УДК 344.633

Питулько Ксения Викторовна,
кандидат юридических наук, доцент,
заведующий кафедрой уголовного права и процесса
Санкт-Петербургский институт (филиал)
Всероссийского государственного университета юстиции
(РПА Минюста России),
г. Санкт-Петербург, Российская Федерация
lokhi@yandex.ru
Сергеева Анжелика Анатольевна,
кандидат юридических наук, доцент,
заместитель директора по учебной и воспитательной работе
Санкт-Петербургский институт (филиал)
Всероссийского государственного университета юстиции
(РПА Минюста России),
г. Санкт-Петербург, Российская Федерация
anzh-sergeeva@yandex.ru

Современные способы хищений, совершаемых с использованием ресурсов глобальной сети «Интернет»

В статье рассматриваются особенности посягательств на денежные средства граждан, совершаемые с использованием ресурсов сети «Интернет». В условиях пандемии количество таких преступлений существенно возросло; в дополнение к хорошо известным приемам манипулирования потерпевшими в арсенале преступников появились новые, связанные с активизацией дистанционной торговли. Их выявление существенно затруднено, поэтому анализ преступного поведения актуализируется. Авторы статьи предлагают использовать способы противодействия хищениям, сопряженным с незаконным доступом к платежным инструментам, апробированные на примере борьбы с терроризмом и экстремизмом и включающим как техническую блокировку сайтов, так и их мониторинг.

Ключевые слова: *преступление, хищение, мошенничество, сеть «Интернет», социальные сети.*

Pitulko Ksenia Viktorovna,
candidate of Legal Sciences, Associate Professor,
Head of the Department of Criminal Law and Procedure
St. Petersburg Institute (branch)
All-Russian State University of Justice
(RPA of the Ministry of Justice of Russia),
St. Petersburg, Russian Federation
Sergeeva Anzhelika Anatol'evna,
candidate of Legal Sciences, Associate Professor,
Deputy Director for Educational and Educational Work
St. Petersburg Institute (branch)
All-Russian State University of Justice
(RPA of the Ministry of Justice of Russia),
St. Petersburg, Russian Federation

Modern methods of theft committed using the resources of the global Internet

The article examines the features of encroachments on citizens' funds, committed using the resources of the Internet. In a pandemic, the number of such crimes has increased significantly; In addition to the well-known methods of manipulating victims, new ones have appeared in the arsenal of criminals related to the activation of distance selling. Their identification is significantly difficult, so the analysis of criminal behavior is updated. The authors of the article propose to use methods of countering theft associated with illegal access to payment instruments, tested on the example of combating terrorism and extremism and including both the technical blocking of sites and their monitoring.

Keywords: *crime, theft, fraud, the Internet, social networks.*

Цифровизация общества является актуальным трендом, в русле которого возникают не только новые социально позитивные отношения, но и специфические проявления криминальной активности. Осознавая это, законодатель предпринял не только установление законного режима общественных отношений, но и разработал меры уголовно-правовой охраны, позволяющие противодействовать той части преступности, которая связана с использованием высоких технологий.

Еще в 2012 г. законодатель установил уголовную ответственность за мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) и за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). В 2015 г. современную редакцию получила ст. 187 УК РФ, предусматривающая юридические последствия неправомерного оборота средств платежа. В 2018 г. квалифицирующие признаки кражи были дополнены таким, как хищение денежных средств с банковского счета, а равно электронных средств платежа (п. «г» ч. 3 ст. 158 УК РФ). С помощью этих норм обеспечивается защита денежных средств граждан, незаконный доступ к которым может быть получен с использованием ресурсов сети «Интернет». Одновременно признак неправомерного использования ресурсов глобальной сети нашел отражение в конструкциях целого ряда составов преступлений (возбуждения ненависти или вражды, пропаганда терроризма, незаконный оборот порнографических предметов и материалов и др.).

