*На правах рукописи*

**Хисамова Зарина Илдузовна**

# УГОЛОВНО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В ФИНАНСОВОЙ СФЕРЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

12.00.08 – уголовное право и криминология;
уголовно-исполнительное право

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2016

Работа выполнена в Федеральном государственном казенном образовательном учреждении высшего образования «Краснодарский университет Министерства внутренних дел Российской Федерации»

**Научный руководитель** – доктор юридических наук, профессор **Ильяшенко Алексей Николаевич**

**Официальные оппоненты:** **Лопашенко Наталья Александровна**, доктор юридических наук, профессор, профессор кафедры уголовного и уголовно-исполнительного права Саратовской государственной юридической академии;

**Фоменко Андрей Иванович,** кандидат юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин Южного университета (ИУБиП)

**Ведущая организация** – Всероссийский государственный университет юстиции (РПА Минюста России)

Защита диссертации состоится 20 октября 2016 г. в 10-00 часов на заседании диссертационного совета Д 203.017.02 при Краснодарском университете МВД России по адресу: 350005, г. Краснодар, ул. Ярославская, 128, корпус «А4», конференц-зал.

С диссертацией можно ознакомиться в библиотеке Краснодарского университета МВД России.

Полный текст диссертации, автореферат диссертации и отзыв научного руководителя размещены на официальном сайте Краснодарского университета МВД России по адресу: www.krdu.mvd.ru

Автореферат разослан «____» июля 2016 г.

Ученый секретарь
диссертационного совета Грибанов Евгений Викторович

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**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. $159^3$, $159^6$, 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 киберпреступность 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 киберпреступностью 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, $159^3$, $159^6$, 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, формально-логический, 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 непосредственного объекта преступного посягательства выступают общественные 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 случае оформления предоплаченной карты или кредитной карты либо использования электронных денежных средств).

Непосредственным объектом мошенничества с использованием платежных карт (ст. $159^3$ 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. $159^6$ УК РФ) выступают общественные отношения, складывающиеся в сфере распределения, перераспределения и использования денежных средств.

6. Установлено, что объективная сторона состава ст. $159^6$ УК РФ представлена рядом альтернативных действий, влекущих хищение чужого имущества или приобретение права на него, которые могут 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 использованием электронных средств платежа следует считать момент «обналичивания» похищенных денежных средств либо их перечисления на иной счет, с которого у злоумышленника появляется реальная возможность распоряжаться и пользоваться ими по своему усмотрению.

8. 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.

9. 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.

11. 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.

12. Доказано, что под компьютерной информацией следует понимать сведения (сообщения, данные) хранящиеся, обрабатываемые, принимаемые и передаваемые, предназначенными для этих целей автоматизированными технологиями.

13. 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. $159^3$, $159^6$, 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. $159^3$ 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. $159^1$ УК РФ указания на ст. $159^3$ и $159^6$ 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 преступления с использованием 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 содержанием диспозиции ст. 187 УК РФ, предусматривающей ответственность за неправомерный оборот средств платежей. Ввиду особенностей экономико-правовой природы криптовалют предложено установить уголовную ответственность за их использование в рам-

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-

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, 2012 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, 2013 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-

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 Северо-Кавказского 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.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, раскрывается степень ее разработанности; определяются объект, предмет, цель и задачи исследования; характеризуются методологическая, нормативная, теоретическая и эмпирическая основы; рассматривается научная новизна; формулируются основные положения, выносимые на защиту; раскрывается теоретическая и практическая значимость работы; приводятся данные об апробации и внедрении полученных результатов исследования.

Первая глава **«Социально-правовая природа уголовной ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий»** включает два параграфа.

В первом параграфе ***«Понятие и классификация преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий»*** рассматривается социаль-

но-правовая природа информационно-телекоммуникационных технологий, а также преступлений, совершаемых в финансовой сфере с их использованием.

На основе анализа различных эмпирических источников установлена необходимость использования для характеристики преступлений в сфере высоких технологий обобщенного понятийного аппарата, наиболее удачным определением для рассматриваемых деяний является термин «преступления в сфере использования информационно-телекоммуникационных технологий», что, по мнению автора, позволит повысить эффективность противодействия уголовно-правовыми мерами общественно опасным деяниям, посягающим на информационную безопасность.

