Хисамова Зарина Илдузовна. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: диссертация ... кандидата Юридических наук: 12.00.08 / Хисамова Зарина Илдузовна;[Место защиты: Краснодарский университет Министерства внутренних дел Российской Федерации.], 2016

**Содержание к диссертации**

Введение

**ГЛАВА 1. Социально-правовая природа уголовной ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий 21**

1.1. Понятие и классификация преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий –

1.2. Сравнительно-правовой анализ зарубежного уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий 47

**ГЛАВА 2. Уголовно-правовая характеристика преступлений, совершаемых в финансовой сфере с использованием информационно-телекомму никационных технологий 75**

2.1. Преступления, совершаемые с использованием электронных средств платежа –

2.2. Преступления, совершаемые в сфере оборота информационно телекоммуникационных технологий 106

**ГЛАВА 3. Основные направления совершенствования уголовно-правовых мер противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуника-ционных технологий 142**

3.1. Совершенствование практики применения уголовно-правовых норм, устанавливающих ответственность за преступления, совершаемые в финансовой сфере с использованием информационно телекоммуникационных технологий

3.2. Перспективные пути оптимизации российского уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно телекоммуникационных технологий 159

Заключение 172

Список литературы

**Введение к работе**

**Актуальность темы исследования.** Стремительное развитие информационно-телекоммуникационных технологий (IT-технологий) в последние десятилетия привело к появлению совершенно новых способов установления и поддержания взаимоотношений между людьми. Широкое внедрение информационных технологий затронуло все сферы жизни современного общества. Финансовая отрасль, наряду с другими, ищет пути увеличения возможностей, которые возникают при использовании новых каналов доставки информации и услуг, таких как Интернет, цифровое телевидение, мобильная связь. Идет процесс перехода банковской деятельности и финансовых структур на расчеты с использованием IT-технологий.

Совершенствование и развитие IT-технологий, расширение сферы их применения, доступность и широкая распространенность среди населения привели к появлению и неуклонному росту в последние годы преступлений, посягающих на информационную безопасность в сфере экономики.

Транснациональный характер посягательств в информационной сфере, обусловленный техническими возможностями, способен нанести непоправимый ущерб экономике сразу нескольких государств, открывает широкие возможности для развития теневого бизнеса.

К сожалению, темпы развития IT-технологий значительно опережают законодательные реагирования на многие возникающие проблемы. Это касается не только уголовного, но и многих других отраслей права, положения которых должны давать адекватную и своевременную оценку угрозам и регулировать отношения, возникающие в сферах, где используются информационно-телекоммуникационные технологии. Действующему уголовному законодательству свойственно отсутствие унифицированного подхода к оценке преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, единства в используемом понятийном аппарате и, как следствие, внесение рассогласованных и бессистемных изменений, которые не дают ожидаемого результата.

Официальную статистику, свидетельствующую о масштабах преступности в сфере использования информационно-телекоммуникационных технологий, получить на сегодняшний день достаточно сложно. Статистическая отчетность ГИАЦ МВД России (отчет о преступлениях, совершенных в сфере телекоммуникаций и

компьютерной информации, – форма 1-ВТ) не отражает объективную картину ввиду фрагментарности содержащейся в ней информации (в форме, например, нет сведений о количестве зарегистрированных преступлений по ст. 1593, 1596, 187 УК РФ). Определенную роль в невозможности отражения реального положения дел сыграло также и отсутствие единообразия при квалификации рассматриваемых деяний с учетом их юридико-экономической природы. Однако, несмотря на объективные недостатки статистической формы, все же можно проследить динамику роста количества зарегистрированных и расследованных преступлений, совершенных в финансовой сфере с использованием информационно-телекоммуникационных технологий. Так, в 2010 г. было выявлено 1819 случаев совершения мошенничества указанным способом, в 2011 г. – 2049, 2012 г. – 2748, 2013 г. – 2196, 2014 г. – 2187, 2015 г. – 13483. При этом в 2014 г. расследовано и направлено в суд только 457 уголовных дел, 1396 приостановлено за неустановлением лица, совершившего преступление, а в 2015 г. направлено в суд только 1352 уголовных дела, приостановлено – 9488. Аналогичная картина наблюдается и с кражей, совершенной с использованием информационно-телекоммуникационных технологий: только каждое 5 преступление расследуется и передается в суд.

Различные коммерческие организации, занимающиеся мониторингом преступности в сфере информационно-телекоммуникационных технологий, наряду с правоохранительными органами и кредитными организациями, предоставляют достаточно разрозненную информацию. Кроме того, в поле зрения официальной статистики попадают лишь сведения о происшествиях, которые в той или иной форме были выявлены и квалифицированы как преступления по существующим на сегодняшний день составам: либо как посягательства в сфере компьютерной информации, либо в совокупности с предикатными составами (ст. 158, 159 УК РФ и др.).

По данным Бюро специальных технических мероприятий МВД России, число киберпреступлений в России в 2014 г. увеличилось на 8,6% и составило более 11 тысяч. В качественном соотношении ки-берпреступность выглядит следующим образом: 37% из числа всех совершенных за этот период компьютерных преступлений приходится на мошенничество, 19% – на неправомерный доступ к информации с целью хищения денежных средств, 16% – на распространение детской порнографии и по 8% – на нарушение авторских и смежных прав и распространение вредоносных программ.

