МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.05.02 Правоохранительная деятельность
(код и наименование направлению подготовки, специальности)

Оперативно-розыскная деятельность
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Преступления в сфере Интернет»

Студент М.О. Кузнецова
(И.О. Фамилия) (личная подпись)

Руководитель канд, экон. наук, С.Б. Сыропятова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Аннотация

Современное социально-экономическое и технологическое развитие мирового сообщества, включая российское государство, проходит активный этап внедрения высоких технологий фактически во все сферы жизнедеятельности – как на уровне корпораций, так и на уровне рядовых граждан. Информационное развитие отечественной цифровой индустрии и Интернет-пространства во многом позволило в настоящий момент сохранить доступность самого широкого спектра услуг и товаров в связи с вынужденными ограничениями, введёнными в России в связи с пандемией коронавирусной инфекции в 2020 г., а также позволило многим и многим организациям от мелкого до крупного бизнеса сохранить своё участие в гражданско-правовом обороте и минимизировать потенциальный ущерб экономике страны в данном контексте. Достоинства происходящих процессов цифровизации всех сфер общественной жизни очевидны, но параллельно с положительными аспектами данных процессов происходит активное внедрение новейших технологий в практику противоправных посягательств, что актуализирует вопрос противодействия данным посягательствам.

Цель работы: комплексный анализ вопросов противодействия преступлениям в сфере Интернет в Российской Федерации.

Вопросы, связанные с преступлениями в сети Интернет, являются предметом исследований многих авторов в последние годы. Следует выделить в данном контексте работы таких авторов как: Дремлюга Р.И., Ефремова М.А., Иванова Л.В., Осипенко А.Л., Тропина Т.Л. и других авторов.

Структурно работа состоит из введения, трёх глав, заключения и списка используемой литературы и используемых источников.

Оглавление

Введение

Актуальность выбранной темы выпускной квалификационной работы заключается в том, что современное социально-экономическое и технологическое развитие мирового сообщества, включая российское государство, проходит активный этап внедрения высоких технологий фактически во все сферы жизнедеятельности – как на уровне корпораций, так и на уровне рядовых граждан.

Не случайно в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, отмечается, что «информационные системы, социальные сети стали частью повседневной жизни россиян. Пользователями сети «Интернет» в России в 2016 году стали более 80 млн. человек» [45].

Сейчас мало кто может представить современную жизнь без использования компьютерных технологий, а также глобальной сети Интернет, которые используются не только для развлечения, как это было в середине 90-х годов XX столетия, а для реализации повседневных нужд, коммуникативного взаимодействия и оперативного решения самого широкого спектра вопросов.

Электронный документооборот активно внедряется в деловую практику, взаимодействие в гражданско-правовом обороте всё больше строится дистанционно, с проведением всех финансовых операций посредством Интернет-технологий. Кроме того, сами отечественные государственные органы активно стимулируют организацию сетевого взаимодействия с гражданами, организуя получение госуслуг через специальный Интернет-портал, дающий возможность оптимизировать, ускорить и сделать максимально «прозрачным» такой процесс.

Информационное развитие отечественной цифровой индустрии и Интернет-пространства во многом позволило в настоящий момент сохранить доступность самого широкого спектра услуг и товаров в связи с вынужденными ограничениями, введёнными в России в связи с пандемией коронавирусной инфекции в 2020 г., а также позволило многим и многим организациям от мелкого до крупного бизнеса сохранить своё участие в гражданско-правовом обороте и минимизировать потенциальный ущерб экономике страны в данном контексте. Достоинства происходящих процессов цифровизации всех сфер общественной жизни очевидны, но параллельно с положительными аспектами данных процессов происходит активное внедрение новейших технологий в практику противоправных посягательств на разные объекты уголовно-правовой охраны, установленные нормами действующего Уголовного кодекса Российской Федерации [43] (УК РФ).

«Ущерб от киберпреступлений оценивается в 2018 году свыше 400 млрд. рублей, а ущерб мировой экономике от подобных деяний по прогнозам за 2020 г. может возрасти до 3 трлн. долларов США» [24] – отмечается в прессе.

Более того, со всей очевидностью можно утверждать, что «преступления такого рода обладают высокой степенью латентности» [40, с. 15], на что обращают внимание специалисты.

Степень разработанности темы исследования. Вопросы, связанные с преступлениями в сети Интернет, являются предметом исследований многих авторов в последние годы. Следует выделить в данном контексте работы таких авторов как: Дремлюга Р.И., Ефремова М.А., Иванова Л.В., Осипенко А.Л., Тропина Т.Л. и других авторов.

Объект исследования – общественные отношения, складывающиеся в связи с противодействием преступлениям в сети Интернет (киберпреступлениям).

Предмет исследования – нормы российского права, а также материалы правоприменительной практики, касающиеся вопросов противодействия преступлениям в сфере Интернет (киберпреступлениям).

Цель исследования – комплексный анализ вопросов противодействия преступлениям в сфере Интернет в Российской Федерации.

Задачи исследования:

- сформулировать понятие преступности в сфере Интернет (киберпреступности);
- определить подход к классификации преступлений в сфере Интернет (киберпреступлений) по УК РФ;
- рассмотреть состояние и тенденции преступности в сфере Интернет (киберпреступности);
- обозначить проблемы квалификации отдельных киберпреступлений;
- сформулировать предложения, направленные на совершенствование нормативного регулирования противодействия преступности в сфере Интернет (киберпреступности) уголовно-правовыми средствами;
- проанализировать проблемы предупреждения киберпреступности.

Теоретическая значимость работы состоит в разработке соответствующих научных категорий, связанных с противодействием преступлениям в сфере Интернет (киберпреступлениям).

Практическая значимость работы обусловлена необходимостью совершенствования нормативно-правовой регламентации положений, касающихся противодействия (в том числе уголовно-правовыми средствами) преступлениям в сфере Интернет (киберпреступлениям), поскольку это может способствовать снижению показателей киберпреступности.

Структура исследования. Работа состоит из введения, трёх глав, разделённых на отдельные параграфы, заключения и списка используемой литературы и используемых источников.

Глава 1 Понятие и общая характеристика преступности в сфере Интернет (киберпреступности)

1.1 Понятие преступности в сфере Интернет (киберпреступности)

В нашей стране нормативные предпосылки для противодействия преступлениям в сфере высоких технологий появились с принятием УК РФ, в котором нашла своё место глава 28 «Преступления в сфере компьютерной информации».

Тем не менее, противоправные деяния, в сфере информационных технологий не сводятся только лишь к обозначенным в вышеназванной главе составам преступлений, с учётом того, что в целом ряде норм УК РФ, посвящённым различным противоправным посягательствам, законодатель предусмотрел соответствующие конструктивные или квалифицирующие признаки, состоящие в использовании виновным электронных, или информационно-телекоммуникационных сетей, в том числе сети Интернет.

В этой связи нуждается в теоретической разработке вопрос определения понятия противоправных посягательств, совершаемых с использованием компьютерных технологий, в том числе, в сфере Интернет, поскольку без такого понятия вопрос классификации таких преступлений и их уголовно-правового и криминологического анализа попросту невозможен.

Только таким образом можно определить круг таких деяний, проанализировать отдельные проблемы, связанные с их квалификацией, сформулировать предложения по совершенствованию существующего нормативного регулирования противодействия совершению данных преступлений уголовно-правовыми средствами, я также по совершенствованию способов предупреждения преступности такого рода.

Следует отметить, что в рассматриваемом контексте в науке и правоприменительной практике используются самые разные обороты с разным смысловым содержанием. Однако, наибольшую популярность обретает использование таких взаимосвязанных категорий, как «киберпреступность» и «киберпреступления».

Само понятие «киберпреступность» появилось ещё в 80-е годы XX века в связи с началом развития компьютерной индустрии, как указывает Л.И. Бутусова [6, с. 28]. На международном уровне этот термин активно используется на протяжении последних десятилетий [7, 18, 37].

Тем не менее, в российском законодательстве такой оборот не раскрывается, хотя в Концепции внешней политики Российской Федерации [46] в числе вызовов и угроз современного мира, имеющих трансграничную природу, называется киберпреступность.

Как указывают отдельные авторы, термин «киберпреступность» используется, в основном, для определения преступности, связанной с компьютеров, информационными технологиями [13, с. 35].

Российский законодатель и правоприменитель, как правило, говоря о преступлениях, связанных с высокими технологиями используют категории «цифровой», «информационный» и т.д.

В Стратегии национальной безопасности Российской Федерации [47] говорится о новых формах противоправной деятельности с использованием «информационных, коммуникационных и высоких технологий».

В Доктрине информационной безопасности Российской Федерации [44], под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием

названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Исходя из такого подхода, «информационная безопасность» и «кибербезопасность», как видится, выступают в качестве синонимов.

В науке спектр треминологических оборотов ещё шире. Помимо категории «киберпреступления», авторы оперируют такими понятиями как: «преступления в сфере информационных технологий» [2; 52], «информационные преступления» [31; 56], «сетевые компьютерные преступления» [30], «интернет-преступления» [12; 54].

Отдельные авторы [14, с. 27] высказывают доводы относительно целесообразности использования категории «киберпреступность» и «киберпреступления» ввиду лаконичности и содержательности понятий.

