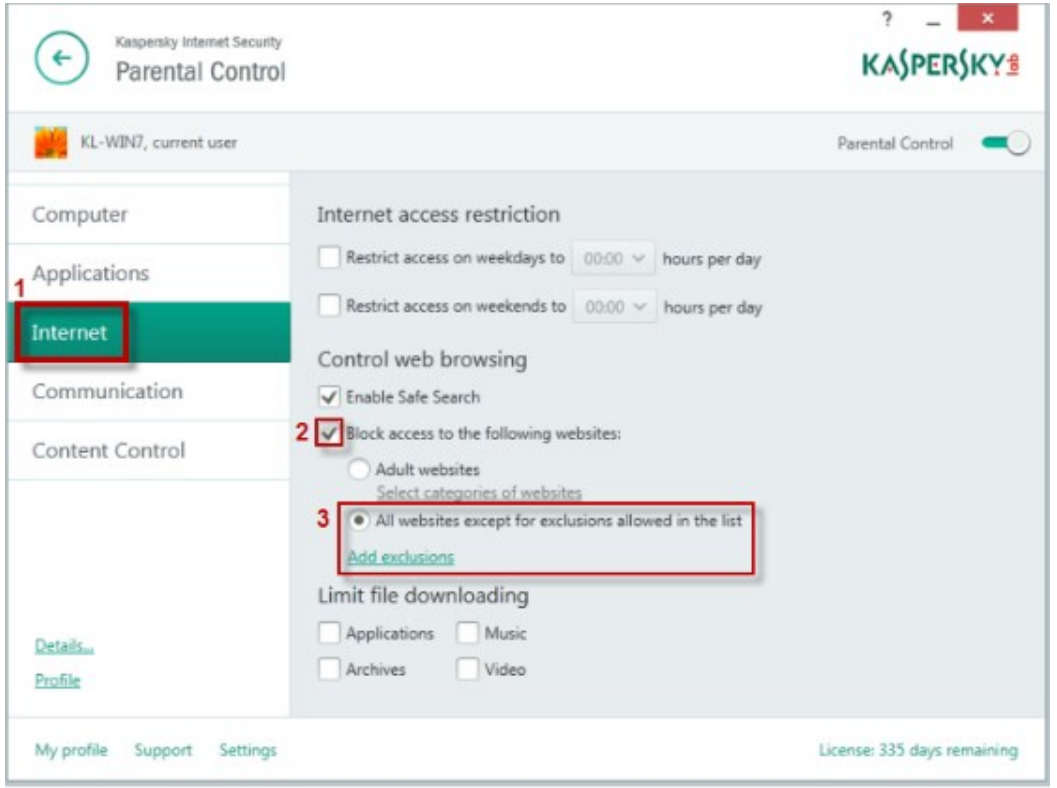
1000 - Mechanisms of Attack

- Engage in Deceptive Interactions - *(156)*
- Abuse Existing Functionality - *(210)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*
- Inject Unexpected Items - *(152)*
- Employ Probabilistic Techniques - *(223)*
- Manipulate Timing and State - *(172)*
- Collect and Analyze Information - *(118)*
- Subvert Access Control - *(225)*