Как отмечает финансово-аналитическая группа Group-IB, ущерб от киберпреступлений в 2012 г. на территории России составил 3,5–4 млрд долл.США. За 2014 г. ущерб, нанесенный киберпре-ступностью российским компаниям и гражданам, составил 2,5 млрд долл. США. В 2015 г., по заявлениям заместителя председателя Сбербанка России Льва Хасиса, ущерб составил около 1 млрд долл. США, или около 70–75 млрд руб. Как утверждают эксперты, рост уровня преступности в этой сфере пропорционален росту оборота денежных средств, проходящих через электронные платежные системы.

Вместе с тем, в СМИ находят отражение лишь инциденты, преданные широкой огласке и связанные с использованием наиболее распространенного вида электронных средств платежа – платежных карт, в то время как большая часть преступлений, связанных с посягательствами в финансовой сфере с использованием информационно-телекоммуникационных технологий, остается без должного внимания. Так, не предаются огласке инциденты утечки данных, касающихся финансовых операций. От действий преступников в 2014 г. треть финансовых компаний (36%) в России, таких как «Qiwi», «Почта России», «Московская Биржа ММВБ-РТС», столкнулась с утечкой важных данных, связанных с осуществлением денежных операций.

Указанные обстоятельства в совокупности определяют актуальность и социальную значимость проведения специального комплексного уголовно-правового исследования вопросов установления и реализации уголовной ответственности за преступления в финансовой сфере, совершаемые с использованием информационно-телекоммуникационных технологий.

**Степень разработанности темы исследования.** Некоторые аспекты уголовно-правового противодействия преступлениям в финансовой сфере, совершаемым с использованием информационно-телекоммуникационных технологий, стали предметом изучения в рамках исследования отдельных составов, касающихся обеспечения безопасности компьютерных технологий и информации, а также кредитных и расчетных карт.

Так, проблемы уголовно-правового противодействия незаконному изготовлению и сбыту поддельных кредитных и расчетных карт рассмотрены в диссертационных исследованиях А.Н. Богомолова, С.В. Васюкова, Д.Н. Ветрова, В.Ф.-о. Джафарли, С.А. Скворцовой и др.

Углубленному изучению правовой природы отношений, возникающих при осуществлении расчетов с использованием платежных карт, посвящены диссертационные исследования Г.Н. Белоглазовой, А.С. Генкина, А.С. Жульева, В.Ю. Иванова, Е.Г. Клеченовой, И.Л. Овсянниковой, И.А. Спиранова, А.В. Шамраева и др.

Отдельные аспекты проблемы предупреждения преступлений, совершаемых с использованием компьютерных и информационных технологий, нашли отражение в работах В.Б. Вехова, Г.И. Волкова, Ю.В. Гаврилина, А.В. Геллера, А.Г. Кибальника, В.П. Коняхина, В.П. Котина, И.Л. Кочои, В.Н. Кудрявцева, В.Д. Ларичева, Ю.И. Ляпунова, О.С. Рудаковой, Т.Л. Тропиной, И.Г. Чекунова, А.Ю. Чупровой, Н.Г. Шурухнова.

Уголовная ответственность за преступления в сфере экономической деятельности в целом и в финансовой сфере в частности анализируется в исследованиях Г.С. Аванесяна, С.А. Бессчастного, Б.В. Волженкина, Ю.П. Гармаева, Л.Д. Гаухмана, А.Э. Жалинского, В.Д. Ларичева, Н.А. Лопашенко, О.Г. Соловьева, П.С. Яни и др.

В отличие от работ вышеназванных авторов, в которых освещены отдельные аспекты противодействия преступлениям в финансовой сфере, совершаемым с использованием информационно-телекоммуникационных технологий, в настоящем диссертационном исследовании указанные преступления рассмотрены комплексно.

**Объект** диссертационного исследования образуют общественные отношения, возникающие в связи с совершением преступлений в финансовой сфере с использованием информационно-телекоммуникационных технологий.

**Предметом** диссертационного исследования выступают уголовно-правовые нормы, предусмотренные ст. 158, 1593, 1596, 187, 272–274 УК РФ, нормы гражданского законодательства и банковского права в данной области, материалы соответствующей правоприменительной практики, результаты социологических исследований и специальных исследований рынка IT-технологий и банковского сектора, а также зарубежное уголовное законодательство.

**Цель и задачи исследования.** Цель диссертационной работы состоит в комплексном уголовно-правовом исследовании вопросов противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий, разработке предложений по повышению эффективности уголовно-правового противодействия данным общественно опасным деяниям.

Для достижения обозначенной цели определены следующие исследовательские задачи:

1. разработка понятия и классификация преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий;
2. сравнительно-правовой анализ законодательства зарубежных государств, предусматривающего уголовную ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий;
3. уголовно-правовой анализ составов преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий;
4. разработка рекомендаций по квалификации преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий;
5. определение основных направлений совершенствования уголовного законодательства, касающегося рассматриваемых преступлений.

**Методологическую основу** диссертационного исследования образуют диалектический метод научного познания, методы анализа и синтеза, системно-структурный, сравнительно-правовой, формальнологический, конкретно-социологический, метод контент-анализа и т. д.

**Нормативная основа** исследования представлена Конституцией РФ, Уголовным кодексом РФ, Гражданским кодексом РФ, Кодексом РФ об административных правонарушениях, федеральными законами («О национальной платежной системе», «Об информации, информационных технологиях и о защите информации», «О персональных данных» и др.) и подзаконными актами.