В ряде работ говорится о том, что категории «киберпреступление» и «киберпреступность» содержательно шире смежных понятий, таких как, например, «компьютерные преступления», или «преступления, с использованием компьютерных технологий», поскольку «включает в себя преступные деяния с использованием как глобальных сетей, информационных технологий, так и компьютеров» [11, с. 316].

Кроме того, А.И. Халиуллина полагает, что данный термин наиболее предпочтителен ещё и «в силу быстро изменяющихся процессов в области информационных технологий и появления новых способов обмена информацией» [50, с. 35].

С данным подходом вполне можно согласиться.

Далее необходимо выделить признаки киберпреступлений. Представляется, что помимо общих признаков, характеризующих деяние как преступное и наказуемое, в соответствии с требованиями УК РФ,

киберпреступления характеризуются дополнительными признаками, позволяющими отграничить их от других категорий преступлений.

К числу отличительных характеристик подобной группы противоправных посягательств следует отнести следующие:

- в качестве средства совершения преступления выступают средства компьютерной (а также иной цифровой техники) и информационно-телекоммуникационные сети, в том числе сеть Интернет, для достижения преступного результата;
- в качестве основного, либо дополнительного объекта противоправного посягательства присутствуют общественные отношения в сфере безопасности обращения компьютерной информации. При этом, дополнительным объектом могут выступать самые разные отношения (отношения собственности, общественные отношений, которые связаны с гарантиями суверенитета и государственной целостности страны и т.д.);
- субъективная сторона такого рода посягательства характеризуется только умышленной формой вины (данные деяния не могут совершаться по легкомыслию, либо по небрежности);
- совершение такого рода посягательства, как правило, требует специальных знаний в сфере компьютерных и (или) Интернет-технологий.

Исходя из отмеченных признаков, можно попытаться сформулировать следующие определения киберпреступления и киберпреступности.

Ведущим признаком киберпреступлений следует считать первый из обозначенных признаков – использование виновным компьютерных (а также иных цифровых) технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, при совершении противоправного посягательства.

Что же касается последнего из признаков – наличие специальных знаний в сфере компьютерных и (или) Интернет-технологий, то этот признак, хотя и присутствует, как правило, при совершении киберпреступлений, тем не менее, включать его в искомое понятие «киберпреступление» не целесообразно, ввиду сложности определения того, какие именно знания в рассматриваемой сфере следует считать специальными, а какие таковыми не являются. Многие знания и навыки работы с компьютерами и сетью Интернет, ввиду распространения данных технологий и пристального внимания к ним со стороны молодёжи, становятся доступны неопределённому кругу молодых людей, в то время как лица более старшего возраста (например, старше 50 лет), оказываются не способными выполнить достаточно простые, доступные даже рядовому школьнику, действия в Интернет-пространстве или с использованием компьютера. Причём, чем старше возраст лица, тем больше вероятность отсутствия у него даже элементарных в современном мире навыков работы с компьютерными и (или) Интернет-технологиями.

Таким образом, опираясь на сказанное, можно сформулировать следующее определение киберпреступления.

Киберпреступление – это умышленное общественно опасное деяние, предусмотренное УК РФ, совершенное с использование виновным компьютерных (а также иных цифровых) технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающее на общественные отношения в сфере безопасности обращения компьютерной информации в качестве основного, либо дополнительного объекта посягательства.

При таком понимании категории «киберпреступление», понятие «киберпреступность» следует понимать следующим образом.

Киберпреступность – это совокупность преступлений, совершаемых с использование виновным компьютерных (а также иных цифровых)

технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающих на общественные отношения в сфере безопасности обращения компьютерной информации в качестве основного, либо дополнительного объекта посягательства.

Сформулировав обозначенные определения, представляется возможным перейти к выделению и классификации преступлений в сфере Интернет (киберпреступлений) в нормах действующего УК РФ.

1.2 Классификация преступлений в сфере Интернет (киберпреступлений) по УК РФ

Действующий УК РФ содержит главу 28 «Преступления в сфере компьютерной информации», включающей в себя всего четыре статьи с 272 по 274.1 УК РФ: неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерное воздействие на критическую информационную инфраструктуру РФ.

Ряд авторов [38, с. 2], отождествляя между собой компьютерные преступления и киберпреступления сводят последние лишь к тем составам противоправных деяний, что содержатся в упомянутой главе 28 УК РФ. Однако, исходя из более широкого подхода, проводить такое равенство нет никаких оснований.

Необходимо помнить о том, что кроме деяний, включённых законодателем в главу 28 УК РФ, в целом ряде статей УК РФ содержится конструктивный, либо квалифицирующий признак совершения деяния «с

использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»».

Конструктивный признак использования высоких технологий при совершении преступления содержится только в ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», а также в ст. 171.2 УК РФ «Незаконные организация и проведение азартных игр», ст. 185.3 УК РФ «Манипулирование рынком», ст. 258.1 УК РФ «Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации», ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».

В виде признака, который увеличивает общественную опасность деяния и, соответственно, влечёт возможность дифференциации ответственности и применения более строгого наказания, совершение деяния с использованием электронных или информационно-телекоммуникационных сетей содержится всего в тринадцати составах уголовного закона:

- три состава в главе «Преступления против жизни и здоровья» (п. «д» ч. 2 ст. 110 УК РФ «Доведение до самоубийства», п. «д» ч. 3 ст. 110.1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства», ч. 2 ст. 110.2 УК РФ «Организация деятельности, направленной на побуждение к совершению самоубийства»);
- один состав в главе «Преступления против семьи и несовершеннолетних» (п. «в» ч. 2 ст. 151.2 УК РФ «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего»);

- один состав в главе «Преступления против общественной безопасности» (ч. 2 ст. 205.2 УК РФ «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»);
- пять составов в главе «Преступления против здоровья населения и общественной нравственности» (п. «б» ч. 2 ст. 228.1 «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», п. «б» ч. 3 ст. 242 УК РФ «Незаконные изготовление и оборот порнографических материалов или предметов», п. «г» ч. 2 ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», п. «г» ч. 2 ст. 242.2 «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов», п. «г» ч. 2 ст. 245 УК РФ «Жестокое обращение с животными»);
- один состав в главе «Экологические преступления» (п. «б» ч. 2 ст. 258.1 «Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации»);
- два состава в главе «Преступления против основ конституционного строя и безопасности государства» (ч. 2 ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности», ч. 2 ст. 280.1 УК РФ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации»).

Исходя из признаков киберпреступления, которые были выделены выше, к числу таковых можно отнести ещё несколько составов противоправных деяний:

- п. «г» ч. 3 ст. 158 УК РФ содержит особо квалифицированный состав – кража с банковского счёта, а равно в отношении электронных денежных средств;
- ст. 159.3 УК РФ устанавливает ответственность за мошенничество с использованием электронных средств платежа.

Отнесение обозначенных деяний к анализируемой нами категории преступлений обусловлено тем, что в качестве средства совершения преступления виновным используются средства компьютерной (а также иной цифровой техники) и информационно-телекоммуникационные сети, в том числе сеть Интернет, для достижения преступного результата.

Кроме того, в данных составах фигурирует особый предмет посягательства (безналичные денежные средства, либо электронные средства платежей, возникшие в гражданско-правовом обороте в результате развития информационных технологий и внедрения их в банковский сектор), доступ к которому обуславливается применением вышеназванных средств совершения противоправного деяния.

Таким образом, с учётом отмеченных особенностей преступлений в сфере Интернет (киберпреступлений) и анализа норм УК РФ, можно сделать вывод о том, что можно выделить следующие разновидности данных деяний и классифицировать их на две категории:

- специальные преступления в сфере Интернет (киберпреступления);
- общеуголовные преступления в сфере Интернет (киберпреступления).

Специальные преступления в сфере Интернет (киберпреступления) – это преступления, посягающие на общественные отношения в сфере безопасности

обращения компьютерной информации в качестве основного объекта. К числу таковых относятся составы преступлений, предусмотренные главой 28 УК РФ:

- ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»;
- ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»;
- ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;
- ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Общеуголовные преступления в сфере Интернет (киберпреступления) – это составы преступлений, совершаемые с использование виновным компьютерных (а также иных цифровых) технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающие на общественные отношения в сфере безопасности обращения компьютерной информации в качестве дополнительного объекта посягательства.

К таковым можно отнести деяния, в основном составе, либо в квалифицирующих признаках которых присутствует признак в виде совершения преступления с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Соответственно к данной категории преступлений в сфере Интернет (киберпреступлений) можно отнести следующие противоправные деяния:

- п. «д» ч. 2 ст. 110 УК РФ «Доведение до самоубийства»;
- п. «д» ч. 3 ст. 110.1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства»;
- ч. 2 ст. 110.2 УК РФ «Организация деятельности, направленной на побуждение к совершению самоубийства»);
- ст. 137 УК РФ «Нарушение неприкосновенности частной жизни»;

- п. «в» ч. 2 ст. 151.2 УК РФ «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего»);
- п. «г» ч. 3 ст. 158 УК РФ «Кража»;
- ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа»;
- ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»;
- ст. 171.2 УК РФ «Незаконные организация и проведение азартных игр»;
- ст. 185.3 УК РФ «Манипулирование рынком»;
- ч. 2 ст. 205.2 УК РФ «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»;
- п. «б» ч. 2 ст. 228.1 «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества»;
- п. «б» ч. 3 ст. 242 УК РФ «Незаконные изготовление и оборот порнографических материалов или предметов»;
- п. «г» ч. 2 ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»;
- п. «г» ч. 2 ст. 242.2 «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов»;
- п. «г» ч. 2 ст. 245 УК РФ «Жестокое обращение с животными»;
- ст. 258.1 УК РФ «Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или)

охраняемым международными договорами Российской Федерации» (включая п. «б» ч. 2 ст. 258.1);

- ч. 2 ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности»;
- ч. 2 ст. 280.1 УК РФ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации»;
- ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».

