МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Уголовная ответственность за преступления, посягающие на информационную безопасность в сфере экономики (ст.159.3,159.6,187 УК РФ)

Болдиной Натальи Александровны

Направление подготовки 40.03.01 – «Юриспруденция»
юридического факультета СГУ им. Н.Г.Чернышевского

Автореферат бакалаврской работы

Научный руководитель
зав. кафедрой уголовного, экологического права
и криминологии, д.ю.н,
профессор _____ Н.Т. Разгельдеев

Заведующий кафедрой
уголовного, экологического права
и криминологии, д.ю.н,
профессор _____ Н.Т. Разгельдеев

Саратов 2020

Введение

Актуальность темы исследования. В последние десятилетия стремительно развиваются информационно-телекоммуникационных технологии (далее - IT-технологии), что привело к появлению совершенно новому формату взаимоотношений в обществе. Широкое внедрение информационных технологий затронуло все сферы жизни современного общества. Финансовая отрасль также 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.

Расширение сферы применения е IT-технологий, их совершенствование и развитие, 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.

Совокупность этих указанных обстоятельств определяет актуальность и социальную значимость проведения уголовно-правового исследования вопросов установления и реализации уголовной ответственности за преступления, посягающие на информационную безопасность в сфере экономики.

Целью выпускной квалификационной работы состоит в комплексном уголовно-правовом исследовании вопросов противодействия преступлениям, посягающим на информационную безопасность в сфере экономики, разработке предложений по повышению эффективности уголовно-правового противодействия данным общественно опасным деяниям.

Для решения поставленной цели поставлены следующие **задачи:**

1) разработка понятия и классификация преступлений, посягающих на информационную безопасность в сфере экономики;

2) сравнительно-правовой анализ законодательства зарубежных государств, предусматривающего уголовную ответственность за преступления, посягающие на информационную безопасность в сфере экономики;

3) уголовно-правовой анализ составов преступлений, посягающих на информационную безопасность в сфере экономики;

4) разработка рекомендаций по квалификации преступлений, посягающих на информационную безопасность в сфере экономики;

5) определение основных направлений совершенствования уголовного законодательства, касающегося рассматриваемых преступлений.

Объект исследования - общественные отношения, возникающие в связи с совершением преступления, посягающего на информационную безопасность в сфере экономики.

Предметом исследования выступают уголовно-правовые нормы, предусмотренные ст. 158, 159.3, 159.6, 187, 272–274 УК РФ, материалы соответствующей правоприменительной практики, результаты социологических исследований и специальных исследований рынка IT-технологий и банковского сектора, а также зарубежное уголовное законодательство.

Теоретическую основу включает в себя результаты исследований, проведенных другими авторами, а также анализа рынка IT-технологий и банковского сектора, проведенные независимыми компаниями, результаты контент-анализа средств массовой информации.

Методологической основой исследования являются общенаучные, специальные и частные методы изучения научного и эмпирического материала. В процессе получения искомой информации использованы также социологические методы: изучение статистических данных, документов,

экспертные оценки. Выводы, полученные в ходе исследования, основываются на достижениях наук отечественного уголовного права, криминологии, общей теории права, психологии, социологии, философии.

В ходе написания работы были проанализированы правовые и иные источники - Конституция РФ, Федеральное законодательство, Указы Президента РФ и Постановления Правительства РФ, а также материалы судебно-следственной практики.

Структура работы обусловлена поставленными целями и задачами и состоит из введения, трех глав, которые разделены на параграфы, заключения и списка используемых источников.

Основное содержание работы

В первой главе ***«Социально-правовая природа уголовной ответственности за преступления, посягающие на информационную безопасность в сфере экономики»*** выпускной квалификационной работы обосновывается актуальность темы исследования, раскрывается степень ее разработанности; определяются объект, предмет, цель и задачи исследования; характеризуются методологическая, нормативная, теоретическая и эмпирическая основы; раскрывается значимость работы.