В диссертационном исследовании отмечается, что ключевыми сферами, в которых наиболее активно используются информационно-телекоммуникационные технологии, являются: организационно-управленческая сфера; сфера управления технологическими и производственными процессами; сфера автоматизированного проектирования и моделирования; дистанционное обучение и образовательные технологии; телемедицина; информационное обслуживание, в том числе оказание государственных и муниципальных услуг; производство и воспроизведение информационно-телекоммуникационных технологий; общение и коммуникация; финансовая сфера.

Автором в рамках настоящего параграфа аргументируется, 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.

В ходе анализа юридической литературы выявлено, что на сегодняшний день не предложена стройная классификация рассматриваемых преступлений, которая бы охватывала широкий диапазон совершаемых деяний.

Проведенным исследованием установлено, что преступные посягательства, совершаемые с использованием информационно-телекоммуникационных технологий, могут быть разделены на следующие виды:

1. Преступления в сфере компьютерной информации (деяния, ответственность за которые предусмотрена гл. 28 УК РФ). Статьи 272–

274 УК РФ имеют своей целью охрану общественных отношений в сфере оборота компьютерной информации.

2. «Сетевые преступления», в которых информационно-телекоммуникационные технологии выступают средством их совершения.

Это составы, предусмотренные ст. $205^2$, ч. 2 ст. $228^1$, ст. $171^2$, 242, $242^1$, $242^2$, 280, 282 УК РФ. Среди иных преступных посягательств, которые могут быть совершены с использованием информационно-телекоммуникационных технологий, но не содержащих квалифицирующего признака, можно отметить следующие: ст. 174, $174^1$, 183, 146, 165, $127^1$, $128^1$, 137, 138, 155 УК РФ.

Автором делается вывод, что перечень преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, весьма значителен, и прогнозы по дальнейшей информатизации общества свидетельствуют о том, что он будет все более расширяться.

3. Преступления, в которых использование информационно-телекоммуникационных технологий выступает неотъемлемым признаком объективной стороны основного состава. В данную группу входят: мошенничество с использованием платежных карт (ст. $159^3$ УК РФ), мошенничество с использованием компьютерной информации (ст. $159^6$ УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ).

Автором отмечается, что преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий, отражены в первой и третьей группе вышеприведенной систематизации. Указанное обстоятельство обусловлено механизмом совершения преступлений в финансовой сфере с использованием информационно-телекоммуникационных технологий.

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.

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.

Выделение указанных самостоятельных групп преступлений продиктовано современными реалиями криминальной картины в рассматриваемой сфере, материалами уголовных дел, статистическими данными, а также действующей нормативной правовой базой, регулирующей отношения в рассматриваемой сфере.

Основными преступлениями, совершаемыми с использованием электронных средств платежа, являются хищения, которые квалифицируются по ряду норм гл. 21 УК РФ. В группу преступлений, совершаемых в сфере оборота информационно-телекоммуникационных технологий, в соответствии с содержанием понятия «информационно-телекоммуникационные технологии», отнесены ст. 187, 272, 273, 274 УК РФ.

Второй параграф ***«Сравнительно-правовой анализ зарубежного уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий»*** содержит результаты компаративного исследования.

В результате сравнительно-правового анализа уголовного законодательства иностранных государств соискателем установлено, что законодательство не всех стран содержит понятия «преступления, совершаемые в сфере использования информационно-коммуникационных технологий», «компьютерные преступления», «электронные средства платежа», «преступления в финансовой сфере» либо эквивалентные им.

Анализ зарубежного опыта противодействия уголовно-правовыми средствами преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий, показал, что наиболее совершенным в вопросе уголовно-правового противодействия посягательствам в указанной сфере на сегодняшний день является законодательство США. В нем криминализирован широкий спектр деяний, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий: мошенничество, совершаемое с использованием «электронных средств платежа, новых методов и услуг», а также создание, распространение и иные манипуляции с электронными средствами доступа и преступления, связанные с «кражей личности». Конструкция норм американского законодательства позволяет привлекать к ответственности за противоправные деяния в финансо-

вой сфере с использованием новых, еще не получивших широкого распространения информационно-телекоммуникационных технологий.

