УДК 343.985.7

Старостенко Нина Игоревна
адъюнкт кафедры криминалистики,
Краснодарский университет МВД России
nstarostenko1996@mail.ru
Starostenko Nina Igorevna
Adjunct of the Department of Forensic Science
Krasnodar University of the Ministry of
Internal Affairs of Russia
nstarostenko1996@mail.ru

Особенности тактики допроса потерпевших при расследовании хищений, совершенных с использованием методов социальной инженерии и информационно-телекоммуникационных технологий

Features of the tactics of interrogating victims in the investigation of thefts committed using social engineering and information and telecommunication technologies

Аннотация. *В статистических данных МВД России наблюдается значительный рост количества общественно-опасных деяний, совершенных с применением информационно-телекоммуникационных технологий. Автор обращает внимание на то, что важными условиями успешного проведения указанного следственного действия являются тщательная подготовка к нему и привлечение к участию специалиста-психолога. В статье сформированы обстоятельства, которые подлежат обязательному уточнению по делам данной категории для обеспечения полноты проведения анализируемого следственного действия.*

Ключевые слова*: криминалистика, расследование преступлений, допрос, социальная инженерия, методы социальной инженерии, информационно-телекоммуникационные технологии.*

Annotation. *In the statistical data of the Ministry of Internal Affairs of Russia, there is a significant increase in the number of socially dangerous acts committed with the use of information and telecommunication technologies. The author draws attention to the fact that the main conditions for the successful implementation of this investigative action are thorough preparation for it and the involvement of a specialist psychologist. The article defines the circumstances that are subject to mandatory clarification in cases of this category to ensure the completeness of the analyzed investigative action.*

Key words*: forensics, crime investigation, interrogation, social engineering, methods of social engineering, information and telecommunication technologies.*

В статистических данных МВД России наблюдается значительный рост количества общественно-опасных деяний, совершенных с применением

информационно-телекоммуникационных технологий. Так, с января по декабрь 2020 г. зарегистрировано на 73,4 % больше таких преступлений, чем за 2019 г., в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%[1]. Исследование таких преступлений позволяет сделать вывод о существенных криминалистических особенностях их совершения. В числе таких особенностей отмечается активное использование в ходе подготовки и совершения таких хищений методов социальной инженерии. Например, как было отмечено главой Центрального банка России Э.С. Набиуллиной, около 70% операций, которые делаются без согласия клиента, совершаются с использованием социальной инженерии[2].

Анализируя многочисленные подходы к дефиниции этого явления, можно обобщенно определить хищение, совершаемое при помощи информационно-телекоммуникационных технологий, с использованием методов социальной инженерии, как противоправное умышленное безвозмездное изъятие чужого имущества (электронных денежных средств жертвы) путем обмана и злоупотреблением доверия, с использованием приемов психологического манипулирования, реализуемых при помощи информационно-телекоммуникационных технологий, с целью побуждения у жертвы желания в предоставлении конфиденциальной информации, осуществления ею денежных переводов на банковские счета сторонних лиц или убеждения ее в выполнении иных действий, создающих благоприятные условия для последующего завладения электронными денежными средствами.

Наиболее распространенным и тактически сложным следственным действием по делам о таких хищениях является допрос потерпевших. Рассматриваемое процессуальное действие признается наиболее существенным по своей юридической природе и доказательственной силе при расследовании преступлений обозначенной категории.

Общие правила тактики производства допроса подробно описаны в криминалистической литературе[3-5], однако, специфика совершения преступлений обозначенного вида вынуждает проанализировать некоторые особенности его проведения.

Необходимым условием успешного проведения допроса потерпевшего является тщательная подготовка к нему. Такая подготовка, как правило, должна включать изучение криминалистической характеристики совершенного деяния, в том числе личности допрашиваемого, механизма и способа совершения преступления. Кроме того, при подготовке к допросу потерпевшего следователь (дознаватель) также должен учесть тот факт, что, в большинстве случаев, допрашиваемое лицо не имеет глубокие познания о возможностях современных информационно-телекоммуникационных технологиях, а также о нюансах банковских операций и в некоторых случаях о действиях, которые повлекли хищение принадлежавших ему электронных денежных средств.

