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

ШАМЬЕНОВ НАИЛЬ РУШАНОВИЧ

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление подготовки 40.04.01 – «Юриспруденция»
юридического факультета СГУ им. Н.Г.Чернышевского

Автореферат магистерской работы

Научный руководитель
к.ю.н, доцент, профессор кафедры уголовного,
экологического права и криминологии Ф.А. Вестов

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

Саратов 2021

Введение

Актуальность темы исследования заключается в том, что проблема компьютерных преступлений или «киберпреступности» хотя и нова, но активно существует уже на протяжении более тридцати лет, а с развитием компьютерных технологий приобретает всё более новые черты и особенности. Поскольку пользование цифровым пространством сети Интернет продолжает набирать обороты, и уже: хранит персональные данные большинства людей планеты, электронные средства платежа, является способом коммуникаций и международным рынком сбыта, местом доступа к хранилищам информации и даже способом организации работы и дистанционного управления инфраструктурой государства, – то не приходится много говорить о важности безопасности, защищенности и целостности передаваемой информации, доступности работы серверов и сетей, а также необходимости всестороннего понимания способов совершения преступных деяний и грамотного описания норм уголовного законодательства в сфере преступлений компьютерной информации.

Каждый сбой работы компьютерной сети причиняет не только моральный (репутационный), но и материальный ущерб для работников предприятий и сетевых администраторов. По мере развития «безбумажного» документооборота, «безналичного» расчёта, дистанционного и автоматизированного управления – каждый серьёзный сбой локальных сетей может, например, парализовать работу целых корпораций и банков, сектора связи, энергетики и медицины, или дестабилизировать координацию деятельности правоохранительных органов, что приводит к ощутимым материальным потерям и иным рискам издержек «стабильности». Говоря не о воздействии на критически важную информационную инфраструктуру государства, любая незаконная манипуляция с компьютерной информации прежде всего затрагивает фундаментальные конституционные права граждан.

Способы совершения преступлений в сфере компьютерной информации чрезвычайно многообразны. Это и несанкционированный

доступ к информации хранящейся в компьютере или сервере, и ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему, и разработка и распространение компьютерных вирусов, и хищение компьютерной информации. Компьютерное преступление также может произойти из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.

Следовательно, актуальность затронутой темы очевидна, поскольку именно от уровня ее теоретической разработки во многом зависят практические результаты.

Степень разработанности темы исследования. В отечественном уголовном праве исследованию проблем противодействия компьютерной преступности, а также проблем квалификации преступлений в сфере компьютерной информации свои научные труды посвятили такие учёные, как Р.В. Амелин, И.Р. Бегишев, В. М. Быков , С. Ю. Бытко, А.Г. Волеводз, А.Н. Попов, А.Л. Репецкая, И.П. Родивилин, В.В. Сверчков, В.Г. Степанов-Егиянц, А.А Шаевич, и др.

Объектом исследования являются общественные отношения, подвергающиеся посягательству в результате совершения преступлений в сфере компьютерной информации. Объектом посягательств могут быть как сами технические средства (компьютеры и устройства) так и программное обеспечение и базы данных, для которых технические средства являются носителем.

Предметом исследования являются применяемые к объекту исследования отечественные уголовно-правовые нормы с сфере компьютерной информации и киберпреступности.

Цель настоящего исследования – провести критический анализ норм 28 Главы УК РФ, рассмотрев уголовно-правовую характеристику путем комплексного и всестороннего исследования действующего законодательства

и международного опыта борьбы с преступлениями в сфере компьютерной информации как части компьютерной преступности, для разработки нового подхода к квалификации преступлений и конкретных предложений направленных на совершенствование уголовного законодательства РФ.

Для достижения поставленной цели необходимо решить следующие **задачи**:

– всесторонне раскрыть уголовно-правовую характеристику объективной и субъективной стороны составов преступлений в сфере компьютерной информации, проанализировав нормы права устанавливающих уголовную ответственность за преступления в сфере компьютерной информации;

– выявить характерные признаки компьютерных преступлений и их отличительные особенности, а также проанализировать конструкции составов преступлений в сфере компьютерной информации;

– изучить международный опыт в сфере компьютерной информации;

– изучить материалы судебной практики по делам преступлений в сфере компьютерной информации;

– определить существующие проблемы и сформулировать предложения по совершенствованию законодательства.