Государства – члены Евросоюза ратифицировали и применяют Европейскую Конвенцию по борьбе с киберпреступностью. Обязательному внедрению в национальное законодательство подлежат только ст. 2 «Незаконный доступ к информационным системам», ст. 3 «Нарушение неприкосновенности системы», ст. 4 «Нарушение неприкосновенности данных», ст. 5 «Подстрекательство, помощь, пособничество и покушение» указанной Конвенции. Национальное законодательство каждого отдельно взятого государства обладает своими специфическими особенностями. Интересным для имплементации в отечественное уголовное законодательство представляются реализованные в законодательстве Франции и Литвы нормы, предусматривающие ответственность лиц, принимающих поддельную платежную карту к оплате.

Автором отмечается, что традиционно уголовное законодательство стран ближнего зарубежья во многом схоже с отечественным. Указанное обстоятельство объясняется также и активным взаимодействием по борьбе с преступлениями в сфере компьютерной информации в рамках СНГ. Положения Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) нашли свое отражение в законодательстве ряда стран – участниц Содружества: в уголовных кодексах Российской Федерации – в гл. 28 (ст. 272 –274) в разд. IX «Преступления против общественной безопасности и общественного порядка»; Армении – в гл. 24 «Преступления против безопасности компьютерной информации» в разд. 9 «Преступления против общественной безопасности, безопасности компьютерной информации, общественного порядка, общественной нравственности и здоровья населения»; Азербайджана – в гл. 30 «Киберпреступления» в разд. X «Преступления против общественной безопасности и общественного порядка»; Молдовы – в гл. XI «Информационные преступления и преступления в области электросвязи»; Туркменистана – в гл. 33 в разд. XIII «Преступления в сфере компьютерной информации»; Кыргызстана – в гл. 28 в разд. IX «Преступления против общественной безопасности и общественного порядка». Вместе с тем, в ряде стран – участниц СНГ наблюдается активный процесс реформирования уголовного закона. В УК Республики Казахстан введена глава «Уголовные правонарушения в сфере информатизации и свя-

зи» (гл. 7), призванная обеспечить надлежащую уголовно-правовую защиту информационной безопасности, инкорпорированы положения гл. 30 «Преступления против информационной безопасности» Модельного Уголовного кодекса для государств – участников СНГ, а также введены новые составы. Особенно следует отметить, что в новом УК РК нашли отражение случаи совершения преступлений против иных объектов уголовно-правовой охраны с использованием информационно-коммуникационных технологий, например ст. 212 УК РК «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели».

В целом 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 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. Ужесточение ответственности за посягательства с использованием IT-технологий, на наш взгляд, с учетом неограниченности круга потенциальных жертв от преступных действий и размеров причиняемого ущерба, должно быть закреплено и в отечественном законодательстве.

Вторая глава **«Уголовно-правовая характеристика преступлений, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий»** включает два параграфа.

В первом параграфе ***«Преступления, совершаемые с использованием электронных средств платежа»*** автором исследуются признаки составов преступлений, предусмотренных ст. 158, $159^3$, $159^6$ УК РФ, являющихся основными нормами, ориентированными на противодействие хищениям, совершаемым с использованием электронных средств платежа.

Преступления, совершаемые с использованием электронных средств платежа, посягают одновременно на два объекта: основным являются общественные отношения, связанные с правом собственности и правом имущественного обязательства, дополнительным – общественные отношения, складывающиеся в сфере безопасного использования электронных средств платежа, функционирования банковской платежной инфраструктуры и обеспечения информационной безопасности.

При хищении с использованием услуг АТМ-банкинга (посредством использования банкомата) в качестве непосредственного объекта преступного посягательства выступают общественные 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 случае оформления предоплаченной карты или кредитной карты, либо использования электронных денежных средств).

Непосредственным объектом мошенничества с использованием платежных карт (ст. $159^3$ 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. $159^6$ УК РФ) выступают общественные отношения, складывающиеся в сфере распределения и перераспределения и использования денежных средств.

Объективная сторона ст. $159^3$ УК РФ может быть выражена сознательным сообщением заведомо ложных, не соответствующих действительности сведений работнику банка, например оператору, либо сотруднику магазина, например кассиру, относительно подлинности и принадлежности карты; умолчанием об истинной принадлежности карты либо в умышленных действиях по представле-

нию к оплате подложной карты с целью введения работника торговой, кредитной или иной организации в заблуждение.

