Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 1. – С. 291–295.

УДК 343.231

ДИСТАНЦИОННЫЕ СПОСОБЫ ХИЩЕНИЯ: РАЗНОВИДНОСТИ И ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ

Колычева А. Н., Зоз В. А.

За последние десять лет дистанционные способы хищения, сопряжённые с использованием электронных технологий, получили значительное распространение в системе преступлений. В статье рассматриваются основные способы дистанционных хищений, что позволяет ориентироваться в тенденциях совершения преступлений. Отражены сущность и особенности таких способов. В частности, отражены уязвимости при использовании мобильных приложений, банковских приложений, действий пользователей при поступлении сообщений или SMS, а также при использовании пластиковых банковских карт. Обозначены отдельные аспекты противодействия дистанционным способам хищения. Отражены проблемы, которые не позволяют противостоять преступлениям указанного вида в полной мере. Указаны случаи привлечения специалистов при расследовании хищений, совершенных дистанционным способом. Вместе с тем акцентировано внимание на том, что цифровой мир и развитие сетевого пространства происходит ежедневно, становясь интересным для злоумышленников в реализации преступного умысла, направленного на развитие новых способов хищений.

Ключевые слова: специальные познания, преступление, экспертиза, личность, собственность, расследование, специалист, эксперт.

Динамика развития информационных технологий на системной основе учитывает постоянное развитие сетевого пространства, что приводит к расширению предлагаемых человеку возможностей для работы, общения и в целом жизни. Расширение диапазона предлагаемых технологических возможностей привлекает значительную часть населения развитых и развивающихся стран в сферу информационных технологий. В настоящее время люди по всему миру активно пользуются разнообразными платёжными системами коммерческих банков, различных агрегаторов, предлагающих множественные услуги эквайринга, а также возможности дистанционно управлять движением денежных средств, находящихся на банковских счетах и электронных кошельках, посредством мобильных технологий. Указанные возможности не остались в стороне интересов преступного мира. В результате чего широко распространяются постоянно обновляемые способы хищений, основывающихся на современных возможностях техники и связи, становясь постоянным вызовом для правоохранительных органов в борьбе с новыми видами и формами совершения преступлений.

Преступные схемы хищений у физических и юридических лиц, с использованием дистанционных способов, постоянно усовершенствуются [1].

Существует, несколько схем, которыми могут воспользоваться мошенники.

1. Мобильные операторы постоянно предлагают всевозможные опции и услуги. Клиентам предлагается такая услуга, как сохранение собственного номера и лишь смена мобильного оператора. Однако многие не хотят заниматься долгой процедурой и просто покупают новую сим-карту с новым номером телефона. Эта, казалось бы, безобидная операция, может привести к серьезным последствиям. Ведь особенность услуги «мобильный банк» заключается в том, что он привязывается к определенному номеру. Довольно обычное явление, когда люди меняют сим-карту или вовсе имеют по две три сим-карты и происходит привязка двух номеров к одному мобильному банку. При этом владелец пользуется одной сим-картой намного чаще,

чем другой и когда карта долгое время не активна, номер может быть передан совершенно другому лицу, путем продажи. Новому владельцу начинают приходить уведомления о действиях, связанных с покупками или иными операциями, сделанных прошлым владельцем. В таких случаях, мошенники не упускают шанс, снимают или переводят денежные средства, получают доступ к личным данным и могут проводить различные манипуляции, направленные на хищения. Мошенники тщательно следят за такой забывчивостью клиентов разных сотовых операторов, мониторя базы вторичной перепродажи старых сотовых номеров. В таких случаях следует соотносить риски, связанные со сменой абонентского номера или возможности перехода номера к другому абоненту, а также уведомлять банк при отключении услуг привязанного абонентского номера.