Научная новизна исследования заключается в выявлении проблем касающихся целого ряда вопросов урегулирования уголовно-правовой охраны компьютерной информации, и выявлении недостатков диспозиции уголовных норм, которые не позволяют квалифицировать новые действия в кибрепространстве как самостоятельные преступления и оставляют часть преступных действий вне рамок уголовно-правовой оценки и квалификации. Автором также будет предпринята попытка предложить новый подход к квалификации ряда компьютерных преступлений посягающих на безопасность и доступность компьютерной информации, с вытекающими предложения по внесению изменений в уголовно-правовые запреты в сфере защиты компьютерной информации в Российской Федерации.

В ходе исследования будет проведён компаративистский анализ уголовного законодательства Российской Федерации, международного права и зарубежного опыта в области противодействия преступлениям в сфере компьютерной информации и компьютерным преступлениям в частности.

Положения выносимые на защиту:

1. Анализ состава ст. 273 УК РФ указал на существующую неопределенность момента, когда вредоносная компьютерная программа считается созданной.

2. В работе проведен глубокий анализ квалификации компьютерных атак и доказывается целесообразность дополнить Главу 28 УК РФ нормой, предусматривающей ответственность за компьютерные атаки, включая DoS и DDoS-атаки повлекшие нарушение функционирования компьютерной информационной системы, поскольку сейчас большая часть всех аспектов деяния находятся вне рамок уголовно-правовой квалификации.

3. В целях совершенствования и последующей результативности противодействия компьютерным преступлениям, ссылаясь на рассмотренную в работе зарубежную практику на примере УК КНР и ввиду имеющихся сложностей квалификации хищения денежных средств ввиду противоречивости П.20 и П.21 ППВС РФ от 30.11.2017 № 48, определена целесообразность введения уголовной ответственности за «создание и владение фишинговыми сайтами» с формальной конструкцией состава преступления.

4. Полноценно раскрыв в работе сущность криптоджекинга, в работе доказывается целесообразность дополнить УК РФ нормой предусматривающий уголовную ответственность за «скрытый майнинг», поскольку сейчас невозможно полноценно подвергать уголовно-правовой оценке все аспекты посягательства и последствия ущерба.

5. Проведенный компаративистский анализ УК ФРГ указывает на целесообразность криминализировать «продажу паролей и кодов доступа» в случае существенности таких данных в количественной или качественной

характеристики, что равным образом согласуется с предложенным в ст. 6 Конвенции Совета Европы о преступности в сфере компьютерной информации.

Теоретическая значимость исследования заключается в том, что изложенные в настоящей работе теоретические положения и выводы обобщают текущее состояние и имеющиеся возможности уголовно-правовой оценки деяний в сфере компьютерной информации и компьютерных преступлений в частности. Проведенный компаративистский анализ отражает зарубежный опыт противодействия компьютерной преступности в целом, так как именно конструкция законодательных норм предопределяет возможности уголовно-правовой квалификации при попытке привлечь к уголовной ответственности правовыми способами.

Практическая значимость исследования заключается в возможности использования полученных выводов с целью дальнейшего совершенствования уголовного законодательства, либо путем использования собранного материала в учебном процессе при подготовке курсов учебных дисциплин читаемых студентам юридического направления.

Апробация результатов. Положения и выводы магистерского исследования докладывались автором на конференции: VII Международная научно-практическая конференция на тему: «Трансформация права и правоохранительной деятельности в условиях развития цифровых технологий в россии, странах снг и европейского союза: проблемы законодательства и социальной эффективности».

По теме исследования опубликованы работы:

1. Вестов Ф.А., Шамьенов Н.Р. Актуальность ответственности DoS и DDoS-атак в уголовном праве в сфере компьютерной информации // Базис. – 2020. – №1 (7). – С. 13 – 16.

2. Вестов Ф.А., Шамьенов Н.Р. Уголовная политика по использованию возможностей цифровых технологий в противодействии мошенничеству // Основы экономики, управления и права. – 2020. – №6 (25). – С. 53 – 57.

3. Шамьенов, Н.Р. Фишинг и фарминг как разновидность компьютерного мошенничества // Трансформация права и правоохранительной деятельности в условиях развития цифровых технологий в России, странах СНГ и Европейского союза: проблемы законодательства и социальной эффективности: материалы VII Международной научно-практической конференции преподавателей, практических сотрудников, студентов, магистрантов, аспирантов, соискателей. Часть 2. Сборник научных статей. Саратов : Саратовский источник, 2020. – 242 с. – С. 192 – 197.

Методологическую основу исследования составит комплексное применение всеобщих, общенаучных, частнонаучных и частноправовых методов познания – диалектического, формально-юридического, сравнительно-правового, юридического толкования, анализа и синтеза.

Теоретической основой данного исследования послужили научные труды в области уголовного права и криминологии.

