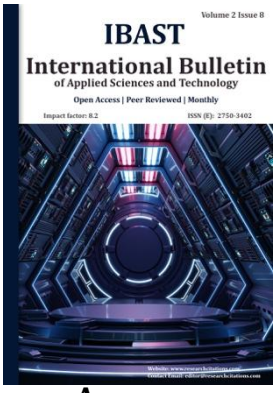

ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ КИБЕРМОШЕННИЧЕСТВА И ИХ СПЕЦИФИЧЕСКИЕ ОСОБЕННОСТИ

У.У.Муродов
Независимый соискатель Академии МВД
Республики Узбекистан
https://doi.org/10.5281/zenodo.19638291

Аннотация: В статье проводится комплексный анализ характеристики и специфических особенностей преступлений, совершаемых в сфере информационных технологий. Рассматриваются понятие, виды и уголовно-правовая квалификация таких деяний, включая преступления в сфере компьютерной информации и общеуголовные преступления, совершаемые с использованием сети Интернет. Особое внимание уделяется отличительным чертам киберпреступлений: высокой латентности, трансграничному (международному) характеру, отсутствию физического контакта между преступником и потерпевшим, анонимности, использованию информационно-телекоммуникационных технологий в качестве орудия, средства или предмета посягательства. Выявляются проблемы выявления, квалификации и расследования данных преступлений, а также предлагаются направления совершенствования противодействия киберпреступности в современных условиях цифровизации общества.

Ключевые слова: преступления в сфере информационных технологий, киберпреступления, интернет-преступления, компьютерные преступления, информационно-телекоммуникационные технологии, латентность преступлений, трансграничная преступность

В процессе глобализации мирового сообщества кибербезопасность занимает особое место. Однако кибермошенничество регулярно стремится причинять вред кибербезопасности, при этом его роль в развитии отношений между государствами, международными организациями, компаниями, финансовыми институтами и людьми, а также в создании безопасного киберпространства в каждой стране, постоянно возрастает.

В частности, ежедневно можно наблюдать, как кибермошенничество наносит ущерб и создает угрозу информационным системам и ресурсам государств, базам данных международных организаций и компаний, информационно-коммуникационным технологиям финансовых институтов, жизни и здоровью людей, конституционным правам и свободам.

Кроме того, отсутствие в действующем уголовном законодательстве понятия «кибермошенничество» и его механизма требует пересмотра законодательства в данной сфере.

В целом, каждый по-своему объясняет понятие кибермошенничества. В частности, это кибератака, направленная на обман пользователей Интернета, включающая кражу конфиденциальной информации, незаконный доступ к системе через взлом, с целью использования личных данных любыми способами, а также имеет различные виды, такие как «нигерийские письма», фишинг, вишинг, фарминг.

По мнению других специалистов, кибермошенничество — это разновидность кибератаки, направленной на причинение материального или иного ущерба через кражу личной информации пользователя, с видами «фишинг», «скимминг» и т.д.

Кибермошенничество — это преступление в области информационных технологий, совершаемое через кражу банковских карт, платежных реквизитов, паролей, распространение вирусов, нарушение работы компьютерных систем.[1]

По мнению ученого В.К. Барчукова, кибермошенничество — это компьютерное мошенничество, заключающееся в нарушении доверия и мошенничестве с использованием внутренней информации для посягательства на чужое имущество.[2]

Д.А. Зыков считает, что преступление кибермошенничества заключается в присвоении чужих денежных средств или нанесении ущерба чужому имуществу с помощью компьютерных технологий через обман и злоупотребление доверием.[3]

Ученый М.А. Ефремова также отмечает, что понятия «кибермошенничество» и «мошенничество с использованием компьютерной информации» идентичны и являются синонимами.[4]

На наш взгляд, мнения вышеупомянутых ученых справедливы: действительно, кибермошенничество осуществляется с помощью информационных технологий и направлено на завладение чужим имуществом путем обмана или злоупотребления доверием лица.