**Теоретическая основа исследования** представлена фундаментальными положениями отечественной уголовно-правовой науки, а также непосредственно связанными с объектом исследования трудами в области теории права и государства, гражданского права, финансового права, банковского права, экономики, административного права, философии права, социологии, и других наук.

В ходе диссертационного исследования использовались непосредственно связанные с темой диссертации работы таких авторов, как Б.В. Волженкин, Л.Д. Гаухман, Н.А. Деуленко, И.А. Клепицкий, А.Г. Кибальник, В.П. Коняхин, Л.Л. Кругликов, В.С. Кузьменко, Б.М. Леонтьев, Н.А. Лопашенко, А.Л. Осипенко, А.И. Рарог, А.И. Фоменко, А.И. Чучаев, А.Ю. Чупрова, П.С. Яни и др.

**Эмпирическая база исследования** включает в себя опубликованную судебную практику; результаты изучения материалов 119 уголовных дел о преступлениях, совершенных в финансовой сфере с использованием информационно-телекоммуникационных технологий; итоги социологического опроса 100 сотрудников правоохранительных органов (70 сотрудников следственных подразделений, 30 – подразделений экономической безопасности и противодействия коррупции) и 15 судей в качестве экспертов; статистические сведения ГИАЦ МВД России. При подготовке диссертации были использованы результаты исследований, проведенных другими авторами, а также анализа рынка IT-технологий и банковского сектора, проведенные независимыми компаниями, результаты контент-анализа средств массовой информации.

**Научная новизна** диссертационной работы заключается в том, что впервые осуществлено монографическое исследование комплекса вопросов уголовно-правового противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий.

Определена социально-правовая природа преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий. В результате комплексного исследования ключевых сфер, в которых наиболее активно используются информационно-телекоммуникационные технологии, определено, что в финансовой сфере преступные посягательства с их использованием совершаются чаще всего. В ходе диссертационного исследования подробно рассмотрена социально-правовая природа отношений в сфере использования IT-технологий, сформулированы авторские определения ключевых понятий в рассматриваемой сфере. Основное отличие авторской позиции от точек зрения, изложенных в предшествующих исследованиях, состоит в том, что в диссертации обосновывается тезис о необходимости выделения из массива преступлений, совершаемых в сфере использования информационно-телекоммуникационных технологий, в отдельную группу посягательств, совершаемых с использованием информационно-телекоммуникационных технологий в финансовой сфере, ввиду масштабов и скорости их распространения, а также степени общественной опасности. Теоретически обосновано авторское определение преступлений, совершаемых в сфере использования информаци-

онно-телекоммуникационных технологий, а также предложена классификация преступлений в указанной сфере, которой охвачены все возможные преступные деяния. В рамках исследования сформулировано определение преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий, сделан вывод о том, что они могут быть разделены на преступления, совершаемые с использованием электронных средств платежа, и преступления, совершаемые в сфере оборота IT-технологий. В отличие от предшествующих исследований по рассматриваемой тематике, автором в ходе компаративного исследования сделан акцент на анализе конструкции юридических норм зарубежного законодательства, а также используемой терминологии для характеристики противоправных деяний в финансовой сфере, совершаемых с использованием информационно-телекоммуникационных технологий; выделены два подхода в уголовно-правовом противодействии указанным преступлениям.

Диссертантом дана уголовно-правовая характеристика преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий, с учетом изменений, внесенных в ст. 187 УК РФ Федеральном законом от 8 июня 2015 г. № 153-ФЗ, сформулированы авторские определения информационно-телекоммуникационных технологий, используемых в финансовой сфере, образующих предмет ст. 187 УК РФ.

По результатам исследования практики применения уголовно-правовых норм в рассматриваемой сфере разработан проект постановления Пленума Верховного Суда РФ, в котором даются разъяснения и толкование используемых в законе понятий, а также определены правила квалификации преступных посягательств в финансовой сфере, совершаемых с использованием информационно-телекоммуникационных технологий. Разработаны конкретные предложения по повышению эффективности отечественного уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий. В целом в ходе исследования решены задачи, имеющие прикладное и теоретическое значение для развития науки уголовного права в части противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий.

Научную новизну диссертационного исследования подтверждают **основные положения, выносимые на защиту**:

1. Аргументировано, что под преступлениями, совершаемыми в сфере использования информационно-телекоммуникационных технологий, следует понимать виновные общественно опасные деяния, причиняющие ущерб общественным отношениям, связанным с безопасностью охраняемой законом информации, соблюдением установленного законом порядка оборота и использования информационно-телекоммуникационных технологий.
2. Определено, что преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий, представляют собой особую группу преступных посягательств на отношения в сфере распределения, перераспределения и использования денежных средств, совершаемых с использованием информационно-телекоммуникационных технологий.
3. Обосновано, что преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий, могут быть разделены на: преступления, совершаемые с использованием электронных средств платежа, и преступления, совершаемые в сфере оборота информационно-телекоммуникационных технологий.
4. Установлено, что в мире на сегодняшний день наблюдается два подхода в уголовно-правовом противодействии преступлениям в финансовой сфере, совершаемым с использованием информационно-телекоммуникационных технологий.

Первый заключается в том, что в уголовном законодательстве зарубежных стран не делается акцент на охране информационных отношений в финансовой сфере. Преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий, находятся под запретом общих норм, обеспечивающих информационную безопасность.

Второй подход обусловлен выделением зарубежным законодателем преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий, в отдельный блок. В специальных нормах детализирована ответственность за посягательства в сфере оборота информационно-телекоммуникационных технологий, а также за преступления с использованием электронных средств платежа, в частности платежных карт.

