ЭВОЛЮЦИЯ подходов к информационной безопасности

Виталий Задорожный
Служба кибербезопасности ПАО Сбербанк

Сбербанк сегодня: беспрецедентный масштаб и положение на рынке

SCST

~80 млн. активных розничных клиентов в России

>1 млн. корпоративных клиентов в России

~16 тыс. точек обслуживания клиентов в России

>300 тыс. сотрудников в Группе

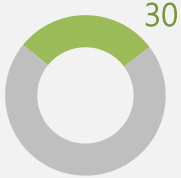
~82 тыс. банкоматов и устройств самообслуживания

~37 млн. пользователей Сбербанк-онлайн

21 страна присутствия

Доли Сбербанка на российском рынке, %

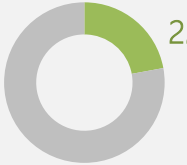
Активы



Сбербанк – крупнейший Банк в России по активам (**23,1 трлн. руб.**) и лидер по чистой прибыли по итогам 2016 года

Депозиты физ.лиц

Депозиты юр.лиц



Кредиты физ.лицам

Кредиты юр.лицам

Мировая статистика

+35% выросло количество DDoS-атак *

58% от всего корпоративного траффика почты - СПАМ*

+3,4% выросло количество утечек конфиденциальной информации*

72% выросло количество программ вымогателей*

Ущерб от действий киберпреступников**

* данные приведены за последние 10 мес.

** в 2016 году, по данным всемирного экономического форума


КИБЕРАТАКА
Прямое воздействие
Косвенное воздействие
Техническая
Информационная
Социальная инженерия

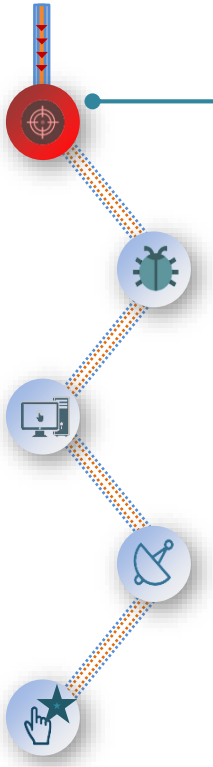
Новая парадигма кибербезопасности

«Классическая» безопасность:

Отсутствие информации о проводимой атаке: безопасность может не знать о проведенной атаке даже после её завершения

Внедрение новых методик

Проактивный подход:



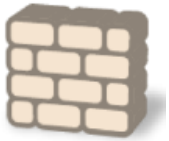
Прерывание цепи: kill chain прерывается ещё на первоначальном этапе

Развитие систем безопасности

До 2000:

Вся информация внутри периметра компании:

- Строительство «стен» вокруг компании
- Вся информация под тотальным контролем



Середина 2000-х:

Кибербезопасность выходит за периметр компании:

- Аутсорсинг
- Информация остается под тотальным контролем

Начало 2010-х:

Понятие периметра исчезает с развитием облаков, byod, соц.сетей:

- Защита информации выходит за периметр компании

Сейчас:

Переход на новую парадигму – «цифровая устойчивость»:

- Риск-ориентированный подход
- Гибкий подход к обеспечению КБ

Инновации в Сбербанке

BIG DATA

- Умные советы: генерация на основе анализа карточных транзакций клиентов
- Прогнозирование загрузки отделений

MACHINE LEARNING

- Выявление фрода при совершении операций
- Разработка скоринговых моделей для андеррайтинга и риск-менеджмента

НЕЙРОННЫЕ СЕТИ

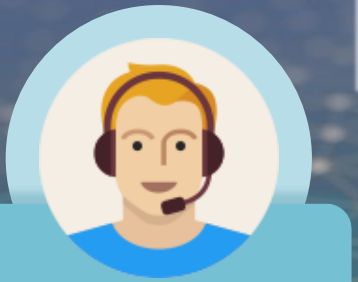
- Выявление оптимальных партнеров для клиентов на основе анализа экономической активности

NATURAL LANGUAGE PROCESSING

- Разработка алгоритмов для чатбота
- Создание алгоритмов для анализа и генерации исковых заявлений

Для чего нужен ИИ* в современном банке?

