Научная статья
https://doi.org/10.24412/2220-2404-2024-6-35
УДК 343.2/.7

УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ В СФЕРЕ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Финкель М.В.
Российский государственный университет имени А.Н. Косыгина

Аннотация. *Цель. В статье произведен всесторонний уголовно-правовой анализ составов цифровых преступлений, посягающих на собственность субъектов предпринимательской деятельности. В процессе изучения были использованы общенаучные (анализ, синтез, индукция и дедукция) и частно-научные (уголовно-правовой, криминологический) методы познания. В ходе подготовки публикации использованы данные официальной статистики, а также отечественные исследования в области уголовного права и криминологии. В результате проведённого анализа сделаны выводы об отсутствии адекватного правоохранительного реагирования на массив организованной цифровой преступности. Выводы и заключения: материалы публикации могут быть использованы в целях оптимизации правоохранительной практики, формирования и развития системы криминологической кибербезопасности сферы предпринимательской деятельности от цифровых посягательств.*

Ключевые слова: *уголовно-правовой анализ, цифровые преступления, цифровая организованная преступность, криминологическая кибербезопасность, сфера предпринимательской деятельности, криминализация бизнес-правоотношений, теневая экономика.*

CRIMINAL LAW ANALYSIS OF DIGITAL CRIMES AGAINST PROPERTY IN THE FIELD OF ENTREPRENEURIAL ACTIVITY

Marina V. Finkel
Kosygin Russian State University

Abstract. *Goal. The article presents the results of a criminal law analysis of digital crimes encroaching on the property of business entities, and a detailed analysis of the composition of such encroachments is carried out. In the process of studying, general scientific (analysis, synthesis, induction and deduction) and private scientific (criminal law, criminological) methods of cognition were used. During the preparation of the publication, official statistics data were used, as well as domestic research in the field of criminal law and criminology. As a result of the analysis, conclusions are drawn about the lack of an adequate law enforcement response to the array of organized digital crime. Conclusions and conclusions: the materials of the publication can be used to optimize law enforcement practice, the formation and development of a system of criminological cybersecurity of the business sphere from digital encroachments.*

Keywords: *criminal law analysis, digital crimes, digital organized crime, criminological cybersecurity, business sphere, criminalization of business relations, shadow economy.*

Введение. Обеспечение эффективного функционирования сферы предпринимательской деятельности требует проведения комплексных превентивных исследований, в том числе, направленных на всесторонний анализ данной сферы преступности, реализуемой в цифровом пространстве. Преступления, посягающие на чужую собственность, в том числе на имущество субъектов предпринимательской деятельности, составляют основной вал цифровых посягательств. Об этом свидетельствует статистика МВД РФ за 2023 г., согласно которой из 677 тыс. преступлений с использованием кибертехнологий краж совершено более 119 тыс., а мошенничеств – более 356 тыс. [1].

Обсуждение. Прежде всего, отметим явную неадекватность государственного правоохранительного реагирования на массив цифровой преступности, приведенный в статистике МВД РФ. Данный факт подтвердил в своем выступлении председатель судебного состава судебной коллегии по уголовным делам Верховного суда РФ Г.П. Иванов, который, касаясь вопроса о числе вынесенных обвинительных приговоров по цифровым преступникам, отметил: «Если в 2020 году

их было всего 137, то в 2022 году - уже 424». При этом представитель ВС РФ отметил, что небольшое количество дел, связанных с преступностью в информационно-телекоммуникационных сетях, доходящих до суда, связано с трудностью выявления таких преступлений, а также получения следствием необходимых доказательств для направления дела в суд [2].

Уголовно-правовой разбор составов таких видов хищений, как кража, мошенничество, присвоение и растрата и вымогательство, совершаемых в отношении имущества субъектов предпринимательской деятельности, с использованием инновационно-технологических ресурсов, позволяет выявить следующую картину.

Кража, совершенная с банковского счета субъекта предпринимательской деятельности, а равно в отношении его электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ).

Основной объект - права собственников финансовых активов, *дополнительные* – отношения, регулирующие предпринимательскую деятельность, прежде всего право компании на защиту и суверенный оборот собственных финансовых активов, а также правоотношения, отраженные в ст. ст. 272-273 УК РФ.

Предмет посягательства – корпоративные цифровые финансовые активы. Под криптовалютой здесь следует понимать «денежный суррогат, эмиссия и учет которого основаны на криптографических методах шифрования компьютерной информации» [3, С. 63].

