

УДК 343

DOI: 10.34670/AR.2022.39.30.060

**Уголовное законодательство об ответственности за
мошенничество в сфере компьютерной информации: сравнение
российского и зарубежного права**

Журкина Ольга Вячеславовна

Кандидат юридических наук, доцент,
завкафедрой организации судебной
и прокурорско-следственной деятельности,
Оренбургский государственный университет,
460018, Российская Федерация, Оренбург, пр. Победы, 13;
e-mail: olga_fv@inbox.ru

Филиппова Елена Олеговна

Кандидат педагогических наук,
доцент кафедры уголовного права,
Оренбургский государственный университет,
460024, Российская Федерация, Оренбург, пр. Победы, 13;
e-mail: Elena56-75@mail.ru

Аннотация

Информация, технологии и безопасность – три ключевых элемента современного общества XXI века. Поскольку каждый современный человек проводит в социальных сетях достаточно времени, имеет, как минимум, рабочую почту, выкладывает личные фотографии и хранит деньги в электронной форме, он надеется на то, что его данные останутся в сохранности. Тем не менее, в последние годы главной международной проблемой стало мошенничество в IT-сфере, которое приобрело свое развитие и в России. Особенно часто, можно встретить попытки мошенников взломать банковские карты, получить личные данные счета или выяснить пин-код. Несмотря на то, что в большинстве своем все эти уловки очевидны, тем не менее, ежедневно мошенники зарабатывают от 50000 рублей, совершая данный вид преступления. Российское государство гарантирует каждому гражданину защиту при нарушении его прав и свобод, но в большинстве случаев безоружно перед преступлением данного вида. Это вызвано тем, данный вид мошенничества сложно расследовать, поскольку оно достаточно новое для российского законодателя и недостаточно урегулировано законом. Одновременно указывается, что российские правоохранительные органы не оснащены современными технологическими средствами, которые могли бы помочь в расследовании данного вида преступления. Зачастую преступники обладают более глубокими знаниями и новой техникой, а органы дознания и следствия ограничены старыми компьютерами и нормами УК РФ. Такие дела превращаются в «висяки», а потерпевшим настоятельно рекомендуют не подавать заявление.

Для цитирования в научных исследованиях

Журкина О.В., Филиппова Е.О. Уголовное законодательство об ответственности за мошенничество в сфере компьютерной информации: сравнение российского и зарубежного права // Вопросы российского и международного права. 2022. Том 12. № 8А. С. 416-422. DOI: 10.34670/AR.2022.39.30.060

Ключевые слова

Информация, технологии, безопасность, преступление, мошенничество, IT-сфера, компьютерная информация, IT-технологии.

Введение

Мошенничество в сфере IT является актуальной проблемой XXI века. Тем не менее, о ней и способах ее предотвращения впервые заговорили в 2012 году, когда и был принят Федеральный закон Российской Федерации от 29.11.2012 г. № 207–ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Именно в этот момент, путем принятия закона, законодатель включил в Уголовный кодекс РФ новую статью ст. 159.6 УК РФ.

Нормы данной статьи посвящены мошенничеству, реализуемому в сфере информации. Именно в указанной статье и дается характеристика данному преступлению, в частности через определение способов: вмешательство; обработка; передача. Кроме того, раскрывается и объект преступления, а именно – данное преступление может быть направлено на: чужое имущество; право на чужое имущество; компьютерную информацию.

Основная часть

При анализе данного состава преступления нередко употребляется термин «компьютерная информация». К счастью, в этот раз российский законодатель дал официальное толкование указанному термину и отметил его значение в примечании 1 к ст. 272 УК РФ: «сведения (сообщения, данные), представленные в форме электрических сигналов независимо от средства их хранения, обработки и передачи».

