ПРЕСТУПЛЕНИЯ С ЭЛЕКТРОННЫМИ СРЕДСТВАМИ ПЛАТЕЖА И НЕКОТОРЫЕ ОСОБЕННОСТИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

CRIMES WITH ELECTRONIC MEANS OF PAYMENT AND SOME FEATURES OF ELECTRONIC EVIDENCE

A. Khodusov

Summary. the article discusses the relationship of the development of the digital economy and forms of electronic commerce with the growth of crime in this area. The types of IT crimes, including crimes with electronic means of payment, are considered. The special specificity of the expression of these criminal acts in the material and digital world is revealed.

A study of the concept and characteristics of electronic evidence, the criteria for their admissibility. Identified certain problems of evidentiary nature.

Keywords: digital economy, cybercrime, electronic means of payment, electronic evidence, classification.

Ходусов Алексей Александрович
К.ю.н., доцент, Международный юридический институт
yustas-73@mail.ru

Аннотация. в статье рассмотрена взаимосвязь развития цифровой экономики и форм электронной торговли с ростом преступности в данной сфере. Рассмотрены виды IT-преступлений, в том числе преступления с электронными средствами платежа. Выявлена особая специфика выражения указанных преступных деяний в материальном и цифровом мире.

Проведено исследование понятия и особенностей электронных доказательств, критерии их допустимости. Выявлены определенные проблемы доказательственного характера.

Ключевые слова: цифровая экономика, киберпреступность, электронное средство платежа, электронные доказательства, классификация.

Сегодня интернет является наиболее важным источником информации, существенная часть контактов и передачи информации осуществляется в электронном виде, в целях обеспечения хранения данных последние оцифровываются.

Цифровая экономика открывает возможности для появления и внедрения новых альтернативных форм оплаты. Это, например, электронные платежные средства, к которым относятся платежные карты, электронные кошельки и программные продукты, так называемые виртуальные деньги. Электронные деньги сегодня во многих странах все еще находится на стадии разработки и постепенного тестирования. Его использование и рост в мировом масштабе ожидается создание соответствующей законодательной среды.

Недостаточное развитие правовой базы электронных торговых отношений вызывает рост преступности в данном направлении.

Согласно статистическим данным, в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65~<949 до 90~<587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% — это почти каждое 20 преступление [10]. Уже в 2018 году Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в РФ в 2018 году. За январь — сентябрь 2018 года правоохранительными органами РФ зарегистрировано 121 тыс. 247 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [13].

В современную эпоху, преступления также имеют цифровое измерение. Они либо совершаются с использованием цифрового оборудования, либо информация, касающаяся преступлений, находится в электронном формате. Эти преступления, совершенные с использованием средств информационно-коммуникационных технологий, в том числе компьютеров, сетей, мобильных телефонов и других электронных средств или инструментов называются киберпреступлениями.

Под киберпреступностью понимают противозаконную деятельность, совершаемую посредством электронных устройств и сети интернет, направленных на нарушение личных прав и свобод граждан [8].

В зависимости от сфер совершения преступлений, в которых используются информационно-коммуникационные технологии, можно выделить следующие группы [9]:

- преступления, совершаемые в сфере дистанционного банковского обслуживания и электронной коммерции, которые, используя специализиро-

ванную терминологию, можно обозначить как преступления, совершаемые с использованием электронных средств платежа;

- преступления, совершаемые в отношении информационно-коммуникационных технологий и установленного законом порядка их оборота;
- иные преступления, совершаемые в сфере информационно-коммуникационных технологий, при совершении которых использование информационно-коммуникационных технологий не является обязательным признаком объективной стороны, так называемые «традиционные» преступления.

Необходимо отметить, что преступления, совершаемые с использованием электронных средств платежа, составляют основной массив IT-преступлений [11].

На законодательном уровне под электронным средством платежа понимают средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств [3].