В целом, кибермошенничество проявляется в различных формах, поэтому его виды также разнообразны, и классификация преступления может базироваться на распространенных формах.

Наиболее распространенным является кибермошенничество через фальсификацию кредитных карт: кража личных данных и карт, их намеренное уничтожение, обман через интернет или телефонные связи, злоупотребление доверием, изготовление дубликатов пластиковых карт, заключение взаимных искусственных сделок, кража карт или их PIN-кодов через банкоматы.

Второй вид — фальсификация депозитов: искусственное уменьшение официального размера депозитов в банковских документах, снятие средств с депозитного счета клиента.

Третий вид — кредитное мошенничество: переработка кредита на основе паспортных данных другого лица, незаконный перевод денежных средств на счета третьих лиц.

Четвертый вид — мошенничество с наличными средствами: изготовление фальшивых банкнот, снятие средств с банковского счета клиента через различные схемы.

[1] С сайта в интернете: https://psm7.com/glossary/kak-borotsya-s-kibermoshennichestvom.htm.

[2] Барчуков В.К. Терминология мошенничества в сфере компьютерной информации. – М.: Пробелы в российском законодательстве. № 4. 2017 г. – С. 163-165.

[3] Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. дис. канд. юрид. наук. Владимир, 2002. – 211 с.

[4] Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. – С. 19 21.

Одной из наиболее распространенных форм кибермошенничества является кредитное мошенничество: злоумышленник, обладая информацией о пострадавшем, его паспорте или других документах, оформляет кредитное соглашение на имя потерпевшего, получает соответствующие средства от банка, причиняя ущерб как пострадавшему, так и банку.

Преступления с наличными средствами осуществляются в основном через недостатки банкоматов и кассовых аппаратов, действуя по сговору с сотрудниками кассы, совершают подбные преступления.

Иными словами, многообразие информационных технологий приводит к увеличению видов кибермошенничества, самой опасной стороной, которых является огромный ущерб, причиняемый этими преступлениями, что требует последовательной работы по их предотвращению.

Преступление кибермошенничества имеет четыре стороны: объект — это социальные отношения, направленные на защиту чужой собственности и (или) имущественных прав.

Субъект, по нашему мнению, помимо лиц, достигших 16-летнего возраста, как и в других мошеннических преступлениях, может включать лиц младше 16 лет, обладающих специальными знаниями в области информационных технологий и коммуникаций, способных совершить кибермошенничество.

Причина в том, что несовершеннолетний, обладая специальными навыками использования информационных технологий и коммуникаций в корыстных целях, может совершить данное преступление. Снижение возраста ответственности, по нашему мнению, приведет к уменьшению подобных преступлений и обеспечит кибербезопасность.

Субъективная сторона преступления заключается в умышленном характере деяния, при котором преступник осознает последствия и желает их наступления.

Объективная сторона проявляется в обмане и злоупотреблении доверием; например, метод кибермошенничества через рекламу обещает пользователю богатство и преступник обманом присваивает денежные средства.

Для наглядности: Республиканский процессинговый центр предупредил клиентов о кибермошенничестве с использованием бренда Uzcard, где был скопирован интерфейс официального сайта и предложено ввести номера карт для получения бонусов.

При злоупотреблении доверием пользователь добровольно передает деньги для увеличения своих средств, а злоумышленник с использованием информационных технологий получает имущество или права на имущество.

Предмет кибермошенничества, как и предмет мошенничества, — это чужое имущество или имущественные права.

С учетом широкой распространенности этих преступлений, их способности причинять значительный ущерб, целесообразно предусмотреть ответственность за них отдельной статьей в Уголовном кодексе.

Согласно ст. 10 УК, каждое лицо, в деянии которого установлено наличие состава преступления, должно подлежать ответственности.

Согласно ст. 4 УК, преступность, наказуемость деяния и иные правовые последствия его совершения определяются только Уголовным кодексом.