Объективная сторона состава ст. $159^6$ УК РФ представлена рядом альтернативных действий, влекущих хищение чужого имущества или приобретение права на него, которые могут быть разделены на две группы:

действия, совершаемые с неправомерным использованием реквизитов доступа легального пользователя системы ДБО;

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

В результате исследования установлено, что моментом окончания хищения с использованием электронных средств платежа следует считать момент «обналичивания» похищенных денежных средств либо их перечисления на иной счет, с которого у злоумышленника появляется реальная возможность распоряжаться и пользоваться ими по своему усмотрению.

Преступление, предусмотренное ст. $159^3$ УК РФ, следует считать оконченным с момента оплаты товаров или услуг по подложной платежной карте либо предъявленной чужой карте.

По ст. $159^6$ УК РФ преступление будет считаться оконченным с момента зачисления денег на банковский счет преступника, т. е. с момента, когда он приобретает возможность распоряжаться поступившими денежными средствами по своему усмотрению, например, осуществлять расчеты от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были перечислены.

Организованным группам, созданным для совершения хищений с использованием информационно-телекоммуникационных технологий, свойственны признаки, характерные для всех организованных групп: устойчивость, наличие организатора или руководителя группы и заранее разработанного плана совместной преступной деятельности, распределение функций между членами группы при подготовке к совершению преступления и осуществлении преступного умысла; а также специфические признаки: техническая оснащенность, выражающаяся в разработке специального программного обеспечения, предназначенного для взлома системы защиты кредитных организаций, получения доступа к базам данных, «узкое» распределение ролей в соответствии с преступной «специализацией» и

анонимность. Использование информационно-телекоммуникационных технологий выступает связующим звеном и инструментом создания преступной группы. Установление указанных признаков является необходимым для характеристики группы как организованной.

С субъективной стороны составы мошенничества в сфере компьютерной информации и использования платежных карт характеризуются виной в форме прямого умысла.

Во втором параграфе ***«Преступления, совершаемые в сфере оборота информационно-телекоммуникационных технологий»*** излагаются результаты рассмотрения норм, предусматривающих ответственность за преступные посягательства на оборот информационно-телекоммуникационные технологий.

В ходе исследования установлено, что нормы главы 28 УК РФ наряду со статьей 187 УК РФ, представляются ключевыми уголовно-правовыми предписаниями, предусматривающими ответственность за посягательства на оборот информационно-телекоммуникационных технологий, используемых в финансовой сфере.

В диссертации определено, что в рамках ст. 187 УК РФ законодателем учтено многообразие информационно-телекоммуникационных технологий, используемых при расчетах в системах дистанционного банковского обслуживания, в отношении которых совершаются незаконные манипуляции.

Статья 187 УК РФ с формальным составом, т.е. преступление считается оконченным при совершении любого из указанных в диспозиции деяний.

Преступление, предусмотренное ст. 187 УК РФ, – двухобъектное. Основным непосредственным объектом рассматриваемого состава 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.

Информационно-телекоммуникационные технологии, используемые в финансовой сфере, перечисленные в ст. 187 УК РФ, образуют предмет преступления.

Под платежной картой следует понимать многоэмитентное электронное средство платежа, позволяющее клиенту оператора по

переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов.

Под распоряжениями о переводе денежных средств следует понимать платежные поручения, инкассовые поручения, платежные требования, платежные ордера, а также иные распоряжения о переводе средств оплаты, применяемые в рамках форм безналичных расчетов и определенные Центральным банком России.

Под электронным средством следует понимать техническое устройство или средство, наделенное функционалом по приему, выдаче и переводу денежных средств

Под электронными носителями информации следует понимать материальные объекты, независимо от средств их хранения, обработки и передачи, на которых записываются и хранятся сведения, позволяющие осуществлять неправомерный прием, выдачу, перевод денежных средств.

Под техническими устройствами следует понимать совокупность считывающих и перехватывающих устройств, предоставляющих доступ к счету физического или юридического лица, информационной системе и базе данных кредитной организации, системам дистанционного банковского обслуживания и электронным средствам платежа.

Под компьютерной программой для целей ст. 187 УК РФ следует понимать программу, заведомо предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования информации для неправомерного осуществления приема, выдачи, перевода денежных средств.

