УДК: 343.71; 343.72
DOI: 10.35750/2071-8284-2020-3-98-105

Е. А. Маркова
адъюнкт
Санкт-Петербургский университет МВД России
Российская Федерация, 198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1
ORCID: 0000-0002-7049-8380. E-mail: markovaespb@yandex.ru

Регламентация ответственности за преступления, совершённые с использованием электронных средств платежа, в законодательстве стран романо-германской правовой семьи

Аннотация: Статья посвящена исследованию вопросов регламентации уголовной ответственности за преступления, совершённые с использованием электронных средств платежа, относящихся к киберпреступлениям, в законодательстве отдельных зарубежных стран романо-германской правовой семьи. В статье отмечается, что романо-германская правовая семья значительно отличается от иных семей не только тем, что обладает в силу исторических традиций многими признаками права древнеримской юриспруденции, но и правовыми особенностями уголовного законодательства в отношении киберпреступности. Отмечается актуальность проблематики киберпреступности, ее дифференциация, основанная на Конвенции о преступности в сфере компьютерной информации (ETS № 185), и об особенностях уголовной регламентации преступлений, совершенных с использованием электронных средств платежа в Швеции, Германии, Франции, Испании, Нидерландах, в Китайской Народной Республике, в странах Балтии. Обозначено, что вопросы противодействия подобным преступлениям имеют особое значение во всех странах романо-германской правовой семьи. Несмотря на различия в позициях законодателей в отношении криминализации деяний, совершенных с использованием электронных средств платежа, во всех странах посягательства на собственность рассматриваются как посягательства на основы государства, а защита от подобных посягательств является одной из важнейших государственных функций. Отмечено, что уголовные кодексы большинства государств включают правовые нормы в отношении: компьютерного мошенничества, компьютерного хищения; получения информации, составляющей коммерческую и банковскую тайну, путём неправомерного доступа к компьютерной информации (коммерческий, банковский шпионаж); вымогательства с использованием средств компьютерной техники. Указано, что первый шаг в направлении уголовно-правовой охраны компьютерной информации, развития уголовного законодательства по противодействию экономической киберпреступности был сделан в Швеции в Законе о компьютерных преступлениях (1973 г.).

Ключевые слова: романо-германская правовая семья, преступление, киберпреступление, мошенничество, обман, кража, компьютерная информация, уголовное законодательство, противодействие.

Для цитирования: Маркова Е. А. Регламентация ответственности за преступления, совершённые с использованием электронных средств платежа, в законодательстве стран романо-германской правовой семьи // Вестник Санкт-Петербургского университета МВД России. – 2020. – № 3 (87). – С. 98–105. DOI: 10.35750/2071-8284-2020-3-98-105.

Elena A. Markova
Graduated
Saint-Petersburg University of the MIA of Russia
1, Pilyutova str., Saint Petersburg, 198206, Russian Federation
ORCID: 0000-0002-7049-8380. E-mail: markovaespb@yandex.ru

Regulation of liability for offences committed with the use of electronic funds of payment in the legislation of the countries of Romano-Germanic of legal system

Annotation: The article is devoted to the study of the regulation of criminal liability for crimes committed using electronic means of payment related to cybercrime in the legislation of certain foreign countries of the Romano-Germanic legal family. The article notes that the Romano-German legal system is significantly distinguished from other families not only by the fact that it possesses, due to historical traditions, many characteristics of the law of ancient Roman jurisprudence, but also by the legal peculiarities of criminal legislation on cybercrime. The relevance of cybercrime, its differentiation based on the Convention on Crime in the Field of Computer Information (ETS No. 185) and the peculiarities of the criminal regulation of crimes committed using electronic means of payment in Sweden, France, Germany, Spain, Netherlands, China and the Baltic States are noted. It is pointed out that the issues of combating such crimes are of particular importance in all countries of the Romano-Germanic legal family. Despite differences in the position of legislators with regard to the criminalization of acts committed by electronic means of payment, in all countries attacks on property are considered as attacks on the foundations of the State, and protection against such attacks is one of the most important State functions. It is noted that the criminal codes of most States include rules on computer fraud, computer theft; Obtaining information constituting commercial and banking secrecy through improper access to computer information (commercial, banking espionage); Extortion using computer equipment. It is stated that the first step towards criminal law protection of computer information, development of criminal legislation to counter economic cybercrime was taken in Sweden in the Law on Computer Crimes (1973).

Keywords: Romano-Germanic legal system, crime, cybercrime, fraud, deception, theft, computer information, criminal legislation, counteraction.