При том условии, что современные способы мошенничества достаточно плотно встроены в киберпространство, тем не менее, специальные нормы УК РФ применяются на практике достаточно редко. По данным Судебного Департамента при Верховном Суде РФ, например, в 2019 г. за совершение мошенничества с использованием электронных средств платежа было осуждено всего 1011 лиц (из них 364 человека – к лишению свободы, мошенничества в сфере компьютерной информации – 33 (11 к лишению свободы), неправомерного оборота средств платежа – 66 (14 к лишению свободы) [2]. В разы чаще выносились приговоры по делам о преступлениях, квалифицированных по общей норме, устанавливающей ответственность за мошенничество, – 16 258 осужденных.

Высокая адаптированность преступности к новейшим достижениям научно-технического прогресса дополнилась в рассматриваемом случае еще и таким пара-

метром, как существенное увеличение объемов дистанционных продаж. Как известно, в связи с пандемией многие производители стали реализовывать товары в сети «Интернет», вследствие чего этот сегмент рынка стал еще более привлекательным для лиц, совершающих мошеннические действия. В соответствии с неблагоприятным криминологическим прогнозом, разработанным в 2017 г. [1, с. 27], количество посягательств с использованием сети «Интернет» будет только расти. В этой части прогноз оказался более чем обоснованным: за девять месяцев 2020 г. МВД России отметило пятикратный рост хищений, сопряженных с незаконным доступом к платежным картам, а в целом число преступлений, совершенных с использованием ресурсов сети «Интернет» выросло на 93,2 %, в том числе, 148,5 тыс. случаев мошенничества и 124,4 тыс. краж [3, с. 30–36]. В Санкт-Петербурге, например, количество таких преступлений выросло более чем в восемь раз.

Как видно, данные о зарегистрированных преступлениях и количестве лиц, осужденных за их совершение, существенно расходятся между собой. Объяснить это можно как их низкой раскрываемостью, так и недостаточной оперативностью расследования уголовных дел. При этом суды предпочитают квалифицировать содеянное по общей норме (ст. 159 УК РФ), что заставляет усомниться в эффективности специальных уголовно-правовых норм, предназначенных для противодействия различным современным способам мошеннических действий. Определенные проблемы имеются и в связи со спорной позицией Пленума Верховного Суда РФ, который полагает необходимым квалифицировать как кражу те случаи завладения денежными средствами, которые сопряжены с неправомерным доступом к конфиденциальной информации о держателе платежных карт, переданной им преступнику самим (п. 17 постановления от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Современные способы совершения действий, известных под обобщенным бытовым названием «мошенничество в Интернете», достаточно многообразны. Типичным их примером является веерная рассылка сообщений или рандомные звонки, информирующие абонента о якобы совершенных подозрительных операциях. Жертва избирается случайно и подвергается психологической обработке, целью которой является получение пин-кода или CVC-кода от его платежной карты, после которого осуществляется обналичивание денежных средств или их перевод. Этот способ чаще всего практикуется лицами, отбывающими наказание в местах лишения свободы, и достаточно давно известен, однако граждане все еще имеют определенные риски стать жертвами такого преступления.

Далее, определенную криминальную популярность имеет веерная рассылка сообщений с просьбой от имени якобы родственника перевести небольшую денежную сумму на мобильный телефон или банковскую карту. Как и в первом случае, эти действия зачастую совершаются лицами, содержащимися в учреждениях уголовно-исполнительной системы.

Своеобразным «открытием» 2020 года стали более интеллектуальные по своей форме мошеннические действия, включающие создание и использование реплик сайтов известных Интернет-магазинов. Если ранее мошенниками активно осуществлялись параллельные продажи билетов на различные зрелищные собы-

тия (например, на чемпионат мира по футболу, официальные продажи билетов на матчи которого были серьезно осложнены), причем в этих целях создавались хорошо структурированные группы, члены которых осуществляли звонки клиентам и подтверждали факт совершения покупки, благодаря чему потерпевшие долгое время пребывали в уверенности, что сделка состоялась, то в 2020 г. эта техника прошла серьезное усовершенствование. Во-первых, лица, вовлеченные в совершение мошеннических действий, стали создавать точные копии официальных сайтов компаний – лидеров дистанционных продаж. Во-вторых, могут использоваться официальные идентификационные данные (логотип, товарный знак). В-третьих, для привлечения посетителей могут использоваться инструменты Интернет-маркетинга. В конечном итоге вплоть до внесения платежа клиент пребывает в заблуждении о том, что в действительности товар им не приобретается.