В большинстве стран наблюдается тенденция по ужесточению ответственности за противоправные посягательства в IT-сфере и непрерывная реформация норм уголовного законодательства как реагирование на возникающие угрозы.

5. Доказано, что при хищении с использованием услуг АТМ-  
банкинга (посредством использования банкомата) в качестве непо  
средственного объекта преступного посягательства выступают об  
щественные отношения по обеспечению и реализации либо права  
собственности (в случае если открыт карточный дебетовый счет, при  
этом сами денежные средства опосредованы безналичной формой),  
либо права, возникающего из имущественного обязательства (в слу  
чае оформления предоплаченной карты или кредитной карты либо  
использования электронных денежных средств).

Непосредственным объектом мошенничества с использованием платежных карт (ст. 1593 УК РФ) выступают общественные отношения, складывающиеся в сфере распределения, перераспределения и использования денежных средств в ходе социального обслуживания населения с использованием отдельной разновидности электронных средств платежа – платежных карт.

Непосредственным объектом мошенничества в сфере компьютерной информации (ст. 1596 УК РФ) выступают общественные отношения, складывающиеся в сфере распределения, перераспределения и использования денежных средств.

6. Установлено, что объективная сторона состава ст. 1596 УК  
РФ представлена рядом альтернативных действий, влекущих хище  
ние чужого имущества или приобретение права на него, которые мо  
гут быть разделены на две группы:

действия, совершаемые с неправомерным использованием реквизитов доступа легального пользователя системы дистанционного банковского обслуживания (ДБО);

действия, совершаемые с использованием уязвимостей электронной платежной системы и системы ДБО без неправомерного использования реквизитов доступа ее легального пользователя.

7. Определено, что моментом окончания хищения с использо  
ванием электронных средств платежа следует считать момент «об  
наличивания» похищенных денежных средств либо их перечисления  
на иной счет, с которого у злоумышленника появляется реальная  
возможность распоряжаться и пользоваться ими по своему усмот  
рению.

1. Установлено, что организованным группам, созданным для совершения хищений с использованием информационно-телекоммуникационных технологий, свойственны специфические признаки: техническая оснащенность, выражающаяся в разработке специального программного обеспечения, предназначенного для взлома системы защиты кредитных организаций и получения доступа к базам данных, «узкое» распределение ролей в соответствии с преступной специализацией, анонимность, использование информационно-телекоммуникационных технологий в качестве связующего звена и «инструмента» создания преступной группы. Установление указанных признаков является необходимым для характеристики группы как организованной.
2. Доказано, что преступление, предусмотренное ст. 187 УК РФ, – двухобъектное. Основным непосредственным объектом преступления являются общественные отношения в сфере экономики, связанные с эмиссией и оборотом информационно-телекоммуникационных технологий в финансовой сфере, дополнительным – общественные отношения, складывающиеся в сфере безопасного использования электронных средств платежа, функционирования банковской платежной инфраструктуры и обеспечения безопасности компьютерной информации.

10. Даны авторские определения информационно-  
телекоммуникационных технологий, используемых в финансовой  
сфере, образующих предмет ст. 187 УК РФ.

1. Аргументировано, что видовой объект преступлений в сфере компьютерной информации – совокупность общественных отношений в сфере обеспечения информационной безопасности, т.е. правомерного, безопасного использования, хранения, распространения и защиты информационно-телекоммуникационных технологий.
2. Доказано, что под компьютерной информацией следует понимать сведения (сообщения, данные) хранящиеся, обрабатываемые, принимаемые и передаваемые, предназначенными для этих целей автоматизированными технологиями.
3. По результатам исследования практики применения уголовно-правовых норм, устанавливающих ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий, сформулированы рекомендации и разъяснения по разграничению преступлений, предусмотренных ст. 1593, 1596, 187, 272, 273 УК РФ, а также рекомендации по квалификации фишинга, скимминга и DDos-атак.

Разработан проект постановления Пленума Верховного Суда, в котором даются разъяснения и толкование используемых в законе понятий, а также определены правила квалификации преступных посягательств в финансовой сфере, совершаемых с использованием информационно-телекоммуникационных технологий.

14. Разработаны основные меры повышения эффективности отечественного уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий:

1. обоснована целесообразность дополнения ст. 1593 УК РФ ч. 5, предусматривающей ответственность за принятие к оплате или совершение иных финансовых сделок с использованием поддельной или принадлежащей другому лицу, не являющемуся предъявителем, кредитной, расчетной или иной платежной карты работником кредитной, торговой или иной организации;
2. обоснована целесообразность исключения из примечания к ст. 1591 УК РФ указания на ст. 1593 и 1596 УК РФ с целью распространения на данные статьи определения крупного и особо крупного размера ущерба, предусмотренного в примечании к ст. 158 УК РФ;
3. аргументирована потребность усиления ответственности за совершение мошеннических действий в сфере компьютерной информации в особо крупном размере либо организованной группой путем увеличения максимального наказания до 15 лет лишения свободы ввиду неограниченности круга потенциальных жертв и размера причиняемого ущерба;
4. доказана необходимость дополнения ст. 63 УК РФ новым обстоятельством, отягчающим наказание, в виде совершения пре-ступлениясиспользованием информационно-телекоммуникационных технологий;
5. сделан вывод о необходимости дополнения ч. 3 ст. 273 УК РФ квалифицирующим признаком, устанавливающим ответственность за совершение преступления с целью скрыть другое преступление или облегчить его совершение;

6) установлено, что оборот криптовалют не охватывается со  
держанием диспозиции ст. 187 УК РФ, предусматривающей ответ  
ственность за неправомерный оборот средств платежей. Ввиду осо  
бенностей экономико-правовой природы криптовалют предложено  
установить уголовную ответственность за их использование в рам-  
13

ках отдельной статьи УК РФ. Разработан авторский текст данной статьи.