For citation: Markova E. A. Regulation of liability for offences committed by using electronic means of payment in the legislation of the Romano-Germanic legal system countries // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2020. – № 3 (87). – P. 98–105. DOI: 10.35750/2071-8284-2020-3-98-105.

Общепризнанной является позиция, признающая значимость и классификацию правовых семей (систем), место правовой семьи на юридической карте мира, сформированная Р. Давидом, выделившим две «великие» правовые семьи: романо-германскую (система континентального права), к которой принадлежат многие европейские страны, в частности, Россия, Германия, Франция, Нидерланды, Испания, Швейцария и др., и семью англо-американского (англо-саксонского права) (система общего права), к которой принадлежат США, Великобритания и др. [1, с. 163].

Исторические источники указывают, что к романо-германской правовой семье относятся государственные системы, имеющие своим истоком государства континентальной Европы. Данная правовая семья имеет специфику, связанную с наличием кодифицированных актов ведущих отраслей материального и процессуального права (уголовное, гражданское); с дифференциацией материального права на частное и публичное с констатацией принципа первостепенности материального права по отношению к процессуальному праву. В качестве основного источника действующего права государств романо-германской правовой семьи признан закон, который не отожествляется с правом, а законопорядок, складывающийся на основе строгого и неуклонного соблюдения требований, содержащихся в законе, никогда не рассматривался как синоним правопорядка[1].

Основные принципы построения романо-германской правовой семьи положены в основу уголовного законодательства, которое включает в себя и киберпреступность. В докладе Совета Европы об актуальной проблематике в сфере киберпреступности в целом и о её дифференциации, сформированной в соответствии с Конвенцией о преступности в сфере компьютерной информации (ETS № 185)[2], данный вид преступлений отмечен в качестве «CIA-offences», т.е. деяния, совершенного против конфиденциаль-

[1] Саидов А. Х. Сравнительное правоведение (основные правовые системы современности) : учебник / под ред. В. А. Туманова. – Москва: Юристъ, 2003. – С. 144.

[2] Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23 ноября 2001 г.) (с изм. от 28 января 2003 г.) [Электронный ресурс] // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/online/ (дата обращения: 10.02.2020).

ности (Confidentiality), целостности (Integrity) и доступности (Availability) компьютерных данных, инновационных систем. В числе видов преступлений, включённых в категорию киберпреступлений, указаны: хакерство, перехват сообщений, обман пользователей интернета (в т. ч., посредством спуфинга, фишинга), компьютерный шпионаж (в т. ч. использование троянских коней и иных подобных технологий), компьютерный саботаж и вымогательство (в т. ч. использование вирусов и червей, ДОС-атаки, спамминг и мейлбомбинг).

Вопросы противодействия подобным преступлениям имеют особое значение во всех странах романо-германской правовой семьи. Несмотря на различия в позиции законодателей в отношении криминализации деяний, совершённых с использованием информационно-коммуникационных технологий, во всех цивилизованных странах посягательства на собственность рассматриваются в качестве подрыва основ государства, а защита от подобных посягательств – одна из важнейших государственных функций[3]. В этой связи уголовные кодексы большинства государств романо-германской правовой семьи включают нормы в отношении: компьютерного мошенничества, компьютерного хищения; получения информации, составляющей коммерческую и банковскую тайну, путём неправомерного доступа к компьютерной информации (коммерческий, банковский шпионаж); вымогательства с использованием средств компьютерной техники[4].

На современном этапе подобные преступные посягательства направлены против отношений собственности, причиняя существенный вред социально-экономической сфере различных стран и отдельным гражданам[5].

Эволюция законодательства зарубежных стран демонстрирует, что первый шаг в направлении уголовно-правовой охраны компьютерной информации, развития уголовного законодательства по противодействию экономической киберпреступности сделан законодателем Швеции с принятием Закона о компьютерных преступлениях (1973 г.)[6]. Данным нормативным правовым актом предусмотрена уголовная ответственность: за противоправное проникновение в систему компьютерной сети; за ввод в компьютерную информацию дезинформации; за совершение хищения таких объектов, как денежные средства (электронные), а также ценные бумага, другие виды имущества и прочие, включая услуги и ценную для определённых кругов информацию. Законом о данных (1974 г.)[7] в уголовное законодательство введена категория «злоупотребление при помощи компьютера».