Фактически «Клондайком» для мошенников являются ресурсы, на которых можно разместить объявления о продаже физическими лицами принадлежащего им имущества (например, «Авито»). В этом случае размещается объявление о продаже, после чего потенциального покупателя склоняют к внесению аванса или полной предоплаты.

Можно упомянуть и о создании фейковых аккаунтов в социальных сетях, использующиеся впоследствии для собирания денежных средств под предлогом организации денежного розыгрыша, либо для введения в заблуждение граждан путем просьб о переводах денежных средств в связи со срочной необходимости.

Перечисленные действия характеризуют далеко не весь спектр киберпреступности, однако в целом отражают ее бытовой, т. е. максимально приближенный к жизни российских граждан, сегмент. О латентности этих способов противоправного поведения можно строить самые негативные предположения: если сумма ущерба незначительна, потерпевшие не обращаются в правоохранительные органы. Если преступление не доведено до конца, поскольку потерпевший не стал совершать покупку, опасаясь стать жертвой мошенничества, уведомлять об этом полицию он, скорее всего, не будет. В ряде случаев затруднительно установить место нахождения преступников, так как они могут осуществлять посягательство, находясь при этом за рубежом.

Подытоживая, можно заключить, что наличие специального барьера киберпреступности во многом является фикцией, не обеспечивающей защиту граждан от преступных посягательств. Как представляется, более эффективным способом противодействия хищениям денежных средств, совершаемым с использованием ресурсов сети «Интернет», было бы своевременное выявление и блокировка мошеннических сайтов, а равно мониторинг социальных сетей. Правоохранительные органы РФ имеют такой опыт в части противодействия терроризму и экстремизму, и эти методики могут быть полезны и в данном случае.

СПИСОК ИСТОЧНИКОВ

1. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор / Антонян Ю. М.,

Бражников Д. А., Гончарова М. В., Коваленко В. И., Шиян В. И., Бицадзе Г. Э., Евсеев А. В. – М. : ВНИИ МВД России, 2018. – 86 с.

2. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лиц, в отношении которых вынесены судебные акты по уголовным делам: форма 10-а // Судебный департамент при Верховном Суде РФ. – URL : http://www.consultant.ru/document/cons_doc_LAW_331982/dc653f328d2f182ee00f2297c7e01b93e8cebeab/ (дата обращения: 05.12.2020).

3. Краткая характеристика состояния преступности в Российской Федерации за январь – сентябрь 2020 года. – URL: https://мвд.рф/reports/item/21551069/ (дата обращения: 05.12.2020).

УДК 342.8

Разживина Анна Витальевна,
магистрант, Костромской государственный университет,
г. Кострома, Российская Федерация.
anna_3096@mail.ru

Перспективы развития электронного голосования в России

Актуальность данной темы связана с процессами интенсивного развития глобальной сети, с глобальной интернетизацией социального пространства в целом (и политической сферы в частности). В статье рассмотрены перспективы развития электронного голосования в России, изучены положительные и отрицательные стороны внедрения данного процесса и представлены соответствующие выводы.

***Ключевые слова**: выборы, цифровые технологии, Интернет, голосование, народ, электронное голосование.*

Razzhivina Anna Vitalievna,
undergraduate, Kostroma State University,
Kostroma, Russian Federation.

Prospects for the development of electronic voting in Russia

The relevance of this topic is associated with the processes of intensive development of the global network, with the global internetization of social space in general (and the political sphere in particular). The article examines the prospects for the development of electronic voting in Russia, examines the positive and negative aspects of implementing this process and presents the corresponding conclusions.

***Keywords:** elections, digital technologies, Internet, voting, people, electronic voting.*

Цифровизация и интернет-коммуникации с каждым годом приобретают все большую актуальность. С этим нельзя не согласиться, ведь почти каждый человек, большую часть времени проводит в сети «Интернет».

Еще несколько лет назад, для того чтобы купить продукты, одежду или оплатить коммунальные платежи, люди стояли продолжительное время у кассы