При этом, вопрос выделения новых составов преступлений в сфере Интернет (киберпреступлений) в Особенной части УК РФ нуждается в дополнительной проработке, необходимость в которой назрела ввиду продолжаемого развития Интернет-технологий и бурной цифровизации всех сфер общественной жизни.

Далее, для получения более чёткого представления о масштабах и динамике преступности в сети Интернет (киберпреступнотси) представляется необходимым проанализировать состояние такой преступности и обозначить основные тенденции, связанные с распространением преступности в сети Интернет (киберпреступнотси) по Российской Федерации.

1.3 Состояние и тенденции преступности в сфере Интернет (киберпреступности)

Киберпреступность, как отмечается в современных публикациях, является одной из глобальных угроз развитого «цифрового» общества. При этом, сам уровень технологического развития на современном этапе, во многом, предопределяет её, поскольку киберпреступность – закономерное следствие глобализации информационно-коммуникационных технологий.

С учётом развития Интернет-индустрии, данный сегмент преступности является наиболее быстрорастущим, так как в настоящее время продолжается

неуклонный рост числа Интернет-пользователей, а также параллельный рост профессионализма лиц, совершающих преступления данного рода.

Как отмечается в публикациях, «любые информационные и технические новации значительно расширяют сферу киберпреступности и создают условия для повышения эффективности хакерских атак. Поэтому киберпреступность растет более быстрыми темпами, чем все другие виды преступности» [9, с. 9].

Согласно обзорам несанкционированных переводов денежных средств Центрального банка России, за 2017 г. количество и объем несанкционированных операций с использованием платежных карт составил 296 698 фактов на объем 1,08 млрд руб. Рост показателей за 2016 г. на 30 % выше аналогичных показателей 2016 г. Официальная статистика преступлений, совершенных с использованием телекоммуникационных и компьютерных технологий за 2017 г., составляет 79 704 преступления.

В 2018 г. объем несанкционированных операций составил 961,3 млн. руб., что меньше аналогичного показателя за 2017 г. на 10,6 %. Количество операций составило 317 178 фактов. Официальная статистика преступлений, совершенных с использованием телекоммуникационных и компьютерных технологий за год, составляет 59 904 преступления.

По данным Банка России, количество несанкционированных операций с использованием карт, имитированных на территории России, увеличилось. Рост операций произошел на 34,6 %. Объем всех несанкционированных операций с использованием платежных карт составил в 2019 г. 1 384,7 млн. руб., что на 44 % больше аналогичного показателя 2018 г. Количество операций составило 416 933 единицы, что больше на 31,4 % аналогичного показателя за 2018 г. (317 178). Официальная статистика преступлений, совершенных с использованием телекоммуникационных и компьютерных технологий за 2019 г., составляет 68 418 преступлений [55].

В соответствии с данными Прокуратуры РФ количество ряда Интернет-преступлений в 2019 году претерпело значительное увеличением – выросло с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России

преступных деяний составляет 4,4 % – это почти каждое 20 преступление. Самыми распространенными преступлениями в сети Интернет, являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). Если в 2019 году зарегистрировано 1 883 таких преступления (+7,7 %), то за первое полугодие 2020 г. – 1 233 (+3,4 %). При этом на 19,6% уменьшилось количество расследованных преступлений по указанным статьям (с 903 до 726), выросло на 30,5 % (с 790 до 1031) число нераскрытых преступлений, раскрываемость данных преступлений составила 41,3%. Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Их количество в первом полугодии 2020 г. возросло в 7 раз [8].

В период с января по октябрь 2020 года правоохранительными органами РФ зарегистрировано 107 тыс. 980 преступлений, совершенных с использованием телекоммуникационных технологий или в сфере компьютерной информации. Ущерб от этих преступлений составил почти 400 млрд. рублей. Это на 44 % больше аналогичного показателя прошлого года [21, с. 53].

По данным, приводимым Д.Н. Карповой, «в списке стран с высоким уровнем совершаемых преступлений в виртуальной среде Россия занимает 1-е место и одновременно относится к группе самых незащищенных от киберугроз государств» [17, с. 46].

В настоящее время сохраняется тенденция высокой латентности преступлений в сфере Интернет, на что обращают внимание многие исследователи. Красноречиво иллюстрирует данный тезис информация из обзора Банка России: «в правоохранительные органы при несанкционированных операциях с использованием платежных карт обращалось только 4 % потерпевших, 1 % не обращались вообще и в 95 % случаев информация отсутствует» [55].

К сожалению, сами физические и юридические лица, выступающие потерпевшими по данного рода преступлениям отказываясь обращаться по фактам противоправных деяний в сфере Интернет в правоохранительные органы таким образом оказывают услугу киберпреступникам, способствуя повышению и без того высокой латентности киберпреступлений, формируя иллюзию безнаказанности и провоцируя дальнейшую преступную деятельность в анализируемой сфере.

Как уже было отмечено ранее, подавляющее большинство киберпретуплений совершается лицами, имеющими специальные знания в сфере информационных технологий.

Как пишут в публикациях, «количество киберпреступлений с использованием специальных знаний в сфере финансово-хозяйственной деятельности, в программном обеспечении банковской деятельности, в операциях с использованием платежных карт, в сфере банковских счетов юридических лиц постоянно растет. Соответственно, особое место в профессиональной преступности занимают киберпреступники» [22, с. 53].

«Киберпреступник не изолирован от общества, поэтому он постоянно повышает преступную квалификацию параллельно с научно-техническим прогрессом в обществе. Тем самым проявляется его специализация в данном виде преступной деятельности» [39, с. 199] – справедливо отмечается исследователями.

Таким образом, одной из тенденций современной киберпреступности является повышение профессионального уровня лиц, совершающих данные преступления.

Несмотря на то, что отдельные киберпреступления могут совершаться лицами, чьи навыки использования компьютерной техники не выходят за рамки общедоступных, однако, совершение сложных по своему характеру киберпреступлений, сопряжённых с вторжением в защищённые компьютерные сети, созданием и использованием вредоносных программ,

требует достаточно высокого уровня подготовки и наличия специальных знаний в рассматриваемой сфере.

Профессиональный преступник, овладев соответствующими навыками в сфере информационных технологий, может длительное время совершать тодественные деяния, используя развитую сеть вывода денежных средств, что позволяет длительное время оставаться не установленным как лицу, совершившему преступление.

Как отмечается отдельными авторами, объединение киберпреступников в группы по профессиональному критерию является также распространённой тенденцией: «У данных лиц имеются отдельные защищенные помещения (съемные квартиры, офисы и т.д.), оборудованные современными технологическими средствами и компьютерами, которые используются в их преступной, корыстной деятельности. Киберпреступники широко используют приемы социальной инженерии» [21, с. 57].

Как указывают отдельные авторы, «киберпреступность носит корыстный характер, но присутствуют и другие мотивы, такие как самоутверждение, деструктивные стремления и протестные настроения. Для киберпреступника противоправная деятельность хоть и, как правило, не является единственным средством к существованию, но относится к основному источнику дохода» [15, с. 37].

С учётом специфики специальных преступления в сфере Интернет (киберпреступлений), виновные, в большинстве ситуаций, совершают не одно, а множество тождественных (или подобных) противоправных деяний, что способствует повышению внутренней уверенности в собственном профессионализме и, как следствие, безнаказанности, а также укрепляя веру в то, что правоохранительные органы не смогут привлечь виновного в такого рода деянии к ответственности, несмотря на наличие соответствующего уголовно-правового запрета.

Таким образом, киберпреступники – это многоэпизодные преступники, однако в абсолютном большинстве не привлекавшиеся к уголовной

ответственности. Вместе с тем 4,7 % из них имеют неснятые и непогашенные судимости за различные преступления [22, с. 54].

Данные криминологических исследований свидетельствуют, что «из числа выявленных лиц, совершивших киберпреступления, в среднем лишь третья часть подвергалась осуждению. Все осужденные киберпреступники – мужчины. Киберпреступников можно распределить по следующим возрастным группам: наиболее криминально активными являются возрастные группы 18-24 лет (39,6 %) и 25-29 лет (30,6 %). На возрастную группу 50 лет и старше приходится около 3 % преступников, что, видимо, связано с меньшей осведомлённостью лиц данной возрастной группы с современными телекоммуникационными устройствами и технологиями» [3, с. 6].

Оценивая уровень образования лиц, совершающих преступления в сфере Интернет, можно констатировать его уровень выше средних показателей. Многие лица, совершающие деяния анализируемой нами категории преступлений имеют высшее образование (примерно 35 % осужденных), среднее специальное образование имеет около 40 %. Подобные сведения относительно образовательного уровня видятся закономерными, так как сам характер совершаемых противоправных деяний требует определенной квалификации, а также соответствующих знаний, связанных с программированием, а также применением высокотехнологического оборудования.

