Научная статья
УДК 343.1

ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА НОВЫХ СПОСОБОВ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В СЕТИ

Иван Михайлович Смирнов
Орловский юридический институт МВД России имени В.В. Лукьянова, Орел, Россия, kadyj@yandex.ru

Аннотация. В настоящей статье рассматриваются основные способы совершения интернет-мошенничества, появившиеся в последние годы. Обращается внимание на основные действия преступников в рамках каждого из способов и на то, как проявляется типичное поведение потерпевшего. Анализируется цифровое мошенничество, которое на сегодняшний день является глобальной проблемой для всех экономик мира. Основной причиной распространения данной проблемы можно считать бурное развитие компьютерных и интернет технологий. Раскрываются виды мошенничества, а также способы его совершения. Описаны схемы, которые часто применяются в мошенничестве.

Ключевые слова: интернет, мошенничество, раскрытие преступлений, способы совершения, фишинг

Для цитирования: Смирнов И. М. Оперативно-розыскная характеристика новых способов совершения мошеннических действий в сети // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 2(91). С. 210-216.

OPERATIONAL AND INVESTIGATIVE CHARACTERISTICS OF NEW WAYS OF COMMITTING FRAUDULENT ACTIONS IN THE NETWORK

Ivan M. Smirnov
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia, Orel, Russia, kadyj@yandex.ru

Abstract: This article discusses the main ways of committing Internet fraud that have appeared in recent years. Attention is drawn to the main actions of criminals within each of the methods and how the typical behavior of the victim manifests itself. Digital fraud is analyzed, which today is a global problem for all economies of the world. The main reason for the spread of this problem can be considered the rapid development of computer and Internet technologies. The types of fraud are disclosed, as well as the ways of its commission. The schemes that are often used in fraud are described.

Keywords: internet, fraud, crime detection, methods of commission, phishing

For citation: Smirnov I. M. Operational and investigative characteristics of new ways of committing fraudulent actions in the network // Scientific Bulletin of the Orel Law Institute of the Ministry of the Interior of the Russian Federation named after V.V. Lukyanov. 2022. No 2(91). P. 210-216.

Отрасль связи и телекоммуникации является инфраструктурной. Оказывая значительное влияние на процессы инновационного развития страны в целом и производственной инфраструктуры других отраслей в частности, она определяет темпы роста национальной экономики, а также занимает существенную и постоянно увеличивающуюся долю в валовом внутреннем продукте.

В настоящее время информационная оснащенность выступает определяющим фактором эффективности функционирования всех сфер деятельности человека и государства. При этом уровень данной оснащенности обусловливается технологическими возможностями и напрямую зависит от наличия мобильных надежных каналов (средств) получения и передачи информации, а также квалифицированных специалистов, которые способны на высоком профессиональном уровне организовать данный процесс.

Вышеизложенное обстоятельство предопределило тот факт, что в последнее время происходит активное внедрение современных средств связи и телекоммуникации в жизнь граждан; осуществляются всеобщая компьютеризация, развитие новых технологий обработки и передачи данных; принимаются передовые инженерные решения создания телекоммуникационных сетей с использованием последних достижений современного рынка IT-технологий и т. д. [1, с. 54].

Наряду с очевидными плюсами развития российского общества в рассматриваемом направлении возникли существенные трудности: появилось множество внутренних и внешних угроз, нетрадиционных каналов утечки информации, несанкционированных доступов к ней, мошенничеств с использованием платежных карт и много других преступлений экономической направленности в подобных условиях защиты ресурсов связи.

Борьба с преступлениями в сфере предоставления услуг связи и телекоммуникации выступает одним из приоритетных направлений деятельности правоохранительных органов по обеспечению безопасности государства, отдельных граждан и их законных интересов. Данное обстоятельство обусловлено высокой степенью латентности рассматриваемых противоправных деяний, сложностью и большим объемом работы по делам о них, а также отсутствием достаточного положительного опыта практики противодействия данному виду преступлений.

Безусловно, практике противодействия хищениям, совершенным дистанционным способом, характерно наличие ряда проблем организационно-тактического и правового характера. С.В. Екимцев в своей статье, исследующей настоящий объект, к числу наиболее острых проблем относит недостаточный уровень подготовки оперативных сотрудников, способных противостоять преступлениям указанных видов [2, с. 72]. Данная проблема обусловлена отсутствием у них опыта раскрытия таких преступлений, а также недостаточным уровнем профессиональной подготовки. Об этом свидетельствует анализ образовательного процесса, который показывает, что даже в тематических планах дисциплин оперативно-розыскной специализации отсутствуют занятия, посвященные рассмотрению вопросов выявления, предупреждения, пресечения и раскрытия хищений денежных средств граждан, совершенных удаленным способом, что крайне негативно сказывается на процессе подготовки высококвалифицированных кадров [3, с. 127].