В начале 90-х гг. XX в. в связи с активизацией киберпреступлений Уголовный кодекс Швеции[8] одним из первых был дополнен положениями, предусматривающими уголовную ответственность за преступления, совершенные с применением компьютерной информации и информационных технологий: за мошенничество, совершенное предоставлением либо неполной, либо неправдоподобной информации, или внесением корректив в компьютерную программу либо в отчётность. Необходимо указать также деяние, совершаемое путём незаконного влияния на непосредственный результат автоматичной обработки компьютерной информации, иной тождественной обработки, повлёкшей выгоду для субъекта преступления и убытки для жертвы. Данную совокупность пополняют: правонарушение, связанное с почтовой или коммуникационной тайной; применение технических механизмов с намерением оказать противоправное влияние на тайну телекоммуникационного свойства; противоправный доступ к процессам по обработке компьютерных данных; противозаконная корректировка, устранение, добавление определённой записи в реестр данных; некоторые иные.

Уголовный кодекс Швеции в ст. 4 гл. 8 «О краже, разбое и других преступлениях, связанных с похищением имущества» регламентирует условия, в соответствии с которыми кража признается крупной, т.е. более тяжким преступлением. Данный факт имеет особое значение в связи с развитием информационных технологий: с 2012 г. в Швеции активно применяется мобильное приложение Swish для Android, иные операционные системы, которые устанавливаются на мобильный телефон и применяются в качестве терминала, коррелирующего счёт в банке с мобильным телефоном, что позволяет осуществить мгновенный платёж, указав любой зарегистрированный в системе ID либо номер

[3] Бойко С. Я. Уголовная ответственность за мошенничество: теоретико-прикладное исследование : дис. … канд. юрид. наук: 12.00.08 / Бойко Сергей Яковлевич. – Москва, 2019. – С. 80.

[4] Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. ... канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. - Москва, 2016. – 28 с.

[5] Саидов А.Х. Указ. соч. – С. 154.

[6] Закон о компьютерных преступлениях (Швеция) от 2 апреля 1973 г. [Электронный ресурс] // Сайт «Law Library of Congress» («Юридическая библиотека Конгресса США»). – URL: http://www.loc.gov/law/help/guide/nations/sweden.php (дата обращения: 10.02.2020).

[7] Закон о данных (Швеция) от 4 апреля 1973 г. [Электронный ресурс] // Сайт «Law Library of Congress» («Юридическая библиотека Конгресса США»). – URL: http://www.loc.gov/law/help/guide/nations/sweden.php (дата обращения: 10.02.2020).

[8] Уголовный кодекс Швеции 1962 г. [Электронный ресурс] // Сайт «Law Library of Congress» («Юридическая библиотека Конгресса США»). – URL: http://www.loc.gov/law/help/guide/nations/sweden.php (дата обращения: 10.02.2020).

телефона[9]. Соответственно, кража мобильного телефона может способствовать краже с банковского счета, равно как в отношении электронных денежных средств и квалифицироваться в качестве кражи на основании ст. 4 гл. 8 «О краже, разбое и других преступлениях, связанных с похищением имущества» УК Швеции.

В Уголовном кодексе Нидерландов[10] законодатель группирует преступления по обману, как способу совершения преступления, выделяя для данных деяний отдельный раздел XXV Уголовного кодекса «Обман», включающий 18 статей. В соответствии с нормами данного акта, к уголовной ответственности привлекаются субъекты, которые с целью извлечь противоправным способом доходы лично для себя либо для других лиц путём присвоения неправдоподобного имени, или путём неправдивой информации, склоняют жертву к отказу от объекта права собственности, представить сведения о денежных средствах, принять долговые обязательства либо отказаться от предъявленных претензий. Данная норма Уголовного кодекса применяется при обмане, совершённом с применением платёжной карты. В отдельные нормы Кодекса, предусматривающие ответственность за такие деяния традиционного характера, как вымогательство, а также кража, совершённая обманным способом, в связи с совершенствованием высоких технологий внесены дополнения об ответственности за деяния, совершенные проникновением к компьютерной информации, которая находится на электронных системах, включая электронные средства платежа, в т. ч. это касается и платёжных карт.

Уголовный кодекс Испании[11], структурно состоящий из трех отдельных Книг, в Книге II содержит раздел XIII «Преступления против собственности и социально-экономической деятельности». Уголовный кодекс выделяет простое, квалифицированное мошенничество, мошенничество в сфере электроснабжения, в сфере кредитования, завладение чужим имуществом обманом с помощью компьютерных программ, кредитных карт, чеков. В соответствии со ст. 253 УК Испании, уголовной ответственности подлежит лицо, которое с целью наживы присваивает потерянную вещь либо вещь, собственник которой на момент совершения преступления неизвестен, – соответственно, кража платежной карты подлежит квалификации по данной норме уголовного закона.

