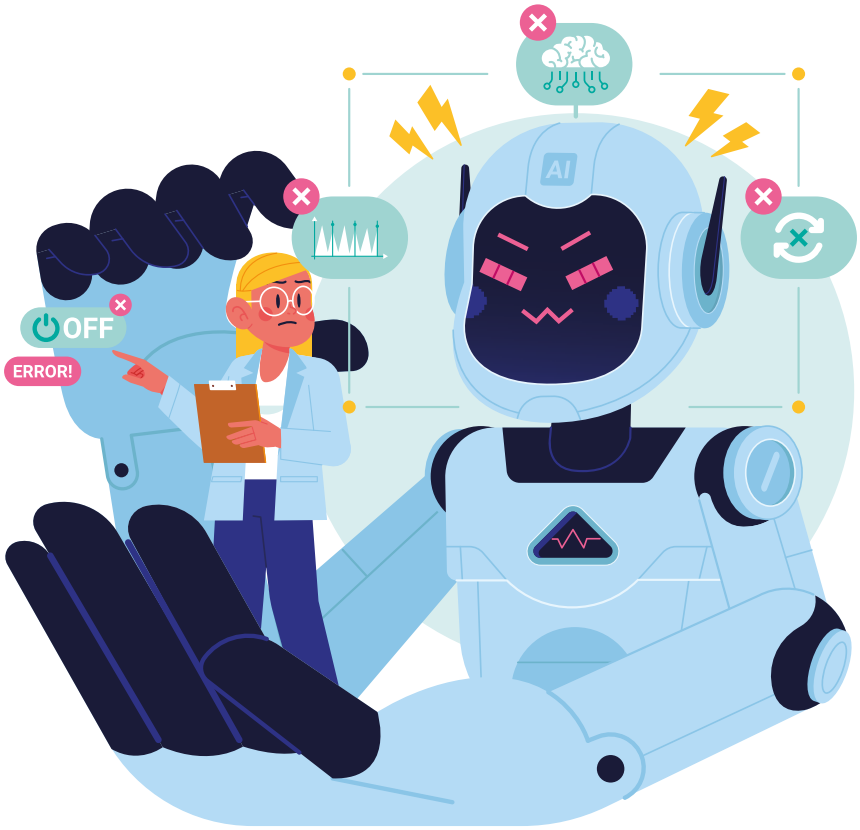
Слишком очевидные связи с реальностью

В условиях растущих угроз кибербезопасности и мошенничества OSINT (Open Source Intelligence, разведка по открытым источникам) становится неотъемлемой частью управления рисками. Плохо то, что технологии Human intelligence, т.е. агентурной разведки, стали доступнее всем



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**



«Мозг человека был инсталлирован 40 тыс. лет назад и с тех пор не апгрейдился. В нем установлен довольно старый процессор. Сознание, по моим наблюдениям, поставили в бета-версии и с тех пор ни разу не патчили. Список уязвимостей, он же список смертных грехов, опубликовали 1,5 тыс. лет назад. Потом Вселенский собор специально собрался и выявил, что главная уязвимость одна — гордыня», — эта фраза **Андрея Масаловича** («Кибердеда»), президента Консорциума «Инфорус», сказанная 15 лет назад в мире экспертов конкурентной разведки (Competitive Intelligence), и сейчас является почти непреложной истиной.

Почему почти? Если с уязвимостями естественного интеллекта все стало понятно давно, то с ИИ исследователи находятся в начальной стадии изучения брешей. Причем ИИ здесь выступает как в роли источника утечек конфиденциальной информации, так и в роли аналитика.

О чем вообще речь?

Конкурентная разведка в финансовом мире существовала со времен появления первых банкирских домов. В отличие от промышленного шпионажа, который тоже не редкость, конкурентная разведка находится в правовом поле, однако есть одна тонкость. Если OSINT — это сбор информации из общедоступных источников, то HUMINT (Human intelligence) — это сбор информации с использованием людей, по сути, сбор информации от человека, в том числе с использованием методов социальной инженерии, которые широко используются при тестировании на проникновение.

Обо всем, что касается экономической и государственной безопасности, а также ИБ, принято говорить скупо. Но кейсы применения OSINT в банковской сфере трудно полностью скрыть. Перечислю некоторые обобщенные направления.

- *Выявление мошеннических схем.* Финансовые учреждения используют открытые источники информации, такие как социальные сети, форумы и специализированные сайты, чтобы отслеживать подозрительную активность. Например, некоторые банки анализируют обсуждения на форумах, где пользо-

ватели делятся опытом о мошенничестве с кредитными картами. С помощью ИИ-алгоритмов обработки естественного языка (NLP) и анализа тональности они могут выявить паттерны, которые указывают на наличие новых мошеннических схем. Это позволяет заранее реагировать на угрозы и защищать своих клиентов.