В этом аспекте приобретает существенную значимость выявление всех обстоятельств совершенного преступления. В связи с тем, что потерпевшие добровольно предоставляют доступ к своим электронным денежным средствам или переводят их на счета мошенников, необходимо устанавливать, какие именно действия подозреваемого привели к разглашению конфиденциальной информации, а также механизм получения несанкционируемого доступа подозреваемого к электронным денежным средствам. Кроме того, подлежит установлению объем ложной информации, сказанной подозреваемым, которая позволила потерпевшему воспринять ее за действительность.

Изучая вопрос об использовании преступником различных техник психологического манипулирования, необходимо рассмотреть возможность участия в проведении рассматриваемого следственного действия лиц, обладающих специальными знаниями. В данном случае актуальным является привлечение к участию специалиста-психолога. Рассматриваемая необходимость обуславливается тем, что в момент противоправного деяния в отношении потерпевшего применялись методы социальной инженерии, а также техники скрытого психологического воздействия. Указанная рекомендация является существенной, так как в основном при проведении допроса потерпевших по данной категории дел используются шаблонные вопросы, которые не раскрывают сущность способа совершения преступления, а также психологического состояния потерпевшего.

В случае отсутствия возможности в привлечении специалистов, то при проведении допроса целесообразно использовать возможности современных систем звуковой аудиозаписи. Это позволит максимально полно и объективно изучить информацию, полученную в процессе следственного действия, а также при возникновении потребности в получении специальных знаний в той или иной области обратиться за разъяснениями к специалисту, предъявив существующую запись следственного действия.

Следственная и судебная практика свидетельствует о том, что наиболее распространенным недостатком в проведении допроса потерпевших является его неполнота. Как показали исследования, в процессе проведения следственного действия не выясняется совокупность обстоятельств, имеющих существенное значение для расследования уголовного дела. К таким обстоятельствам можно отнести: отсутствие подробного описания способа совершения преступления, его специфики, особенностей действий злоумышленников при реализации корыстного умысла, участников преступной группы, а также характеристики механизма манипулятивного воздействия, оказываемого на потерпевшего[6, с.140-144].

В процессе допроса потерпевшего, установив с ним психологический контакт, необходимо предпринять меры по расположению допрашиваемого к даче показаний в форме свободного рассказа. Исходя из тематики рассматриваемой проблемы, мы не будем затрагивать вопросы по установлению психологического контакта с потерпевшим при допросе, так как они широко освещены в криминалистической литературе.

Остановимся более подробно на обстоятельствах, которые подлежат обязательному уточнению для обеспечения полноты проведения допроса:

1. Информация о банковском счете и банковской карте потерпевшего (полное наименование банка и иные его реквизиты, включая юридический адрес, дата, место, цель открытия банковского счета и приобретения банковской карты).

2. Информация о выполнении транзакций с электронными денежными средствами с использованием банковского счета и банковской карты потерпевшего (сведения о проводимых финансовых операциях, обстоятельствах использования банковского счета (карты), наименование сервиса дистанционного банковского обслуживания, круг лиц, имеющий доступ к счету(карте)).

3. Информация о неправомерном доступе к банковскому счету (карте) третьими лицами (дата и время обнаружения хищения денежных средств с банковского счёта, обстоятельства, при которых потерпевшему стало известно о хищении электронных денежных средств).

4. Характеристика электронных устройств и программных компонентов, используемых потерпевшим до и в момент совершения в отношении него мошеннических действий (наименование электронного устройства, модель, марка, серийный номер, наименование программных компонентов).

5. Наименование оператора сотовой связи, абонентский номер, привязанный к банковскому счету (карте) потерпевшего, Ф.И.О. лица, на которого зарегистрирован абонентский номер.