Развитие постиндустриального общества и цифровых технологий вывели на первое место и утвердили в качестве наиважнейшего ресурса информацию. Сегодня IT-технологии уже достигли пика своего развития и ежегодно набирают все большие обороты. Безусловно, все это влияет на большинство сфер жизнедеятельности общества и человека. Все позитивные моменты от использования возможностей Интернета успели осознать не только добросовестные граждане, но и преступники, ищущие мате-

риальную выгоду от совершения различных противоправных деяний в отношении доверчивых людей. Одним из наиболее распространенных преступных деяний, совершаемых с использованием сети Интернет, является мошенничество. Можно отметить, что в условиях развития IT-технологий традиционные способы совершения мошеннических действий постепенно отходят на второй план. Сейчас все реже можно услышать в открытых источниках об использовании «кукол», «ломок» или «пустышек» для хищения денежных средств у граждан. Сегодня можно говорить о постепенном переносе интереса мошенников на электронное пространство. Это связано с рядом ключевых факторов, среди которых:

- Удобство. Мошеннические действия такого рода совершаются дистанционно, что позволяет находиться в любой точке мире; также это расширяет круг потенциальных жертв.

- Повышенные шансы избежать ответственности. Вопросам конфиденциальности в сети уделяется достаточно много внимания в последние годы. Одним из ее негативных последствий является возможность для мошенников скрыться от преследования со стороны правоохранительных органов. Для этого уже существует множество различных облачных сервисов, анонимайзеров и т. п.

- Потенциальная выгода. О традиционных способах совершения мошеннических действий сегодня не знает только ленивый. А вот интернет-пространство позволяет мошенникам реализовать весь свой творческий потенциал, придумав новые способы совершения преступлений, которые неизвестны мнительным гражданам и которые с наибольшей вероятностью принесут результат.

- Виктимологические особенности. Именно в электронном пространстве наиболее просто отыскать потенциальных жертв мошеннических действий. Интернет-пространство полно пользователей, обладающих высокой степенью доверчивости, что привлекает преступников еще больше [4, с. 100].

Анализ современных новостных и иных информационных источников позволяет выделить ряд основных способов совершения мошенничества в сети, которые появились в последние годы.

1) Фишинг – данный способ совершения мошеннических действий нельзя назвать новым. Он появился достаточно давно, еще когда интернет лишь начинал распространяться для широких масс. Его суть состоит в рассылке специальных сообщений, которые различными средствами вынуждают жертв к передаче личной информации: паролей, пин-кодов и т. п. Традиционный фишинг, как правило, связан с высылкой уведомлений о блокировке аккаунта, банковских уведомлений, писем с просьбой перейти на сайт и восстановить доступ и т. д. [4, с. 246]. Однако ежегодно появляется множество новых способов осуществления фишинга, что заставляет обратить внимание на эту сферу. В первую очередь нужно говорить о способе, который был выявлен не так давно. Злоумышленники создают сайты-зеркала банковских ссылок для оплаты каких-либо товаров. Получая специальные коды, мошенники могут списывать отдельные суммы с банковских карт потерпевших. В последний год получил распространение фишинг посредством приложения «Blablacar», который используется для поиска попутчиков в совместных поездках по городам. Мошенники покупают аккаунты с хорошими рейтингами и выкладывают информацию о поездках по популярным маршрутам. Получив обращения потенциальных клиентов, злоумышленники просят перейти в сторонний мессенджер, так как само приложение не дает возможности реализовать дальнейший преступный замысел (маскируются номера, показываются предупреждения и т. п.) [5, с. 56]. Позже мошенники в переписке сообщают, что готовы взять пассажира, но нужно осуществить оплату на сайте организации. Далее жертве приходит СМС-

сообщение на фишинговый сайт, замаскированный под страницу «blablacar.ru», откуда преступники и получают доступ к необходимой информации по картам потерпевших.