Объективная сторона такого рода кражи выражается в действиях, отраженных в диспозициях ст. 158 и 272 УК РФ.

Обращение к ст. 272-273 УК РФ обусловливает необходимость в применении совокупности данных составов с п. «г» ч. 3 ст. 158 УК РФ.

В качестве *средства совершения рассматриваемого преступления* выступают информационно-коммуникационные технологии, а *способ* заключается в дистанционном воздействии на объект посягательства.

Субъект преступления - лицо, достигшее 14 лет, в том числе обладающее достаточно высокой киберквалификацией, что позволяет говорить о наличии признаков специального субъекта.

Субъективная сторона характеризуется наличием умысла, корыстного мотива и цели завладения имуществом субъекта предпринимательской деятельности.

Мошенничество, то есть хищение имущества субъекта предпринимательской деятельности или приобретение права на его имущество путем обмана или злоупотребления доверием (ст. 159-159⁶ УК РФ).

Что касается специального относительно рассматриваемой нами сферы состава мошенничества, сопряженного с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, то, как представляется, он не применим в регулировании правоотношений, возникающих при преступных посягательствах на собственность субъектов предпринимательской деятельности с использованием ИТ-ресурсов.

Основной и дополнительные объекты, а также предмет посягательства в мошенничестве схожи с отмеченными выше признаками инновационной кражи. При этом отметим, что в мошенничествах речь идет не только о хищении чужого имущества, но и о приобретение права на чужое имущество.

Объективная сторона инновационного мошенничества выражается в действиях, отраженных в диспозициях ст. 272-273 УК РФ: мошенничество, то есть хищение цифровых финансовых активов субъекта предпринимательской деятельности или приобретение права на его цифровые финансовые активы путем обмана или злоупотребления доверием, далее по тексту диспозиций отмеченных «компьютерных» составов.

Особенность преступных действий относительно обязательного применения специфических способов мошенничества заключается в том, что представитель субъекта предпринимательской деятельности может быть введен в заблуждение неким финансово заманчивым предложением с прилагаемой ссылкой для перехода к интересной информации. Такого рода предложение может поступить представителю компании от мошенника, либо данный представитель может самостоятельно обнаружить в Сети мошенническую ловушку, замаскированную под интересную рекламу. Переход по ссылке активизирует фишинговую или троянскую программу, что предоставляет злоумышленникам доступ к цифровым активам компании или к кодам доступа к ним. Главным здесь является наличие обязательного отклика от потерпевшего или его представителя.

Обращение к ст. 272-273 УК обусловливает необходимость в применении совокупности данного состава со ст. 159 УК.

В качестве *средства совершения рассматриваемого преступления* выступают информационно-коммуникационные технологии, а *способ* заключается в дистанционном воздействии на объект посягательства.

Субъект преступления - лицо, достигшее 16-ти лет, в том числе обладающее достаточно высокой киберквалификацией, что позволяет говорить о наличии признаков специального субъекта.

Мошенничество может быть совершено и лицом, не обладающим специальными знаниями, когда электронное устройство выступает в качестве средства связи с потерпевшим, который может быть введен в заблуждение сообщением по электронной почте или иному мессенджеру. При этом не образуется совокупность составов мошенничества с приведенными «компьютерными» нормами.

Субъективная сторона характеризуется наличием умысла, корыстного мотива и цели завладения имуществом субъекта предпринимательской деятельности.

Уголовно-правовой анализ специальных составов мошенничества схож с произведенным разбором основного состава данного преступления, поскольку в специальных составах применен весьма спорный так называемый «сферный» принцип. Заложенные законодателем в двух нормах – ст. 159^3 и 159^6 УК - элементы технологической инновационности, содержат в себе достаточно много недостатков. Относительно первой нормы возникает вопрос о тавтологичности ее состава с составом ст. 187 УК РФ в части использования заведомо подложных средств платежа для неправомерного осуществления приема, выдачи, перевода денежных средств, вторая же норма не является мошенничеством по причине отсутствия в нем указания на применение преступником обмана или злоупотребления доверием [4, С. 85-88; 5, С. 88-89; 6, С. 224-225].

Присвоение или растрата, то есть хищение имущества субъекта предпринимательской деятельности, вверенного виновному (ст. 160 УК РФ).