Если бы он это не сделал, еще одной актуальной проблемой стало бы определение данного термина, выявление его сути и содержания. Законодатель предупредительно облегчил себе задачу и регламентировал понятие, однако, а целом это не решило все проблемы. Нельзя не отметить, что в Российской Федерации вопрос о мошенничестве в сфере IT развит посредственно и как отмечалось в первой части исследования не ратифицированы многие акты международного права, которые могли бы поставить точку во многих проблемных вопросах.

Тем не менее, кроме главного источника, регламентирующего данный вопрос, а именно УК РФ, действует и разъяснения Постановления Пленума Верховного Суда РФ № 51 от 27 декабря 2007 года «О судебной практике по делам о мошенничестве, присвоении и растрате». В данном акте закрепляются общие положения, касающиеся данного вопроса:

- преступление будет признано завершенным в тот момент, когда имущество поступило в незаконное владение виновного;
- преступление будет признано завершенным, в тот момент, когда преступник получил реальную возможность пользоваться или распоряжаться судьбой имущества

[Номоконов, 2020].

Наличие всего двух актов – недостаточно для разрешения столь актуального вопроса. Именно поэтому следует отметить, что регулируется данное преступление в зарубежных странах, за исключением международных конвенций и договоров.

В качестве первой страны для анализа следует выбрать США. Именно здесь в 1978 году приняли законопроект, регулирующий преступления в сфере IT-технологий. Поскольку в Россию данная сфера пришла намного позже, в США напротив же, в 1978 году законодатель задумался о предупреждении преступлений данного вида.

Для успешного урегулирования данного вопроса было необходимо дать законодательное закрепление термину мошенничеству IT-технологий, которое представляло собой действия, направленные на нарушение, уничтожение, изъятие данных и программ другого пользователя. В тот период времени были особенно распространены вредоносные внешние носители, которые позволяли получать информацию другого пользователя [Шульга, 2017].

Через 10 лет, цифровые технологии шагнули вперед и потребовали принятия новой нормы. Следующий акт от 1984 года, ввел термин «злоупотребление использованием компьютеров». Речь шла о том, какие злоупотребления можно признать преступлениями (если они нарушают права, в том числе и имущественные, другого человека) и в данном акте было отражена ответственность за подобные действия.

Поскольку законодательство США разрознено, на территории каждого штата действует право этого конкретного штата. Это также касается и данного вида преступления, однако, в целом мошенничество признается видом хищения, которое характеризуется своим распространением и негативным влиянием на экономические отношения.

Здесь следует отметить и то, что согласно ст. 223.1 УК США хищение – единое посягательство. Однако оно включает в себя и подвиды, а именно: похищение; растрату имущества; мошенничество; вымогательство; шантаж; обманное обращение чужого имущества в свою пользу; приобретение похищенного имущества.

В России предусмотрено более мягкое наказание за рассматриваемое преступление. В ст. 159.6 УК РФ за мошенничество в сфере IT максимальное наказание составляет не более 1,5 лет. В США за данное преступление предусмотрено лишение свободы до 5 лет. Но если речь будет идти о рецидиве, то есть повторном нарушении нормы, то наказание может увеличиться и до 20 лет. Законодатель оставил применение данной нормы на усмотрение суда.

В качестве следующего объекта анализа следует выбрать Великобританию. По аналогии, с США, рассматриваемая сфера технологий, развивалась здесь быстрее, чем в России. Именно поэтому первые законы, предусматривающие ответственность за отдельные виды мошенничества, появились в 1978.

В качестве базиса в УК Великобритании отражено то, что мошенничество – видовое понятие, а его главная цель направлена на извлечение прибыли. Данное преступление по законодательству Великобритании носит материальный состав и связано, как с извлечением прибыли, так и с причинением ущерба [Васильев, 2016].

Поскольку данный вопрос имеет особую актуальность для всех стран Европы, каждое государство стремится принять такую норму, чья эффективность могла бы повлиять на уменьшение развития преступного деяния. Именно поэтому в 2010 году в Великобритании был принят Закон, раскрывающий компьютерное мошенничество как преступление. В нем было отмечено, что указанное преступление представляет собой обманные действия, а в качестве способ совершения нередко выступают средства связи. За его совершение может быть

назначено наказание в виде лишения свободы сроком 5 лет.