В Германии система уголовного права признана достаточно сложной и разнообразной ввиду многочисленности и многоуровневости источников данной отрасли правовой системы. Уголовный кодекс Германии, несмотря на отсутствие дефиниции «уголовное наказание», определяемой в доктрине как справедливая компенсация за вину (Schuldausgleich), как особое государственное средство предупреждения преступлений и возмещения ущерба жертве [3, с. 117], уделяет особое внимание преступлениям, совершаемым в сфере использования информационно-коммуникационных технологий, в т. ч. экономическим киберпреступлениям[12]. Данный кодифицированный акт в разделе 22 Особенной части УК Германии «Мошенничество и злоупотребление доверием» содержит отдельные нормы, предусматривающие ответственность за различные виды мошенничества и злоупотребления доверием (§ 263a «Компьютерное мошенничество», § 264 «Получение субсидий мошенническим путём», § 264a «Мошенничество при капиталовложении», § 265 «Злоупотребление при страховании», § 265a «Получение услуг путём обмана», § 266 «Злоупотребление доверием», § 266a «Утаивание и растрата заработной платы», § 266b «Злоупотребление с чеками и кредитными картами»), фундаментальные основы которых содержатся в диспозиции § 263 УК Германии «Мошенничество».

В соответствии с § 263 УК Германии, «кто, намереваясь получить для себя или третьего лица противоправную имущественную выгоду, причиняет вред имуществу другого лица тем, что вводит в заблуждение или поддерживает это заблуждение, утверждая заведомо ложные факты или искажая, или скрывая подлинные факты, наказывается…». В качестве момента окончания преступления признается момент причинения вреда имуществу потерпевшего, а не момент обогащения виновного или иного третьего лица. Ущерб возникает исключительно тогда, когда изымается либо часть имуществ потерпевшего, либо ущерб отягощается обязательствами и тем самым уменьшается стоимость подобного имущества в целом [3, с. 450]. В качестве способа совершения деяния данная норма Уголовного кодекса Германии предусматривает обман.

Исходя из законодательной конструкции мошенничества, многие виды подобных преступлений (§ 263a «Компьютерное мошенничество»,

[9] Безналичное общество в Швеции: даже Бог принимает карточку [Электронный ресурс] // Сайт «Mobium». – RL: https://mobiumapps.com/beznalichnoe-obshhestvo-v-shvecii-dazhe-bog-prinimaet-kartochku/ (дата обращения: 10.02.2020).

[10] Уголовный кодекс Нидерландов от 3 марта 1881 года [Электронный ресурс] // Сайт «Российский правовой портал: Библиотека Пашкова». – URL: http://constitutions.ru/archives/5854 (дата обращения: 10.02.2020).

[11] Уголовный кодекс Испании 1995 г. [Электронный ресурс] // Сайт «Crimpravo.ru – научная сеть». – URL: http://crimpravo.ru (дата обращения: 10.02.2020).

[12] Уголовное Уложение (Уголовный кодекс Германии) (Strafgesetzbuch, StGB) от 15 мая 1871 г. [Электронный ресурс] // Сайт «Российский правовой портал: Библиотека Пашкова». – URL: http://constitutions.ru/archives/5854 (дата обращения: 10.02.2020).

§ 266b «Злоупотребление с чеками и кредитными картами») и новые составы преступлений, охватывающие наиболее опасные деяния, активизирующиеся в сфере информационно-коммуникационных технологий (§ 202-a «Действия, направленные на получение сведений», § 303-a «Изменение данных», § 303-6 «Компьютерный саботаж» и § 269 «Подделка данных, имеющих доказательственное значение») включены законодателем в Уголовный кодекс следующими законами: от 15 мая 1985 г. – Вторым законом «О борьбе с экономической преступностью»[13] и от 22 декабря 2003 г. – Тридцать пятым законом о внесении изменений в уголовное законодательство[14] (в связи с имплементацией Германией решения Совета Европейского Союза «О борьбе с обманными действиями и подделкой в отношении безналичных средств платежа», принятого 28 мая 2001 г.[15]).

Параграф 263a УК Германии, устанавливающий уголовную ответственность за компьютерное мошенничество, предусматривает: «Кто действует с целью получения для себя или третьего лица противоправной имущественной выгоды и этим наносит вред имуществу другого лица тем, что он воздействует на результат обработки данных ЭВМ, составляя неправильные программы, используя неправильные или неполные данные, неправомочно применяя данные или влияя на такой процесс каким-либо иным неправомочным воздействием, наказывается лишением свободы до пяти лет или штрафом».