2) Интернет-магазины. Ряд мошенников предпочитают заработать на желании людей покупать товары значительно дешевле, чем у официального продавца. Суть способа проста: создаются сайты или страницы в социальных сетях, где объявляется о продаже вещей по сниженной цене. Далее преступный замысел реализуется по двум основным схемам:

- мошенники получают деньги и перестают выходить на связь;
- мошенники получают деньги и высылают товар из самых дешевых материалов, даже близко не соответствующий рекламе.

В последние годы распространение данный способ получает на игровых платформах. Молодые люди, желающие получить популярные игры или расширения для них недорого, становятся жертвами мошенников, отправляя денежные средства «перекупщикам».

3) Работа с предоплатами – практикуется в различных сферах продаж. Наиболее часто встречается на сайтах, где размещаются объявления («Авито», «Юла», «Моя реклама», «Авто.ру», «ЦИАН» и т. д.). Мошенник выкладывает информацию о потенциально интересном товаре по выгодной цене. В личной беседе с покупателями выставляется условие о предоплате, которую человек вынужден заплатить, чтобы не потерять возможность приобрести товар или арендовать объект. Естественно, что позже такие лица свои обязательства не исполняют [6, с. 82].

4) Письма-просьбы – способ распространен достаточно давно, однако в последние годы приобретает особые формы. Очень часто страницы людей в социальных сетях взламываются, и мошенники рассылают всем друзьям в аккаунте просьбы о займах. Способы реализации данного метода достаточно разнообразны: некоторые пытаются играть на жалости, рассказывая про тяжелые болезни, операции и т. п., а некоторые пытаются имитировать обычные дружеские беседы, попутно прося «взаймы». Естественно, что подобные взломы страниц выявляются достаточно быстро – в течение 30 минут, однако и за это время часть доверчивых лиц успевает перечислить требуемые суммы[1].

5) Брокерские услуги – суть способа сводится к получению доступа к электронному устройству жертвы. Наиболее часто мошенничество распространяется в сфере предоставления брокерских услуг. Лицу предлагается несложный заработок. От него требуются лишь вложения и некоторые простые действия по установке и регистрации. Жертва все это выполняет и даже получает первую прибыль. Далее ему предлагается возможность увеличить свой капитал, но с привлечением профессионального брокера, который гарантирует стопроцентный результат. Потерпевший соглашается, и ему высылается пакет приложений, среди которых программа для удаленного доступа к его техническому устройству. Злоумышленник получает этот доступ и выводит все необходимые средства со счетов жертвы [7, с. 247].

6) Ставки на спорт – лицу предлагаются прогнозы для букмекерских контор, которые считаются договорными, то есть сделанными специально для извлечения прибыли. Жертве рекламируются указанные прогнозы с обещанием удвоения или утроения денежных вливаний. Также прилагаются отзывы всех ранее пользовавшихся услугами. Оплатив прогнозы, лицо получает информацию о прогнозе, который сделан «наугад». В результате потерпевший теряет деньги при оплате, а также при самой ставке, поскольку уверен в результате.

[1] Официальный сайт МВД России [Электронный ресурс]. URL: https://мвд.рф/-document/11700239

Не так давно получил распространение и новый способ – лицо предлагает совместными усилиями увеличить банк в букмекерских конторах. С него – аналитические способности со стопроцентным исходом, с жертвы – денежные средства. Мошенник дает прогнозы доверившемуся лицу. Если исход верен, деньги делятся пополам, если неверен – аналитик пропадает [8, с. 52].

Таким образом, нами были рассмотрены основные способы совершения мошенничества в сети Интернет, появившиеся в последние годы. Преступники постоянно пытаются найти новые возможности для извлечения материальной выгоды, поэтому потенциальным жертвам крайне важно всегда быть бдительными и не пытаться найти выгоду там, где ее быть не может.

Список источников

1. Князьков А.С. Следственная ситуация как предпосылка тактико-криминалистической деятельности следователя // Криминалистические чтения на Байкале – 2012: материалы Всероссийской научно-практической конференции. Иркутск, 2012. С. 54-60.

2. Екимцев С.В. Особенности раскрытия мошенничества, совершенного с использованием // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 1(90). С. 71-75.

3. Завезёнова И.А., Краюшкин К.Д., Нестерова А.В., Ососко Я.С. Цифровое мошенничество в финансовой сфере: новые типы обмана в контексте дигитализации: материалы Международного студенческого научно-практического форума по финансовой грамотности, Волгоградский государственный университет. 2018. С. 125-144.

4. Михайленко И.А. К вопросу о способах мошенничества в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5(13). С. 98-104.