Также следует отметить и особенности законодательства Новой Зеландии. Несмотря на то, что данную страну обычно не выбирают для проведения исследования, нельзя не отметить, что данное преступление нашло свое законодательное закрепление в уголовных нормах Зеландии.

В частности, отмечается, что ответственность за компьютерное мошенничество предусмотрена в ст. 250 УК Новой Зеландии и подразумевает использование компьютерной системы для незаконных целей. Тем не менее, стоит указать, что расположение данной нормы достаточно необычно, ведь она помещена в группу преступлений, связанных с компьютерами. Следовательно, в трех предыдущих государствах, в том числе и в России, данная норма закреплена в главе о преступлениях против собственности.

Тем не менее, выбор, сделанный Новой Зеландией несколько правильнее, о чем длительное время пишут исследователи уголовного права. Именно поэтому и предлагается в УК РФ выделить раздел, который был бы посвящен компьютерным преступлениям.

Проведенное исследование также подводит к выводу о некой разобщенности норм англосаксонской правовой системы. В большинстве свое мошенничество выступает лишь обобщающим понятием, однако, ответственность за него находит свое отражение сразу в нескольких законах [Волеводза, 2017].

В этом плане, законодательство России во многом удобнее, поскольку в УК РФ термин един и выделяется несколько составов за каждый вид мошенничества, соответственно.

Кроме того, в Европейских государствах лишение свободы предусмотрено за любой вид мошенничества, направленный на сферу IT-технологий. Однако в УК РФ лишение свободы предусматривается только за квалифицированный вид мошенничества (ч. 4 ст. 159.6 УК РФ). Такая мягкость российского законодателя также не идет ему на пользу, но и чрезмерная жесткость, например, США не показывает положительных успехов в предупреждения данного вида преступления.

Тем не менее, развитие мошенничества данного вида в большей мере приходится именно на РФ и США, что показывает наличие общего признака, скрытно влияющего на развитие преступления. Возможно, это вызвано сильной зависимостью граждан обеих стран от сети Интернет, где можно свободно получить большее количество информации.

Данный вопрос нашел свое отражение и в зарубежном законодательстве. Поскольку российское уголовное право не совсем готово к быстрому развитию компьютерных технологий, следует обратить внимание на немецкую систему права.

Так в Уголовном кодексе Германии существует понятие «компьютерное мошенничество». Однако данное преступление – это самостоятельная форма мошенничества, за которое уголовная ответственность не может превышать пяти лет лишения свободы. В качестве альтернативного наказания выступает назначение денежного штрафа.

Исследователи обращают внимание на то, что данная статья может быть применена лишь при условии, что лицо хотела получить для себя имущественную выгоду. Это в принципе характеризует не только российскую систему права, но и немецкое право, поскольку имущественная выгода главное основания для признания преступления мошенничеством. Следовательно, по аналогии с российским правом главная цель преступника – это корысть.

Кроме того, в Уголовном кодексе Германии обращается внимание на причинение имущественного вреда. Например, это возможно путем создания неправомерных программ, воздействующих на внутренние файлы компьютера, которые будут исправлять данные владельца.

Данная норма является открытой и подлежит расширительному толкованию, учитывая особенности конкретного преступления.

Указанное положение является ключевым отличием от российского понимания термина «мошенничество», поскольку в УК РФ изъятие имущества предшествует причинению вреда.

Уголовный кодекс Германии разделяет мошенничество в сфере компьютерной информации на несколько видов: простое мошенничество; квалифицированный состав мошенничества [Шигуров, 2017].

В зависимости от конкретного вида используются различные способы совершения преступления. Тем не менее, в любом случае это касается сферы преступного деяния.