Данное преступление является наиболее опасным из компьютерных преступлений. В качестве виновного выступает лицо, которым с целью извлечения имущественной выгоды, как в отношении себя, так и иного лица, причинен вред имуществу, осуществлено воздействие на результаты обработки данных путём неправильного создания компьютерных программ, иного противозаконного воздействия на результат обработки: введение в компьютер недостоверных, неполных данных, неправомерное использование данных либо умышленное, превышающее полномочия воздействие на ход процесса обработки [4]. В качестве способа совершения деяния выступает не обман, а оказание негативного информационного воздействия: в первом случае воздействие оказывается на человека (потерпевшего, иное связанное с ним лицо), во втором – на процесс обработки данных, производимый при помощи компьютерных технологий.

В соответствии с § 266b УК Германии «Злоупотребление чековыми и кредитными картами» предусмотрена уголовная ответственность за злоупотребление доверием кредитной организации, выпустившей чековую или кредитную карту, которое оказано лицу, получившему подобную карту на законных основаниях. Исходя из законодательной конструкции данной нормы, «Кто злоупотребляет возможностями, предоставленными ему чековой или кредитной картой, и этим принуждает владельца карты произвести оплату, нанося ему ущерб, наказывается лишением свободы на срок до трех лет или денежным штрафом». При совершении мошенничества лицо злоупотребляет доверием банка, выпускающего платежные карты, используя в обороте более значительные суммы, чем ему доверено [3, с. 451]. Подобное преступление имеет направленность на причинение ущерба охраняемому благу – имуществу, способствуя наступлению негативных правовых последствий.

Уголовный кодекс Германии проводит, однако, различие между преступлениями, совершенными в сфере компьютерного мошенничества, в сфере незаконных действий с чеками и с кредитными картами, и деяниями имущественного характера, которые совершены обманным путём, а также злоупотребления доверием, определив данные преступления в самостоятельный параграф национального кодифицированного источника права.

Данным преступлениям особое внимание уделено в нормативных правовых актах других государств романо-германской правовой семьи.

Уголовный кодекс Франции 1992 г.[16] изменил систему правовых норм о юридической ответственности за преступления и проступки против собственности, отграничив формы посягательств, сформировав признаки таких преступлений, ужесточив санкции за проступки и преступления [5, с. 170]. Французское законодательство, регламентируя простую кражу и кражу отягощенную (гл. I Книги III УК Франции), предусматривая квалифицирующие признаки деяния, не включает в её дифференциацию кражу с банковского счёта, равно как в отношении

[13] Второй закон «О борьбе с экономической преступностью» от 15 мая 1986 года (ФРГ) [Электронный ресурс] // Сайт «Российский правовой портал: Библиотека Пашкова». – URL: http://constitutions.ru/archives/5854 (дата обращения: 10.02.2020).

[14] Тридцать пятый закон о внесении изменений в уголовное законодательство от 22 декабря 2003 года (ФРГ) [Электронный ресурс] // Сайт «Российский правовой портал: Библиотека Пашкова». – URL: http://constitutions.ru/archives/5854 (дата обращения: 10.02.2020).

[15] Рамочное решение Совета Европейского союза «О борьбе с обманными действиями и подделкой в отношении безналичных средств платежа» от 28 мая 2001 года № 2001/413/JHA Рамочное решение Совета Европейского союза «О борьбе с обманными действиями и подделкой в отношении безналичных средств платежа» от 28 мая 2001 г. № 2001/413/JHA [Электронный ресурс] // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/online/ (дата обращения: 10.02.2020).

[16] Уголовный кодекс Франции (CodePénal) от 22 июля 1992 г. [Электронный ресурс] // Сайт «Российский правовой портал: Библиотека Пашкова». – URL: http://constitutions.ru/archives/5854 (дата обращения: 10.02.2020).

электронных денежных средств. В Уголовном кодексе Франции предусмотрены отдельные нормы об уголовной ответственности за преступления в сфере информационно-коммуникационных технологий.

Уголовный кодекс Франции, не включающий специальных правовых норм о хищении с банковского счета, равно как и в отношении электронных денежных средств, обеспечивает, соответственно, уголовно-правовую охрану как личных данных и телекоммуникационных систем, так и устанавливает уголовную ответственность за совершение мошеннических посягательств, которые могут применяться в отношении электронных денежных средств. Вопросы уголовной ответственности в отношении хищения электронных денежных средств решены во Франции на уровне специального нормативного правового акта – Закона № 91-1383 «О безопасности чеков и платежных карточек»[17], предусматривающего уголовную ответственность за следующий вид обмана: за подделку, переделывание и сознательное использование платежной карты, за сознательное волеизъявление принять неправомерную оплату подобной картой [5, с. 170]. Одновременно данным источником права на держателя платежной карты (до момента уведомления о потере или краже) возлагается уголовная ответственность за убытки, причинённые её несанкционированным использованием (в объёме до 150 евро). Подобная норма не применяется, однако, при наличии неосторожности, грубой ошибки держателя платежной карты, а также при отсутствии уведомления о блокировании карты [6, с. 47].