Основной и дополнительные объекты, а также предмет посягательства в данной норме схожи с отмеченными выше признаками инновационной кражи.

Объективная сторона преступления. Совокупность данной нормы с «компьютерными» составами может возникнуть в том случае, когда сотрудник, наделенный финансово-хозяйственными полномочиями, используя свое служебное положение, самостоятельно либо с помощью соучастника совершить «взлом» корпоративной системы.

Субъект преступления - лицо, достигшее 16-ти лет, в том числе обладающее достаточно высокой киберквалификацией, что позволяет говорить о наличии признаков специального субъекта.

Данное преступное посягательство может быть совершено и лицом, не обладающим специальными знаниями, когда электронное устройство выступает в качестве средства связи с потерпевшим, который может быть введен в заблуждение сообщением по электронной почте или иному мессенджеру. При этом не образуется совокупность ст. 160 УК РФ со ст. ст. 272-273 УК РФ.

Субъективная сторона характеризуется наличием умысла, корыстного мотива и цели завладения имуществом субъекта предпринимательской деятельности.

Вымогательство, то есть требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких (ст. 163 УК РФ).

Объекты и предмет преступления аналогичны тем, что характерны для совершения кражи.

Объективная сторона. Инновационное вымогательство сопряжено со «взломом» корпоративной системы, после чего злоумышленник требует у руководства компании или индивидуального предпринимателя передачи денег под угрозой распространения конфиденциальных сведений.

В качестве средства совершения рассматриваемого преступления выступают информационно-коммуникационные технологии, а способ заключается в дистанционном воздействии на объект посягательства. Помимо этого, следует особо отметить наличие специально созданных вредоносных программ-«вымогателей» («шантажистов») (англ. ransomware - контаминация слов ransom - выкуп и software - программное обеспечение), блокирующих доступ к компьютерной системе или предотвращающих считывание данных в этой системе посредством криптографических методов, а затем требующих выкупа для восстановления статус-кво.

Также, вымогательство денежных средств субъекта предпринимательской деятельности в совокупности со ст. 138^1 УК РФ может

быть осуществлено, когда злоумышленник незаконно приобретает и использует специальные технические средства, предназначенные для негласного получения информации, с помощью которых собирает данные о личной жизни руководителя/сотрудника компании или же в отношении индивидуального предпринимателя/его сотрудников, после чего требует у юридического или физического лица передачи денег под угрозой распространения сведений, которые могут причинить существенный вред правам и законным интересам субъекта предпринимательской деятельности.

Отметим, что по данной норме, уголовная ответственность наступает с 14-ти лет.

Что касается составов иных преступлений против собственности предпринимателей, то отметим следующее.

Причинение имущественного ущерба субъекту предпринимательской деятельности путем обмана или злоупотребления доверием при отсутствии признаков хищения, совершенное в крупном размере (ст. 165 УК РФ).

Основной и дополнительные объекты, а также предмет посягательства в данной норме схожи с отмеченными выше признаками инновационной кражи.

Объективная сторона преступления. Такого рода посягательство в совокупности с «компьютерными» преступлениями может быть сопряжено, к примеру, с подключением к интернет-траффику компании, пользуясь которым бесплатно, преступник, тем самым, причиняет субъекту предпринимательской деятельности ущерб на сумму, превышающую 250 000 руб.

Субъективная сторона рассматриваемого преступления характеризуется прямым умыслом, а *субъектом преступления* является лицо, достигшее возраста 16-ти лет.

Умышленные уничтожение или повреждение имущества субъекта предпринимательской деятельности (ст. 167 УК РФ).

Помимо отмеченных выше *основных и дополнительных объектов*, а также *предмета посягательства*, потенциально, в качестве *дополнительного объекта* могут выступить сферы интересов личности, его жизни и здоровья.

С объективной стороны рассматриваемое преступление характеризуется двумя альтернативными действиями в виде уничтожения или повреждения чужого имущества. Учитывая охват цифровой экономики технологическими новациями, очевидна возможность причинения материального ущерба субъекту предпринимательства не только традиционно существующими способами взрыва или поджога, но и посредством действий, содержащихся в ст. 272-273 УК РФ. Квалификация в данном случае последует по совокупности ст. 167 со ст. 272-273 УК РФ.

