УДК/UDC 343.98

Некоторые аспекты методики расследования хищений, совершенных посредством использования информационных технологий

Малиев Руслан Таймуразович
студент юридического факультета
Кубанский государственный аграрный университет им. И. Т. Трубилина
г. Краснодар, Россия
e-mail: rmaliiev@mail.ru

Аннотация

Современное развитие информационных технологий позволяет осуществлять дистанционное обслуживание банковских счетов и операций. Это обуславливает увеличение количества преступлений в банковской сфере. Рост хищений, связанных с банковскими счетами и операциями, вызван в т. ч. возможностью дистанционного доступа в личный кабинет клиентов посредством Интернета. В статье рассматриваются некоторые аспекты методики расследования хищений, совершенных с использованием информационных технологий. Отмечается, что на эффективность и оперативность расследования оказывает влияние скорость передачи информации от потерпевших правоохранительным органам. Подробно анализируются следственные действия, характерные для начального этапа расследования преступлений данной категории: допросы, обыски (выемки) и осмотры. Положения методики, изложенные в данной работе, могут послужить основой планирования расследования подобного рода преступлений.

Ключевые слова: расследование, информационные технологии, хищение, банковская системы, современные технологии.

Some aspects of the investigation of theft committed through the use of information technology

Maliyev Ruslan Taymurazovich
student of the Faculty of Law
Kuban State Agrarian University
Krasnodar, Russia
e-mail: rmaliiev@mail.ru

Abstract

The modern development of information technologies allows remote servicing of bank accounts and transactions. This leads to an increase in the number of crimes in the banking sector. The increase in theft related to bank accounts and operations was caused, among other things, by the possibility of remote access to the clients' personal account via the Internet. The article discusses some aspects of the methodology for investigating thefts committed using information technology. It is noted that the speed of transmission of information from victims to law enforcement agencies affects the effectiveness and efficiency of the investigation. The investigative actions characteristic of the initial stage of the investigation of crimes of this category are analyzed in detail: interrogations, searches (seizures) and examinations. The provisions of the methodology outlined in this work can serve as the basis for planning the investigation of such crimes.

Key words: investigation, information technology, theft, banking systems, modern technologies.

С развитием научно-технического прогресса и цифровизации большинства секторов экономики наблюдается рост киберпреступности, появление новых способов хищений, включая использование расчетных и кредитных банковских карт. При хищении денежных средств с расчетных и личных счетов клиентов банка часто используются платежные банковские системы. Преступники действуют, как правило, удаленно, совершая интернет-атаки, похищая электронные ключи с цифровыми подписями клиентов банка, а затем совершают незаконные операции. Хищение денежных средств маскируется под атаки на сайты банков, поэтому клиенты не могут в режиме реального времени зайти в личный кабинет и

проверить состояние своих счетов и проводимых операций (транзакций) [1].

Для противодействия подобного рода преступлениям необходимо использовать эффективные меры уголовно-правового характера. Кроме того, в данном случае на эффективность и оперативность расследования оказывает влияние скорость передачи информации от потерпевших правоохранительным органам. При расследовании хищений, совершаемых с использованием электронных счетов, на первоначальном этапе расследования наиболее распространенными следственными действиями являются допросы, обыски (выемки) и осмотры [2].

При проведении допроса подозреваемого (обвиняемого) следует установить момент возникновения преступного умысла, время, место и способ совершения хищения, а также действия, которые были связаны с подготовкой к хищению, поскольку в них отражаются его профессиональные навыки. Подготовительные действия заключаются, как правило, в подборе сим-карт, открытии банковских счетов, подключении услуг сотового оператора, поиске сообщников, покупке и настройке оборудования [3]. Также подготовительные действия связаны с приобретением и установкой вредоносных программ, разработкой алгоритмов данных программ. Подготовка технических средств необходима для преодоления средств компьютерной защиты. Зачастую для этого требуется смартфон, на котором установлено приложение «Мобильный банк», кроме того, посредством вредоносных программ преступники получают информацию о банковских операциях, о движении средств по счету.

Материалы уголовного дела также должны включать в себя копии документов, которые подтверждают получение сведений, используемых для совершения преступления: распечатки смс-сообщений, сведения о движении средств по счету, чеки, подтверждающие факт оплаты товара, обналичивание денежных средств [1].

Допрашивая потерпевшего, следователь должен установить наименование банка, в котором потерпевший обслуживается, условия использования банковских услуг. В материалах уголовного дела в обязательном

порядке должен быть договор банковского вклада, сведения о подключении услуг «Мобильного банка», сведения о датах подключения и использовании мобильного банка, сведения об использовании абонентского номера и о лицах, которые пользовались номером. Если абонентский номер зарегистрирован на другое лицо, необходимо допросить также и его [4].

Затем следует установить, в какой момент потерпевший обнаружил пропажу денежных средств со счета, а также приобщить сведения, подтверждающие снятие со счета денежных средств. Нужно оценить причиненный ущерб, приобщить к материалам дела документы, подтверждающие, что ущерб является крупным или значительным (например, справку о доходах, сведения о членах семьи).

Допрос необходимо проводить также в отношении разработчиков системы программного обеспечения и технических средств защиты. В рамках допроса данных специалистов следует получить сведения о пароле, коды доступа. Допрашивая сотрудников кредитных организаций, следует установить круг их обязанностей, порядок осуществления платежей, получить выписки по лицевому счету, проверить правомерность списания денежных средств [2].