Уголовным кодексом Китайской Народной Республики[18] преступлениям, совершённым в форме мошенничества (мошенничество и мошеннические деяния), посвящено 15 статей (ст. 167, 187, 192–198, 266, 269, 287, 319, 382, 406). Принимая во внимание структуру Уголовного кодекса Китая, включающего Общую и Особенную части, каждая из которых дифференцирована на титулы (разделы) и соответствующие статьи, мошенничество и мошеннические деяния не связаны родовым признаком и располагаются в различных титулах (разделах) УК: преступления против социалистической рыночной экономики (ст. 140–231), преступления против собственности (ст. 263–276), против порядка управления (ст. 277–367), против коррупции (ст. 382–396), должностные преступления (ст. 397–419).

В соответствии со ст. 265 УК КНР, «незаконное завладение каналами связи других людей, дублирование чужого номера электронной почты или пользование заведомо похищенными, дублированными электронными оборудованием и устройствами с целью извлечения прибыли, – наказываются в соответствии со статьей 264 настоящего Кодекса», т.е. данное преступление по степени общественной опасности приравнено к хищению государственного или частного имущества, совершенному в крупном размере или многократно. Соответственно, ответственность установлена за осуществление мошеннической деятельности с кредитными картами, совершённое в особо крупном размере, при иных особо отягчающих обстоятельствах.

Государства Балтии, которые принадлежат к романо-германской правовой семье, вошли в состав Европейского союза (ЕС) в 2004 г. в ходе масштабного пятого расширения интеграционной группы на страны Восточной Европы [7, с. 8]. Процесс политической интеграции балтийских государств был реализован через комплекс экономических и правовых мероприятий, в т. ч. в рамках противодействия киберпреступности. Данными государствами в 2001 г. была ратифицирована Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Conventionon Cybercrime CETS)[19], установлена уголовная ответственность за киберпреступления и иные уголовно-наказуемые деяния, связанные с оборотом электронных средств платежа (мошенничество).

Информация в странах Балтии, как и во всем цивилизованном мире, является ключевой составляющей развития общества, однако преступники умело пользуются недостатками в обеспечении безопасности в сфере применения современных средств связи, сети интернет, совершения киберпреступления, которые наносят вред обществу и гражданам [8, с. 220].

В Эстонской Республике положениями Пенитенциарного кодекса[20] в подразделе 1 «Мошенничество» раздела 2 «Преступные деяния против имущества в целом» (ст. 210–213 УК Эстонии) регламентирована уголовная ответственность за мошенничество. В ст. 209 УК Эстонии раскрывается дефиниция общего мошенничества

[17] Закон от 30 декабря 1991 года № 91-1383 «О безопасности чеков и платежных карточек» (Франция) (в ред. от 01.01.2200 г.) [Электронный ресурс] // Сайт «Российский правовой портал: Библиотека Пашкова». – URL: http://constitutions.ru/archives/5854 (дата обращения: 10.02.2020).

[18] Уголовный кодекс Китайской Народной Республики от 14 марта 1997 года [Электронный ресурс] // Сайт «LawInfoChina.com». – URL: http://www.lawinfochina.com/ (дата обращения: 10.02.2020).

[19] Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003) [Электронный ресурс] // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/online/ (дата обращения: 10.02.2020).

[20] Пенитенциарный кодекс Эстонской Республики от 06 июня 2001 года (ред. от 01.01.2020) [Электронный ресурс] // Сайт «Jurist Aitab» («Юрист помогает»). – URL: https://v1.juristaitab.ee/sites/www.juristaitab.ee/ (дата обращения: 10.02.2020).

как «причинение другому лицу имущественного вреда путём создания заведомо ложного представления о фактических обстоятельствах с целью получения имущественной выгоды». Законодатель Эстонской Республики разграничивает путём введения дифференциации специальные виды мошенничества: мошенничество при получении льгот (ст. 210), инвестиционное мошенничество (ст. 211), страховое мошенничество (ст. 212) и компьютерное мошенничество (ст. 213). Данная категория определяется как «причинение имущественного вреда другому лицу путём незаконного ввода, изменения, удаления, порчи, блокирования компьютерных программ, данных, путём незаконного вмешательства в процесс обработки данных иным способом с целью получения имущественной выгоды» (ст. 213). При этом Пенитенциарный кодекс не предусматривает уголовно-правовых норм о хищении чужого имущества, приобретении права на подобное имущество, устанавливая уголовную ответственность за причинение имущественного вреда или получение имущественной выгоды.