Никто не может быть признан виновным в совершении преступления и подвергнут наказанию иначе как по приговору суда и в соответствии с законом.

Согласно ст. 14 УК, преступлением признается виновное общественно опасное деяние (действие или бездействие), запрещенное настоящим Кодексом под угрозой применения наказания.

Согласно ст. 16 УК, основанием ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного настоящим Кодексом.

Таким образом, отсутствие в законодательстве понятия кибермошенничества и ответственности за него подтверждает необходимость включения этой категории преступлений в уголовное законодательство, с гарантией защиты имущественных прав.

В настоящее время, для привлечения к ответственности лиц, совершивших социально опасные деяния, следует учитывать, что за указанные преступления ответственность не установлена, а любое деяние, не запрещённое законом, не признается преступлением. Исходя из вышеуказанного зарубежного опыта, предлагается: дополнить статью 169 Уголовного кодекса дополнительной специальной нормой по кибермошенничеству или, на основании Постановления Президента Республики Узбекистан от 14 мая 2018 года № ПП–3723 «О мерах по кардинальному совершенствованию системы уголовного и уголовно-процессуального законодательства»[5], включить отдельную статью в разрабатываемый Уголовный кодекс в новой редакции. Одновременно рекомендуется исключить из действующей части 2 пункта «в» статьи 168 Уголовного кодекса соответствующую норму.

Несмотря на существующие проблемы, привлечение к ответственности за кибермошенничество повышает эффективность цифровой экономики, укрепляет доверие населения к информационным технологиям и обеспечивает цели судебно-правовой реформы — поддержание общественного порядка, защиты прав граждан и их безопасности.

Информационные технологии являются основным элементом управления информационными системами, непосредственно связанными с особенностями работы подразделений МВД. Особое внимание в органах внутренних дел уделяется внедрению и использованию системы электронного документооборота.[6]

Процесс информатизации охватывает многие сферы человеческой деятельности и не обошел МВД стороной. Компьютер стал «рабочим инструментом» юриста, а компьютерная преступность — новым видом преступлений, связанной с незаконным присвоением, копированием и распространением информации.

Развитие требует от сотрудников МВД знаний современных информационных технологий и информационной культуры.

[5] Постановления Президента Республики Узбекистан от 14 мая 2018 года № ПП–3723 «О мерах по кардинальному совершенствованию системы уголовного и уголовно-процессуального законодательства»//Қонун ҳужжатлари маълумотлари миллий базаси, 15.05.2018 й., 07/18/3723/1225-сон, 01.10.2018 й., 06/18/5547/1975-сон. 309

[6] Приказ Министра внутренних дел Республики Узбекистан от 19 апреля 2015 года № 64 «О утверждении Инструкции по внедрению и использованию системы электронного документооборота в органах внутренних дел».

Компетенция современного специалиста включает знание принципов работы компьютера и устройств, современных принципов сбора, хранения и обработки информации, телекоммуникаций и искусственного интеллекта.

Управление связано с процессом приема и обработки информации: руководитель передает распоряжения исполнителю, а исполнитель предоставляет необходимые данные. Эффективное управление зависит от правильной организации информационных процессов.

Сотрудники МВД, занимающиеся управлением и предотвращением преступлений, расследованием и охраной общественного порядка, выполняют задачи сбора, обработки, анализа данных и разработки управленческих решений.

В МВД сбор и обработка информации зависят от должности: оперативный работник уголовного розыска или инспектор профилактики расследует преступления, проверяет обращения граждан, оценивает оперативную ситуацию, планирует работу.

Сотрудники МВД используют сеть базы данных «Банк интеграции информации Узбекистана», включающую сведения о разыскиваемых и пропавших лицах, зарегистрированных и угнанных транспортных средствах, утраченных оружии и цифровых устройствах, телефонных номерах. Система обеспечивает корпоративную компьютерную сеть МВД.