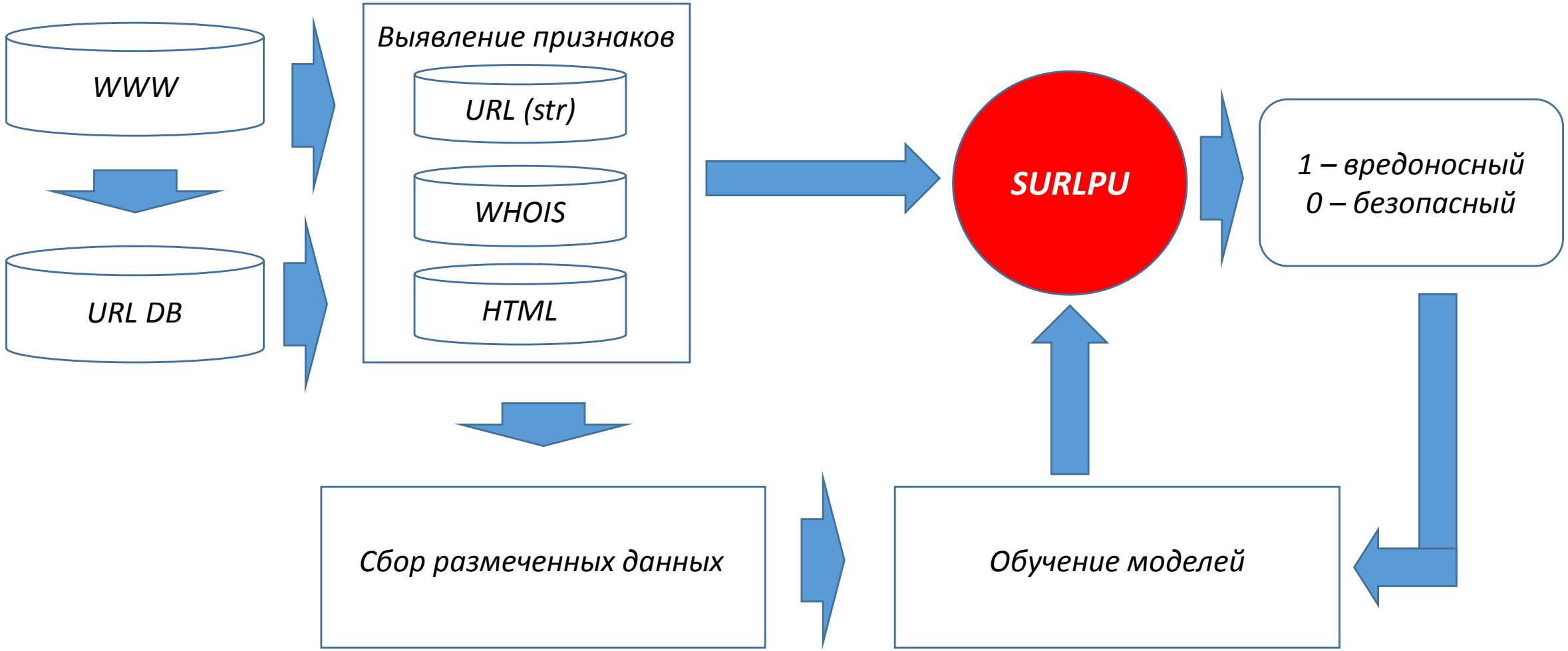
View Metrics

	CAPECs in this view		Total CAPECs
Attack Patterns	518	out of	519
Categories	9	out of	49
Views	0	out of	9
Total	**527**	out of	577