В качестве еще одного примера для анализа следует обратить внимание на законодательство Швейцарии. В данном случае Уголовный кодекс Швейцарии по аналогии с УК РФ выделяет данный вид преступления в главе «преступления против собственности».

Однако, в УК РФ прямо выделен объект преступления. В свою очередь, в УК Швейцарии предмет весьма условен. В частности, это делает данный вопрос проблемным, поскольку правоохранительным органом непонятно, какие посягательства следует признать преступлением.

И наконец, последним источником анализа станет Уголовный кодекс Болгарии, где ответственность за данный вид мошенничества также относится к преступлениям против собственности».

В УК Болгарии указано на то, что мошенничество будет признано таковым, если лицо вводит кого-либо в заблуждение и делает это из корыстных целей.

Следует отметить и то, что подделка электронной подписи является составом мошенничества, согласно Уголовному Кодексу Болгарии. Тем не менее, данное преступление не является разновидностью мошенничества согласно УК РФ.

Заключение

Таким образом, анализ законодательства правовых систем зарубежных стран обращает внимание на то, что мошенничество – это посягательство в сфере собственности. Как правило, мошенничество воздействует на несколько объектов: – чужое имущество; право; услуга.

В любом случае отягчающее обстоятельство по данному виду преступления – крупный размер мошенничества, который определяется каждым государством самостоятельно. Квалифицирующий признак преступления – это повторность или неоднократность его совершения, что находит свое отражение в законодательстве США.

Отечественному законодателю следует обратить внимание на зарубежный опыт, для того чтобы внести некие изменения в УК РФ. Несмотря на то, что данное преступление часто выделяется среди преступлений против собственности, ему необходима отдельная глава, куда следует включить все компьютерные преступления, существующие на данный момент.

Это позволило бы обобщить судебную практику по данному вопросу и сделать законодательство более удобным.

Библиография

1. Васильев А.И. Новеллы уголовного законодательства об ответственности за хищения. М.: Новеллы права, 2016. 117 с.
2. Волеводза А.Г. Уголовно-процессуальное законодательство. М.: БЕК, 2017. 151 с.

3. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2020. № 24. С. 114.
4. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федер. закон: принят Гос. Думой 17 ноября 2011 г.; одобрен Советом Федерации 29 ноября 2011 г.
5. Уголовный кодекс Российской Федерации: федер. закон: принят Гос. Думой 24 мая 1996 г.; одобрен Советом Федерации 5 июня 1996 г.
6. Шигуров А.В. Уголовное судопроизводство. М.: БЕК, 2017. 218 с.
7. Шульга А.В. Хищения в условиях развития современных информационных технологий и рынка инновационных товаров. М.: Юрайт, 2017. 110 с.
8. Mosechkin I. N. Artificial intelligence and criminal liability: problems of becoming a new type of crime subject. – 2019.
9. Khatuev V. B. Criminal law regulation of liability for suicide in the Russian criminal legislation: the past and present // Actual Problems of Russian Law. – 2019. – №. 11. – С. 81-95.
10. Buribayev Y. A. et al. Legislative regulation of criminal liability for environmental crimes // Journal of Environmental Accounting and Management. – 2020. – Т. 8. – №. 04. – С. 323-334.

Criminal legislation on liability for fraud in the sphere of computer information: comparison of Russian and foreign law

Ol'ga V. Zhurkina

PhD in Law, Associate Professor,
Head of the Department of Organization of Judicial and
Prosecutorial and Investigative Activities,
Orenburg State University,
460018, 13, Pobedy ave., Orenburg, Russian Federation;
e-mail: olga_fv@inbox.ru

Elena O. Filippova

PhD in Pedagogy,
Associate Professor at the Department of Criminal Law,
Orenburg State University,
460024, 13, Pobedy ave., Orenburg, Russian Federation;
e-mail: Elena56-75@mail.ru