**Теоретическая значимость исследования** заключается в том, что результаты настоящей работы вносят существенный вклад в развитие научного понимания системы уголовно-правовых средств противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий, выступают предпосылкой для проведения дальнейших научных уголовно-правовых исследований в рассматриваемой сфере. Научно обоснованные выводы и предложения по результатам исследования закладывают теоретические основы дальнейшего развития знаний о преступлениях в сфере экономической деятельности и использования информационно-телекоммуникационных технологий.

**Практическая значимость исследования** выражается в том, что его результаты могут быть использованы в процессе совершенствования уголовного законодательства Российской Федерации об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий; в правоприменительной деятельности судов и правоохранительных органов при квалификации преступлений в сфере экономической деятельности и компьютерной информации, их разграничении с иными составами преступлений; в научно-исследовательской работе при дальнейшем анализе преступлений, связанных с использованием IT-технологий; в учебном процессе юридических образовательных организаций и факультетов при преподавании курса уголовного права, соответствующих спецкурсов; в системе повышения квалификации и служебной подготовки сотрудников правоохранительных органов и специалистов по информационной безопасности.

**Степень достоверности результатов исследования**. Теоретическая часть научного труда базируется на использовании широкого круга российских и зарубежных научно-правовых источников, научной и учебной литературы, опубликованных материалов конференций, семинаров различного уровня, материалов аналитических отчетов. Научные выводы и положения основываются на анализе теоретической части исследования, результатах обобщения. При формулировании теоретических и прикладных положений автор использовал данные судебной практики, уголовной статистики и экономической аналитики. При разработке научных положений использованы современные методики сбора, обработки и анализа эм-14

пирической базы исследования. Степень достоверности результатов проведенного исследования обеспечена также результатами апробирования разработанных положений на практике и в учебном процессе, что подтверждается актами внедрения.

**Апробация результатов исследования.** Основные результаты диссертационного исследования заслушивались на заседаниях кафедры уголовного права и криминологии Краснодарского университета МВД России; докладывались и обсуждались на региональной конференции «Уголовно-правовые, уголовно-процессуальные, криминалистические и иные проблемы в деятельности следственных подразделений правоохранительных органов» (Челябинск, 2009 г.), Всероссийской научно-практической конференции «Проблемы борьбы с преступностью в странах СНГ» (Воронеж, 2011 г.), Международной научно-теоретической конференции «Актуальные проблемы юридических и общественных наук в Республике Казахстан» (Караганда,

1. г.), Всероссийской научно-практической конференции «Проблемы и перспективы развития права и правосудия в современном мире» (Краснодар, 2012 г.), Всероссийской научно-практической конференции «Актуальные проблемы правоохранительной деятельности органов внутренних дел» (Екатеринбург, 2012 г.), VI Международной научно-практической конференции «Безопасность личности, общества и государства: теоретико-правовые аспекты» (Санкт-Петербург, 2012 г.), III Международной научно-практической конференции «Современные проблемы уголовной политики» (Краснодар, 2012 г.), II Всероссийской научно-практической конференции «Проблемы и перспективы развития права и правосудия в современном мире» (Краснодар, 2013 г.), Всероссийской научно-практической конференции «Актуальные вопросы науки и практики» (Краснодар, 2013 г.), Межрегиональной конференции «Актуальные проблемы борьбы с преступностью на современном этапе» (Волгоград, 2013 г.), Международной научно-практической конференции «Криминалистика и судебно-экспертная деятельность в условиях современности» (Краснодар, 2013 г.), VII Международной научно-практической конференции «Безопасность личности, общества и государства: теоретико-правовые аспекты» (Санкт-Петербург,
2. г.), IV Международной научно-практической конференции «Современные проблемы уголовной политики» (Краснодар, 2013 г.), V Международной научно-практической конференции «Современные проблемы уголовной политики» (Краснодар, 2014 г.), III Всероссий-15

ской научно-практической конференции «Криминалистика и судебно-экспертная деятельность в условиях современности» (Краснодар, 2015 г.), Международной научно-практической конференции «Уголовный закон: алгоритм и стратегии развития», посвященной 170-летию принятия Уложения о наказаниях уголовных и исправительных 1845 года (Краснодар, 2015 г.), VI Международной научно-практической конференции «Современные проблемы уголовной политики» (Краснодар, 2015 г.).

Основные положения исследования внедрены в учебный процесс Краснодарского университета МВД России и СевероКавказского федерального университета, практическую деятельность Главного управления МВД России по Краснодарскому краю, Главного управления МВД России по Ставропольскому краю, Верховного Суда Республики Адыгея; нашли отражение в 21 научной публикации, 7 из которых опубликованы в изданиях, рекомендованных Минобрнауки России.

Структура диссертации определена ее целью и задачами и состоит из введения, трех глав (шести параграфов), заключения, списка литературы и приложения. Диссертация оформлена в соответствии с требованиями ВАК при Минобрнауки России.