В процессе расследования требуется получить сведения о том, на основании каких документов, удостоверяющих личность, были открыты счета, какие действия, связанные с управлением счетом, были совершены. При необходимости следует истребовать записи с камер видеонаблюдения.

При проведении обыска и выемки предметами поиска являются не только компьютеры и имеющаяся на них информация, но также и документы, которые содержат правила совершения операций. Помимо этого, следует обратить внимание на мобильные телефоны, машинные носители информации, специальные приспособленные технические устройства, а также бланки, фрагменты, тексты программ [3].

При производстве выемки и обыска, связанных с изъятием электронных носителей, требуется участие специалиста. Особое внимание

следует уделить предметам, которые содержат в себе пароли, коды доступа, идентификационные номера, названия, электронный адрес, а также сведения о пользователях компьютерных систем и алгоритмов [5].

При осмотре персонального компьютера необходимо обратить внимание на системные блоки, на носителей информации, данные оперативной памяти, жесткие диски, на системы хранения информации и карты памяти. В процессе осмотра носителей информации в протоколе отражаются внешние индивидуальные признаки, сведения о заводских характеристиках, о повреждениях. Затем следует перейти к осмотру компьютерной информации, которая содержится на машинных носителях. В протоколе осмотра необходимо отразить наличие индивидуальных черт и свойств, которые позволят отличить осматриваемый предмет от других: наличие голографии, штрих-кода, эмбоссинга, перфорации, личной подписи и т. д.

Часто при расследовании хищений с использованием компьютерных средств назначается судебная компьютерная экспертиза, связанная с исследованием компьютерной информации. С помощью экспертизы можно установить состояние носителя компьютерной информации, свойства продукта, общие характеристики программного обеспечения, версию программы, наличие защитных устройств и механизмов, позволяющих преодолевать защиту, состав файлов программного обеспечения, его параметры. Кроме того, проведение компьютерной экспертизы позволяет выявить наличие текстов и иной информации на носителе, установить функции вредоносных программ, возможность удаленного подключения, а также перехвата номеров банковских операций и хищения конфиденциальной информации [5].

Посредством экспертизы происходит установление свойства и вида представленной информации, первоначальное состояние информации, способы и время воздействия, условия изменения свойств исследуемой информации, способы выявления данных, данные о собственнике.

По делам рассматриваемой категории часто проводятся дактилоскопические, почерковедческие и технико-криминалистические экспер-

тизы документов, а также экспертизы веществ, изделий и материалов. Поэтому расследование уголовных дел, связанных с хищением посредством использования технических средств, невозможно проводить без учета специфических особенностей объекта и предмета преступления [6].

Таким образом, расследование уголовных дел указанной категории невозможно без учета специфических особенностей способа совершения преступления, которые способствуют установлению круга вопросов, подлежащих доказыванию. Рассмотренные в данной работе некоторые аспекты методики раскрытия хищений, совершенных посредством использования информационных технологий, могут послужить основой планирования расследования подобного рода преступлений.

Список литературы

1. Влезько Д. А. Проблемы определения объекта и предмета криминалистики // В сборнике: Научное обеспечение агропромышленного комплекса. Сборник статей по материалам IX Всероссийской конференции молодых ученых, посвященной 75-летию В. М. Шевцова / Отв. за вып. А. Г. Кощаев. Краснодар: КубГАУ, 2016. С. 517–519.

2. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: Приказ МВД России от 29.06.2005 № 511 // Российская газета. 2005. № 191. 30 авг.

3. О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга: Письмо Банка России от 30.01.2009 № 11-Т // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_100931/ (дата обращения: 03.12.2020).

4. Влезько Д. А. Личность преступника в системе элементов криминалистической характеристики убийств // Итоги научно-исследовательской работы за 2017 год: сборник статей по материалам 73-й научно-практической конференции преподавателей / Отв. за вып. А. Г. Кощаев. Краснодар: КубГАУ, 2018. С. 649.

5. Алегин А. П. Источники криминалистической информации о преступлениях, связанных с изготовлением и использованием поддельных пластиковых расчетных карт // Российский следователь. 2017. № 20. С. 2–4.

6. Скобелин С. Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42–44.

References

1. Vlezko D. A. Problems of determining the object and subject of criminalistics // Scientific support of the agro-industrial complex: collection of articles based on the materials of the IX all-Russian conference of young scientists, vol. 75th anniversary Of V. M. Shevtsov / responsible for the issue A. G. Koshchaev. - Krasnodar: Kubgau, 2016. Pp. 517-519.

2. Questions of the organization of production of judicial examinations in expert and criminalistic divisions of internal Affairs bodies of the Russian Federation: Order of the Ministry of internal Affairs of Russia of June 29, 2005 No. 511 // Rossiyskaya Gazeta. 2005. No. 191. 30 Aug.

3. About recommendations for credit organizations on additional information security measures when using Internet banking systems: Letter of the Bank of Russia dated January 30, 2009 No 11-T // Consultant Plus. URL: http://www.consultant.ru/document/cons_doc_LAW_100931/ (access date: December 03, 2020).

4. Vlezko D. A. Personality of the criminal in the system of elements of criminalistic characteristics of murders // Results of research work for 2017: collection of articles based on the materials of the 73rd scientific and practical Conf. of teachers / OTV. for issue A. G. Koshchaev. - Krasnodar: Kubgau, 2018. P. 649.

5. Alegin A. P. Sources of forensic information about crimes related to the manufacture and use of fake plastic payment cards // Russian investigator. 2017. No. 20. Pp. 2-4.

6. Skobelin S. J. Digital forensics: the object and direction of development // Russian investigator. 2020. No 4. Pp. 42-44.