В рамках диссертационного исследования 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.

Также было установлено, что под компьютерной информацией следует понимать сведения (сообщения, данные), хранящиеся, обрабатываемые, принимаемые и передаваемые предназначенными для этих целей автоматизированными технологиями.

Третья глава **«Основные направления совершенствования уголовно-правовых мер противодействия преступлениям, со-**

**вершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий»** посвящена вопросам разработки мер по повышению эффективности уголовно-правовой борьбы с преступлениями в финансовой сфере, совершаемыми с использованием информационно-телекоммуникационных технологий.

Первый параграф ***«Совершенствование практики применения уголовно-правовых норм, устанавливающих ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий»*** содержит результаты разработки предложений по оптимизации соответствующей правоприменительной деятельности.

Так, сформулированы рекомендации по квалификации преступлений:

1. Характер использования информационно-телекоммуникационных технологий в финансовой сфере, в частности при совершении хищений, диктует необходимость использования при квалификации рассматриваемых посягательств расширенного толкования понятия мошенничества в сфере компьютерной информации. Вследствие вышеизложенного представляется уместным квалифицировать по ст. $159^6$ УК РФ все хищения в сети Интернет, совершаемые со всеми видами вмешательств в функционирование средств хранения, обработки и передачи компьютерной информации, в том числе и случаи неправомерного доступа и использования систем дистанционного банковского обслуживания, электронных кошельков и реквизитов платежных карт. Такое понимание мошенничества в сфере компьютерной информации, на наш взгляд, позволит сделать данную норму универсальной и применимой ко всем видам корыстных посягательств в IT-сфере.

Вместе с тем, отмечается, что санкционированный перевод средств лицом, являющимся владельцем электронного средства платежа, подвергнутым обману либо введенным в заблуждение относительно подлинности и целей проводимых им действий, квалифицируются по ст. 159 УК РФ.

2. Статья $159^6$ УК РФ является специальной нормой по отношению к ст. 272, 273 УК РФ, так как неправомерный доступ к компьютерной информации, обращаемой в системах дистанционного банковского обслуживания, из корыстной заинтересованности представляет собой действия, направленные на хищение, т.е. компьютерная информация выступает средством доступа к чужому имуществу,

что охватывается объективной стороной ст. $159^6$ УК РФ, ввиду чего в силу ч. 3 ст. 17 УК РФ дополнительной квалификации по ст. 272 УК РФ преступных посягательств в IT-сфере не требуется.

3. Под уголовно-правовой запрет ст. $159^3$ УК РФ подпадают действия, характеризующиеся сознательным сообщением заведомо ложных, не соответствующих действительности сведений работнику банка, например оператору, либо сотруднику магазина или кассиру относительно подлинности платежной карты либо умолчанием об истинной принадлежности карты или в умышленных действиях по представлению к оплате подложной карты с целью введения работника торговой, кредитной или иной организации в заблуждение.

Иные виды незаконных действий по использованию платежной карты под действие данной нормы не подпадают, и должны быть квалифицированы либо по ст. 158 УК РФ как тайное хищение – при использовании банкомата (в соответствии с разъяснениями, данными в постановлении Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»), либо по ст. $159^6$ УК РФ – при иных видах хищений и использовании различных видов информационно-телекоммуникационных технологий.

4. Статья 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 (т.е. в целях фишинга или скимминга), ввиду чего дополнительной квалификации деяния по ст. 273 УК РФ не требуется.

5. DDos-атаки (распределенные атаки на информационно-телекоммуникационное устройство, направленные на вывод его из строя) в зависимости от направленности умысла могут быть разделены на совершаемые с целью:

получить имущественную выгоду;

скрыть другое преступление;

привлечь внимание общественности к той или иной проблеме либо выразить протест, а также из хулиганских побуждений;

оправдать террористическую деятельность либо публично призывать к осуществлению террористической или экстремистской деятельности.

При совершении DDos-атаки с целью получить имущественную выгоду содеянное следует квалифицировать по ч. 2 ст. 273 УК РФ, так как: 1) действия совершаются из корыстной заинтересованности; 2) программа, используемая для DDos-атаки, создается и используется для блокирования компьютерной информации.

При совершении DDos-атаки с целью скрыть другое преступление содеянное также следует квалифицировать по ч. 1 ст. 273 УК РФ.