Среди осужденных за противоправные деяния, совершаемые с использованием сети Интернет (киберпреступления) имеются представители всех социальных слоев населения, преобладают рабочие (23,4 %) и служащие (14,4 %) [3, с. 7].

Нравственно-психологическая характеристика личности киберпреступника может включать достаточно много разнообразных составляющих. Отдельный интерес представляет потребностно-мотивационной сфере. Как отмечается в ряде публикаций, «ведущими

мотивами киберпреступников являются самоутверждение, корысть, деструктивные стремления и протестные настроения» [19, с. 36].

Причём желание самоутвердиться часто не только переплетается с корыстным мотивом, но и доминирует над ним. Для личности киберпреступника могут быть свойственны трудности в коммуникативном взаимодействии с социумом, правовой нигилизм.

По итогам первой главы работы сформулируем основные выводы.

В плане терминологии в науке и правоприменительной практике используются самые разные обороты с разным смысловым содержанием. Однако, наибольшую популярность обретает использование таких взаимосвязанных категорий, как «киберпреступность» и «киберпреступления». Российский законодатель и правоприменитель, как правило, говоря о преступлениях, связанных с высокими технологиями используют категории «цифровой», «информационный» и т.д.

Тем не менее, категории «киберпреступление» и «киберпреступность» содержательно шире смежных понятий, таких как, например, «компьютерные преступления», или «преступления, с использованием компьютерных технологий».

Исходя из отмеченных выше признаков, можно сформулировать следующие определения киберпреступления и киберпреступности.

Киберпреступление – это умышленное общественно опасное деяние, предусмотренное УК РФ, совершенное с использование виновным компьютерных (а также иных цифровых) технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающее на общественные отношения в сфере безопасности обращения компьютерной информации в качестве основного, либо дополнительного объекта посягательства.

Киберпреступность – это совокупность преступлений, совершаемых с использование виновным компьютерных (а также иных цифровых)

технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающих на общественные отношения в сфере безопасности обращения компьютерной информации в качестве основного, либо дополнительного объекта посягательства.

Киберпреступность, как отмечается в современных публикациях, является одной из глобальных угроз развитого «цифрового» общества. При этом, сам уровень технологического развития на современном этапе, во многом, предопределяет её, поскольку киберпреступность – закономерное следствие глобализации. С учётом развития Интернет-индустрии, данный сегмент преступности является наиболее быстрорастущим, так как в настоящее время продолжается неуклонный рост числа Интернет-пользователей, а также параллельный рост профессионализма лиц, совершающих преступления данного рода.

Одной из ключевых тенденций современной преступности в сфере Интернет (киберпреступности) является сохранение её высокой латентности, а также дальнейшее усиление профессионализма киберпреступников, что предопределяет необходимость противодействия данному негативному явлению как уголовно-правовыми средствами, так и средствами криминологической профилактики.

Далее уделим внимание проблемам квалификации отдельных преступлений, совершаемых в сфере Интернет (киберпреступлений), а также сформулируем предложения, направленные на совершенствование нормативного регулирования противодействия преступности в сфере Интернет (киберпреступности) уголовно-правовыми средствами.

Глава 2 Анализ проблем квалификации преступлений в сфере Интернет (киберпреступлений)

2.1 Проблемы квалификации отдельных преступлений, совершаемых в сфере Интернет (киберпреступлений)

В рамках анализа проблем квалификации отдельных преступлений, совершаемых в сфере Интернет (киберпреступлений), представляется возможным уделить внимание лишь некоторым составам таких уголовно наказуемых деяний – актуальным и обсуждаемым в современных научных публикациях.

Относительно проблем квалификации неправомерного доступа к компьютерной информации (ст. 272 УК РФ) в правоприменительной практике есть сложности в плане толкования такого квалифицирующего признака рассматриваемого деяния, как совершение деяния из корыстной заинтересованности, ввиду смешения данного состава преступления с преступлениями против собственности.

Корыстная заинтересованность означает стремление виновного получить для себя или других лиц выгоду имущественного характера (денег, имущества или прав на его получение и т. п.).

В частности, сложности на практике представляет оценка действий лиц, выразившихся в получении различных материальных благ посредством использования учетных данных законных пользователей.

Так, согласно описательной части постановления Железнодорожного районного суда г. Рязани, «О., являясь работником ПАО «Р.», получил логин и пароль для доступа цифровому телевидению, которые имел право использовать только в служебных целях. Однако с помощью полученных данных О. осуществил подключение своего домашнего телевизора и приобрел платный контент на сумму 30 509 руб. Следственные органы квалифицировали деяния О. по ч. 2 ст. 272 УК РФ, т.е. как неправомерный

доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, совершенный из корыстной заинтересованности» [32].

Тем не менее, подобная юридическая оценка представляется спорной. В соответствии с Постановлением Пленума Верховного Суда РФ от 30.11.2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [33] «в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным, такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети» (п. 21 Постановления).

В приведенном примере виновный лишь ввел имеющиеся у него логии и пароль, и никаким образом в работу самих информационно-телекоммуникационных сетей не вмешивался.

Правильным в этом контексте видится подход, реализованный Козельским районным судом Калужской области. «П. передала своему знакомому Р. свою банковскую карту Сбербанка России во временное пользование, сообщив при этом «пин-код» карты. Не уведомив П., Р. с помощью банкомата подключил к указанной банковской карте банковские услуги «Мобильный банк» и «Сбербанк Онлайн», привязав их к номеру своего сотового телефона и получив тем самым необходимые пароли для доступа к системе и возможность контролировать баланс карты и осуществлять перевод денежных средств. В последующем Р. зашел в систему «Сбербанк онлайн» и перевел с лицевого счета П. на лицевой счет своей банковской карты денежные средства в сумме 8400 руб. Органами предварительного следствия действия Р. были квалифицированы по п. «в» ч. 2 ст. 158 УК РФ, ч. 3 ст. 183 УК РФ и ч. 2 ст. 272 УК РФ. Однако по ходатайству государственного обвинителя Д. суд исключил из предъявленного Р. обвинения излишне

вмененные ч. 3 ст. 183 УК РФ и ч. 2 ст. 272 УК РФ, поскольку умысел Р. был направлен на хищение денежных средств, а получение пароля к «Сбербанк Онлайн» явилось лишь способом совершения преступления» [34].

Сложности связаны и с разграничением состава преступления, предусмотренного ст. 159.6 УК РФ со смежными составами противоправных уголовно наказуемых деяний.

В объективной действительности хищения с использованием компьютерных технологий совершаются различными способами, однако законодатель фактически вынуждает правоприменителя квалифицировать такие преступления по статье 159.6 УК РФ «Мошенничество в сфере компьютерной информации».

Когда с использованием компьютерных технологий совершается тайное хищение имущества, на практике имеют место квалификация и по ст. 158 УК РФ и по статье 159.6 УК РФ при сходных обстоятельствах. Подобную противоречивую квалификацию можно встретить в случаях, когда правоохранительные органы исходят из того, что не все устройства именуются компьютерами.

Так, «Г., заключив договор на обслуживание с компанией сотовой связи, обнаружил, что номер его сим-карты подключен к банковской карте другого лица. Г. произвел перевод денежных средств с банковской карты потерпевшего на счет своего друга З. З. вместе с Г. распорядились данными средствами по своему усмотрению. Действиям Г. и З. судом была дана оценка как кража по пункту «а» ч. 2 ст. 158 УК РФ. Органы предварительного следствия и суд посчитали, что средства связи, а именно мобильный телефон, не относятся к средствам хранения, обработки и передачи компьютерной информации. По мнению правоохранительных органов и суда, сеть оператора сотовой связи не является информационно-телекоммуникационной сетью» [35].

Говоря о проблемах конкуренции ст. 159.6 УК РФ и ст. 272, 273 УК РФ, следует сказать о том, что в литературе по этому вопросу имеют место достаточно категоричные формулировки.

Так, З.И. Хисамова пишет, что «ст. 159.6 УК РФ является специальной по отношению к ст. 272, 273 УК РФ. Суть ее рассуждений заключается в том, что неправомерный доступ к компьютерной информации из корыстной заинтересованности является действием, направленным на хищение, следовательно, компьютерная информация выступает средством доступа к чужому имуществу, что входит в объективную сторону ст. 159.6 УК РФ. В силу требований ч. 3 ст. 17 УК РФ дополнительной квалификации по статьям 272, 273 УК РФ не требуется» [53, с. 119].

Внёс ясность Пленум Верховного Суда РФ, выразивший свою позицию в уже упомянутом выше Постановлении от 30.11.2017 г. № 48: «Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст.ст. 272, 273 или 274.1 УК РФ» (п. 20 Постановления).

В рамках данного параграфа, представляется целесообразным рассмотреть также ряд проблем, связанных с введением в УК РФ сравнительно недавно нескольких новых составов преступлений, совершаемых в сфере Интернет (киберпреступлений). К числу таковых относятся составы противоправных деяний, предусмотренных ст. 110.1 «Склонение к совершению самоубийства или содействие совершению самоубийства» и ст. 110.2 «Организация деятельности, направленной на побуждение к совершению самоубийства».

Обозначенные деяния в качестве преступных и наказуемых были внесены в УК РФ относительно недавно – в 2017 г. Федеральным законом от 07.06.2017 г. № 120-ФЗ [49] в качестве реакции на возникновение новой формы противоправной деятельности, совершаемой в сети «Интернет» и

способной причинить огромнейший вред обществу, поскольку данная деятельность направлена на причинение смерти, путём склонения к совершению самоубийства неопределённого числа людей, преимущественно несовершеннолетних, как наиболее уязвимой для соответствующего воздействия категории.