На сегодняшний день основными нормами отечественного уголовного законодательства, ориентированными на противодействие посягательствам, совершаемым с использованием электронных средств платежа, являются нормы, содержащиеся в ст.ст. 158, 159.3, 159.6 УК РФ, то есть деяния квалифицируются как различные виды хищений [4].

Преступления, совершенные с использованием электронных платежных средств и систем, имеют специфику по способам совершения, которая основывается на закономерных особенностях, присущих сфере электронных платежей:

1. правовое регулирование осуществляется несколькими отраслями права: гражданским, банковским, уголовным, информационным и др.;
2. применяется категория «виртуальный» документ, который имеет особый правовой статус и форму представления;
3. функционирование электронных систем имеет свои технические особенности, которые позволяют выявлять «виртуальный след» преступлений;
4. вовлеченность сетевых серверов в процесс совершения преступлений, что увеличивает круг лиц, подозреваемых в преступлении.

Указанные особенности рассматриваемых преступлений, взаимосвязи отдельных элементов их криминалистической классификации мы выделили два типичных способа совершения преступлений, совершенных с использованием электронных платежных средств и систем:

- Использование уязвимости электронной платежной системы без неправомерного использования реквизитов доступа ее легального пользователя;
- Неправомерное использование реквизитов доступа легального пользователя электронной платежной системы [12].

Информация, относящаяся к любому преступлению, которая хранится или передается в цифровой форме, называется электронными доказательствами.

Таким образом, в судебном процессе или уголовном преследовании доказательства часто встречаются и собираются в цифровом виде от услуг цифровой связи и / или цифровых носителей информации. Доказательства в электронной форме служат тем же целям что и традиционные доказательства.

Формальные правила, касающиеся допустимости электронных доказательств, различаются в разных правовых системах, тем не менее, в основном рассматривают шесть таких критериев во время их оценки: допустимость, аутентичность, точность, полнота, доказательность в суде, законность получения [7].

Анализ научных публикаций позволил выделить некоторые отличия традиционных доказательств от электронных:

Во-первых, трудно изменить структуру традиционных / физических доказательств. При этом, электронные данные могут изменяться в пределах компьютера и/или линии передачи в любой момент времени.

Во-вторых, в случае изменения (воздействия в целях сокрытия) физических доказательств вероятнее всего останутся следы воздействия или, по крайней мере, изменения будут заметны, однако электронные доказательства могут быть легко обнаружены.

В-третьих, электронные доказательства можно гораздо легче изменить или исказить, чем физические доказательства в процессе сбора.

В-четвертых, традиционные доказательства могут быть найдены (восприняты) с первого взгляда, в то время как поиск и выявление большинства непосредственных электронных доказательств могут быть обнару-

жены либо специалистами в сфере информационных технологий, либо специальными компьютерными программами.

В российской правовой литературе проблема классификации электронных доказательств не стала предметом активных научных изысканий, что объясняется неразработанностью вопроса общей допустимости компьютерных доказательств в целом [5].

Анализ имеющихся научных публикаций позволил выделить несколько критериев классификации электронных доказательств [6]:

1. по происхождению: данные, которые хранятся на электронных носителях и доказательство, созданное компьютером в соответствии с заложенной программой;
2. по сущности доказательств: исходные данные, базы данных, Коды, необходимые для расшифровки электронной информации, особенности алгоритма программирования или обработки данных, программное обеспечение коммерческого характера, компьютерные системы;
3. по форме представления: твердая (или жесткая) копия (hard copy) и машиночитаемая копия.

Для электронных доказательств существуют некоторые вопросы конфиденциальности, касающиеся их сбора. Так, согласно второму пункту статьи 8 Европейской конвенции по правам человека в демократическом обществе в интересах национальной безопасности, общественной безопасности или экономического благополучия страны, для предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или для защиты прав и свобод других может иметь место вмешательство в осуществление права на неприкосновенность частной жизни [1].