6. Характеристика действий потерпевшего совершенных в результате применения методов социальной инженерии (открыл ссылку, полученную из смс, сообщил злоумышленнику данные карты, код из смс от банка или CVV-код, осуществил перевод денежных средств на счет подозреваемого, загрузил файл и др.)

7. Характеристика конфиденциальной информации, которую потерпевший сообщил подозреваемому, а также обстоятельства, повлекшие предоставление подозреваемому персональных данных или банковских сведений.

8. Характеристика требований или дополнительных указаний, поступавших от подозреваемого лица в момент совершения преступления.

9. Информация о психологических приемах воздействия на потерпевшего (условия, которые вызвали доверие и спровоцировали сообщение конфиденциальной информации подозреваемому, описание мошеннических приемов, которые применил подозреваемый для доступа к конфиденциальным данным и электронным денежным средствам потерпевшего).

10. Информация о подозреваемом (способ совершения преступления, характеристика личности, особенности взаимодействия: голос, манера общения, текст сообщения и иные приметы, позволяющие идентифицировать подозреваемых лиц т.д., в случае если потерпевшему известны некоторые

установочные данные подозреваемого, Ф.И.О., абонентский номер сведения о номере счета (карты) получателя денежных средств и др.).

11. Информация о банковском терминале (наименование, местонахождение и др.), через который были переведены денежные средства.

12. Информация о наличии следов преступной деятельности подозреваемого (платежные документы, справки, записи телефонного разговора с подозреваемым, снимков экрана электронного устройства потерпевшего, констатирующих выполнение финансовых операций, взаимодействие с подозреваемым, оказание им психологического воздействия на потерпевшего и др.).

13.Информация о сумме электронных денежных средств потерпевшего (сумма денежных средств, находившаяся на банковском счете (карте) до неправомерного доступа и после.

14. Информация о мерах, которые предпринял потерпевший после совершенного в отношении него преступления.

15. Информация о личностях возможных свидетелей преступления.

Следует отметить, что приведенный перечень обстоятельств не считается исчерпывающим. В зависимости от ситуации и способа совершения хищений с использованием методов социальной инженерии и информационно-телекоммуникационных технологий характер обстоятельств, требующих уточнения, может быть дополнен.

Литература

1. Официальный сайт МВД [Электронный ресурс] URL: https://мвд.рф/reports/item/21551069/ (дата обращения 28.08.2021 г.)

2. Глава ЦБ рассказала о способах защиты от мошенников [Электронный ресурс] URL: https://ria.ru/20200625/1573453411.html (дата обращения: 01.09.2021).

3. Бахин В.П. и др. Допрос на предварительном следствии. Алма-Ата, 1999.

4. Гримак Л.П., Скрыпников А.И. Психологические методы активизации памяти свидетелей и потерпевших. М., 1999.

5. Зорин Г.А. Руководство по тактике допроса. М., 2001.

6. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита / Е. Л. Доценко. — М.: ЧеРо — Издательство МГУ, 1997. — С. 140-144.

Literature

1. Official website of the Ministry of Internal Affairs [Electronic resource] URL: https: //mvd.rf/reports/item/21551069/ (date of treatment 08/28/2021)

2. The head of the Central Bank told about the methods of protection against fraudsters [Electronic resource] URL: https://ria.ru/20200625/1573453411.html (date of access: 01.09.2021).

3. Bakhin V.P. and others. Interrogation at the preliminary investigation. Alma-Ata, 1999.

4. Grimak L. P., Skrypnikov A. I. Psychological methods of activating the memory of witnesses and victims. M., 1999.

5. Zorin G.A. Interrogation tactics guide. M., 2001.

6. Dotsenko E. L. Psychology of manipulation: phenomena, mechanisms and protection / E. L. Dotsenko. - M .: CheRo - Publishing house of Moscow State University, 1997. - S. 140-144.