Факты осуществления подобной деятельности получили огласку в 2016 г., став, настоящей проблемой, всколыхнувшей общественность.

Речь идет о так называемых «группах смерти», которые в данный период стали возникать на просторах Интернет-пространства, обретая широкую аудиторию в лице многочисленных подростков, активно пользующихся социальными сетями для общения и развлечения.

Наибольшую популярность приобрели данные сообщества, созданные в одной из самых популярных российских социальных сетей – в социальной сети «ВКонтакте».

На момент выявления соответствующей противоправной деятельности, посягающей на наиболее важную ценность – жизнь человека, правоприменитель столкнулся с определённым правовым пробелом, связанным с тем, что гипотеза ст. 110 УК РФ не предполагала возможность привлечения к уголовной ответственности лицо за склонения к самоубийству или содействия совершению самоубийства, а также организации деятельности, направленной на побуждение к совершению самоубийства.

До внесения соответствующих корректив в действующее уголовное законодательство, путём криминализации указанных действий, привлечь к ответственности за доведение до самоубийства (или покушения на самоубийство) можно было лишь тогда, когда виновный для достижения данного преступного результата применял к потерпевшему угрозы, жестокое обращение или же систематически унижал его человеческое достоинство.

Законодатель не предполагал, что склонение неопределённого числа лиц к совершению самоубийства может возникнуть в качестве целенаправленной деструктивной деятельности, реализуемой в соучастии, имеющей в своей

основе чёткое следование поставленной преступной цели, а также психологическую базу, позволяющую манипулировать неокрепшей подростковой психикой.

В контексте криминализации подобной деятельности, с введением ст.ст. 110.1 и 110.2 УК РФ, законодатель расширил и дополнил ч. 2 ст. 110 УК РФ, включив в неё в качестве отягчающих ответственность целый ряд критериев:

- несовершеннолетний возраст потерпевшего, а равно нахождение потерпевшего заведомо для виновного в беспомощном состоянии либо в материальной или иной зависимости от виновного;
- совершение преступления в отношении женщины, заведомо для виновного находящейся в состоянии беременности;
- совершение преступления в отношении двух или более лиц;
- совершение преступления группой лиц по предварительному сговору или организованной группой;
- совершение преступления посредством публичного выступления, публично демонстрируемого произведения, СМИ или информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Ответственность за квалифицированные виды доведения до самоубийства была установлена на порядок более суровая, чем за совершение деяний по ч. 1 ст. 110 УК РФ: лишение свободы на срок от 8 до 15 лет.

В рамках новых составов преступлений (ст. 110.1 и 110.2 УК РФ) ответственность дифференцирована, но за совершение деяния при наличии особо квалифицирующих вину обстоятельств, ответственность установлена аналогичной строгости – до 15 лет лишения свободы.

Несмотря на то, что рассматриваемые составы не предполагают обязательное совершение деяния посредством сети «Интернет», тем не менее, на практике данные деяния совершаются именно с использованием глобальной сети, позволяющей обезличено и дистанционно воздействовать на

личность. В этой связи, представляется целесообразным уделить внимание обозначенным противоправным деяниям в рамках данного параграфа работы.

Несмотря на общую целесообразность и правильность выделения указанных выше новых составов преступлений, многие авторы говорят о различных погрешностях, допущенных законодателем при криминализации рассматриваемых деяний.

Как пишет А.Н. Никитина, «несмотря на внимание законодателя к данным деяниям, по-прежнему можно обнаружить недостатки в регламентации уголовной ответственности за их совершение» [26, с. 26].

В частности, отмечается необоснованность дифференциации ответственности за склонение и за содействие в совершении самоубийства – законодатель включил каждое из обозначенных действий в разные части ст. 110.1 УК РФ – склонение в ч. 1, а содействие в ч. 2.

«В большинстве случаев субъект не только склоняет лицо к совершению суицида, но и, последовательно претворяя в жизнь свое желание, оказывает содействие самоубийце, предоставляя средства лишения жизни, давая советы, каким образом это лучше осуществить. Возникает ситуация, при которой единое преступление, направленное на формирование у лица желания уйти из жизни, сопряженное с предоставлением для этого определенных средств, надлежит квалифицировать как два преступления» [48, с. 152] – отмечает Т.Д. Устинова.

Действительно, подобная ситуация вряд ли приемлема. Решением данной дилеммы может стать объединение склонения и содействия, в качестве альтернативных деяний, в рамках ч. 1 ст. 110.1 УК РФ с установлением наказания за такое деяние, имеющееся в настоящее время в ч. 2 ст. 110.1 УК РФ.

К тому же, вопрос о том, какое из данных альтернативных действий имеет большую общественную опасность, является спорным.

Также вызывают вопросы, перечисленные законодателем способы склонения к совершению самоубийства и содействия в совершении самоубийства.

«Склонение» определено по аналогии со ст. 150 УК РФ, однако, целесообразно ли в ряду способов склонения, указание на подкуп? Данный способ для лица, имеющего намерение уйти из жизни, выглядит странным, с учётом того, что материальная выгода и намерение уйти из жизни вряд ли совместимы.

«Содействие» же определено путём перечисления признаков пособничества, указанных в ч. 5 ст. 33 УК РФ. Однако, данные признаки, актуальные в плане содействия в совершении преступления, являются бесполезными и даже абсурдными при определении содействия в совершении самоубийства – сказанное актуально, например, относительно такого способа содействия, как «обещание скрыть орудия или средства совершения самоубийства».

Относительно несовершеннолетнего возраста потерпевшего, как квалифицирующего признака, указанного в п. «а» ч. 2 ст. 110 УК РФ и ч. 3 ст. 110.1 УК РФ, представляется более правильным указать на «заведомость» несовершеннолетия потерпевшего для виновного. Такой подход, с учётом необходимости осознания виновным несовершеннолетнего возраста потерпевшего, представляется правильным с точки зрения теории уголовного права. Формальный подход в плане вменения данного признака неприемлем, что находит свою поддержку в науке.

Интересная точка зрения, относительно отдельных категорий потерпевших по ст. 110.1 УК РФ, высказана в науке: «нельзя не вспомнить о малолетних детях, невменяемых и иных лицах, страдающих психическими расстройствами, которые не позволяют им адекватно воспринимать окружающую действительность и понимать существо поступка, который предлагают им совершить, и его последствия. Считаем, что склонение указанных лиц к самоубийству должно расцениваться как приготовление к

убийству, а лишение себя жизни самим склоняемым – как опосредованное совершение убийства и квалифицироваться по соответствующей части ст. 105 УК РФ» [48, с. 156].

Подобная точка зрения высказывается и в работах других специалистов: «доведение до самоубийства или склонение к самоубийству малолетнего ребенка или психически больного, не отдающих отчета в своих действиях, следует рассматривать как убийство путем опосредованного причинения смерти» [4, с. 165].

Сказанное имеет смысл и может быть принято в качестве руководства к квалификации деяния при описываемых обстоятельствах.

Формулировки же, использованные законодателем при регламентации ответственности за организацию деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2 УК РФ), видится достаточно корректными.

Представляется, что, если лицо, организовавшее подобную деятельность (например, создав группу «ВКонтакте»), осуществило склонение конкретного участника данной группы к самоубийству, или оказало ему содействие в этом, должно привлекаться к уголовной ответственности не только по соответствующей части ст. 110.2 УК РФ, но и по соответствующей части ст. 110.1 УК РФ.

Предложение об установлении ответственности за преступления, предусмотренные ст. 110, 110.1 и 110.2 УК РФ лишь по достижению виновным возраста 18 лет [48, с. 158] вряд ли приемлемо. Общий возраст субъекта данных преступлений (16 лет) является соответствующим характеру и степени общественной опасности указанных преступлений.

Представляется целесообразным предусмотреть в качестве квалифицирующего признака совершения преступлений, предусмотренных ст. 110 и 110.1 УК РФ совершение преступления родителем, педагогическим работником либо иным лицом, на которое законом возложены обязанности по

воспитанию несовершеннолетнего. В данном случае аналогия со ст. 150 УК РФ была бы вполне оправданна.

Очевидно, что с ростом числа людей, активно пользующихся ресурсами сети «Интернет», ежегодно увеличивается и количество преступлений, совершаемых посредством этой системы, а также расширяется спектр возможностей сети «Интернет», которые могут быть использованы виновными для совершения общественно опасных действий, что обуславливает необходимость законодателя реагировать на подобные факты, подвергая их криминализации.

Как верно отмечается отдельными авторами, наряду с корыстными мотивами все чаще стали свершаться преступления, целью которых являются жизнь и здоровье человека. Жертвами подобных преступлений чаще всего становятся дети и подростки, в силу своей несформировавшейся и неустойчивой психики. Совершение новых преступлений в системе «Интернет», связанных с целью склонения или доведения до самоубийства, обусловливает ужесточение контроля за контентом, размещенным на различных Интернет-ресурсах [25, с. 15].