Правовой основой исследования послужили: Конституция Российской Федерации, современное уголовное законодательство России, Указы Президента, Федеральные Законы и Постановления Пленумов Верховного Суда Российской Федерации, а также нормативные акты РФ.

Структура работы состоит из введения, трех глав состоящих из одиннадцати параграфов, заключения и списка использованной литературы.

Основное содержание работы

В первой главе магистерской работы рассматривается уголовно-правовой анализ преступлений в сфере компьютерной информации ст. 272-274.1 УК РФ.

В частности первый параграф посвящен определению предмета и объективных признаков преступлений в сфере компьютерной информации.

Во втором параграфе рассматриваются субъективные признаки преступлений в сфере компьютерной информации.

В третьем параграфе были раскрыты особенности квалификации преступлений в сфере компьютерной информации, совершаемых группой лиц.

Вторая глава «Особенности и проблемы квалификации преступлений в сфере компьютерной информации» состоит из пяти параграфов, каждый из которых индивидуально рассматривает вопросы квалификации различных форм компьютерных преступлений, совершаемых в сфере компьютерной информации.

В первом параграфе второй главы раскрывается: неправомерный доступ к компьютерной информации; существующая ненаказуемость за юридически неправомерное владение и распоряжение аутентификационными данными; квалификация перехвата цифровой информации.

Во втором параграфе рассматриваются терминологические вопросы определения вредоносности, заведомости, момента создания, и предоставления вредоносной компьютерной программы исходя из действующей формулировки ст. 273 УК РФ, а также невозможность полноценно подвергать уголовно-правовой оценке все аспекты посягательства и последствия ущерба скрытого майнинга, квалификация которого на данный момент исходит от ст. 273 УК РФ.

В третьем параграфе раскрывается квалификация должностного нарушения правил работы с информацией.

В рамках четвертого параграфа второй главы рассмотрена квалификация компьютерных атак и способы их совершения, особо рассмотрена разновидность DoS и DDoS-атак, совершение которых нарушает функциональность компьютерных систем без неправомерного доступа и путем использования вредоносного ПО не в отношении потерпевшего, что оставляет вне уголовно-правовой оценки суть деяния.

В пятом параграфе исследованы вопросы квалификации фишинга и фарминга как разновидности компьютерного мошенничества.

Третья глава магистерской работы посвящена исследованию международного и зарубежного опыта в борьбе с компьютерными преступлениями.

В частности в первом параграфе третьей главы рассматривается Конвенция Совета Европы о компьютерных преступлениях.

Во втором параграфе проводится компаративистский анализ уголовного законодательства Казахстана, Германии (ФРГ), Австрии, Китая (КНР) на предмет преступлений в сфере компьютерной информации, в частности компьютерных преступлений в целом.

Третий параграф третьей главы посвящен предложениям, направленным на совершенствование мер уголовно-правовой борьбы с преступлениями в сфере компьютерной информации.

Заключение

В заключении обращается внимание на статистику, причины латентности, не заинтересованность лиц обращаться в правоохранительные органы, практические и процессуальные проблемы правоприменителя, нехватку специалистов, отсутствие политической воли создать удобные механизмы пресечения фишинга, а также подводятся итоги магистерского исследования.

В ходе проведенного исследования напрашиваются теоретические и практические выводы, согласно которым необходимо:

1) законодательно определить, в какой момент для квалификации по ст. 273 УК РФ вредоносное ПО следует считать созданным. Сформулировать определение можно следующим образом: «*признак создания вредоносной компьютерной программы* в пригодном для применения виде выражается в *наличии завершенной для работы структуре программного кода и пользовательского интерфейса* с помощью которого возможно управление программой, а равно в случае передачи *наличие вместе всех из необходимых частей алгоритмов и текстов программ которым не хватает компиляции*,

равно в случае если присутствует неполноценный программный код (условно созданный) требующий активация по прилагающейся инструкции»;

2) законодательно определить, что диспозиция ст. 273 УК РФ предусматривает ответственность за распространение вредоносных компьютерных программ в том числе путем «предоставления» доступа к вредоносным программам. Предлагаемая формулировка диспозиции в ч. 1 ст. 273 УК РФ: «Создание, распространение, *предоставление* или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»;

3) улучшить формулировку материального по конструкции состава ч. 2 ст. 274.1 УК РФ в отношении такого элемента состава преступления как «причинение вреда» КИИ для однозначной интерпретации уровня общественной опасности. Предлагается замена формулировки в ст. 274.1 «причинение вреда» на термин «причинение крупного ущерба» широко используемый в ст. 272-274 УК РФ – это ущерб, сумма которого превышает один миллион рублей. Предлагаемая формулировка ч. 2 ст. 274.1 УК РФ: «Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек *причинение крупного ущерба* критической информационной инфраструктуре Российской Федерации»;