Abstract

Information, technology and security are the three key elements of modern society in the 21st century. Since every modern person spends enough time on social networks, has at least a work email, uploads personal photos and stores money in electronic form, he hopes that his data will remain safe. However, in recent years, fraud in the IT sphere has become the main international problem, which has also developed in Russia. Especially often, you can meet fraudsters trying to hack bank cards, get personal account information or find out a pin code. Despite the fact that for the most part all these tricks are obvious, nevertheless, daily scammers earn from 50,000 rubles by committing this type of crime. Russian state guarantees protection to every citizen in case of violation of his rights and freedoms but often stays unarmed in the face of a crime of this type. This is due to the fact that this type of fraud is difficult to investigate, since it is quite new for the Russian legislator and is not sufficiently regulated by law. The Russian law enforcement agencies are not

equipped with modern, technological means that could help in the investigation of this type of crime. Often, criminals have deeper knowledge and new technology, while the bodies of inquiry and investigation are limited by old computers and the norms of the Criminal Code of the Russian Federation. Such cases remain cold, and the victims are strongly advised not to file a complaint.

For citation

Zhurkina O.V., Filippova E.O. (2022) *Ugolovnoe zakonodatel'stvo ob otvetstvennosti za moshennichestvo v sfere komp'yuternoi informatsii: sravnenie rossiiskogo i zarubezhnogo prava* [Criminal legislation on liability for fraud in the sphere of computer information: comparison of Russian and foreign law]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 12 (8A), pp. 416-422. DOI: 10.34670/AR.2022.39.30.060

Keywords

Information, technology, security, crime, fraud, IT-sphere, computer information, IT-technologies.

References

1. Nomokonov V.A. (2020) *Kiberprestupnost' kak novaya kriminal'naya ugroza* [Cybercrime as a new criminal threat]. *Kriminologiya: vchera, segodnya, zavtra* [Criminology: yesterday, today and tomorrow], 24, p. 114.
2. *O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii: feder. zakon: prinyat Gos. Dumoi 17 noyabrya 2011 g.; odobr. Sovetom Federatsii 29 noyabrya 2011 g.* [On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation: Feder. law: adopted by the State. Duma November 17, 2011; approval Federation Council November 29, 2011].
3. Shigurov A.V. (2017) *Ugolovnoe sudoproizvodstvo* [Criminal litigation]. Moscow: BEK Publ.
4. Shul'ga A.V. (2017) *Khishcheniya v usloviyakh razvitiya sovremennykh informatsionnykh tekhnologii i rynka innovatsionnykh tovarov* [Embezzlement in the context of the development of modern information technologies and the market of innovative goods]. Moscow: Yurait Publ.
5. *Ugolovnyi kodeks Rossiiskoi Federatsii: feder. zakon: prinyat Gos. Dumoi 24 maya 1996 g.; odobr. Sovetom Federatsii 5 iyunya 1996 g.* [Criminal Code of the Russian Federation: Feder. law: adopted by the State. Duma on May 24, 1996; approval Federation Council June 5, 1996].
6. Vasil'ev A.I. (2016) *Novelly ugolovnogo zakonodatel'stva ob otvetstvennosti za khishcheniya* [Novels of the criminal legislation on liability for theft]. Moscow: Novelly prava Publ.
7. Volevodza A.G. (2017) *Ugolovno-protsessual'noe zakonodatel'stvo* [Criminal procedure legislation]. Moscow: BEK Publ.
8. Mosechkin, I. N. (2019). Artificial intelligence and criminal liability: problems of becoming a new type of crime subject.
9. Khatuev, V. B. (2019). Criminal law regulation of liability for suicide in the Russian criminal legislation: the past and present. *Actual Problems of Russian Law*, (11), 81-95.
10. Buribayev, Y. A., Khamzina, Z. A., Suteeva, C., Apakhayev, N. Z., Kussainov, S. Z., & Baitekova, K. Z. (2020). Legislative regulation of criminal liability for environmental crimes. *Journal of Environmental Accounting and Management*, 8(04), 323-334.