Секция «10.7 Обеспечение экономической безопасности государства в условиях современных глобальных вызовов: экономико-правовые аспекты (совместно с Экономическим факультетом Белорусского государственного университета)»

Социальные сети и мессенджеры как инфраструктура экономических преступлений: от мошенничества до вербовки

Научный руководитель – Тарасёнок Зоя Николаевна

Шебалкова А.А.[1], *Палатинская Д.Ю.*[2]

1 - Белорусский государственный университет, Экономический факультет, Минск, Беларусь, *E-mail: shebalkova.5050@mail.ru*; 2 - Белорусский государственный университет, Экономический факультет, Минск, Беларусь, *E-mail: palatinskaya07@mail.ru*

Социальные сети и мессенджеры как инфраструктура экономических преступлений: от мошенничества до вербовки

Палатинская Д.Ю., Шебалкова А.А.

Студент, студент

Белорусский Государственный Университет, Экономический факультет, Минск, Беларусь

E-mail: mailto:palatinskaya07@mail.ru**,** mailto:shebalkova.5050@mail.ru

В условиях глобальной цифровизации социальные сети и мессенджеры перестали быть просто инструментами коммуникации, они превратились в серьезную систему, через которую проходят миллиарды долларов рекламных бюджетов, торговых сделок и частных переводов. Фактически речь идет о формировании параллельной цифровой среды экономической активности, обладающей собственными правилами и трансграничным характером.

Цель статьи – проанализировать трансформацию социальных сетей и мессенджеров в инфраструктуру экономической преступности, раскрыть механизмы функционирования мошеннических и вербовочных схем.

Социальные сети и мессенджеры являются идеальной средой для мошенничества, поскольку в них стирается грань между реальным и виртуальным общением. Современные схемы выходят далеко за рамки примитивных фишинговых рассылок и представляют собой многоступенчатые операции с использованием психологического давления и новейших технологий.

Одной из популярных схем мошенничества являются фейковые инвестиционные платформы. Злоумышленники используют таргетированную рекламу в социальных сетях и тематические чаты в мессенджерах для поиска жертв, которым обещают большой доход от торговли на бирже или же вложениях в криптовалюту. Как отмечают эксперты Т-Банка, жертву регистрируют на фальшивой платформе, где первые сделки якобы приносят прибыль, создавая иллюзию успеха [5]. Однако при попытке вывести средства возникают проблемы: требуется оплатить «комиссию», «налог» или «страховой взнос» [4]. В результате, после получения денег мошенники исчезают.

Традиционный фишинг эволюционировал и стал больше похож на персонализированные атаки. На сегодняшний день более 40 % успешных фишинговых атак используют социальную инженерию, и мессенджеры стали одним из главных каналов их распространения [1]. Мошенники создают фейковые аккаунты друзей, родственников или начальников, и от их имени рассылают сообщения с просьбой перейти по ссылке или же принять участие в опросе. Особую опасность представляет вишинг, осуществляемый с использованием мессенджеров: звонки из службы безопасности банка или же звонки от операторов сотовой связи для продления договора [2].

Сегодня мессенджеры - это не просто приложения для общения, а закрытый мир с миллиардами пользователей, где каждый чат может стать стартовой точкой криминальной карьеры. Шифрование end-to-end, исчезающие сообщения, массовые рассылки и группы по сотни человек делают их раем для вербовщиков.

Процесс вербовки можно представить в нескольких этапах. Первым шагом является маскировка под легальный бизнес. На популярных платформах, в социальных сетях активно размещается таргетированная реклама вакансий с размытыми должностными обязанностями: “менеджер по работе с клиентами”, “помощник трейдера”, “администратор по переводам” или “оператор по сопровождению транзакций”. Основным триггером для потенциальной жертвы выступает акцент на сверхлояльные условия: удаленная работа, отсутствие требований к опыту и неоправданно высокий доход. Такая подача нацелена, в первую очередь, на социально уязвимые группы или молодежь.

Для масштабирования процессов вербовки преступные сообщества активно внедряют чат-боты. В мессенджере создаются автоматизированные воронки найма, где боты проводят “собеседования”. В свою очередь, использование технологичного интерфейса выполняет важную психологическую функцию: оно снижает уровень тревожности и создает ложную иллюзию работы в инновационной компании, а не в криминальной структуре.

На вершине данной инфраструктуры стоят специализированные “дроп-сервисы”, т.е. глубоко законспирированные теневые площадки и закрытые сообщества, где процесс вовлечения новых участников поставлен на поток. В отличие от разрозненных групп мошенников, дроп-сервисы выполняют роль централизованных операторов по обналичиванию похищенных денежный средств [3]. Они выступают посредниками между организаторами киберпреступлений и реальным финансовым сектором, обеспечивая “разрыв” следственной цепочки.

Таким образом социальные сети и мессенджеры постепенно трансформировались из нейтральных коммуникационных платформ в полноценную инфраструктуру экономических преступлений, где объединяются механизмы привлечения жертв, и технологические инструменты сокрытия следов.

В данных условиях важно совершенствовать регулирование цифровых платформ, повышать цифровую грамотность населения и развивать межгосударственное сотрудничество. Такой подход обеспечит, в первую очередь, устойчивость экономической безопасности в эпоху цифровых трансформаций.

Источники и литература

1) 1. Anti-Malware.ru. Фишинг 2.0: как мессенджеры и дипфейки стали оружием кибермошенников: https://www.anti-malware.ru/analytics/Threats_Analysis/Phishing20-messengers-deepfakes?utm_source=google&utm_medium=email&utm_campaign=amdelivery
2) 2. Администрация Заволжского района. Предупреждение хищения денежных средств путем дистанционного мошенничества: https://zavolgia73.gosuslugi.ru/deyatelnost/prokuratura-razyasnyaet/novosti_8070.html
3) 3. Методические рекомендации по расследованию преступлений в сфере компьютерной информации / И. Г. Чекунов и др.; под ред. И. Г. Чекунова: Московский университет МВД России имени В.Я. Кикотя, 2018. С. 60
4) 4. Т-Банк. Как распознать мошеннических брокеров и сохранить деньги: https://www.tbank.ru/invest/social/profile/T_Protection/5601be01-e381-4b30-b56f-2a9b650356a9/?author=profile

5) 5. Т-Банк. Обман на миллион: Как избежать мошенничества в инвестициях и трейдинге: https://www.tbank.ru/invest/social/profile/lilly_nd/3bab569d-3628-467d-803e-e61b1b29f6cd/?author=profile