В целях совершенствования уголовного законодательства и возможности полноценно подвергать уголовно-правовой оценке все аспекты посягательства и последствий ущерба, необходимо:

4) дополнить Главу 28 УК РФ нормами, предусматривающими ответственность за компьютерные атаки повлекшие нарушение функционирования компьютерной информационной системы. Сформулировать диспозицию статьи про кибератаки, охватывающей в том числе DoS и DDoS-атаки, можно следующим образом: Компьютерная атака – *«целенаправленное информационное воздействие на вычислительную систему с помощью троянских программ, сетей ботнет, и иных программ или программно-аппаратных средств, направленное на нарушение её функционирования или лишившее пользователей возможности получения доступа к запрашиваемому электронному ресурсу*». С принятием этой нормы, в случае, если такая атака осуществляется с помощью вредоносных программ, то их использование охватывается предложенным составом и не требует дополнительной квалификации по статье 273 УК РФ, являясь способом совершения преступления;

5) ввести новую уголовную ответственность за «создание и владение фишинговыми сайтами» с формальной конструкцией состава преступления. Сформулировав диспозицию статьи следующим образом: «*Создание и владение поддельными интернет-ресурсами* (настоящих организаций, банков, интернет-магазинов, социальных сетей и т.п.) *вводящими в заблуждение по внешнему виду и схожей ссылке веб-сайта*, с *целью неправомерно завладеть аутентификационными и персональными данными* (банковскими реквизитами), *либо денежными средствами* (в случае покупки с такого сайта)»;

6) дополнить УК РФ нормой, предусматривающий ответственность за криптоджекинг. Сформулировать диспозицию статьи за «скрытый майнинг» можно следующим образом: «*использование чужих вычислительных устройств* (компьютеров, смартфонов, планшетных ПК, серверов и т.п.) *с помощью вредоносных программ* (майнер-бот) *без ведома их владельцев с целью скрытого майнинга криптовалют*». С принятием этой нормы, использование майнер-бота (не вредящего компьютерной информации, а

использующего вычислительные ресурса устройства) будет охватываться предложенным составом и не требовать дополнительной квалификации по статье 273 УК РФ, являясь способом совершения преступления. Санкция данной статьи должна быть взаимозависима от суммарного причиненного ущерба и размера незаконно полученной прибыли, а полученный результат конфисковаться (поскольку слишком привлекательным выглядит преступление), а в случае добровольной выдачи – служить смягчающим обстоятельством;

7) криминализировать «продажу паролей и кодов доступа» в случае существенности таких данных в количественной или качественной характеристики. Предлагаемая формулировка новой статьи: «*хранение* (для себя и в целях продажи)*, продажа или передача другому лицу паролей или других кодов безопасности, которыми лицо не имеет юридического права обладать и распоряжаться, и за счет которых можно получить неправомерный доступ* к компьютерной информации, электронному кошельку, учетной записи и т.п»;

И поскольку на данный момент присутствуют противоречия в П. 20 и 21 ППВС РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»., так в 1 абзаце П. 21 сказано, что вне зависимости от того, каким образом преступник получил доступ к логину и паролю потерпевшего, деяние должно квалифицироваться как кража, однако 2 абзац П. 21 прямо утверждает, что такое преступление является мошенничеством. В этом усматривается внутреннее противоречие толкования Верховным Судом РФ уголовно-правовых запретов, установленных статьями 158, 159, 159.3 и 159.6 УК РФ. Однако основным объектом в преступлениях, связанных с хищениями, являются общественные отношения по охране собственности, поэтому вносить какие-либо изменения в статьи Главы 28 УК РФ в связи с возможностью хищения денежных средств с помощью неправомерного доступа к компьютерной информации, представляется менее нецелесообразным. Однако более подробные и чёткие

разъяснения на уровне Пленума Верховного Суда РФ по поводу квалификации хищений совершенных с помощью фишинга и его более опасной формы фарминга способствовали бы более правильному и последовательному применению норм Главы 28 и Главы 21 Уголовного кодекса Российской Федерации.

В свою очередь, комплексная разработка правовых механизмов в области майнинга и криптовалюты способствовала бы процессуальному облегчению процедуру доказывания и расширению доступного инструментария правоприменителя при привлечению «криптозлоумышленников» к уголовной ответственности.