Государства, подписавшие Конвенцию о киберпреступности, должны обеспечивать условия и безопасность, которые обеспечивают надлежащую защиту прав человека, в частности право на конфиденциальность [2]. Примечательно, что Россия не подписала указанную конвенцию, что рождает проблемы с обеспечением конфиденциальности сбора электронных доказательств в РФ в той форме, в которой это представляется на международном уровне.

Помимо законодательных проблем, первая трудность в применении электронных доказательств заключается в том, что географический охват электронного поиска нелегко определить. Чтобы избежать такой проблемы, необходимо обеспечивать разработку методологической базы для работы с такого рода доказательственной базой, а также обучение сотрудников правоохранительных органов по соответствующему направлению.

Трудности также вызывает неопределенность предмета и объекта поиска, их фактического расположения в сети и критерии обнаружения.

Сегодня уровень подготовки лиц, осуществляющих раскрытие и расследование рассматриваемых деяний, недостаточен, поэтому требуется регулярное повышение их квалификации.

Таким образом, развитие цифровой экономики и форм электронной торговли стало причиной роста преступности в данной сфере. Одним из видов IT-преступлений являются преступления с электронными средствами платежа, которые имеют особую специфику выражения в материальном и цифровом мире. Эти специфические черты должны лежат в основе методологических аспектов расследования и доказывания данного типа преступлений.

В основе таких стадий уголовного процесса лежат электронные доказательства, которые должны быть в пределах определенных критериев допустимости. Вместе с тем, существуют определенные проблемы доказательственного характера, которые также следует устранять в целях обеспечения обвинения в суде и соблюдения прав, интересов и правовых границ конфиденциальности информации.

Особое значение в расследовании данного типа преступлений имеет профессионализм работников правоохранительных органов, который следует постоянно поддерживать в соответствии с уровнем развития IT-отрасли.

ЛИТЕРАТУРА

1. Конвенция о защите прав человека и основных свобод ETS № 005 (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г.) / Собрание законодательства Российской Федерации от 8 января 2001 г., № 2, ст. 163,
2. Конвенция о преступности в сфере компьютерной информации ETS N185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс] Режим доступа: https://base.garant.ru/2564796/.
3. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 28.11.2018) / Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 03.08.2018.

4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 01.04.2019) / Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 01.04.2019.
5. Вехов В. Б. Электронные доказательства: проблемы теории и практики / Правопорядок: история, теория, практика. 2016. № 4 (11). С. 46–50.
6. Иванов Н. Допустимость компьютерных доказательств в процессуальном праве / [Электронный ресурс] — Режим доступа: http://www.blog.servitutis.ru/?p=88.
7. Овчинникова О. В. Собирание электронных доказательств, размещенных в сети интернет / Правопорядок: история, теория, практика. 2016. № 4 (11). С. 67–70.
8. Робул В. И. К вопросу о проблемах расследования киберпреступлений // Научное сообщество студентов: междисциплинарные исследования: сб. ст. по мат. LVI междунар. студ. науч.-практ. конф. № 21(56). [Электронный ресурс] — Режим доступа: https://sibac.info/archive/meghdis/21(56).pdf.
9. Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. 2015. № 3 (33). С. 127–132.
10. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий [Электронный ресурс] Режим доступа: https://genproc.gov.ru/smi/news/news-1431104/.
11. Отчет о тенденциях высокотехнологичных преступлений за 2018 год [Электронный ресурс] Режим доступа: https://www.group-ib.ru/resources/threat-research/2018-report.html.
12. Способы совершения преступлений с использованием электронных платежных средств и систем [Электронный ресурс] Режим доступа: http://kreditp.ru/kreditniy-pomoshnik/94-prestupleniya-elektronnye-platezhnye-sistemy.html.
13. Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в РФ в 2018 году [Электронный ресурс] Режим доступа: https://tass.ru/proisshestviya/5733551.

© Ходусов Алексей Александрович (yustas-73@mail.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»