

**ТАКОВ Асланбек Заурбиевич,**

*преподаватель кафедры огневой подготовки Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России, капитан полиции,*

*e-mail: mail@law-books.ru*

## **НЕКОТОРЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ СОВЕРШЕНИЮ КИБЕРПРЕСТУПЛЕНИЙ**

**Аннотация.** В представленной статье автор рассматривает вопросы присвоения чужого имущества посредством информационных систем. Рассматриваются средства и методы совершения киберпреступлений против граждан. Особое внимание обращено на необходимость проведения профилактических и воспитательных мероприятий с целью предотвращения дистанционного мошенничества.

**Ключевые слова:** кибербезопасность, кибермошенничество, телефонное мошенничество, противодействие преступным действиям в информационной среде.

**TAKOV Aslanbek Zaurbievich,**

*Lecturer at the Department of Fire Training of the North Caucasus Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, police captain*

## **SOME ISSUES IN COUNTERING CYBERCRIME**

**Annotation.** In the presented article, the author considers the issues of assigning someone else's property through information systems. Means and methods of committing cybercrimes against citizens are considered. Particular attention is paid to the need for preventive and educational measures in order to prevent remote fraud.

**Key words:** cybersecurity, cyber fraud, telephone fraud, countering criminal actions in the information environment.

Рассматривая данный вид преступных деяний необходимо помнить о том, что вымогатели и мошенники являются хорошими психологами. В ходе общения они воздействуют на своих жертв в плане того, что от их решения зависит судьба данных лиц. Злоумышленники психологически подводят данных лиц к тому, что в настоящее время от них зависит вопрос привлечения к уголовной ответственности данных лиц за совершение действий заключающихся в высказываниях различных комментариях в социальных сетях, в которых усматриваются признаки преступления, предусмотренные статьей 282 УК РФ. Они сообщают, что им необходимо явиться в территориальный орган с паспортом для предоставления объяснения по существу материала проверки для последующей передачи в следственное подразделение.

Киберпреступники пугают, что на основании данных материалов в отношении них будет возбуждено уголовное дело. Злоумышленники предупреждают, что удаление комментариев ничего не изменит, так как это все

уже сохранено в базе данных.

После психической «обработки» своих жертв злоумышленник в ходе общения намекает, что есть возможность освобождения от уголовной ответственности и не распространение данной информации при определенных условиях. Тем самым преступники совершают объективные действия, предусмотренные статьей 159 УК РФ – это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием.

Преступники тщательно готовятся к звонкам жертвам. Представляются именами реально существующих сотрудников правоохранительных органов, в ходе общения если жертва как-то сомневается, то они предлагают проверить эту информацию на официальных сайтах Министерства внутренних дел Российской Федерации, а затем перезванивают с тех номеров, которые можно увидеть на официальном сайте ведомства.

Для этого злоумышленники пользуются различными платными программами подмены

номеров, поэтому доверять любым номерам, которые определились на вашем экране мобильного устройства, с которых звонят «сотрудники» крайне не рекомендуется. Единственный способ уберечь себя от обмана, если по телефону представляются сотрудниками силовых структур и правоохранительных органов – завершить разговор и самостоятельно перезвонить на официальный телефонный номер ОВД.

Главное правило общения с киберпреступниками – не вести никаких переговоров. Не отвечайте на их сообщения, не старайтесь показать, что вы считаете такой вид деятельности недостойным: это только позабавит преступника.

Не показывайте, что вы напуганы, расстроены или взбешены: шантажист может использовать ваши эмоции против вас.

И, конечно, ни в коем случае ничего не оплачивайте. У злоумышленников ничего на вас нет, он вас не знает. Подобные сообщения он каждый день рассылает десятками совершенно незнакомых людей.

Пожалуйста в поддержку социальной сети и добавьте профиль преступника в черный список. Найдите в интернете официальный телефон отдела внутренних дел, которое вам назвали мошенники, и позвоните туда. Например, могут сказать «отдел МВД России по г. Пятигорск» или «Управление МВД России по г. о. Нальчик». Спросите, есть ли у них сотрудник, который вас набирал, и о каком материале проверки он говорил.

Данную информацию так же вы можете узнать у участкового уполномоченного полиции, который обслуживает район вашего проживания. Скорее всего, вам скажут, что это был мошенник или вымогатель. Также настоящий сотрудник полиции, обращаясь к вам по телефону, всегда полностью назовет свое свою должность, звание, подразделение и территориальный орган в котором проходит службу.