Рассмотрим пример, произошедший в Алтайском крае. Гражданин А., в целях подключения Интернета через модем, приобрёл новую сим-карту у своего знакомого. Сим-карта была активирована через мобильный телефон. Далее он перенёс сим-карту в модем, после чего Интернет был настроен и доступ в информационно-телекоммуникационную сеть был установлен. На данный номер начали приходить сообщения о поступлении денежных средств на карту «МИР», однако данная карта не принадлежала гражданину А. Обвиняемый А., сообразив, что к его новому номеру, привязана чья-то карта, не принадлежащая ни ему, ни его знакомому решил воспользоваться данной информацией. Так как на карту были зачислены денежные средства, то у гражданина А. появилась возможность перевода их на свою карту и дальнейшие манипуляции. Для реализации своих корыстных побуждений, он оплатил свои услуги на конкретную сумму, отправив команду на номер 900, тем самым совершил хищение денежных средств со счёта, не принадлежащего ему [2].

В результате расследования данного преступления следователь квалифицировал данное деяние по п. «г» ч. 3 ст. 158 УК РФ.

2. Продвинутые и изобретательные дистанционные мошенники только в редких случаях дают себя обнаружить. Если рассматривать один из частых случаев, такой как оставление телефона без присмотра, мошенники работают очень быстро и практично. Их целью не является хищение самого телефона, для них намного важнее та информация, которая находится непосредственно в нём. Они могут и вовсе сами отдать телефон лицу, которому он принадлежит, но до этого момента совершают некоторые манипуляции, например, установка вирусных программ. Впоследствии это ведет к списанию денежных средств и получения доступа к личной информации пользователя.

3. Ещё одним способом кражи денежных средств являются приложения. Каждый из нас загружает обычные приложения, например, игры, полезные приложения, вроде подсчета шагов или измерение пульса и другое. Но мошенники создают собственные приложения-шпионы. Визуально узнать эти приложения невозможно, поскольку злоумышленники имеют замечательные навыки редактирования и создания яркой обложки, которая привлекает немало клиентов. Однако при использовании такого приложения, пользователя может насторожить большое количество запросов на пользование личными данными, например, запрос на доступ к просмотру изображений, использование и отправку SMS, доступ в Интернет. Данные запросы должны заставить задуматься о том, стоит ли скачивать подобное приложение или программу, если её вторжение в личные данные так велико.

4. Следующим минусом, который тоже связан с банковскими приложениями является вирус-троян, который пользователи устанавливают вместе с приложением.

Данная схема рассчитана на интернет – пользователей, полностью уверенных в источниках, с которых они скачивают информацию и приложения. Но это не является проблемой для мошенников. В 2017 году жертвами мошенников стали пользователи даже сервиса «Яндекс.Директ». С помощью него размещались рекламы вредоносных сайтов, связанных с банковскими операциями. Суть этой схемы состоит в перехвате всей важной информацией, связанной с переводом средств и сменой пароля клиента. В этом процессе – клиент становится частью вируса, поскольку считываются данные о его контактах и высылаются ссылки на такое же приложение. При этом невозможно проследить за тем, что программа постоянно рассылает другим пользователям данное приложение. При этом мошенники также распространяют это через SMS-рассылку, рекламные баннеры или по электронной почте.

5. В нашем мире достаточно часто случаются мошенничества через сообщения или SMS. Владельцу на его номер поступает информация о том, что его карта заблокирована или с неё списаны денежные средства и необходимо предотвратить попытку взлома, при этом необходимо перейти по ссылке или позвонить по предложенному номеру. В случае перехода по ссылке или осуществления звонка, мошенники могут представиться «сотрудниками банка» или вовсе «сотрудниками полиции», после чего втираются в доверие и узнают личную информацию, связанную с банковскими картами и разговор с клиентом прекращается, чтобы не вызвать лишних подозрений. Другой разновидностью завладения личных данных жертвы становятся открытые источники информации, размещенные на различных ресурсах Сети [3], которые на системной основе мониторят злоумышленники [4].