2.2 Предложения, направленные на совершенствование нормативного регулирования противодействия преступности в сфере Интернет (киберпреступности) уголовно-правовыми средствами

Проведённые анализ отдельных видов преступлений в сфере Интернет (киберпреступлений) позволяет сделать вывод о том, что в действующем УК РФ формулирование отдельных составов преступлений в сфере Интернет (киберпреступлений) произведено с некоторыми погрешностями, нуждающимися в нормативной корректировке, направленной на повышение эффективности правоприменени, а также обеспечения непротиворечивой и правильной квалификации соответствующих деяний.

Относительно рассмотренных проблем, связанных с нормативной регламентацией составов, связанных с доведением до самоубийства, а также склонением или содействием в совершении такового, что как правило, учитывая современное развитие технологий и существующие тенденции, совершается с использованием сети «Интернет», представляется необходимым скорректировать текст ст. 110 и 110.1 УК РФ.

В качестве рекомендуемых изменений:

- объединение склонения и содействия, в качестве альтернативных деяний, в рамках ч. 1 ст. 110.1 УК РФ с установлением наказания за такое деяние, имеющееся в настоящее время в ч. 2 ст. 110.1 УК РФ;
- корректировка способов совершения склонения к самоубийству, а также содействия в совершении самоубийства, указанных в ст. 110.1 УК РФ;
- указание на «заведомость» несовершеннолетия потерпевшего для виновного при формулировании п. «а» ч. 2 ст. 110 УК РФ и ч. 3 ст. 110.1 УК РФ;
- включение в текст ч. 2 ст. 110 УК РФ и ч. 2 предлагаемой редакции ст. 110.1 УК РФ п. «а.1», содержащего в качестве квалифицирующего признака совершение преступления родителем, педагогическим работником либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего.

Учитывая высказанные критические замечания по поводу конструкции данных составов преступлений, представляется целесообразным предложить следующую редакцию ст. 110 УК РФ:

«1. Доведение лица до самоубийства или до покушения на самоубийство путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего -

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до семи лет или без такового либо

лишением свободы на срок от двух до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до семи лет или без такового.

2. То же деяние, совершенное:

а) в отношении несовершеннолетнего или лица, заведомо для виновного находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного;

а.1) в отношении несовершеннолетнего родителем, педагогическим работником либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего;

б) в отношении женщины, заведомо для виновного находящейся в состоянии беременности;

в) в отношении двух или более лиц;

г) группой лиц по предварительному сговору или организованной группой;

д) в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»), - наказывается лишением свободы на срок от восьми до пятнадцати лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до десяти лет или без такового и с ограничением свободы на срок до двух лет или без такового».

Новая редакция ст. 110.1 УК РФ может выглядеть следующим образом:

«1. Склонение к совершению самоубийства путем уговоров, предложений, обмана или иным способом при отсутствии признаков доведения до самоубийства, или содействие совершению самоубийства советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению - наказывается ограничением свободы на срок до трех лет, либо принудительными работами на срок до трех лет с лишением права занимать

определенные должности или заниматься определенной деятельностью на срок до четырех лет или без такового, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до четырех лет или без такового.

2. Деяние, предусмотренное частью первой настоящей статьи, совершенные:

а) в отношении заведомо несовершеннолетнего или лица, заведомо для виновного находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного;

а.1) в отношении несовершеннолетнего родителем, педагогическим работником либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего;

б) в отношении женщины, заведомо для виновного находящейся в состоянии беременности;

в) в отношении двух или более лиц;

г) группой лиц по предварительному сговору или организованной группой;

д) в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»), - наказываются принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

3. Деяние, предусмотренное частью первой настоящей статьи, повлекшее самоубийство или покушение на самоубийство, - наказываются ограничением свободы на срок от двух до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные

должности или заниматься определенной деятельностью на срок до шести лет или без такового, либо лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет или без такового.

4. Деяние, предусмотренное частью первой настоящей статьи, повлекшее самоубийство или покушение на самоубийство несовершеннолетнего, либо лица, заведомо для виновного находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного, либо женщины, заведомо для виновного находящейся в состоянии беременности, - наказываются лишением свободы на срок от шести до двенадцати лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до семи лет или без такового.

5. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие самоубийство двух или более лиц, - наказываются лишением свободы на срок от восьми до пятнадцати лет».

Говоря о выявленных проблемах нормативного регулирования преступлений, совершаемых в сфере Интернет (киберпреступлений) в общем и целом, прослеживается определённая непоследовательность в выделении соответствующих составов – отсутствие единой концепции таких законодательных корректировок, что является недостатком существующего регулирования вопросов ответственности за данного рода деяния.

По какому именно принципу федеральный законодатель вводит указанный признак в уголовно-правовую норму не до конца ясно. Например в ч. 3 ст. 137 УК РФ предусмотрена ответственность за незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание

полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия. Но аналогичный признак законодатель не включает в основной состав деяния в ч. 1 ст. 137 УК РФ.

Особенно непоследовательным и странным данное обстоятельство выглядит в связи с тем, что в ч. 1 ст. 137 УК РФ законодатель говорит о распространении таких сведений в СМИ, или в публичном выступлении, но ничего не говорит о распространении такой информации в сети «Интернет», хотя, как представляется, именно распространение информации подобным образом может позволить виновному достичь максимального охвата аудитории в обнародовании, с учётом того, что опубликованная заметка в социальных сетях, или на популярном сайте сразу становится доступной к восприятию огромного числа людей из любой точки мира, что повышает общественную опасность деяния.

Высокая популярность среди пользователей сети «Интернет» различных социальных сетей («ВКонтакте», «Одноклассники», «Мой мир» и т.д.) позволяет с уверенностью утверждать, что опубликование информации в какой-нибудь местной газете или журнале делает информацию доступной во много раз меньшей аудитории, чем опубликование данной информации на популярной странице пользователя социальной сети, или в популярном сообществе.

Таким образом, когда речь идёт о разглашении данных, о распространении информации, на что законодателем наложен уголовно-правовой запрет, возможность такого распространения в сети Интернет должна в обязательном порядке предусматриваться законодателем либо в основном составе деяния, либо в качестве квалифицирующего признака, наряду с распространением информации в СМИ.

Фрагментарность указания на совершение деяния с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», применительно к различным составам преступлений, осуществляемая законодателем в последнее время вызывает оправданную критику [14, с. 26]. Представляется, что в данном вопросе законодателю следует проявлять последовательность и вносить данный признак в нормы особенной части УК РФ системно.

Представляется, что не только обозначенные ранее составы, в рамках классификации киберпреступлений, конструктивно связанные законодателем с возможностью их совершения с использованием средства компьютерной (а также иной цифровой техники) и информационно-телекоммуникационные сети, в том числе сеть «Интернет», могут быть совершены обозначенным способом.

Законодатель по какой-то причине, не видит такой возможности в отношении целого ряда других посягательств, очевидно нуждающихся в дополнении соответствующим квалифицирующим признаком.

Незаконное приобретение или сбыт оружия может осуществляться, в том числе, через Интернет, однако в ст. 222 УК РФ, это квалифицирующее обстоятельство не обозначено, в отличие от ст. 228.1 УК РФ применительно к наркотическим средствам, психотропным веществам или их аналогам.

Аналогичный вывод справедлив в отношении состава преступления, предусмотренного ст. 171.4 УК РФ «Незаконная розничная продажа алкогольной и спиртосодержащей пищевой продукции».

И это несмотря на высокие показатели доходности «теневого» рынка продажи алкогольной продукции через «Интернет».

Специалисты отмечают, что «средняя посещаемость сайта, реализующего алкоголь с доставкой, составляет 190 пользователей в сутки или 5700 человек в месяц. При конверсии 0,7% и средней стоимости одной

покупки в 1 100 рублей, 4 000 онлайн-магазинов зарабатывают от 174,5 млн рублей в месяц. Таким образом, оборот нелегальной интернет-продажи алкоголя по итогам 2018 года составил порядка 2,1 млрд. рублей, что на 23% выше, чем годом ранее» [1].

Учитывая, что совершение преступления посредством цифрового пространства становится всё более распространенным, облегчает виновному достижение преступной цели, а, следовательно, повышает общественную опасность содеянного, представляется необходимым включение в качестве квалифицирующего признака совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»» и в иные статьи Особенной части УК РФ. Для того, чтобы это реализовать, правда, придётся критически проанализировать огромное количество составов для того, чтобы понять, какое именно преступление может быть реализовано с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а какое нет.

Очевидной является невозможность совершения ряда преступлений подобным образом – убийство матерью новорожденного ребенка (ст. 106 УК РФ), или же заражение ВИЧ-инфекцией (ст. 122 УК РФ) и т.д., однако, во многих случаях такой вывод не столь очевиден.

Есть и иной вариант решения данной проблемы – простой и доступный, не требующий глубокого анализа составов преступлений, обозначенных в действующем УК РФ: это включение в ст. 63 УК РФ нового отягчающего обстоятельства в виде совершения умышленного преступления с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Такое нормативное изменение позволит учесть данный аспект реализации преступного умысла в тех случаях, когда ни в конструкции состава преступления, ни в квалифицирующих признаках нет указания на данный

способ совершения преступления и, таким образом, дифференцировать наказание.

По итогам третьей главы работы обозначим следующие выводы.

Относительно рассмотренных проблем, связанных с нормативной регламентацией составов, связанных с доведением до самоубийства, а также склонением или содействием в совершении такового, что как правило, учитывая современное развитие технологий и существующие тенденции, совершается с использованием сети «Интернет», представляется необходимым скорректировать текст ст. 110 и 110.1 УК РФ.