## Сравнительно-правовой анализ зарубежного уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий

В. Стэллингз приводит классификацию в зависимости от способа противоправного вмешательства в процесс передачи данных: «блокирование процесса передачи данных; неправомерный доступ к передаваемым данным; неправомерное изменение данных; организация подложного сеанса связи»1. На наш взгляд, автором оставлены без внимания преступные посягательства, в которых процесс передачи данных выступает только лишь средством достижения преступного результата.

Д. Уолл, являющийся одним из наиболее авторитетных западных исследователей преступности в сфере IT-технологий, предлагает следующую классификацию2: преступления, нарушающие работу компьютера, куда отнесены взлом, блокирование и модификация компьютерной информации; преступления связанные с содержанием сетевых ресурсов, к которым отнесены распространение порнографических материалов, публикаций расистского и экстремистского характера; преступления с использованием компьютеров, которые основаны на применении сетевых компьютеров для осуществления финансовых махинаций и мошеннических схем. Описанная классификация представляется весьма удачной, однако перечень преступлений, «связанных с содержанием сетевых ресурсов», может быть значительно расширен.

Аналогичный подход наблюдается и в международном законодательстве. Так, в Европейской Конвенции по борьбе с киберпреступностью выделены пять основных типов преступлений3: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; преступления, связанные с использованием компьютерных средств; преступления, связанные с содержанием данных; преступления, связанные с нарушением авторского и смежных прав, распространением информации расистского и другого характера, подстрекающей к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающейся на расовой, национальной, религиозной или этнической принадлежности. На наш взгляд, оставление в рамках приведенной классификации без внимания преступлений, посягающих на информационный оборот в финансовой сфере, с одновременным акцентированием внимания на нарушении авторских и смежных прав, преступлениях расистского характера представляется не совсем оправданным, так как во всем мире основной сегмент киберпреступности составляют преступления в финансовой сфере. Различные подходы к классификации характерны и для работ отечественных ученых. Е.В. Громов1 и В.В. Хилюта2 подразделяют подобного рода противоправные деяния на следующие группы: «преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации; преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ, где компьютерная информация является объектом преступного посягательства и преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве орудия или средства совершения корыстного преступления и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации». Приведенные классификации представляются весьма разрозненными и не содержащими единого критерия, что, на наш взгляд, лишает их научной ценности.

В.С. Карпов классифицирует преступления на две большие группы: «компьютерные преступления, внутри которой выделяются: компьютерный саботаж, компьютерное мошенничество, несанкционированный доступ к компьютерной информации, неправомерное завладение компьютерной информацией, модификация компьютерной информации; изготовление и сбыт специальных средств для получения несанкционированного доступа к компьютерной системе или сети; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети и преступления смежные с компьютерными преступлениями»1. На наш взгляд, автором приведен весьма подробный перечень посягательств, отнесенных им к «компьютерным преступлениям», однако вторая группа «смежных с компьютерными преступлений» не детализирована, ввиду чего, не совсем ясно, что под ними следует понимать.

А.Л. Осипенко вся совокупность «сетевых преступлений» разделяется на четыре основных типа: «несанкционированное проникновение в компьютерную систему, имеющую подключение к глобальной компьютерной сети; нарушение нормального функционирования сетевой компьютерной системы, ведущее к блокированию доступа к информации; несанкционированное внесение изменений в компьютерные данные с корыстными целями; размещение в глобальных компьютерных сетях материалов противоправного характера»2. Вместе с тем, в приведенной классификации не нашли отражения преступления, в которых информационно-телекоммуникационные технологии выступают лишь в качестве средства совершения преступления. К примеру, незаконный оборот наркотических средств, психотропных веществ и их аналогов. Обобщая вышеизложенные позиции, следует отметить, что ни одна из предложенных классификаций на сегодняшний день не является совершенной и исчерпывающей. По нашему мнению классификация преступных посягательств, совершаемых с использованием информационно-телекоммуникационных технологий, должна учитывать все возможные противоправные посягательства.

## Преступления, совершаемые с использованием электронных средств платежа

Под родовым объектом преступления понимается «часть однородных общественных отношений, охраняемых группой норм уголовного закона»4. Родовым объектом, положенным в основу группирования норм в разделы Особенной части УК РФ, применительно к рассматриваемым составам, являются отношения в сфере экономики, видовым объектом выступает право собственности на имущество или имущественные обязательства. «Содержание отношений собственности образуют фактические отношения владения, пользования и распоряжения предметами (вещами), принадлежащими их собственнику»5. Определение непосредственного объекта преступного посягательства в каждом отдельном случае напрямую связано с предметом посягательства и способом незаконного использования электронного средства платежа.

Обратим внимание, что дуалистическая природа рассматриваемых отношений в сфере использования информационно-телекоммуникационных . технологий диктует необходимость выделения дополнительного непосредственного объекта преступного посягательства, которым, по мнению Н.И. Коржанского, «является то общественное отношение, посягательство на которое не составляет сущности данного преступления, но которое этим преступлением нарушается или ставится в опасность нарушения наряду с основным объектом»1. Как справедливо отмечает А.Ю. Чупрова, «при совершении запрещенных уголовным законодательством экономически значимых действий …производители и поставщики услуг нарушают не только базовые общественные отношения, которым непосредственно причиняется вред, но и установленный законом и соглашениями с информационными посредниками … порядок получения услуг информационно-телекоммуникационных сетей, обеспечивающий возможность бесперебойного и безопасного их использования каждым пользователем …. нарушаются общественные отношения, регулирующие безопасность и бесперебойность работы информационно – телекоммуникационных сетей и информации, в этих сетях содержащейся»2. Вышеизложенное дает основание полагать, что дополнительным объектом преступного посягательства выступают общественные отношения, складывающиеся в сфере безопасного использования электронных средств платежа, функционирования платежной инфраструктуры и обеспечения информационной безопасности. Одним из неотъемлемых компонентов которого является «защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем»3.