Преимущества использования ИИ:



для Банка

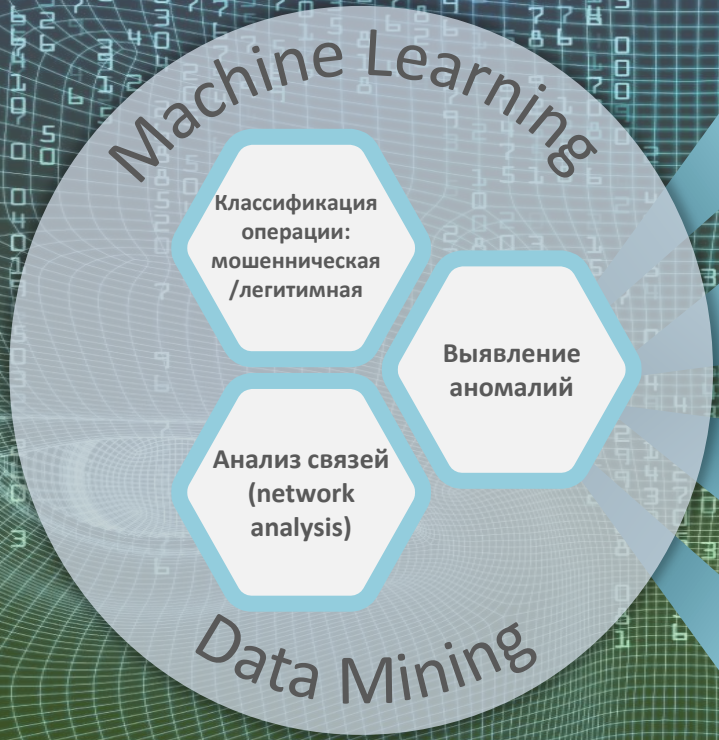
- Минимизация влияния человеческого фактора
- Снижение издержек
- Распознавание мошеннических операций
- Улучшение банковских продуктов

для Клиента

- Персонализированные рекомендации и продукты
- Грамотное управление личными финансами и инвестициями
- Ускорение обслуживания и принятия решений по заявкам

*ИИ – искусственный интеллект

Machine learning и Data mining в рамках противодействия кибермошенничеству



- Выявление мошеннических операций и счетов злоумышленников
- Определение счетов, использующихся для обналичивания средств
- Обнаружение фактов подготовки к мошенничеству с участием сотрудников
- Выявление DDoS-атак на начальных этапах, зараженных вирусами компонент сети

Проактивная работа

ЛЮДИ

ТЕХНОЛОГИИ

3 Культура кибербезопасности
Формирование единой культуры кибербезопасности для Банка и клиентов

2 Эволюция обучения пользователей
Автоматизация обучения
Обучение клиентов
Геймификация

1 Обучение пользователей
Объяснить всем пользователям важность кибербезопасности

Threat intelligence 3
Создание ландшафта угроз
Использование Big Data и машинного обучения
Использование kill chain
Риск-ориентированный подход

Поиск уязвимостей 2
Поиск скрытых вредоносных программ, подозрительного трафика и т. д. ИТ-системах

Сканирование на уязвимости 1
Использование сканеров для обнаружения уязвимостей до киберпреступников

Проактивный подход отсутствует

Человек будущего в кибербезопасности

SCST

«ВОСПИТЫВАЙ ЛИДЕРОВ, КОТОРЫЕ ДОСКОНАЛЬНО ЗНАЮТ СВОЕ ДЕЛО, ИСПОВЕДУЮТ ФИЛОСОФИЮ КОМПАНИИ И МОГУТ НАУЧИТЬ ЭТОМУ ДРУГИХ» , ДЖЕФФРИ ЛАЙКЕР, «ДАО TOYOTA…»

Soft skills

- ИННОВАЦИОННОСТЬ И DIGITAL-НАВЫКИ
- СИСТЕМНОЕ МЫШЛЕНИЕ И РЕШЕНИЕ ПРОБЛЕМ
- УПРАВЛЕНИЕ СОБОЙ
- РАЗВИТИЕ КОМАНД И СОТРУДНИЧЕСТВО
- УПРАВЛЕНИЕ РЕЗУЛЬТАТАМ И ОТВЕТСТВЕННОСТЬ
- КЛИЕНТОЦЕНТРИЧНОСТЬ

Hard skills

- РАЗВИТИЕ НОВЫХ КОМПЕТЕНЦИЙ И ЗНАНИЙ
- УНИКАЛЬНЫЙ ОПЫТ

Компетенции будущего

WHITE TEAM
Тестируют и пытаются найти слабости во всех новых цифровых приложениях и продуктах Банка перед их запуском в продуктив

RED TEAM
Атакуют промышленные приложения, пытаясь найти уязвимости, а также занимаются провокациями в отношении сотрудников, в том числе с использованием инструментов социальной инженерии

HUNTERS
Пытаются обнаружить в ИТ системах банка скрытые внедренные вирусы, в том числе «спящие», подозрительный трафик и т.д.

DATA SCIENTISTS АНАЛИТИКИ, МОДЕЛИСТЫ
Математика «больших данных» и наука машинного обучения, разработка гипотез, аналитических моделей кибербезопасности и проверка их на практике