Blacklists



Описание технологии, продукта проекта и ключевых характеристик



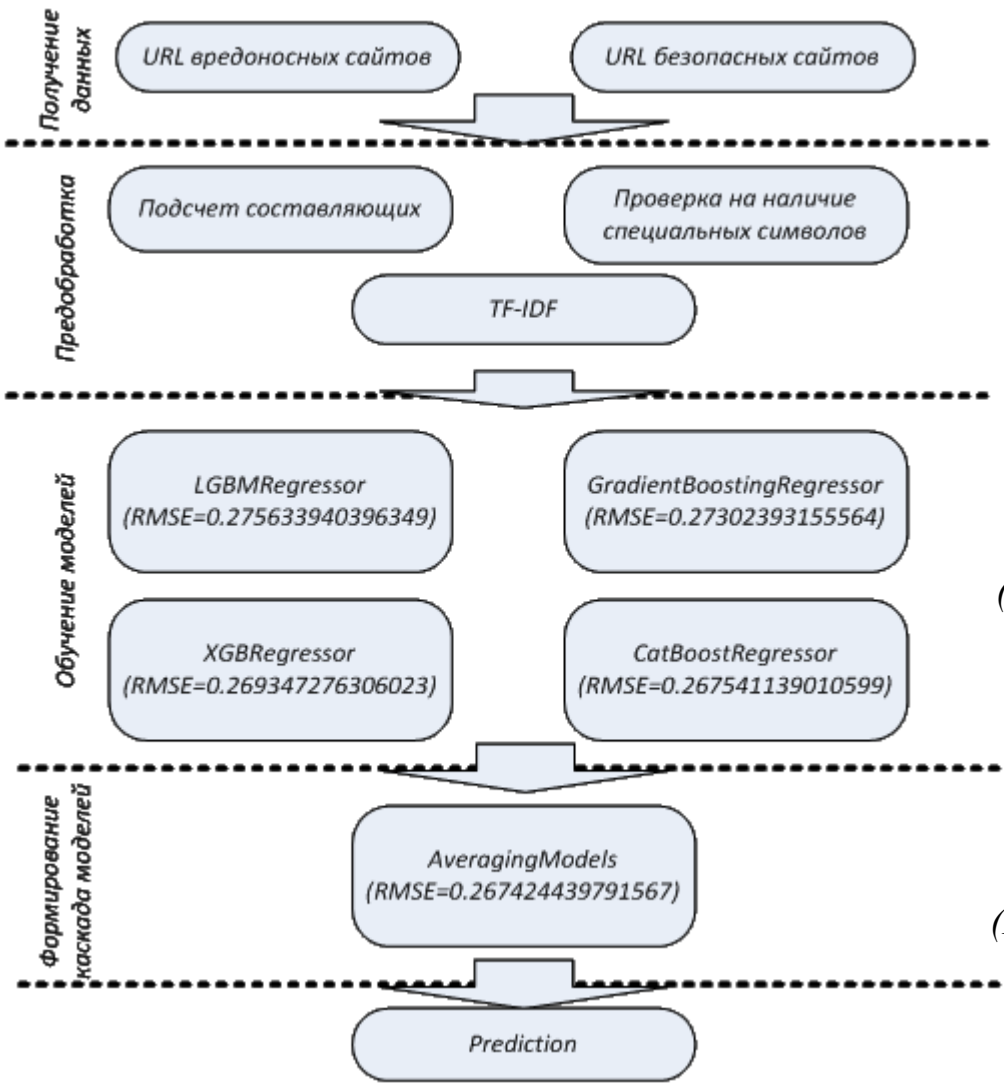
Описание задач, которые решает продукт

Комплексная обработка и выявления признаков, связанных с:

- *URL (ключевые слова, длина и т. д.),*
- *характеристикой домена (длина имени домена, используется ли IP-адрес в качестве имени домена и т. д.),*
- *признаков, относящихся к каталогу (длина каталога, количество токенов подкаталогов и т. д.),*
- *признаков имени файла (длина имени файла, количество разделителей и т.д.),*
- *контент сопроводительного письма, в котором содержался URL-адрес.*

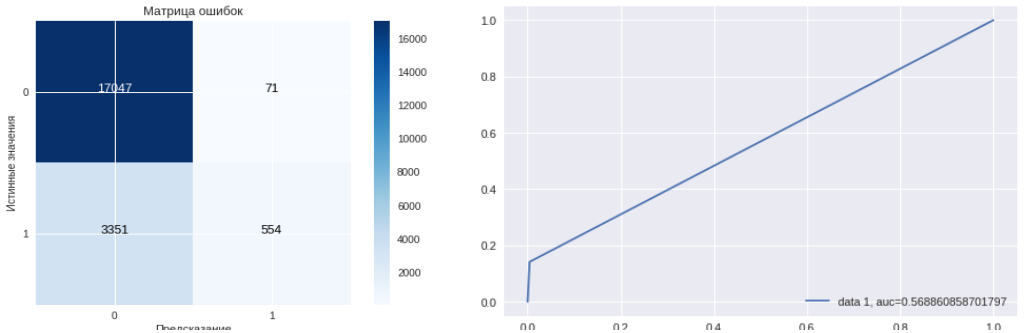
Возможность интеграции с почтовыми сервисами (Outlook, Whatsapp, Telegram, Email, социальные сети).

Новизна и инновационность идеи

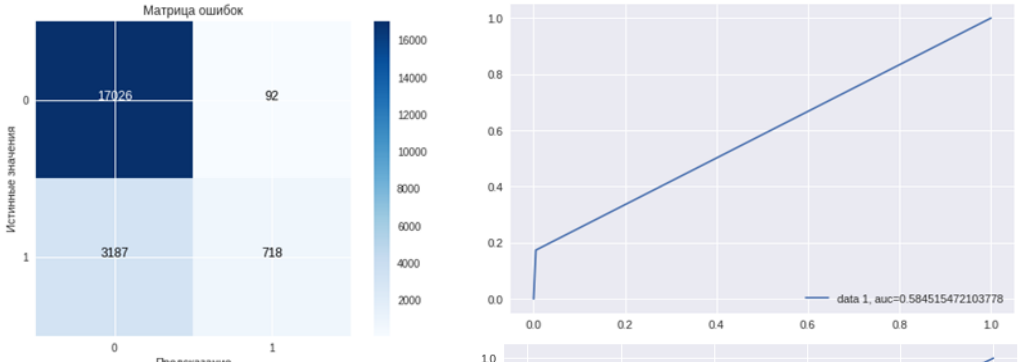


Только часть лексических признаков (TF-IDF)

