

УДК 4414

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ
В ФИНАНСОВОЙ СФЕРЕ¹

Кузьмина Каролина Алексеевна, студент магистратуры

Российского экономического университета им. Г.В. Плеханова

Адрес: 115093, г. Москва, Стремянный пер., 36

Аннотация: В статье проанализированы отдельные теоретические и практические аспекты профилактики и противодействия совершению киберпреступлений в финансовой сфере.

Ключевые слова: киберпреступления, информационные технологии, цифровизация, сеть «Интернет», компьютерная информация, финансовая сфера.

COUNTERING CYBERCRIME IN THE FINANCIAL SECTOR

Kuzmina Karolina Alekseevna, a graduate student

Plekhanov Russian University of Economics

Address: 36 Stremyanny Lane, Moscow, 115093

Abstract: The article analyzes certain theoretical and practical aspects of preventing and combating the commission of cybercrimes in the financial sector, мошенничество.

Key words: cybercrime, information technology, digitalization, Internet, computer information, financial sector, fraud.

На протяжении длительного времени происходит активная цифровизация всех сфер общественной жизни. Новые технологии развиваются с огромной скоростью, существенно упрощая жизнь граждан, ускоряя операционные процессы и способствуя повышению качества жизни в целом. Между тем,

¹ Статья написана в рамках выполнения научно-исследовательской работы, финансируемой из средств ФГБОУ ВО «РЭУ им. Г.В. Плеханова» по теме исследования: «Совершенствование правового регулирования в области обеспечения социальной безопасности граждан»

возникают угрозы, связанные в том числе с повсеместным использованием современных технологий для противоправных действий, в том числе в финансовой сфере. Совершенствование и усложнение информационных технологий напрямую влияет на способ совершения киберпреступлений, которые модернизируются каждый день. Новостные порталы регулярно публикуют новости о новых видах мошенничества с использованием современных технологий. Изменения способов совершения киберпреступлений имеют галопирующий темп, в связи с чем законодательство не успевает подстраиваться под новые реалии, а правоохранительные органы в свою очередь не обладают достаточными знаниями для раскрытия преступлений, совершенных с использованием информационных технологий.

Разработка наиболее эффективных способов профилактики и противодействия киберпреступлениям в финансовой сфере – важнейшее направление деятельности уполномоченных государственных органов в области обеспечения социальной безопасности граждан.

Актуальность исследования заключается в возрастающем количестве преступлений, совершенных с использованием информационных технологий, наличием дискуссий в части определения правовой сущности киберпреступлений, а также необходимостью выработки эффективных мер, направленных на защиту граждан от киберпреступлений в финансовой сфере.

Задачей исследования является осуществление системного анализа теоретических и практических аспектов защиты граждан от неправомерных действий, направленных на хищение денежных средств с использованием информационных технологий.

Термин «киберпреступление» имеет иностранное происхождение, используется в международных актах, а также в законодательстве зарубежных стран. В действующем законодательстве Российской Федерации не используется понятие «киберпреступления». Глава 28 Уголовного кодекса Российской Федерации посвящена преступлениям в сфере компьютерной

информации. Ряд правоведов отождествляют понятие киберпреступлений с преступлениями в сфере компьютерной информации, что на наш взгляд не в полной мере отражают сущность данного термина.

По нашему мнению, понятие «киберпреступления» наиболее обширное и включает в себя как преступления в сфере компьютерной безопасности, так и иные виды преступлений, совершенных с использованием электронных и информационно-телекоммуникационных сетей.

В отдельных статьях Уголовного кодекса Российской Федерации использование информационно-телекоммуникационной сети для совершения преступления является обстоятельством, отягчающим наказание, например, в ст. 133 УК РФ. При этом нормы, касающиеся преступлений в экономической сфере, не содержат аналогичных положений. Считаем, что закрепление аналогичных положений в статьях УК РФ, посвященных преступлениям в экономической сфере, может оказать положительное влияние на профилактику киберпреступлений.

Одними из наиболее распространенных видов киберпреступлений в финансовой сфере является мошенничество в сети «Интернет», которое характеризуется огромным разнообразием видов, в том числе фишинг, мошенничество через рассылку на электронной почте, мошенничество в сфере криптовалют, мошенничество путем создания копий сайтов интернет-магазинов и многие другие. Одной из проблем, связанной с раскрытием данных преступлений, является то, что преступники для получения денежных средств зачастую используют банковские карты иных лиц, в связи с чем установить лиц, совершивших преступления достаточно сложно.

Подводя общий итог необходимо отметить, что появление киберпреступлений и модернизация способов их совершения является закономерным процессом развития общественных отношений. Разумеется, полностью нейтрализовать данный вид преступности невозможно, ввиду объективных причин. При этом возможно минимизировать количество данных

преступлений, повысив уровень социальной безопасности граждан. В данных целях необходимо дальнейшее совершенствование правовых механизмов противодействия киберпреступлениям, внедрение новых технологий для выявления и пресечения киберпреступлений, осуществление повышения квалификации сотрудников правоохранительных органов. Кроме того, в целях профилактики немаловажно регулярно осведомлять граждан о новых способах совершения преступлений и правилах кибербезопасности, которые необходимо соблюдать.

Библиографический список

1. Головинов О.Н., Погорелов А.В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. – 2016. – № 6 (1). – С. 73–88. – DOI: 10.18334/vines.6.1.35353.
2. Долбилов Алексей Владимирович ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ СОВЕРШЕНИЮ КИБЕРПРЕСТУПЛЕНИЙ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ // Криминологический журнал. 2022. №1. URL: <https://cyberleninka.ru/article/n/otdelnye-aspekty-protivodeystviya-soversheniyu-kiberprestupleniy-v-finansovokreditnoy-sfere>.
3. Иванова Лилия Викторовна Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. №1. URL: <https://cyberleninka.ru/article/n/vidy-kiberprestupleniy-po-rossiyskomu-ugolovnomu-zakonodatelstvu>.
4. Кочкина Эльвира Леонидовна Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. №3 (17). URL: <https://cyberleninka.ru/article/n/opredelenie-ponyatiya-kiberprestuplenie-otdelnye-vidy-kiberprestupleniy>.
5. Могунова М. М. ПОНЯТИЕ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ И СПОСОБЫ СОВЕРШЕНИЯ ФИНАНСОВО-ОРИЕНТИРОВАННЫХ КИБЕРПРЕСТУПЛЕНИЙ // Вестник ОмГУ. Серия.

Право. 2022. №1. <https://cyberleninka.ru/article/n/ponyatie-sovremennoy-kiberprestupnosti-i-sposoby-soversheniya-finansovo-orientirovannyh-kiberprestupleniy-orientirovannyh-kiberprestupleniy>.