6. В наше время бесконтактная оплата становится незаменимой. Люди привыкают к тому, что покупка товаров банковскими картами и телефоном, без ввода пинкода и прикладывания карты экономит время, а также проще в осуществлении. Цифровое общество ежегодно развивается, следовательно, мошенники осваивают новые системы получения компьютерной информации. В их арсенале появляются переносные терминалы, в которых заранее настроен определенный лимит списание средств. Если терминал приложить к сумке или чему-то подобному, где лежит банковская карта, то без подтверждения будет списана заранее определенная сумма, то есть бесконтактная оплата.

7. Атаки мошенников могут распространяться не только на пластиковые карты, но и на сами банкоматы. Около пяти лет назад активно использовалась методика загрузки вируса на банкомат, это заключалось в принудительной выдаче купюр, активации происходила путем ввода специального кода.

Однако последние две схемы из указанных выше, за последние годы теряют свою актуальность, поскольку противодействие, оказываемое сотрудниками правоохранительных органов, приносит свои положительные. Такая положительная динамика связывается с привлечением узких специалистов.

При совершении такого рода преступлений нельзя точно сказать, сколько компьютерного оборудования было применено. В настоящее время разработано большое количество научных методических рекомендаций, однако до сих пор они не охватывают весь массив современной техники. Исходя из этого у следователя, специалиста, оперативного сотрудника возникают проблемы в сборе доказательств [5].

При расследовании преступлений с самого начала особую роль играют привлекаемые специалисты. Беседа, консультация, консультативно-справочная деятельность, совместное планирование, обмен информацией, совместный анализ полученных результатов, подготовка к следственным действиям и оперативно-розыскным мероприятиям и т.д.

Консультации могут быть необходимы в случаях [6]:

- при установлении особенностей работы мобильного банкинга;
- подготовки следственного действия – допрос, а именно составления грамотных вопросов и материалов, которые будут использованы;
- процесса функционирования мобильного банкинга;
- в случаях изъятия технических средств, их упаковка и хранение, а также комплектации техники и носителей информации;
- помощь при назначении экспертизы, составления вопросов, входящих в постановление следователя, определения объектов, которые будут направлены в ЭКЦ;
- организационно-техническое содействие, такое как помощь в расшифровке кодов, подготовка необходимых средств, используемых в следственных действиях.

Стоить также отметить, что в соответствии с УПК РФ закреплено, обязательно участие специалиста при производстве такого следственного действия как выемка, а именно связная с электронными носителями информации и компьютерной техникой. Также по ходатайству лиц, законно владеющих изымаемыми объектами, о копировании информации, специалист лично должен одобрить данные действия, так как он является ответственным лицом за сохранение полученной информации. Специалист имеет право корректировать следователя, если используется неверная терминология и заменять в соответствии с установленными нормами. Особое внимание следует уделять назначению и производству экспертиз.

Вопросы противодействия рассмотренным преступным схемам стоят перед правоохранителями очень остро. Острота проблематики по данному вопросу заключается в разнообразных факторах, связанных с правовыми пробелами, отсутствием универсальных организационно-тактических рекомендаций, низкой подготовленностью субъектов расследования. Последний связан отсутствием качественной профессиональной подготовки кадров [7], способных своевременно и профессионально реагировать на новые вызовы преступного мира.

Таким образом, систематизация преступных схем, анализ следственной и судебной практики, а также разработанные на их основе актуальные криминалистические рекомендации, на основе которых будет осуществляться обучение правоохранителей, смогут способствовать улучшению ситуации с расследованием преступлений в сфере информационных технологий.

Список литературы:

1. Бадиков Д.А., Гришечкина Д.А. Пробелы правового регулирования информационно-телекоммуникационных преступлений в деятельности правоохранительных органов // Актуальные проблемы уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности: сборник статей. Орел, 2022. С. 6-9.
2. Приговор Кытмановского районного суда Алтайского края от 10 декабря 2018 г. № 1-75/2018. URL: sudact.ru (lata обращения: 01.11.2023).
3. Даниленко Ю.А. Криминалистическое распознавание в тактике производства следственных действий при расследовании преступлений в сфере компьютерной информации // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2023. Т. 9 (75). № 2. С. 294-298.