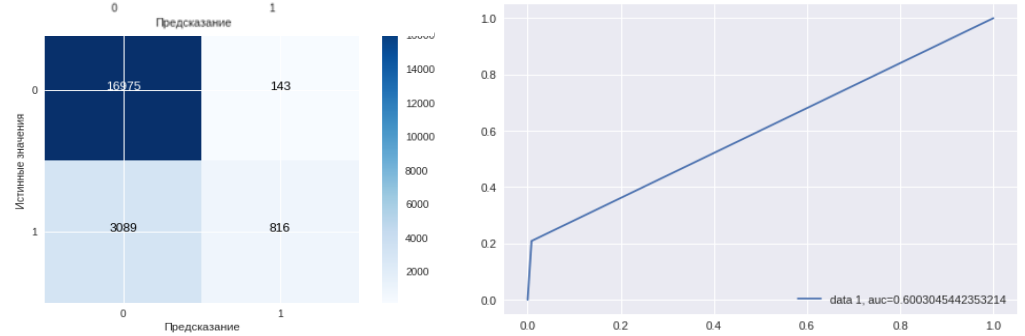
LGBM (ROC-AUC=0,5688



CatBoost (ROC-AUC=0,5845)



Проект (ROC-AUC=0,6003



Описание рынка

Ключевые сегменты клиентов

- *крупные предприятия, государственные организации, поставщики услуг кибербезопасности*

Тенденции

- *расширение партнерских связей с Security Solution,*
- *увеличение доступности решений информационной безопасности для малого и среднего бизнес*
- *увеличение использования ИБ сервисов в нетрадиционных секторах,*
- *растущее внедрение облачных сервисов в правительственных ведомствах*
- *рост числа атак на облачные сервисы*
- *растущее использование облачных сервисов для хранения критически важных данных*
- *повышение мобильности сотрудников*

Основными игроками *являются Fortinet Inc., Checkpoint Software Technologies Ltd, Cisco Systems Inc., Trend Micro Inc. и Symantec Corporation.*

ИБ компании делают упор на снижении затрат, связанных с внедрением стратегий безопасности, путем перехода от продуктов к предложениям услуг. Растущая тенденция к обеспечению безопасности как услуги увеличивает распространение услуг, а ключевые игроки интегрируются с основными поставщики услуг для удовлетворения потребительского спроса.