Обращение типа «это Главное управление МВД» или «ОСБ МВД по банкам» и так далее следует игнорировать. Можно задавать собеседнику уточняющие вопросы. Если вы уловите в его интонации нетерпение, угрозу, растерянность – разговор следует закончить. Лучшим решением будет попросить собеседника пригласить вас в территориальный орган для

объяснения в письменном виде по существу материала проверки.

Преступники будут всеми силами убеждать жертву в том, что ей не нужно приходить в территориальный орган полиции, проблему можно решить по телефону [1].

Существует тактика убеждения, которыми пользуются киберпреступники. В числе преступных организованных групп находятся на службе опытные психологи, которые постоянно разрабатывают новые схемы совершения киберпреступлений, где есть важные моменты, которые имеют ключевое значение для убеждения жертв и успешного совершения преступления.

1. обращение по фамилии, имени, отчеству и датой рождения.
2. представление от лица «майора полиции», «следователя следственного комитета», «оперуполномоченного уголовного розыска», «сотрудника отдела по борьбе с экономическими преступлениями и противодействию коррупции»;

Киберпреступник строит разговор примерно следующим образом:

«В отношении вас собран материал проверки и возбуждено уголовное дело, поэтому вам надо оставаться на месте, к вам сейчас придет следственно оперативная группа, кстати, вы проживаете по зарегистрированному адресу?»;

Некоторые преступники после удачной телефонной обработки встречаются с жертвой преступления для получения денежных средств. Встречу назначают в тех местах, где не установлены камеры видеонаблюдения [2]. Часто пользуются услугами курьеров или таксистов, которые не знают, что их используют для получения денежных средств обманым путем.

Сложность противодействия будет зависеть от личности лица, совершившего киберпреступления, виктимологических особенностей личности, проводимых оперативно-розыскных мероприятий, направленных на выявление и раскрытие преступлений, а также возможностей легализации результатов их проведения [3].

Помимо практической сложности противодействия киберпреступности, трудности возникают и на научном уровне. Например,

чтобы выработать единую нормативно-правовую базу противодействия, необходимо обеспечить единообразное понимание материального права.

При разных правовых семьях это сложно: разный подход к содержанию общественной опасности, возрасту уголовной ответственности [4], конструкции составов, разнообразие способов совершения преступления, исходя из технического прогресса конкретного государства, разное понимание вины в уголовном

праве. Как следствие - разные качественные и количественные показатели преступности, разное понимание профилактической работы, сложности в определении признаков личности преступника, виктимологических признаков [5]. Уголовно-правовые и криминологические аспекты ведут к отсутствию единых элементов криминалистической характеристики, разному подходу к институту доказательств в уголовном процессе.

#### Список литературы:

[1] Хрусталева Е. Т. О., Еостюрин Г. А. Киберугрозы: причины и рекомендации по предотвращению // Национальные интересы и безопасность. 2019. Т. 15. № 6 (375). С. 1185-1194. DOI: 10.24891/ni.15.6.1185

[2] Пракаш С. У., Новианди Нур 77. Е. Анализ кибершпионажа в международном праве и индонезийском праве // Обзоры гуманитарных и социальных наук. 2019. Т. 7. № 3. С. 38-44.

[3] Фурнелл С., Доулинг С. Киберпреступность: портрет ландшафта // Журнал криминологических исследований, политики и практики. 2019. Т. 5. № 1. С. 13-26.

[4] Сухаренко А. Противодействие киберугрозам в России: состояние, динамика и тенденции // Диалог: политика, право, экономика. 2018. № 2 (9). С. 26-35.

[5] Машекуашева М.Х. О значимости информационно-психологической защиты индивида и социума: особенности воздействующего потенциала. Право и управление. 2024. № 2. С. 375-377. Право и управление. 2024. № 2. С. 375-377.

#### Spisok literatury:

[1] Khrustalev E. T. O., Eostyurin G. A. Cyber threats: reasons and recommendations for prevention// National interests and security. 2019. VOL. 15. № 6 (375). S. 1185-1194. DOI: 10.24891/ni. 15.6.1185

[2] Prakash SW, Noviandi Hyp 77. E. Analysis of cyber espionage in international law and Indonesian law//Reviews of the humanities and social sciences. 2019. VOL. 7. № 3. S. 38-44.

[3] Furnell S, Dowling S. Cybercrime: Landscape Portrait//Journal of Criminology Research, Policy and Practice. 2019. VOL. 5. № 1. S. 13-26.

[4] Sukharenko A. Countering cyber threats in Russia: state, dynamics and trends//Dialogue: politics, law, economics. 2018. № 2 (9). S. 26-35.

[5] Mashekuasheva M.Kh. On the importance of information and psychological protection of an individual and society: features of the influencing potential. Law and governance. 2024. № 2. P. 375-377. Law and management. 2024. № 2. PP. 375-377.