Хищение денежных средств с использованием ATM-банкинга (посредством использования банкомата) образует состав тайного хищения чужого имущества, то есть кражи. При хищении с использованием услуг АТМ-банкинга предполагается разумным определить в качестве непосредственного объекта преступного посягательства общественные отношения по обеспечению и реализации 1) либо права собственности (в случае если открыт карточный дебетовый счет, при этом сами денежные средства, как таковые, опосредованы безналичной формой); 2) либо права, возникающего из имущественного обязательства (в случае оформления предоплаченной карты или кредитной карты, либо использования электронных денежных средств), так как в данном случае банк обязуется предоставить клиенту денежные средства либо услуги на определенную сумму на условиях, предусмотренных договором (будь то договор карточного счета либо кредитный договор). Учитывая, что тайное хищение чужого имущества как таковое, а также ст.158 УК РФ не раз выступали предметом изучения в монографических и диссертационных исследованиях, и научной доктриной выработано четкое понимание указанных юридических категорий, считаем целесообразным остановиться на особенностях, предопределенных специфическим способом совершения преступлений, не рассматривая в рамках настоящей работы общеизвестные особенности уголовно-правовой характеристики кражи и мошенничества.

Для мошенничества, также как и для кражи, как формы хищения, характерны все основные признаки. Объект основного состава мошенничества составляют общественные отношения, складывающиеся в сфере реализации и обеспечения права собственности. Непосредственным объектом мошенничества с использованием платежных карт (ст. 1593 УК РФ) выступают общественные отношения, складывающиеся в сфере распределения, перераспределения и использования денежных средств в ходе социального обслуживания населения с использованием отдельной разновидности электронных средств платежа – платежных карт. С указанным тезисом согласились 75 % респондентов. Учитывая, что статья 1596 УК РФ определена как специальный вид мошенничества, то логично предположить, что объектом посягательства выступают общественные отношения, складывающиеся в сфере распределения, перераспределения и использования денежных средств. В то же время законодателем указан специфический способ совершения преступления: «путем ввода, удаления, блокирования, модификации компьютерной информации или иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей», который не может оказывать влияния на объект.

Общепризнанно, что «противоправное воздействие субъекта в формах, предусмотренных законом, на вещественную основу отношений собственности включает предметы материального мира в структуру элементов состава хищения, в силу чего они приобретают уголовно-правовое значение предмета преступного посягательства»1, «установление которого облегчает выяснение механизма причинения ущерба самому объекту преступления»2.

## Преступления, совершаемые в сфере оборота информационно телекоммуникационных технологий

Исходя из смысла п. 1.12 рассматриваемого Положения к распоряжениям о переводе денежных средств, применяемым в рамках форм безналичных расчетов, могут быть отнесены: платежные поручения, инкассовые поручения, платежные требования, платежные ордера. Указанным Положением, а также приказом Минфина России от 12 ноября 2013 г. № 107н1 определен перечень и описание реквизитов для указанных документов. Однако необходимо отметить, что перечень распоряжений о переводе денежных средств, приведенный выше, не является исчерпывающим. Так, в соответствии с положением № 383-П «распоряжения, для которых не установлены перечень реквизитов и формы, составляются отправителями распоряжений с указанием установленных банком реквизитов, позволяющих банку осуществить перевод денежных средств, и по формам, установленным банком или получателем средств по согласованию с банком»2. К примеру, 3 главой положения Центробанка РФ «Об эмиссии платежных карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004 года № 266-П предусмотрено составление при совершении операции с использованием платежной карты документа на бумажном носителе и (или) в электронной форме, который и является основанием для осуществления расчетов по указанным операциям и служит подтверждением их совершения. Положением для «документа» определены обязательные реквизиты. С учетом изложенного, имеются основания утверждать, что указанный документ представляет собой распоряжение о переводе средств оплаты.

Необходимо отметить, что правоприменительной практикой вышеперечисленные распоряжения о переводе средств оплаты, а также все виды платежных карт и до внесения изменений в ст. 187 УК РФ признавались предметом преступного посягательства. К примеру, Фарафонов М.Л., являясь генеральным директором ООО «Соцснабсервис», с целью обналичивания денежных средств и . использования их по своему усмотрению для получения имущественной выгоды изготовил несколько платежных поручений. Так, он обратился к ранее ему знакомому М. с предложением оформить на последнего за вознаграждение несколько юридических лиц, а также открыть расчетные счета данных юридических лиц в ОАО АКБ «Пробизнесбанк», с условием того, что М. не будет принимать участия в управлении данными юридическими лицами. Получив полный доступ к дистанционному и обезличенному управлению расчетным счетом ООО «Лидер плюс» в ОАО АКБ «Пробизнесбанк» через систему «банк-клиент» посредством использования персонального компьютера, Фарафонов М.Л. приобрел возможность бесконтрольно осуществлять бестоварные расчеты в безналичной форме по данному расчетному счету путем изготовления и сбыта поддельных платежных документов, не являющихся ценными бумагами, а именно – платежных поручений, похитив тем самым денежные средства1. Однако, вызывает вопрос трактовка понятия «сбыт», использованного судом по данному уголовному делу. На наш взгляд, действия Фарафонова М.Л. характеризуются понятием «использование», так как таким образом им обналичивались денежные средства. Действия указанного лица по использованию подложных платежных поручений, представляется целесообразным квалифицировать также по совокупности со ст. 1596 УК РФ.

