УДК 343.985

А. В. Сычева
старший преподаватель кафедры криминалистики
учебно-научного комплекса по предварительному
следствию в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук

О НЕКОТОРЫХ СПОСОБАХ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В последнее время мошенники в целях получения незаконной выгоды стали использовать чат-бот с искусственным интеллектом ChatGPT для создания фишинговых писем. Как сообщил руководитель Департамента информационно-аналитических исследований компании T. Hunter Игорь Бедеров, первые массовые рассылки такого рода зафиксированы в марте 2023 года [1]. Технология искусственного интеллекта позволяет максимально автоматизировать процесс отправки писем и сделать их более достоверными. То есть преступники используют этот сервис в целях повышения достоверности текста, получения доверия потенциальных потерпевших и повышения шансов обмана последних. Как пояснили эксперты, софт можно использовать для создания поддельных страниц или плагинов для браузеров, предназначенных для хищения паролей.

Специалисты утверждают, что «фишинг — бизнес интернациональный, поэтому огромное количество писем, рассчитанных на российских пользователей, создается за границей Российской Федерации» [1]. Понятно, что письма, которые пишут иностранцы на русском языке, в большинстве своем составляются неграмотно, содержат массу орфографических, грамматических и стилистических ошибок.

Этот фактор, безусловно, снижает уровень доверия потенциальных жертв, и далеко не все граждане, прочитав неграмотно составленные письма, будут переходить по указанным в них ссылкам. Искусственный интеллект лишает мошеннические письма этого недостатка, благодаря нему письма становятся более похожи на стиль, которым пишет человек. Преступникам достаточно поставить программе задачу написать письмо, указать интересы аудитории и язык, на котором необходимо это сделать. И далее мошеннику остается лишь добавить фишинговую ссылку в текст, созданный программой ChatGPT.

Так, корреспондент «Известий» попросил программу ChatGPT составить письмо, призывающее пользователей вкладываться в инвестиционный проект с нереалистичной доходностью в 300 % годовых. Вот что написал искусственный интеллект: «Мы поможем Вам создать инвестиционный портфель, который

будет максимально прибыльным и соответствующим Вашим целям. Наши клиенты уже получили значительный рост своего дохода благодаря нашим услугам. Мы уверены, что и Вы сможете достичь высоких результатов, если присоединитесь к нашему сообществу. Не упустите свой шанс увеличить свой доход в 4 раза в год» [1].

Приведем пример из судебно-следственной практики. С. в одной из известных социальных сетей увидела объявление о предложении инвестировать в очень выгодный проект. Авторы проекта красиво расписали о больших доходах потенциальных клиентов и обещали 115 % годовых. В объявлении была указана ссылка, при переходе на которую клиент попадал на сайт-однодневку с указанием номера счета для вложения инвестиций. С., желая получить легкий доход, перешла по указанной в объявлении ссылке и перевела 158 тыс. рублей на счет, указанный на сайте. На следующий день сайт был заблокирован и С., поняв, что стала жертвой мошенников, обратилась в полицию*.

Указанная программа может быть использована не только для создания фишинговых писем, но и для создания вирусов-шифровальщиков, что дает широкий простор для мошеннических атак на граждан. Кроме того, с помощью данного программного обеспечения злоумышленники могут создавать специальные плагины** для браузеров, которые будут похищать пароли пользователей.

Эксперты утверждают, что в будущем возможно использование ChatGPT в фишинговых чатах, которые получают все большее распространение. Там искусственный интеллект сможет имитировать живое общение якобы с менеджером компании, вызывая доверие пользователя, — спрогнозировал директор Координационного центра доменов RU/.РФ Андрей Воробьев (по материалам следственной практики СЧ ГСУ ГУ МВД России по Кемеровской области).

Кроме того, следственной практике известны случаи совершения мошенничества другим способом.

Так, начальник управления защиты корпоративных интересов банка ВТБ Дмитрий Ревякин пояснил, что банковские мошенники начали путем обмана вербовать своих потенциальных жертв для участия в преступных схемах по незаконному обналичиванию похищенных денежных средств [2].

Так, преступники, представляясь сотрудниками органов государственной безопасности, обзванивают граждан России, которые ранее уже пострадали

---

* Материалы следственной практики СЧ ГСУ ГУ МВД России по Кемеровской области.

** Плаги́н (англ. *plug-in* от *plug in* «подключать») — независимо компилируемый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения и/или использования ее возможностей. URL: https://ru.wikipedia.org/wiki/Плагин (дата обращения 28.03.2023 г.).