В качестве рекомендуемых изменений:

- объединение склонения и содействия, в качестве альтернативных деяний, в рамках ч. 1 ст. 110.1 УК РФ с установлением наказания за такое деяние, имеющееся в настоящее время в ч. 2 ст. 110.1 УК РФ;
- корректировка способов совершения склонения к самоубийству, а также содействия в совершении самоубийства, указанных в ст. 110.1 УК РФ;
- указание на «заведомость» несовершеннолетия потерпевшего для виновного при формулировании п. «а» ч. 2 ст. 110 УК РФ и ч. 3 ст. 110.1 УК РФ;
- включение в текст ч. 2 ст. 110 УК РФ и ч. 2 предлагаемой редакции ст. 110.1 УК РФ п. «а.1», содержащего в качестве квалифицирующего признака совершение преступления родителем, педагогическим работником либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего.

Учитывая высказанные критические замечания по поводу конструкции данных составов преступлений, представляется целесообразным изменить действующие редакции ст. 110 и 110.1 УК РФ.

Говоря о выявленных проблемах нормативного регулирования преступлений, совершаемых в сфере Интернет (киберпреступлений) в общем

и целом, прослеживается определённая непоследовательность в выделении соответствующих составов – отсутствие единой концепции таких законодательных корректировок, что является недостатком существующего регулирования вопросов ответственности за данного рода деяния.

Как представляется, «снабжать» отдельные составы преступлений, совершение которых может быть сопряжено с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», соответствующим квалифицирующим признаком – не единственное возможное решение. Тем более, что системное внесение такого квалифицирующего признака требует глубокой проработки.

Целесообразным же представляется включить в ст. 63 УК РФ новое отягчающее обстоятельство в виде совершения умышленного преступления с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Глава 3 Анализ проблем противодействия преступности в сфере Интернет (киберпреступности)

3.1 Основные причины и условия преступности в сфере Интернет (кибепреступности)

Причины и условия преступности в целом и отдельных категорий преступности являются одной из фундаментальных категорий, изучаемых наукой криминологией.

Как отмечается отдельными авторами, «причинами преступности называется совокупность социальных явлений и процессов, которые во взаимодействии с обстоятельствами, играющими роль условий, детерминируют существование преступности как социального явления, наличие отдельных составных ее частей, а на индивидуальном уровне – совершение конкретных преступлений» [20, с. 43].

В данном определении проявляется связь рассматриваемого понятия с философской категорией «детерминизм», определяющей взаимосвязь явлений окружающей действительности. В этом смысле причинность понимается как одна из форм детерминации, отражающей всеобщую связь, взаимозависимость и взаимообусловленность явлений и процессов бытия.

Детерминанты преступности непосредственно порождают, воспроизводят преступность и преступления как свое закономерное следствие [36, с. 110].

Другими словами, причины, в едином комплексе с условиями преступности, выступают в качестве порождающих преступность детерминант, именуемых также в науке факторами преступности.

Как указывается специалистами, «условиями преступности являются различные явления социальной жизни, которые не порождают преступность, но содействуют, способствуют ее возникновению и существованию. Причина

создает возможность определенного следствия. Условия же способствуют реализации этой возможности» [16, с. 34].

О соотношении категорий причин и условий преступности в науке есть множество дискуссий, однако, авторы едины во мнении о том, что причины и условия, выступая в качестве детерминант преступности, действуют не в отрыве друг от друга, а в комплексе, обуславливая преступность.

Именно поэтому целесообразно рассматривать причины и условия преступности как части целого.

Представляется сложным эффективно противостоять преступности в сфере Интернет (киберпреступности) без наличия представлений о причинах и условиях таковой.

Вопрос о причинах и условиях киберпреступности относится к разряду неоднозначных и дискуссионных. Киберпреступность, как отмечается отдельными авторами, с одной стороны, порождается теми же причинами и условиями, что и преступность вообще. С другой стороны, она имеет свои сугубо специфические причины и условия вследствие ее особенностей [5, с. 140].

К числу детерминант киберпреступности можно отнести:

- широкую распространённость и всё большую доступность информационных технологий;
- растущее число пользователей глобальной сети «Интернет» как в мире, так и в Российской Федерации, а также растущий спрос на информационные технологии и программное обеспечение, что, в свою очередь, обуславливает рост объёма хранимой и обрабатываемой цифровой информации;
- возрастающую зависимость функционирования отдельных сфер общественной жизни (социальной, экономической и т.д.) от современных информационных технологий;

- рост в структуре национальной экономики торговли и оказания услуг через электронные (компьютерные) средства телекоммуникации (в частности, Интернет-торговля);
- стремительное развитие информационных технологий, сопряжённое с возникновением новых технологий и средств доступа в сеть «Интернет», а также новых средств обработки цифровой информации;
- отсутствие единых устоявшихся апробированных практикой и имеющих должную научную и техническую основу методических рекомендаций по раскрытию и расследованию киберпреступлений;
- несовершенство средств защиты информации в сети «Интернет» при использовании информационно-коммуникационных технологий в отдельных процессах, равно несовершенство средств защиты телекоммуникационных систем и их сетей и т.д.

Эффективному же противодействию совершению киберпреступлений препятствует, как отмечается в отдельных работах:

- отсутствие скоординированной и комплексной государственной политики в сфере обеспечения информационной безопасности;
- несоответствие темпа развития средств выявления и противодействия киберпреступлениям объективным темпам развития средств и способов совершения противоправных посягательств, а также сокрытия следов данных посягательств;
- отсутствие единой терминологии, применяемой при описании диспозиций соответствующих составов киберпреступлений и (или) её несоответствие современному объективному уровню развития информационных технологий, что обуславливает сложности квалификации соответствующих деяний;
- возможность совершения преступных посягательств в сети «Интернет» из любой точки планеты, имея доступ к сети и соответствующие устройство, обеспечивающее доступ в сеть и

возможность использования необходимого для этого программного обеспечения;

- обезличенность (анонимность) взаимодействия, осуществляемого через сеть «Интернет», возможность скрывать индивидуализирующие пользователя сети данные о местонахождении, точке доступа в сеть;
- низкий уровень специальной подготовки сотрудников правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере информационных технологий и т.д.

Отдельные авторы, ввиду множества причин и условий киберпреступности, предлагают их классифицировать. В частности, В.А. Бугаев и А.В. Чайка предлагают следующую классификацию факторов киберпреступности:

- факторы, связанные с информационными сетями, информационной средой и инфраструктурой;
- факторы, связанные с особенностями данной категории преступных посягательств;
- факторы, связанные с обеспечением информационной безопасности [5, с. 141].

Так, или иначе, подобное разделение детерминант киберпреступности имеет условный характер и применимо для решения отдельных исследовательских задач.

Одним из современных факторов киберпреступности является довольно стихийный и, во многом, неподготовленный переход к дистанционным, опосредованным сетью «Интернет» формам работы, в связи с пандемией COVID-19. Именно поэтому в современный период продолжающегося действия вынужденных ограничений, вызванных распространением коронавирусной инфекции, вопросы противодействия киберпреступлениям

приобретают повышенную важность, обусловленную задачами обеспечения национальной безопасности.

Многие рядовые граждане перешли от традиционных способов совершения операций в режим онлайн, также поступили и киберпреступники. В то время, как масштабы и изощренность киберпреступлений растет, и увеличивается количеств жертв.

В этих условиях киберпреступники «переместили» свое внимание с простых людей и небольших организаций на государственные органы, учреждения здравоохранения и крупные корпорации, чтобы максимизировать свою прибыль и разрушения, вызванные коронавирусом. Из-за внезапного глобального перехода к удаленной рабочей среде во время пандемии многим организациям пришлось быстро развертывать удаленные системы, сети и приложения. В результате возник риск уязвимости в обеспечении безопасности при организации удаленной работы, что и используется киберпреступниками.

Как отмечается авторами, в глобальной сети преступники обновили свои онлайн-мошеннические и фишинговые схемы, часто выдавая себя за правительственные и медицинские органы, чтобы обманом заставить жертв предоставлять личные данные и загружать вредоносный контент. Так, в течение первых двух недель апреля 2020 г. произошел небывалый всплеск атак вымогателей в сети «Интернет», чего не наблюдалось ранее [36, с. 111].

По мере того, как пандемия коронавируса и карантинные меры затягиваются, и случаи заболевания продолжают расти, можно предположить, что масштабы киберпреступлений будут огромными, особенно по причине того, что экономика «слабеет» и люди будут страдать от финансовых последствий коронавируса. В связи с этим возникает необходимость минимизации и ограничения потенциальных киберугроз, а также улучшения системы кибербезопасности.

Далее представляется целесообразным рассмотреть непосредственно пути и способы профилактики и предупреждения преступности в сфере «Интернет» (киберпреступности).

3.2 Меры, направленные на противодействие преступности в сфере Интернет (киберпреступности)

Как представляется, достаточно эффективное и целенаправленное противодействие преступности, как негативному социальному явлению, и обеспечение защиты общества и государства от противоправных посягательств – это одна из наиболее важных проблем, что стоит в современном российском обществе и государстве. Не самые благоприятные тенденции в развитии преступности в целом и преступности в сфере Интернет (киберпреступности) в частности, диктуют необходимость поиска наиболее доступных и максимально эффективных путей решения данной проблемы.