Учитывая факт подключения современных компании к системам жизнеобеспечения через компьютерные сети, следует ожидать, что уничтожение сетевых коммуникаций способно привести к полной остановке или дезорганизации работы предприятия, выразиться в смерти человека, а также в иных тяжких последствиях (ч. 2 ст. 167 УК РФ).

Субъективная сторона рассматриваемого преступления характеризуется прямым умыслом, а *субъектом преступления* является лицо, достигшее возраста 16 лет, по ч. 2 ст. 167 УК РФ - 14 лет.

Результаты. Произведенный уголовно-правовой анализ, демонстрирует криминальные потенциалы как цифровых средств, так и лиц, обладающих навыками во «взломе» компьютерных систем и получении доступа к чужой компьютерной информации. При этом организованной цифровой преступной деятельности государство, по сути, противопоставляет лишь деятельность небольшого числа высококлассных сотрудников Управления МВД РФ по организации борьбы с противоправным использованием информационно-коммуникационных технологий. Соответственно, адекватной реакцией на массив цифровых посягательств не происходит.

Заключение. Отмеченное выше позволяет предложить ряд конкретных мер, нацеленных на выправление существующей негативной ситуации.

Во-первых, необходимы меры правового, организационного и образовательного характера, нацеленные на информационно-технологическую подготовку и переподготовку действующих и будущих сотрудников правоохранительных органов, прежде всего тех, в чьи функциональные обязанности входит предупреждение экономической преступности.

Во-вторых, необходимо учесть пример положительного взаимодействия Федеральной службы безопасности РФ с Лабораторией Касперского в рамках государственно-частного партнерства, нацеленного на обеспечение безопасности критической информационной инфраструктуры, включающей в себя ряд значимых для государства объектов.

На наш взгляд, весь комплекс цифровой экономики, включающий в себя деятельность и

ресурсы субъектов предпринимательской деятельности, также должен быть охвачен государственной системой криминологической кибербезопасности от инновационных посягательств.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года. - URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 28.05.2024).

2. Судья ВС сообщил о росте числа осужденных в РФ за киберпреступления. - URL: https://www.bfm.ru/news/527035 (дата обращения: 08.06.2024).

3. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дисс. канд. юрид. наук. М., 2016. С. 63.

4. Джафарли В.Ф. Критический уголовно-правовой анализ статьи 159.6 Уголовного кодекса Российской Федерации «Мошенничество в сфере компьютерной информации» // Евразийская адвокатура. 2017. № 5 (30). С. 85-88.

5. Джафарли В.Ф. Критический уголовно-правовой анализ статьи 187 УК РФ «Неправомерный оборот средств платежей» // Евразийская адвокатура. 2018. № 3 (34). С. 88-89.

6. Джафарли В.Ф. Критический уголовно-правовой анализ статьи 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» // Евразийский юридический журнал. 2018. № 8 (123). С. 224-225.

References:

1. A brief description of the state of crime in the Russian Federation in January – December 2023. - URL: https://мвд.рф/reports/item/47055751 / (date of appeal: 05/28/2024).

2. The judge of the Supreme Court reported an increase in the number of people convicted of cybercrime in the Russian Federation. - URL: https://www.bfm.ru/news/527035 (date of appeal: 06/08/2024).

3. Prostoserdov M.A. Economic crimes committed in cyberspace and measures to counteract them: dissertation of the candidate. Jurid. M., 2016. p. 63.

4. Dzhafarli V.F. Critical criminal law analysis of Article 159.6 of the Criminal Code of the Russian Federation "Fraud in the field of computer information" // Eurasian Advocacy. 2017. No. 5 (30). pp. 85-88.

5. Dzhafarli V.F. Critical criminal law analysis of Article 187 of the Criminal Code of the Russian Federation "Illegal turnover of means of payment" // Eurasian Advocacy. 2018. No. 3 (34). pp. 88-89.

6. Dzhafarli V.F. Critical criminal law analysis of Article 159.3 of the Criminal Code of the Russian Federation "Fraud using electronic means of payment" // Eurasian Legal Journal. 2018. No. 8 (123). pp. 224-225.

Информация об авторе:

Финкель Марина Вячеславовна, преподаватель кафедры уголовного права и адвокатуры, Российский государственный университет имени А.Н. Косыгина, e-mail: m.finkel@lawyerspro.ru

Marina V. Finkel, Lecturer at the Department of Criminal Law and Advocacy, Kosygin Russian State University.