Не совсем понятным представляется и значение понятия «электронное средство», использованного законодателем. Содержание понятия «электронное средства платежа», данного в п. 19 ст.3 ФЗ «О национальной платежной системе», как уже отмечалось нами, представляется более обобщающим и применимым для описания всех информационно-телекоммуникационных технологий, являющихся предметом статьи, в связи с чем можно сделать вывод, что указанные понятия не тождественны и соотносятся как «общее» и «частное». Полагаем, что данным понятием охватываются все иные, не отраженные в диспозиции нормы, электронные средства платежа, такие как, например, универсальная электронная карта (УЭК). По функционалу УЭК объединяет в себе идентификационное и платежное средство, позволяя осуществлять легальный прием, выдачу и перевод денежных средств1, вместе с тем, функционал УЭК позволяет использовать ее и для неправомерного приема, выдачи и перевода денежных средств. На наш взгляд, неправомерный оборот УЭК охватывается диспозицией рассматриваемой нормы в рамках неправомерного оборота электронных средств. Таким образом, можно сделать вывод, что под электронным средством следует понимать техническое устройство или средство, наделенное функционалом по приему, выдачи и переводу денежных средств.

Определенные трудности вызывает и понятие «электронный носитель информации». По определению содержания данного понятия также нет единого мнения. В соответствии с ГОСТом под электронным носителем понимается «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники»2. В ст. 2 закона Российской Федерации «О государственной тайне» дается определение «носителей сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов»3.

## Перспективные пути оптимизации российского уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно телекоммуникационных технологий

Долгое время однозначного ответа на данный вопрос не было, кроме того эксперты и аналитики были едины во мнении, что конструкция ст. 187 УК РФ неэффективна. Однако внесенные Федеральным законом от 19 июня 2015 г. № 153-ФЗ «О внесении изменений в статью 187 Уголовного кодекса РФ», изменения также порождают ряд вопросов правоприменительного плана, среди которых разграничение этого общественно опасного деяния с другими преступными посягательствами.

Указание в диспозиции рассматриваемой нормы на создание компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, на наш взгляд, создает конкуренцию со ст. 273 УК РФ, предметом которой является «компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации».

Неправомерный оборот средств платежей выражен рядом альтернативных действий: изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт средств платежей, таких как: поддельные платежные карты, распоряжения о переводе денежных средств, документов или средств оплаты, электронные средства, электронные носители информации, технические устройства, компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи и перевода средств.

Так, создание, распространение вредоносной компьютерной программы в целях фишинга – действий, направленных на получение конфиденциальной информации о владельце средств платежа, посредством установки на компьютер клиента вредоносного программного обеспечения либо путем перенаправления на подложный сайт1, охватывается ст. 187 УК РФ, так как действия по созданию указанной вредоносной программы, заведомо предназначенной для копирования и модификации компьютерной информации, посягают в первую очередь на общественные отношения в сфере установленного законом порядка эмиссии, выпуска и оборота информационно-телекоммуникационных технологий в финансовой сфере, а затем уже на отношения, складывающиеся в сфере безопасного использования электронных средств платежа, обеспечения информационной безопасности в сфере компьютерной информации. Ввиду чего представляется, что ст. 187 УК РФ выступает в качестве специальной по отношению к ст. 273 УК РФ в случаях создания, распространения или использования электронных средств, электронных носителей информации, технических устройств или компьютерных программ для неправомерного осуществления приема, выдачи, передачи денежных средств.

Обратимся к наглядному примеру. В ноябре 2015 года в ходе совместной операции управления «К» МВД России и центра информационной безопасности ФСБ России был задержан предполагаемый главарь преступной группы, похищавшей денежные средства у клиентов крупного российского банка с помощью Андроид-троянца. Было установлено, что злоумышленники действовали на территории России около полутора лет и использовали «банкер» для хищения данных, необходимых для проведения мошеннических транзакций. В целом преступникам удалось заразить более 16 тыс. мобильных устройств на базе операционной системы «Андроид». Украденная у их владельцев информация передавалась на четыре командных сервера, размещенных на территории Украины. Материалами предварительной проверки установлено, что реализацией мошеннической схемы руководил задержанный житель Ярославля. Все C&C-серверы банковского троянца обезврежены1. Представляется уместным квалифицировать действия указанного лица по ч. 4 ст. 1596 УК РФ. Вместе с тем, подозреваемый также должен быть привлечен к ответственности за действия по изготовлению, в данном случае созданию либо приобретению компьютерной программы для фишинга. Указанные действия должны быть квалифицированы по ч. 2 ст. 187 УК РФ.

Необходимо отметить, что ряд депутатов Государственной Думы предлагают внести изменения в Уголовный кодекс и предусмотреть в рамках 28 главы отдельную норму за фишинг2, что, на наш взгляд, необоснованно и лишено достаточной аргументации, ввиду того, что указанные действия охватываются объемом диспозиции ст. 187 УК РФ. Анализ преступных посягательств в сфере использования информационно-телекоммуникационных технологий свидетельствует о распространении DDos-атак3, представляющих собой атаки на сайты. Они блокируют доступ к сайтам, работу дополнительного программного обеспечения, осуществляют массовую рассылку пользователям вредоносного программного обеспечения или рекламы.