УДК 343

Мошенничество в сфере компьютерной информации

Филиппова Елена Олеговна

Кандидат педагогических наук, доцент,
доцент кафедры уголовного права,
Оренбургский государственный университет,
460018, Российская Федерация, Оренбург, просп. Победы, 13;
e-mail: elena56-75@mail.ru

Аннотация

В статье рассматривается мошенничество в сфере компьютерной информации. В России, как и в любом другом государстве, такого рода незаконные действия сопровождают товарно-денежные обмен и идут рука об руку с развитием рынка. В нашей стране с приходом рыночных отношений в начале 90-х годов обман в форме мошенничества получил серьезный стимул для развития, ведь большое количество граждан получили доступ к денежным потокам экономики страны, а соблазн быстрого обогащения всегда являлся существенным фактором, подталкивающим людей к совершению такого злодеяния. На протяжении сотен лет мошеннический обман являлся негативной стороной рынка и сопровождал торгово-денежные отношения, но постепенно вместе с неумолимым техническим прогрессом мошенничество в виду соей высокой приспособляемости к окружающим реалиям начало приобретать новые виды и формы.

Для цитирования в научных исследованиях

Филиппова Е.О. Мошенничество в сфере компьютерной информации // Вопросы российского и международного права. 2024. Том 14. № 6А. С. 360-365.

Ключевые слова

Мошенничество, компьютерная информация, торгово-денежные отношения, кибертехнологии, инфотехнологии, цифровизация, теневая экономика, электронный документ, технический прогресс.

Введение

Мошенничество – преступление, берущее свое начало еще в древност, оно известно во всех уголках нашей планеты и ассоциируется у большинства людей с обманом.

Актуальность темы выражается в следующем. Во-первых, прогрессивный современный мир и в том числе наше Отечество не обошли стороной и новые виды мошеннических действий. Находчивости и выдумке криминальных элементов на современном этапе развития общества могут позавидовать ведущие научные фантасты, так что жертвой мошеннических посягательств пали и современные цифровые технологии. Эволюция такого рода злодеяний порождает разнообразные вариации совершения обмана и злоупотребления доверием, а в условиях стремительного проникновения компьютерных устройств во все слои и сферы общества выявление мошенничеств становится сложной задачей, требующей не только знания правового поля, но и наличия специальных навыков в сфере кибернетических, информационных технологий, а также методов социальной инженерии.

Во-вторых, лавинообразный как в мире, так и в России рост использования компьютерных и инфотехнологий вкупе с появлением новых способов реализации кибертехнологий повлекли развитие разнообразных форм коммуникаций между человеческими индивидуумами. Практически все сферы жизни и общения человека буквально пронизаны всевозможными гаджетами, цифровыми устройствами и сетевыми технологиями. Финансово-экономическая сфера на сто процентов использует возможности сетевых и информационных технологий и ставит на службу все больше цифровых устройств и электронных помощников, а в ходе интеграции в глобальную сеть Интернет существенно расширилось поле действия. В нашей стране активно протекает процесс перехода структур, регулирующих финансовые потоки, в виртуальное измерение. Положительные стороны цифровизации общества и услуг сопровождают и негативные последствия, ведь способы, технологии, устройства могут служить не только на благо общества, но и для корыстных целей криминальных структур, чем и незамедлительно воспользовались преступные элементы, поставив самые прогрессивные технологии на службу своим темным делам.

В-третьих, правонарушения в виртуальном пространстве имеют признак глобализации и не знают понятий «граница» и «государство», такое положение во многом обусловлено возможностями сетевых технологий. Ущерб, нанесенный государствам, может исчисляться миллионами долларов, являясь чувствительным даже для сильнейших экономик мира, а перспектива крупной наживы привлекает большое количество криминала и способствует развитию теневой экономики.

Основная часть

Мошенничество в сфере компьютерной информации – это преступные действия, связанные с незаконным доступом, уклонением от уплаты, подделкой, воровством, хищением и манипуляцией информацией, связанной с компьютерами, сетями и цифровыми устройствами. Преступники могут использовать различные методы для осуществления мошенничества в этой сфере, включая фишинг, мошенничество с использованием вредоносных программ, кражу личной информации, мошенничество с кредитными картами и т.д.

Примеры мошенничества в сфере компьютерной информации включают в себя следующие виды:

1. Фишинг – это метод, при котором злоумышленники выдают себя за доверенное лицо или организацию, чтобы получить доступ к личной информации пользователей. Они могут отправлять поддельные электронные письма или создавать фальшивые веб-сайты, чтобы заполучить логины, пароли и финансовые данные пользователей.

2. Мошенничество с использованием вредоносных программ – злоумышленники могут использовать вредоносные программы, такие как вирусы, трояны или шпионские программы, для получения доступа к компьютерам пользователей и кражи их личной информации или контроля над системой.

3. Кража личной информации – злоумышленники могут использовать различные методы для получения доступа к личной информации пользователей, такие как использование слабых паролей, атака на сетевую безопасность или физическая кража устройств хранения данных.