В частности в первом параграфе *«Понятие и классификация преступлений, посягающих на информационную безопасность в сфере экономики»* рассматривается социально-правовая природа информационно-телекоммуникационных технологий, а также преступлений, посягающих на информационную безопасность в сфере экономики, совершаемых с использованием IT-технологий.

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

сфере экономики, совершаемые с использованием IT-технологий, могут быть разделены на преступления, совершаемые с использованием электронных средств платежа, и преступления, совершаемые в сфере оборота информационно-телекоммуникационных технологий.

Во втором параграфе *«Сравнительно-правовой анализ зарубежного уголовного законодательства об ответственности за преступления, посягающие на информационную безопасность в сфере экономики»* проведенными исследованиями установлено, что наиболее совершенным в вопросе уголовно-правового противодействия посягательствам в указанной сфере на сегодняшний день является законодательство США. В этом законодательстве криминализирован широкий спектр деяний, совершаемых в экономической сфере с использованием IT-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 финансовой сфере с использованием новых, еще не получивших широкого распространения IT-технологий.

Государства – члены Евросоюза ратифицировали и применяют Европейскую Конвенцию по борьбе с киберпреступностью. Национальное законодательство каждого отдельно взятого государства обладает своими специфическими особенностями. Интересным для имплементации в отечественное уголовное законодательство представляются реализованные в законодательстве Франции нормы, предусматривающие ответственность лиц, принимающих поддельную платежную карту к оплате.

В целом на сегодняшний день в мире наблюдается два подхода в уголовно-правовом противодействии преступлениям, посягающим на информационную безопасность в сфере экономики, совершаемых с использованием IT-технологий.

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

Второй подход обусловлен выделением преступлений, посягающих на информационную безопасность в сфере экономики, совершаемых с использованием IT-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.

Вторая глава ***«Уголовно-правовая характеристика преступлений, посягающих на информационную безопасность в сфере экономики»*** состоит из двух параграфов.

В первом параграфе второй главы *«Преступления, совершаемые с использованием электронных платежных средств и систем*» исследуются признаки составов преступлений, предусмотренных ст. 158, 159.3, 159.6 Уголовного Кодекса РФ, являющихся основными нормами, ориентированными на противодействие хищениям, совершаемым с использованием электронных средств платежа.

Установлено, что преступления, совершаемые с использованием электронных средств платежа, являются двухобъектными.

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, либо права, возникающего из имущественного обязательства.

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 относительно подлинности и принадлежности карты; умолчанием об истинной принадлежности карты либо в умышленных действиях по представлению 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.

Установлено, что организованным группам, созданным для совершения хищений с использованием информационно-телекоммуникационных технологий, свойственны признаки характерные для всех организованных групп. Использование информационно-телекоммуникационных технологий выступает связующим звеном и инструментом создания преступной группы.

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

Во втором параграфе выпускной квалификационной работы *«Преступления, совершаемые в сфере оборота IT-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.

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.

Для целей ст. 187 УК РФ рассмотрены следующие определения: платежной карты, распоряжений о переводе денежных средств, электронных средств, электронных носителей информации, технических устройств, компьютерной программы, компьютерной информации.

В рамках работы 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.

Третья глава ***«Необходимость усовершенствования уголовного законодательства в части противодействия преступлениям, посягающим на информационную безопасность в сфере экономики»*** 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, посягающие на информационную безопасность в сфере экономики»* содержит результаты разработки предложений по оптимизации соответствующей правоприменительной деятельности.

Так, сформулированы рекомендации по квалификации преступлений:

1. Характер использования IT-технологий в финансовой сфере, в частности при совершении хищений, диктует необходимость использования при квалификации рассматриваемых посягательств расширенного толкования понятия мошенничества в сфере компьютерной информации.

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 относительно подлинности платежной карты либо умолчанием об истинной принадлежности карты или в умышленных действиях по представлению к оплате подложной карты. Иные виды незаконных действий по использованию платежной карты под действие данной нормы не подпадают.

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.

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

Разработаны основные пути оптимизации отечественного уголовного законодательства об ответственности за преступления, посягающие на информационную безопасность в сфере экономики, совершаемым с использованием информационно-телекоммуникационных технологий.

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