4. Матросова Л.Д., Кислицин И.А. Инструменты для поиска оперативно-значимой информации по открытым источникам // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4(93). С. 65-72.
5. Чаплыгина В.Н., Красова А.А. Проблемные аспекты механизма реализации системы оценки следственной деятельности // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2020. № 2(83). С. 101-107.
6. Новгородская В.Б. Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л. А. Новоселовой. М.: Проспект, 2019.
7. Морозова Н.В. Некоторые особенности расследования компьютерных преступлений // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: сборник материалов международной научно-практической конференции, посвященной 100-летию принятия УПК РСФСР 1922 г., 20-летию действия УПК РФ. Орел, 2022. С. 240-245.

Kolycheva A.N., Zoz V.A. Remote methods of theft: varieties and individual aspects of counteraction // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 1. – P. 291–295.

Over the past ten years, remote theft methods involving the use of electronic technologies have become widespread in the crime system. The article discusses the main methods of remote theft, which allows you to navigate the trends of crime. The essence and features of such methods are reflected. In particular, vulnerabilities are reflected when using mobile applications, banking applications, user actions when receiving messages or SMS, as well as when using plastic bank cards. Certain aspects of countering remote methods of theft are outlined. The problems that do not allow us to fully confront crimes of this type are reflected. The cases of involvement of specialists in the investigation of theft committed remotely are indicated. At the same time, attention is focused on the fact that the digital world and the development of the network space occur daily, becoming interesting for intruders in the implementation of criminal intent aimed at the development of new methods of theft.

Keywords: special knowledge, crime, expertise, personality, property, investigation, specialist, expert.

Spisok literatury:

1. Morozova N.V. Nekotorye osobennosti rassledovaniya komp'yuternyh prestuplenij // Sovremennoe ugolovno-processual'noe pravo – uroki istorii i problemy dal'nejshego reformirovaniya: sbornik materialov mezhdunarodnoj nauchno-prakticheskoj konferencii, posvyashchennoj 100-letiyu prinyatiya UPK RSFSR 1922 g., 20-letiyu dejstviya UPK RF. Orel, 2022. S. 240-245.
2. Badikov D.A., Grishechkina D.A. Probely pravovogo regulirovaniya informacionno-telekommunikacionnyh prestuplenij v deyatel'nosti pravoohranitel'nyh organov // Aktual'nye problemy ugolovno-processual'nogo prava, kriminalistiki i operativno-rozysknoj deyatel'nosti: sbornik statej. Orel, 2022. S. 6-9.
3. Prigovor Kytmanovskogo rajonnogo suda Altajskogo kraya ot 10 dekabrya 2018 g. № 1-75/2018. URL: sudact.ru (lata obrashcheniya: 01.11.2023).
4. Danilenko YU.A. Kriminalisticheskoe raspoznavanie v taktike proizvodstva sledstvennyh dejstvij pri rassledovanii prestuplenij v sfere komp'yuternoj informacii // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2023. T. 9 (75). № 2. S. 294-298.
5. Matrosova L.D., Kislicin I.A. Instrumenty dlya poiska operativno-znachimoj informacii po otkrytym istochnikam // Nauchnyj vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. 2022. № 4(93).S. 65-72.
6. CHaplygina V.N., Krasova A.A. Problemnye aspekty mekhanizma realizacii sistemy ocenki sledstvennoj deyatel'nosti // Nauchnyj vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. 2020. № 2(83).S. 101-107.
7. Novgorodskaya V.B. Novye tekhnologii (blokchejn / iskusstvennyj intellekt) na sluzhbe prava: nauchno-metodicheskoe posobie / pod red. L. A. Novoselovoj. M.: Prospekt, 2019.