Сравнение с конкурентами и конкурентными решениями

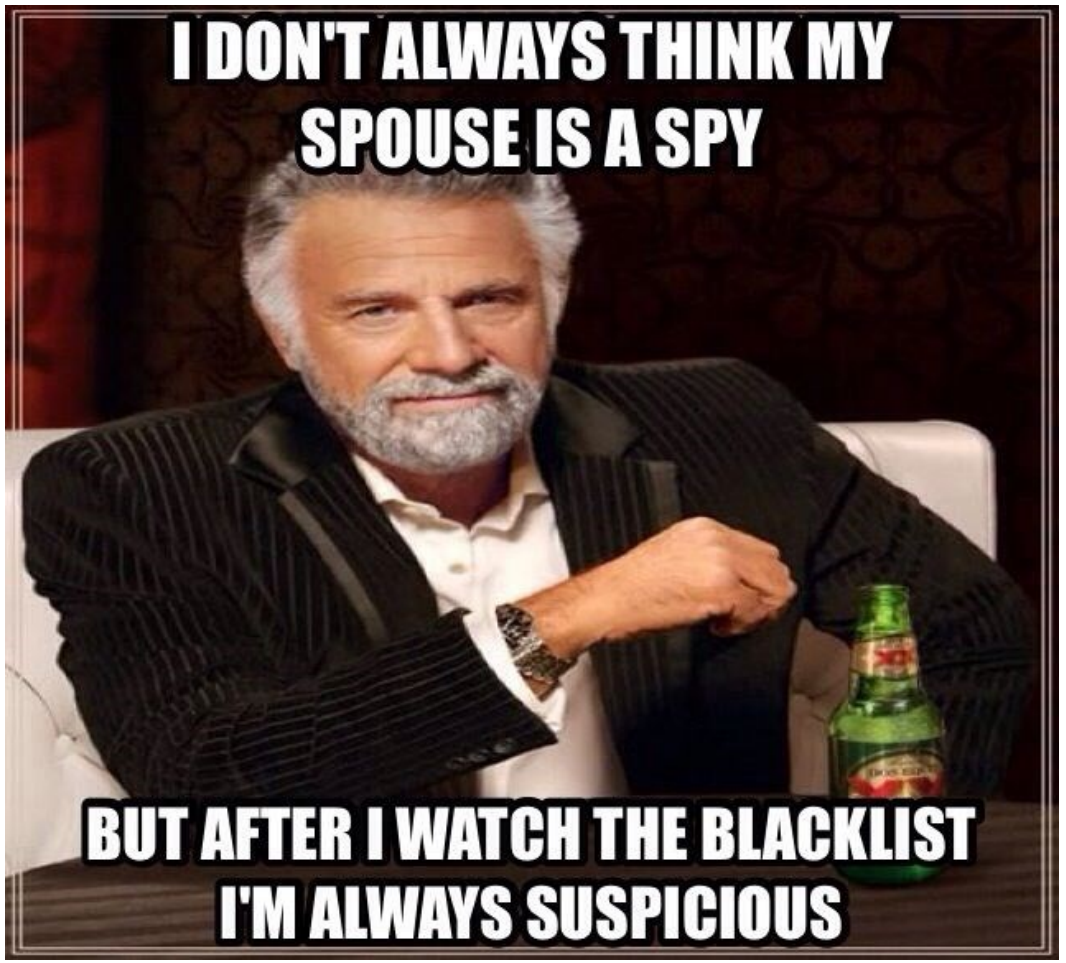
virustotal

Advanced features & tools

ReScan.pro
by Revisium

web inspector
Inspect, Detect, Protect

zvelo
We categorize the Web



Source: https://www.google.com/search?q=blacklists+meme

Ключевые члены команды и компетенции

Разработчик, DS, НТИ

Личное участие в следующих мероприятиях:

- постоянно действующем семинаре ВКА имени А.Ф. Можайского "Сбор и обработка информации" в 2015, 2016 гг.;

- конференции военно-научного общества ВКА имени А.Ф. Можайского, 2015 г.;

- V Всероссийском конгрессе молодых ученых, 2016 г. (лучший доклад секции);

- IV Всероссийской научной конференции «Проблемы военно-прикладной геофизики и контроля состояния природной среды», 2016 г.;

- Десятого Всероссийского форума СПбПУ, 2016 г.;

- конференции «Традиции и инновации» СПБГТИ 2017 г.;

- 70-й региональной научно-технической конференции СПБГУТ, 2017 г.;

- VI Всероссийском конгрессе молодых ученых, 2017 г.;

- УМНИК 2016 года - финалист;

- Бирже интеллектуальной собственности, 2016 г.;

- Хакатон по технологиям в рекламе и маркетинге ADHACK GALAXY 2017 г. - призер;

- Лучший IT проект Министерства обороны РФ, 2017 г. - победитель;

- Всероссийский хакатон NEURO MEDIA - 2017 - победитель;

- конкурс Фонда перспективных технологий - победитель.

*За время научно-педагогической деятельности опубликовал **28 научных и учебно-методических работы**, в том числе **2 учебных пособия**, 4 объекта интеллектуальной собственности, 4 отчета о НИР в соавторстве.*

Свидетельства о регистрации программ на ЭВМ № 2017611597, № 2018603414, № 201857893.

Патент на полезную модель № 2018110447.

Описание ключевых направлений расходования денежных средств

Этапы	Длительность (недель)	Стоимость (рублей)
Организация процесса контроля почтовых систем и сервисов	3	100 000
Разработка алгоритма	4	250 000
Тестирование работы алгоритма	2	50 000
Передача работ по проекту	1	20 000

Спасибо за внимание!

Менисов Артем Бакытжанович
men.arty@yandex.ru
+7 911 984 13 77