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.

Второй параграф ***«Перспективные пути оптимизации российского уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий»*** посвящен вопросам совершенствования нормативных основ противодействия преступлениям в финансовой сфере, совершаемым с использованием информационно-телекоммуникационных технологий.

В диссертации разработаны основные пути оптимизации отечественного уголовного законодательства об ответственности за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий.

Аргументирована целесообразность дополнения ст. $159^3$ УК РФ ч. 5 в следующей редакции:

«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, –

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо арестом на срок до шести месяцев».

Обоснована целесообразность исключения из примечания к ст. $159^1$ УК РФ указания на ст. $159^3$ и $159^6$ УК РФ с целью распространения на данные статьи определения крупного и особо крупного размера ущерба, предусмотренного в примечании к ст. 158 УК РФ.

Аргументирована необходимость 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.

Доказана необходимость дополнения ч. 1 ст. 63 УК РФ пунктом «н[1]»: «совершение преступления с использованием информационно-телекоммуникационных технологий».

Соискателем установлено, что оборот криптовалют не охватывается содержанием диспозиции ст. 187 УК РФ, предусматривающей ответственность за неправомерный оборот средств платежей. Ввиду особенностей экономико-правовой природы криптовалют видится необходимым установление уголовной ответственности за их использование в рамках отдельной нормы, предусматривающей ответственность за оборот денежных суррогатов.

«Статья 187[1]. Оборот денежных суррогатов

1. Изготовление (выпуск), приобретение в целях использования или сбыта, а равно сбыт или использование денежных суррогатов, –

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо лишением свободы на срок до пяти лет.

2. Те же деяния, совершенные организованной группой, а равно лицом, выполняющим управленческие функции в финансовой организации, –

наказываются лишением свободы на срок до семи лет либо штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от двух до четырех лет.

Примечание. Под денежными суррогатами в настоящей статье понимаются любые нелегитимные средства, не являющиеся валютой Российской Федерации и иностранной валютой, оборот которых установлен законодательством Российской Федерации, способные выполнять функции меры стоимости, средства обращения, платежа, накопления и мировых денег».

В **заключении** подведены итоги исследования, сформулированы основные выводы и предложения.

**Основные научные результаты диссертации опубликованы в следующих работах автора:**

***Научные статьи, опубликованные в изданиях, рекомендованных Минобрнауки России:***

1. Хисамова З.И. Сравнительно-правовой анализ уголовного законодательства стран ближнего зарубежья, предусматривающего ответственность за преступления в сфере осуществления расчетов с использованием электронных средств платежа // Юристъ-Правоведъ. – 2014. – № 4. – С. 83–88 (0,7 п. л.).
2. Хисамова З.И. Понятие и сущность преступлений, посягающих на информационную безопасность в сфере экономики // Общество и право. – 2015. – № 1. – С. 157–161 (0,6 п. л.).
3. Хисамова З.И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. – 2015. – № 3. – С. 127–132 (0,7 п. л.).
4. Хисамова З.И. Неправомерный оборот средств платежей в контексте норм об ответственности за преступления, совершаемые в отношении информационно-коммуникационных технологий // Общество и право. – 2015. – № 4. – С. 139–144 (0,7 п. л.).
5. Хисамова З.И. Уголовно-правовое противодействие новым видам угроз в информационной сфере // Вестник Краснодарского университета МВД России. – 2015. – № 4. – С. 136–139 (0,5 п. л.).
6. Хисамова З.И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий // Юридический мир. – 2016. – № 2. – С. 58–62 (0,5 п. л.).
7. Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. – 2016. – № 1. – С. 117–120 (0,6 п. л.).

***Научные статьи, опубликованные в иных изданиях:***

8. Хисамова З.И. Использование пластиковых банковских карт при хищении денежных средств // Материалы III студенческой юридической олимпиады Краснодарского края: сб. ст. – Краснодар: Вика-Принт, 2012. – С. 282–286 (0,3 п. л.).
9. Хисамова З.И. Карточное мошенничество в современной России // Актуальные проблемы правоохранительной деятельности

органов внутренних дел: сб. ст. по материалам Всерос. науч.-практ. конф. – Екатеринбург: Уральский юридический институт МВД России, 2012. – С. 145–148 (0,3 п. л.).