Латвийский законодатель (ст. 177.1 УК[21]) аналогично эстонской позиции (ст. 213 УК Эстонии) устанавливает уголовную ответственность за компьютерное мошенничество, как за преступление, совершённое путём сознательного введения недостоверных сведений в систему автоматизированной обработки данных (незаконное вмешательство в процесс обработки).

В Уголовном кодексе Литовской Республики[22] в главе XVIII «Преступные деяния в отношении собственности» содержится норма права (ст. 177.1 УК), ч. 1 которой предусматривает уголовную ответственность за умышленное посягательство на собственность или на имущественные права либо обязательства путём введения ложных данных в автоматизированную систему обработки данных. Уголовная ответственность за противозаконное использование электронных средств платежа установлена в гл. XXXII УК Литвы «Преступления и уголовные проступки против финансовой системы». В ст. 215 УК предусмотрена уголовная ответственность за заведомо противозаконное использование средства платежа, за незаконную передачу данных его идентификации, за использование подлинных и подложных данных идентификации при инициации, при совершении финансовой операции электронным средством платежа.

Уголовным кодексом Литовской Республики состав мошенничества предусмотрен в ст. 182 гл. XXVII «Преступления и уголовные проступки против собственности, имущественных прав и имущественных интересов». Под мошенничеством литовский законодатель, как и в Уголовном кодексе Латвии, предусмотрел приобретение чужого имущества, прав на подобное имущество путём злоупотребления доверием, обмана (ст. 177 УК Латвии, 182 УК Литвы), уклонения от имущественного обязательства, его отмены (ст. 182 УК Литвы).

Развитие общества в настоящий период связано, таким образом, с цифровизацией практически всех сфер жизнедеятельности во всех цивилизованных странах [9, с. 27]. Киберпреступности уделяется особое внимание во всем мировом сообществе. На официальном сайте Международного валютного фонда (International Monetary Fund, IMF), специализированной организации ООН, размещена статистическая информация, отражены пути решения наиболее актуальных проблем, связанных с хищениями с использованием IT-технологий[23], с легализацией доходов, полученных преступным путём, как неправомерных действий, направленных на сокрытие источника происхождения денежных средств и придание законного вида доходам, появившимся в результате преступных действий. В результате лица, совершившие преступление, инвестируют денежные средства в различные преступные сферы общества, наносят вред государству, всему мировому сообществу, в т.ч. глобальным финансовым системам, чем осуществляется подрыв экономики, валют, формируется угроза международной безопасности.

Этими актуальными вопросами, включая формирование алгоритма действий уполномоченных органов в сфере профилактики данных видов уголовно-наказуемых деяний, активно занимается международная организация «PositiveTechnologies», европейский лидер в этой области, осуществляющая разноуровневый анализ необходимой защищённости соответствующих систем, их соответствия признанным стандартам защиты.

Специалисты этой организации утверждают, что на общую статистику таких преступлений оказывает влияние комплекс факторов, которые должны позволить сформировать новый алгоритм действий по профилактике преступлений. Во-первых, в информационном пространстве возросло количество специалистов, входящих в преступные кибергруппировки, с высоким уровнем квалификации,

[21] Уголовный закон [Уголовный кодекс] Латвийской Республики от 17 июня 1998 года [Электронный ресурс] // Сайт «Законы Латвии по-русски». – URL: http://www.pravo.lv/likumi/07_uz.html (дата обращения: 10.02.2020).

[22] Уголовный кодекс Литовской Республики от 26 сентября 2000 г. [Электронный ресурс] // Сайт «OK Pravo». – URL: http://okpravo.ru/zarubezhnoe-pravo/ugolovnoe-pravo-zarubezhnyh-stran/уголовный-кодекс-литвы.html (дата обращения: 10.02.2020).

[23] Международный валютный фонд [Электронный ресурс] // Официальный сайт МВФ. – URL: https://www.imf.org/external/Russian/ (дата обращения: 10.02.2020).

имеющих значительную технологическую оснащённость и, во-вторых, государственная политика в сфере информационной безопасности требует принятия прогрессивных правовых и иных контрмер, направленных на усиление мер противодействия в отношении обнаружения, предупреждения, профилактики и локализации преступлений[24].

[24] Яковлева М. А. Органы внутренних дел как один из субъектов в системе профилактики преступности : дис. … канд. юрид. наук: 12.00.08 / Яковлева Маргарита Александровна. – Москва, 2019. – 270 с.

Список литературы

1. *David R.* Les grands systems de droit contemporains (Droit comparé). – Paris: Dalloz, 1964. – P. 133.