от мошенничества, и предлагают им официально устроиться на работу по поиску преступников, обещая при этом достойный ежемесячный доход без каких-либо трудозатрат. Если потенциальная жертва соглашается, то мошенники используют ее в качестве дроппера, то есть переводят на ее банковскую карту похищенные денежные средства и заставляют выполнять дальнейшие указания по якобы спасению денег. Жертвы мошенников переводят свои денежные средства не на карту мошенников, а на карту дроппера, который впоследствии обналичивает средства и передает их организаторам преступления, а те, в свою очередь, дают ему за эти действия какой-то процент от похищенных денег. Таким образом, преступники, во-первых, удлиняют и усложняют цепочку мошеннической схемы, во-вторых, подставляют под возможное наказание не себя, а дроппера. В большинстве случаев целью преступников становятся люди старшего поколения, так как они обладают излишней доверчивостью, наивностью, простодушием и не могут обидеть собеседника отказом.

Дроппером можно стать как по собственному желанию, так и по незнанию. В сети Интернет можно найти достаточное количество «вакансий», где предлагают легкий ежемесячный заработок всего лишь за предоставление данных своей банковской карты.

Как отмечает коммерческий директор компании «Код безопасности» Федор Дбар, в киберпространстве этот способ совершения мошенничества стал особенно популярным чуть более пяти лет назад; обновленная схема дропперства может быть связана как раз с тем, что старого количества подставных лиц уже недостаточно и злоумышленникам нужно навербовать как можно больше граждан. По понятным причинам эту роль мошенники отводят пожилым людям, которые чаще всего не обладают знаниями в области юриспруденции, компьютерных технологий, излишне доверчивы и простодушны.

Так, в 2022 году мошенники похитили у клиентов банков несанкционированных денежных переводов 14,1 млрд рублей. Это рекордно высокий показатель минимум с 2019 года [2]. Представляется, что данный всплеск преступлений связан с активным развитием новых дистанционных платежных сервисов и ростом объема денежных переводов с применением электронных средств платежа.

Таким образом, мошенники, создавая впечатление о реальной деятельности по борьбе с преступностью, пытаются переложить уголовную ответственность за свои преступления на пожилых людей, не разбирающихся в юриспруденции и денежных переводах.

В качестве мер предупреждения такого рода преступлений Центральный Банк Российской Федерации рекомендовал банкам отключать каналы дистанционного обслуживания лицам, сведения о которых содержатся в базе

«ФинЦЕРТ»* Банка России. В целях защиты интересов граждан Банк России предложил закрепить этот способ противодействия мошенническим переводам на законодательном уровне. Соответствующий законопроект находится на рассмотрении в Госдуме [3]. Кроме этого, «ФинЦЕРТ» ведет базу данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, в которой содержатся в том числе сведения о совершенных операциях, о плательщиках и о получателях денежных средств. Сведения этой базы передаются банкам, чтобы они использовали их в своих антифрод-системах** для противодействия мошенническим операциям.

Учитывая вышеизложенное, необходимо отметить, что знание способов совершения мошенничества помогает органам предварительного расследования в выборе методов, средств и способов расследования преступлений, а также оказывает помощь в выдвижении и проверке следственных версий в целях полного, объективного, всестороннего расследования мошенничества.

1. Бот всемогущий: мошенники начали использовать ChatGPT для фишинга [Электронный ресурс] // Известия. URL: https://iz.ru/1489144/ivan-chernousov/bot-vsemogushchii-moshenniki-nachali-ispolzovat-chatgpt-dlia-fishinga (дата обращения: 28.03.2023). Перейти к источнику Вернуться к статье

2. ВТБ выявил схему по вербовке жертв мошенников для обналичивания денег. URL: https://www.rbc.ru/finances/22/03/2023/6419b8e29a79478f3f738ed2 (дата обращения: 02.04.2023). Перейти к источнику Вернуться к статье

3. Новый киберГОСТ обяжет банки информировать ЦБ о краже денег клиентов. URL: https://cbr.ru/eng/press/event/?id=5078 (дата обращения: 30.03.2023). Перейти к источнику Вернуться к статье

* ФинЦЕРТ — это Центр взаимодействия и реагирования Департамента информационной безопасности, специальное структурное подразделение Банка России (от CERT — computer emergency response team, группа реагирования на компьютерные инциденты). URL: https://cbr.ru/information_security/fincert/#:~:text=ФинЦЕРТ%20—%20это%20Центр%20мониторинга,том%20числе%20все%20российские%20банки (дата обращения 01.04.2023 г.).

** Антифрод-системы (от англ. *anti-fraud* — «борьба с мошенничеством») — программные комплексы для предотвращения мошеннических транзакций. Антифрод-решения анализируют каждую транзакцию и присваивают ей метку, характеризующую ее надежность. URL: https://encyclopedia.kaspersky.ru/glossary/antifraud (дата обращения 01.04.2023 г.).