10. Хисамова З.И. К вопросу о защите рынка пластиковых карт // Современные проблемы уголовной политики: материалы III Междунар. науч.-практ. конф., 28 сент. 2012 г.: в 2 т. / под ред. А.Н. Ильяшенко. – Краснодар: Краснодарский университет МВД России, 2012. – Т. II. – С. 388–393 (0,4 п. л.).

11. Хисамова З.И. Кардерство в современной России // Вестник Краснодарского университета МВД России. – 2012. – № 3. – С. 97–100 (0,5 п. л.).

12. Хисамова З.И. Преступления в сфере дистанционного банковского обслуживания // Актуальные вопросы науки и практики: материалы Всерос. науч.-практ.конф. – Краснодар: Краснодарский университет МВД России, 2013. – Т. III. – С. 139–145 (0,4 п. л.).

13. Хисамова З.И. Возможности дистанционного банковского обслуживания для транснациональной организованной преступности // Юридическая практика (трибуна молодых ученых): сб. ст. – Нижний Новгород: Нижегородская академия МВД России, 2013. – С. 258 – 262 (0,3 п. л.).

14. Хисамова З.И. Преступления в сфере дистанционного банковского обслуживания как вид транснациональной организованной преступности // Безопасность личности, общества и государства: теоретико-правовые аспекты: материалы VII Междунар. науч.-практ. конф. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2013. – С. 137–141 (0,3 п. л.).

15. Хисамова З.И. К вопросу о предмете преступлений, совершаемых с использованием электронных средств платежа // Современные проблемы уголовной политики: материалы IV Междунар. науч.-практ. конф., 27 сент. 2013 г.: в 3 т. / под ред. А.Н. Ильяшенко. – Краснодар: Краснодарский университет МВД России, 2013. – Т. III. – С. 242–252 (0,6 п. л.).

16. Хисамова З.И. Криминалистическая характеристика механизма легализации («отмывания») доходов, полученных преступным путем через банковскую систему // Криминалистика и судебно-экспертная деятельность в условиях современности: материалы Междунар. науч.-практ. конф.: в 2 т. – Краснодар: Краснодарский университет МВД России, 2013. – Т. II. – С. 8–15 (0,4 п. л.).

17. Хисамова З.И. Проблемы уголовно-правовой квалификации мошенничества в сфере компьютерной информации с использо-

ванием электронных средств платежа // Современные проблемы уголовной политики: материалы V Междунар. науч.-практ. конф., 3 окт. 2014 г.: в 3 т. / под ред. А.Н. Ильяшенко. – Краснодар: Краснодарский университет МВД России, 2014. – Т. III. – С. 166–174 (0,5 п. л.).

18. Хисамова З.И. К вопросу об уголовной ответственности за преступления, совершаемые в сфере оборота информационно-коммуникационных технологий // Криминалистика и судебно-экспертная деятельность в условиях современности: материалы III Всерос. науч.-практ. конф., 24 апр. 2015 г. – Краснодар: Краснодарский университет МВД России, 2015. – С. 330–337 (0,5 п. л.).

19. Хисамова З.И. Уголовная ответственность за преступления, совершаемые в отношении информационно-коммуникационных технологий // Современные проблемы уголовной политики: материалы VI Междунар. науч.-практ. конф., 25 сен. 2015 г.: в 2 т. – Краснодар: Краснодарский университет МВД России, 2015. – Т. II. – С. 271–278 (0,5 п. л.).

20. Хисамова З.И. Генезис развития отечественного уголовного законодательства за преступления, совершаемые в сфере использования информационно-коммуникационных технологий // Уложение о наказаниях уголовных и исправительных 1845 года: концептуальные основы и историческое значение (к 170-летию со дня принятия): материалы Междунар. науч.-практ. конф., г. Геленджик, 2–3 октября 2015 г. – Краснодар: Кубанский государственный университет; Просвещение-Юг, 2016. – С. 599 – 603 (0, 2 п. л.).

**Иные публикации:**

21. Хисамова З.И. Кардинг как новый вид IT-преступности: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2013. – 108 с. (6,3 п. л.).

Подписано в печать 13.07.2016. Печ. л. 1,5.
Тираж 120 экз. Заказ 467.

---

Краснодарский университет МВД России.
350005, Краснодар, ул. Ярославская, 128.