4. Мошенничество с кредитными картами – это метод, при котором злоумышленники получают доступ к кредитной информации пользователей и использованию ее для совершения незаконных финансовых операций.

Следует отметить, что прогресс киберцифровых технологий имеет высокие темпы развития, законодатель ввиду стремительного, а иногда кардинального изменения методик не успевает купировать возникающие проблемы. Также свою лепту вносит отсутствие специальных знаний в кибернетике. С трудностями такого рода сталкиваются абсолютно все отрасли правового регулирования, которые призваны противостоять своевременным угрозам и выступать в роли регулятора отношений на кибернетическом поприще и в виртуальном пространстве.

Уголовный кодекс России на сегодняшний день не может похвастаться систематизированным подходом в деле противодействия угрозам криминальных групп в виртуальном пространстве, также нет четкого и единого понятийного аппарата, изменения зачастую не оказывают должного эффекта.

Информация стремительно ворвалась и приобрела важное значение для современного социума. Так как она является одновременно продуктом деятельности и потребления общества, то само общество постоянно стимулирует прогресс в области ее производства. Основными производственными мощностями являются компьютеры и их системы.

Как итог, информационный ресурс как продукт общественных социокультурных отношений приобрел товарные черты и начал активно покупаться и продаваться. Следствием таких процессов, протекающих в современном социуме, является становление нового вида социокультурной коммуникации, что накладывает существенный отпечаток на традиционных и давно сформировавшихся общественных отношениях. Новые отношения связаны с изготовлением, хранением, преобразованием, декодированием, передачей, накоплением и использованием различной информации, программного обеспечения ОС, файлов, содержащих звук, видео, фото, целых баз данных и систем управления ими и многое др.

Компьютер в специализированной литературе – комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач [Першиков, Савинков, 1991, 163], юридическая наука не может принять такое определение, так как не проводит строгой разграничительной линии между ЭВМ в традиционном понимании и узкоспециализированными компьютерными устройствами, такими как ККМ, банкоматы, мобильные терминалы, сетевые устройства, имеющие некое подобие операционной системы, МФУ, сервера, сетевые хранилища, цифровое оборудование автомобилей и т. д.) и иные цифровые электронные устройства.

О.Я. Баев и В.А. Мещеряков предлагают держать ориентир на общепринятые и признанные

труды в области кибернетики [Баев, Мещеряков, 1998, 8]. В них используют понятие «автоматные модели» – устройства, преобразующие информацию. Данные признаки могут упростить работу по классификации различных устройств, таких как компьютеры, или нет. Хотя нужно признать, что отождествление устройств по этому признаку – сложный процесс работников правоохранительной системы. Использовать этот признак необходимо для проведения экспертиз.

О.Я. Баев и В.А. Мещеряков предлагают более простое определение: под ЭВМ (компьютером) понимается комплекс технических средств, включающий:

1) процессор (или другое электронное устройство), выполняющий функции преобразования информации, представленной в машинном виде, и реализующий одно или несколько действий (программу) по обработке информации;

2) устройство хранения управляющих программ и (или) данных, необходимых для реализации процессором его целевых функций;

3) оборудование (приспособление), позволяющее каким-либо образом изменять или перезаписывать управляющие программы и (или) данные, необходимые для реализации процессором его целевых функций [ГОСТ Р ИСО ТО 13569-2007: Финансовые услуги. Рекомендации по информационной безопасности, 9].

Трактовку термина «электронный документ» очень часто делают равной понятию «компьютерная информация». Федеральный закон «Об информации, информационных технологиях и о защите информации» [Федеральный закон от 27 июля 2006 г. № 149-ФЗ, www] определяет его как документированную информацию, представленную в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием ЭВМ, а также для передачи по ИТК сетям или обработки в информационных системах. Еще один важный признак компьютерной информации заключается в том, что она всегда имеет вид, позволяющий обработать ее на компьютерных машинах.

Заключение

Развитие ИКТ – это довольно масштабный и сложный процесс. Важно, чтобы было понимание происходящего, того, что чем больше с течением времени и по мере развития усиливается слияние виртуальных цифровых технологий, тем более незаметной становится грань между низкоуровневым кодом и бытовыми данными. Это наблюдение справедливо и для ЭВМ с входящими в их состав аппаратными частями. Информация, представленная в графической форме (текст, в том числе рукописный, фотографии, видео и т.п.) и в виде аудиозвуковых файлов и непосредственной речи человека, уже давно и с легкостью обрабатывается различными ОС, подтверждением тому служит появление голосовых помощников в операционных системах Windows, MAC OS, IOS, Android, в приложении Сбербанка.

Спорные ситуации по идентификации такого устройства, как компьютер, необходимо разрешать с помощью экспертиз.

Библиография

1. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации // Конфидент. 1998. № 7. С. 8-9.
2. ГОСТ Р ИСО ТО 13569-2007: Финансовые услуги. Рекомендации по информационной безопасности.