2. *Смирнов А. М.* Некоторые проблемы квалификации мошенничества как специфичного способа хищения // Новый юридический вестник. – 2019. – № 1. – С. 53–55.

3. *Жалинский А. Э.* Современное немецкое уголовное право. – Москва: Проспект, 2004. – 560 с.

4. *Ястребов Д. А., Ивановский П. С., Брянцева Н. В.* Институт уголовной ответственности за компьютерные преступления в Германии [Электронный ресурс] // Электронный научный журнал «NaukaRus». – 2007. – URL: http://naukarus.com/institut-ugolovnoy-otvetstvennosti-za-kompyuternye-prestupleniya-v-germanii (дата обращения: 10.02.2020).

5. *Чернякова А. В.* Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. – 2018. – № 4 (46). – С. 168–179.

6. *Корчагин А. Г., Трушова И. В.* Проблемы правового регулирования расчётов банковскими картами // Юридические исследования. – 2012. – № 3. – С. 43–77.

7. *Шамахов В. А., Еремина Н. В., Межевич Н. М.* Основные характеристики политического развития стран Прибалтики и их экономические последствия // Управленческое консультирование. – 2019. – № 3. – С. 8–23.

8. *Кудрявцев Р. В.* Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. – 2019. – № 24 (262). – С. 218–221.

9. *Иванова Л. В.* Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. – 2019. – № 1. – С. 25–33.

10. *Пчёлкина Е. В.* Эволюция развития мошенничества, совершаемого с использованием банковской гарантии // Проблемы правоохранительной деятельности. – 2019. – № 4. – С. 45-49.

11. *Лапшин В. Ф.* Уголовно-правовые средства противодействия незаконной банковской деятельности // Проблемы правоохранительной деятельности. – 2020. – № 2. – С. 6-10.

References

1. *David R.* Les grands systems de droit contemporains (Droit comparé). – Paris: Dalloz, 1964. – P. 133.

2. *Smirnov A. M.* Nekotoryye problemy kvalifikatsii moshennichestva kak spetsifichnogo sposoba khishcheniya // Novyy yuridicheskiy vestnik. – 2019. – № 1. – S. 53–55.

3. *Zhalinskiy A. E.* Sovremennoye nemetskoye ugolovnoye pravo. – Moskva: Prospekt, 2004. – 560 s.

4. *Yastrebov D. A., Ivanovskiy P. S., Bryantseva N. V.* Institut ugolovnoy otvetstvennosti za komp'yuternyye prestupleniya v Germanii [Elektronnyy resurs] // Elektronnyy nauchnyy zhurnal «NaukaRus». – 2007. – URL: http://naukarus.com/institut-ugolovnoy-otvetstvennosti-za-kompyuternye-prestupleniya-v-germanii (data obrashcheniya: 10.02.2020).

5. *Chernyakova A. V.* Mezhdunarodnyy i zarubezhnyy opyt ugolovno-pravovogo protivodeystviya khishcheniyam, sovershayemym s ispol'zovaniyem komp'yuternoy informatsii // Yuridicheskaya nauka i pravookhranitel'naya praktika. – 2018. – № 4 (46). – S. 168–179.

6. *Korchagin A. G., Trushova I. V.* Problemy pravovogo regulirovaniya raschotov bankovskimi kartami // Yuridicheskiye issledovaniya. – 2012. – № 3. – S. 43–77.

7. *Shamakhov V. A., Yeremina N. V., Mezhevich N. M.* Osnovnyye kharakteristiki politicheskogo razvitiya stran Pribaltiki i ikh ekonomicheskiye posledstviya // Upravlencheskoye konsul'tirovaniye. – 2019. – № 3. – S. 8–23.

8. *Kudryavtsev R. V.* Organizatsiya deyatel'nosti po raskrytiyu distantsionnykh moshennichestv // Molodoy uchenyy. – 2019. – № 24 (262). – S. 218–221.

9. *Ivanova L. V.* Vidy kiberprestupleniy po rossiyskomu ugolovnomu zakonodatel'stvu // Yuridicheskiye issledovaniya. – 2019. – № 1. – S. 25–33.

10. *Pcholkina Ye. V.* Evolyutsiya razvitiya moshennichestva, sovershayemogo s ispol'zovaniyem bankovskoy garantii // Problemy pravookhranitel'noy deyatel'nosti. – 2019. – № 4. – S. 45–49.

11. *Lapshin V. F.* Ugolovno-pravovyye sredstva protivodeystviya nezakonnoy bankovskoy deyatel'nosti // Problemy pravookhranitel'noy deyatel'nosti. – 2020. – № 2. – S. 6–10.

Статья поступила в редакцию 17.06.2020 г.