5. Яковлев А.Н., Олиндер Н.В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методи-ческое пособие. М., 2012. 240 с.

6. Кузьмин И.А. Актуальные направления подготовки сотрудников ОВД, осуществляющих противодействие хищениям денежных средств с использованием информационно-коммуникационных технологий // Подготовка кадров для силовых структур: современные направления и образовательные технологии: материалы двадцать второй Всероссийской научно-методической конференции. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2015. С. 81-83.

7. Коровин Н.К., Щербина М.А. Способы совершения мошенничества в сети Интернет как элементы криминалистической характеристики // Лучшая научная статья 2018: сборник статей XVII Международного научно-исследовательского конкурса, Пенза, 30 мая 2018 года. Пенза: МЦНС «Наука и Просвещение», 2018. С. 245-247.

8. Иногамова-Хегай Л.В. Квалификации преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции, Москва, 24-25 января 2019 года. М.: РГ-Пресс, 2019. С. 51-55.

References

1. Knyaz'kov A.S. Sledstvennaya situaciya kak predposylka taktiko-kriminalisticheskoj deyatel'nosti sledovatelya // Kriminalisticheskie chteniya na Bajkale – 2012: materialy Vserossijskoj nauchno-prakticheskoj konferencii. Irkutsk, 2012. S. 54-60.

2. Ekimcev S.V. Osobennosti raskrytiya moshennichestva, sovershennogo s ispol'zovaniem // Nauchnyj vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. 2022. № 1(90). S. 71-75.

3. Zavezyonova I.A., Krayushkin K.D., Nesterova A.V., Ososko Ya.S. Cifrovoe moshennichestvo v finansovoj sfere: novye tipy obmana v kontekste digitalizacii: materialy Mezhdunarodnogo studencheskogo nauchno-prakticheskogo foruma po finansovoj gramotnosti, Volgogradskij gosudarstvennyj universitet. 2018. S. 125-144.

4. Mihajlenko I.A. K voprosu o sposobah moshennichestva v seti Internet // Sibirskie ugolovno-processual'nye i kriminalisticheskie chteniya. 2016. № 5(13). S. 98-104.

5. Yakovlev A.N., Olinder N.V. Osobennosti rassledovaniya prestuplenij, sovershennyh s ispol'zovaniem elektronnyh platezhnyh sredstv i sistem: nauchno-metodicheskoe posobie. M., 2012. 240 s.

6. Kuz'min I.A. Aktual'nye napravleniya podgotovki sotrudnikov OVD, osushchestvlyayushchih protivodejstvie hishcheniyam denezhnyh sredstv s ispol'zovaniem informacionno-kommunikacionnyh tekhnologij // Podgotovka kadrov dlya silovyh struktur: sovremennye napravleniya i obrazovatel'nye tekhnologii: materialy dvadcat' vtoroj Vserossijskoj nauchno-metodicheskoj konferencii. Irkutsk: FGKOU VPO VSI MVD Rossii, 2015. S. 81-83.

7. Korovin N.K., Shcherbina M.A. Sposoby sovershheniya moshennichestva v seti Internet kak elementy kriminalisticheskoj harakteristiki // Luchshaya nauchnaya stat'ya 2018: sbornik statej XVII Mezhdunarodnogo nauchno-issledovatel'skogo konkursa, Penza, 30 maya 2018 goda. Penza: MCNS «Nauka i Prosveshchenie», 2018. S. 245-247.

8. Inogamova-Hegaj L.V. Kvalifikacii prestuplenij s ispol'zovaniem komp'yuternyh tekhnologij // Ugolovnoe pravo: strategiya razvitiya v XXI veke: materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii, Moskva, 24-25 yanvarya 2019 goda. M.: RG-Press, 2019. S. 51-55.

Информация об авторе

Иван Михайлович Смирнов. Преподаватель кафедры оперативно-разыскной деятельности ОВД. Кандидат исторических наук.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, Россия, г. Орел, ул. Игнатова, д. 2.

Information about the author

Ivan M. Smirnov. Teacher of the chair of Operational Search Activity of the Internal Affairs Bodies. Candidate of historical sciences.

Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.

302027, Russia, Orel, st. Ignatova 2.

Статья поступила в редакцию 10.03.2022; одобрена после рецензирования 24.03.2022; принята к публикации 21.04.2022.

The article was submitted March 10, 2022; approved after reviewing March 24, 2022; accepted to the writing of the article for publication April 21, 2022