3. Елагина А.С. Интерпретация трендов уровня преступности: нормальные и шоковые изменения // Вопросы российского и международного права. 2018. Том 8. № 11А. С. 144-152.
4. Елагина А.С. Подходы к совершенствованию международного уголовного права // Вопросы российского и международного права. 2018. Том 8. № 10А. С. 96-101.
5. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ (с изменениями и дополнениями). URL: https://base.garant.ru/12148555 (дата обращения: 14.08.2023).
6. Першиков В.И., Савинков В.М. Толковый словарь по информатике. М.: Финансы и статистика, 1991. 439 с.
7. Gërxhani K., Cichocki S. Formal and informal institutions: understanding the shadow economy in transition countries //Journal of Institutional Economics. – 2023. – Т. 19. – №. 5. – С. 656-672.
8. Mishchuk H. et al. Impact of the shadow economy on social safety: The experience of Ukraine //Economics and sociology. – 2020. – Т. 13. – №. 2. – С. 289-303.
9. Lyulyov O. et al. Determinants of shadow economy in transition countries: Economic and environmental aspects //International journal of global energy issues. – 2021. – Т. 43. – №. 2-3. – С. 166-182.
10. Medina L., Schneider F. The evolution of shadow economies through the 21st century //The Global Informal Workforce: Priorities for Inclusive Growth, International Monetary Fund, Washington DC, USA. – 2021. – С. 10-6.

Fraud in the sphere of computer information

Elena O. Filippova

PhD in Pedagogy,
Associate Professor,
Associate Professor of the Department of Criminal Law,
Orenburg State University,
460018, 13, Pobedy ave., Orenburg, Russian Federation;
e-mail: elena56-75@mail.ru

Abstract

The article deals with fraud in the field of computer information. In Russia, as in any other state, such illegal actions accompany the exchange of goods and money and go hand in hand with the development of the market. In our country, with the advent of market relations in the early 90s, fraud in the form of fraud received a serious impetus for development, because a large number of citizens gained access to the cash flows of the country's economy, and the temptation to get rich quick has always been a significant factor pushing people to commit such a crime. For hundreds of years, fraudulent deception was the negative side of the market and accompanied trade and money relations, but gradually, along with the inexorable technological progress, fraud, due to its high adaptability to the surrounding realities, began to acquire new types and forms.

For citation

Filippova E.O. (2024) Moshennichestvo v sfere komp'yuternoi informatsii [Fraud in the sphere of computer information]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (6A), pp. 360-365.

Keywords

Fraud, computer information, trade and money relations, cyber technologies, information technologies, digitalization, shadow economy, electronic document, technical progress.

References

1. Baev O.Ya., Meshcheryakov V.A. (1998) Problemy ugolovno-pravovoi kvalifikatsii prestuplenii v sfere komp'yuternoi informatsii [Problems of criminal-legal qualification of crimes in the sphere of computer information]// Konfident. № 7. pp. 8-9.
2. GOST R ISO TO 13569-2007: Finansovye uslugi. Rekomendatsii po informatsionnoi bezopasnosti [GOST R ISO TO 13569-2007: Financial services. Recommendations on information security].
3. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: feder. zakon ot 27 iyulya 2006 g. № 149-FZ (s izmeneniyami i dopolneniyami) [On information, information technologies and on information protection: federal law of July 27, 2006 No. 149-FZ (with amendments and additions)]. URL: https://base.garant.ru/12148555.
4. Pershikov V.I., Savinkov B.M. (1991) Tolkovyi slovar' po informatike [Explanatory dictionary of informatics]. M.: Finansy i statistika, 439 p.
5. Elagina A.S. (2018) Interpretatsiya trendov urovnya prestupnosti: normal'nye i shokovye izmeneniya [Interpretation of crime trends: normal and shock changes]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (11A), pp. 144-152.
6. Elagina A.S. (2018) Podkhody k sovershenstvovaniyu mezhdunarodnogo ugolovnogo prava [Approaches to the improvement of international criminal law]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (10A), pp. 96-101.
7. Gërxhani, K., & Cichocki, S. (2023). Formal and informal institutions: understanding the shadow economy in transition countries. Journal of Institutional Economics, 19(5), 656-672.
8. Mishchuk, H., Bilan, S., Yurchyk, H., Akimova, L., & Navickas, M. (2020). Impact of the shadow economy on social safety: The experience of Ukraine. Economics and sociology., 13(2), 289-303.
9. Lyulyov, O., Paliienko, M., Prasol, L., Vasylieva, T., Kubatko, O., & Kubatko, V. (2021). Determinants of shadow economy in transition countries: Economic and environmental aspects. International journal of global energy issues, 43(2-3), 166-182.
10. Medina, L., & Schneider, F. (2021). The evolution of shadow economies through the 21st century. The Global Informal Workforce: Priorities for Inclusive Growth, International Monetary Fund, Washington DC, USA, 10-6.