- *Оценка кредитоспособности клиентов.* Кредитные учреждения начинают использовать OSINT для более точной оценки финансового состояния клиентов. Традиционные методы, такие как проверка кредитной истории, могут быть недостаточными, особенно для молодых людей или тех, кто не имеет долгой кредитной истории. Могут быть использованы данные из открытых источников, такие как профили в социальных сетях, публикации в блогах и даже упоминания в новостях, чтобы лучше понять финансовое состояние потенциального клиента. Например, активное участие в общественной жизни или наличие положительных отзывов от коллег может быть индикатором надежности человека. Это помогает банкам принимать более обоснованные решения о предоставлении кредитов.
- *Анализ конкурентов и рыночных трендов.* Финансовые учреждения могут собирать данные о новых продуктах и услугах, предлагаемых конкурентами, а также о реакциях клиентов на эти предложения. Например, банк может использовать OSINT для мониторинга социальных сетей и специализированных финансовых форумов, чтобы выявить, какие услуги наиболее востребованы у клиентов. Это позволяет не только адаптировать свои предложения под текущие потребности рынка, но и предугадывать изменение трендов, что дает конкурентное преимущество.

Видно, что OSINT — важная составляющая информационной безопасности в наше время. Зная о планах противника, можно лучше подготовиться к кибератаке и даже пресечь ее. Именно по этой причине соответствующее подразделение входит в департаменты ИБ отечественных банков.

Одним из эффектов этой работы стал в целом непубличный, но получивший известность кейс о действиях конкурирующей группировки, которая в одну из пятниц в самом конце рабочего дня запустила в соцсетях слух о том, что несколько банков с довольно разветвленными банкоматными сетями должны в ближайший уикенд прекратить обслуживание клиентов. Все выходные эта сплетня активно обсуждалась в соцсетях. В итоге в понедельник один из этих банков столкнулся с опустошенными клиентами банкоматами и очередями у касс, а второй работал как ни в чем не бывало. Расчет был на то, что у служб OSINT будут нерабочие дни. Так и было, но только у того банка, который в итоге оказался банкротом. А его коллеги сумели вовремя отреагировать и провести успешную борьбу с фейками. Все это было у нас в стране, и не так уж давно.

Как мухи на мед

А вот о том, что может случиться в недалеком будущем усилиями «продвинутых» хакеров, взявших на вооружение OSINT, можно было узнать на 3-й Практической конференции «ЦФА: инвестиции нового поколения», которую медиапроект «Банковское обозрение» провел 27 июня 2024 года в Москве. Андрей Масалович, подписавший на этот раз свою презентацию как «специалист по связям с реальностью», в подробностях описал, «как именно будут ломать» операторов информационных систем (ОИС) и их клиентов».

Всякая новая технология притягивает к себе мошенников, как мед — мух. Однако многочисленные попытки взломать блокчейн как IT-систему ни к чему не привели. Поэтому «взламывают» людей, эксплуатируя при этом, по сути, исключительно «гордыню» как ключ к уязвимостям мозга. При этом социальные сети как будто специально созданы для того, чтобы люди могли этот смертный грех с максимальным для себя комфортом выставить у всех на виду. В частности, был приведен пример неудачной «фотосессии» **Джеймса Чжуна**, хакера, который десять лет назад похитил 50 тыс. биткоинов. Полиция конфисковала эту сумму, которая стала второй по величине в истории такого рода хищений. Еще один пример связан с использованием ИИ для кражи 35 млн долларов из одного известного банка. Все это яркие примеры поиска информации о жертве с помощью HUMINT, разновидности OSINT.

Рынок ЦФА как молодой и привлекательный, по мнению эксперта, крайне чувствителен к утечкам персональных данных его участников и проявлению ими чрезмерных амбиций, гонора и обычной болтовни в тематических чатах и форумах. Специалистам в области HUMINT и социальной инженерии остается только потирать руки, «общаясь» с подобными персонажами.

Объемы рынка

OSINT начинался с анализа FTP-серверов компаний, которые у себя на сайтах обожали писать «лидирующая», «лучшая», «процветающая» и т.д. В подавляющем большинстве случаев в их хранилищах в открытом доступе находили файлы с паролями от IT-систем и списками лиц, допущенных к тем или иным ресурсам. Одно слово: «гордыня».

Сейчас все сильно усложнилось, но принципиально не изменилось. Приходится анализировать множество источников, включая социальные сети, форумы, чаты, а также дата-сеты для обучения моделей ИИ. В результате OSINT превратился в довольно крупную индустрию.

На конференции о работе с данными «DataTalks 5.0», проведенной «Ростелекомом» в сентябре 2024 года, **Тимур Меджидов,** менеджер по развитию поисково-аналитической OSINT-платформы IQPLATFORM компании IQMen, раскрыл информацию об объеме этого рынка. По его словам, в 2024 году объем мирового рынка OSINT оценивается в 10 млрд долларов с прогнозом роста до 50 млрд долларов в ближайшие пять лет. Эти системы полезны широкому кругу пользователей — от частных лиц до секретных служб. И все они готовы платить круглые суммы, чтобы первыми получить нужную информацию. А вот потенциальным жертвам ИБ-офицеры советуют не уходить с головой в виртуальную реальность с ее «розовыми пони», а сохранять связь с реальностью! Б.О