В первую очередь, следует определить понятие противодействия преступности и провести разграничение его с иными смежными категориями, которые достаточно активно используются в научной и учебной литературе.

С.И. Ожегов определяет понятие «противодействие» следующим образом: «действие, препятствующее другому действию» [27, с. 541].

Тем не менее, лексическое значение данного понятия, применительно к исследуемой проблематике, не позволяет нам уяснить суть рассматриваемой категории.

Относительно научных определений, наиболее верным и содержательным представляется определение, сформулированной В.К. Дуюновым, который под противодействием преступности понимает «направление деятельности государства (при участии и поддержке институтов гражданского общества и отдельных граждан), связанное с разработкой и реализацией стратегии и тактики (генеральной линии) организованного сопротивления преступности и иным правонарушениям» [41, с. 38].

Это требует в качестве важнейшего условия разработку и реализацию единой, научно обоснованной и грамотно реализуемой государством (при безусловном и активном участии общественности, институтов гражданского общества) политики, определяющей стратегию и тактику противодействия преступности.

Наряду с понятием «противодействие преступности» в науке используются иные термины для обозначения подобного вида государственной и общественной деятельности: «борьба», «контроль», «предупреждение», «реагирование» и др.

Из всех обозначенных категорий, «противодействие преступности» видится в качестве наиболее удачного и содержательного, так как является комплексным: в отличие от термина «борьба», не включающего в себя меры обшесоциального характера, или термина «предупреждение», не охватывающего меры реагирования на уже совершённое преступление; также противодействие преступности предполагает наступательный характер, в отличие от термина «контроль».

Объединить все усилия государства и общества в противодействии преступности, обеспечить их научную обоснованность, придать им организованный, целенаправленный и наступательный характер как раз и призвана политика противодействия преступности, которая заключается в «поиске, разработке и целенаправленном использовании в интересах безопасного развития общества имеющихся в распоряжении государства и общества ресурсов, наиболее эффективных общесоциальных и специальных предупредительных мер» [41, с. 39].

При этом, представляется правильным включение в контекст политики противодействия преступности не только деятельностного, но и идеологического (концептуального) аспекта. Именно соответствующая идеология позволяет определить стратегию и тактику противодействия преступности: цели, принципы, основные направления (формы), методы,

содержание, характер и перспективы соответствующих усилий государства и общества в данном направлении.

Цель противодействия преступности – это обеспечение минимизации преступности, максимально возможное её ограничение.

Противодействие преступности включает в себя предупреждение преступлений, которое считается важнейшей составной частью противодействия преступности, поскольку, при должном уровне эффективности предпринимаемых предупреждающих действий, позволяет не допустить совершение преступления как такового.

Ю.П. Оноколов считает, что «предупреждение преступлений – это деятельность различных структур, направленная на недопущение самого события преступления» [28, с. 24].

Однако, приведённое определение слишком краткое и абстрактное. Более точным и содержательным видится определение, сформулированное В.К. Дуюновым, который под предупреждением преступлений понимает «направление деятельности государства, связанное с поиском, разработкой, исследованием и реализацией целей, принципов, основных направлений, содержания, форм и методов, эффективных общесоциальных и специальных средств воздействия на причины и условия совершения преступлений в целях предупреждения (сдерживания) и сокращения преступности и иных правонарушений» [41, с. 78].

Обращаясь же к ещё одному понятию, связанному с предупреждением преступлений – понятию «профилактика преступности», следует сказать о том, что его, как правило, отождествляют с «предупреждением преступлений».

«Профилактика – это совокупность предупредительных мероприятий» [27, с. 543] – указывается С.И. Ожеговым. То есть, даже с точки зрения лексики, термин «профилактика» раскрывается через термин «предупреждение».

Таким образом, противодействие преступности в сфере Интернет (киберпреступности) включает в себя комплекс разноплановых мер, включая меры предупреждения совершения киберпреступлений. Именно этот аспект противодействия киберпреступности наиболее полно представлен в современных научных публикациях, с учётом того, что недопущение совершения конкретных киберпреступлений, посредством эффективного предупреждения данных преступлений – желаемый в обозначенном направлении результат. Реагирование на уже совершённое преступление – вынужденная мера, находящаяся на последующем этапе противодействия, когда меры предупреждения оказались не эффективными и преступление (или покушение на его совершение) всё же состоялось.

Как отмечается отдельными исследователями, «основные направления противодействия киберпреступности сегодня должны быть нацелены на решение проблем, связанных с расширением законодательства, выработкой мер предупреждения и снижением уровня латентности преступлений, совершаемых в киберпространстве» [51, с. 47].

По мнению А.С. Ханахмедова, внимание государства в противодействии киберпреступности на данном этапе должно быть сосредоточено на следующих направлениях:

- выработке новых комплексных решений по предупреждению и пресечению киберпреступлений;
- совершенствовании системы международного обмена информацией о киберугрозах;
- качественном повышении уровня подготовки российских специалистов по противодействию преступлений, совершаемых в информационной среде;
- развитии и внедрении в деятельность правоохранительных органов новых технологий как эффективного средства контроля за преступностью [51, с. 48].

Данные направления предупреждения киберпреступности, от части, учитывают тот спектр детерминант киберпреступности, который выделялся выше. В этой связи, данные направления предупреждения представляются перспективными и нуждаются в последовательной реализации, так как призваны воздействовать на причины и условия киберпреступности, такие как:

- отсутствие скоординированной и комплексной государственной политики в сфере обеспечения информационной безопасности;
- возможность совершения преступных посягательств в сети «Интернет» из любой точки планеты, имея доступ к сети и соответствующие устройство, обеспечивающее доступ в сеть и возможность использования необходимого для этого программного обеспечения;
- низкий уровень специальной подготовки сотрудников правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в рассматриваемой сфере и т.д.

Примечательно, что относительно такой детерминанты киберпреступности, как обезличенность (анонимность) взаимодействия, осуществляемого через сеть «Интернет», возможность скрывать индивидуализирующие пользователя сети данные о местонахождении, точке доступа в сеть, отдельные авторы высказывают предложения о введении обязательной регистрации официальных данных пользователей в сети «Интернет» для возможности их идентификации.

Применительно к сети «Интернет» в целом, это видится недопустимым. Тем не менее, применительно к отдельным ресурсам это представляется возможным, как, например, это предлагают А.В. Леонов и А.Я. Назаренко относительно сайтов частных объявлений в целях предупреждения кибермошенничеств: «В процессе регистрации новых пользователей необходимо ввести идентификацию с указанием персональных данных, а

именно, обязательное указание паспортных данных пользователя, и возложить на администраторов данных сайтов обязанность тщательной проверки каждого зарегистрированного пользователя» [23, с. 168].

Хотя и данная мера видится спорной, ввиду существенного вторжения государства в сферу частной жизни и частного взаимодействия. Даже будучи продиктованными благими намерениями, подобные меры не должны вводиться необдуманно, равно, как и иные ограничительные меры.

В любом случае, предпринимаемые со стороны государства меры, направленные, в первую очередь, на предупреждение киберпреступлений, должны носить системный характер, должны объединяться едиными задачами, быть последовательными в их реализации. В противном случае разрозненные, противоречивые меры не будут эффективными.

В этой связи, следует поддержать идею о принятии Концепции стратегии кибербезопасности Российской Федерации, выдвинутой к обсуждению в рамках парламентских слушаний ещё в ноябре 2013 г. Уже в 2014 г. данный проект документа был представлен к общественному обсуждению, для чего предлагаемая Концепция была размещена на официальном сайте Совета Федерации.

По замыслу разработчиков целью документа является обеспечение кибербезопасности личности, организации и государства. Стратегия предусматривает содействие формированию культуры информационной безопасности и повышению уровня цифровой грамотности граждан России.

Обозначенный нормативный документ предполагает ряд ключевых направлений реализации:

- принятие общесистемных мер по обеспечению кибербезопасности;
- совершенствование нормативно-правовой базы и правовых мер обеспечения кибербезопасности;
- проведение научных исследований в области кибербезопасности;
- создание условий для разработки, производства и применения средств обеспечения кибербезопасности;

- совершенствование кадрового обеспечения и организационных мер обеспечения кибербезопасности;
- организация внутреннего и международного взаимодействия действующих лиц по обеспечению кибербезопасности;
- формирование и развитие культуры безопасного поведения в киберпространстве и безопасного использования его сервисами.

Обозначенная в проекте стратегия кибербезопасности базируется на следующих основных принципах:

- принципе гарантированности конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
- принципе максимальной защищенности личности, организаций, в том числе обеспечивающих функционирование критической информационной инфраструктуры, и государственных органов в части функционирования информационных ресурсов, информационных систем и информационно-телекоммуникационных сетей в киберпространстве;
- принципе конструктивного сотрудничества всех субъектов информационного общества – личности, организаций и государства – в области обеспечения кибербезопасности;
- принципе баланса между установлением ответственности за несоблюдение требований кибербезопасности с одной стороны и введением избыточных ограничений – с другой;
- принципе приоритезации рисков кибербезопасности в соответствии с вероятностями реализации киберугроз и размерами негативных последствий от инцидентов кибербезопасности;
- принципе систематической актуализации средств и методов обеспечения кибербезопасности в целях противостояния изменяющимся киберугрозам.

Рассматриваемая Концепция могла заложить основы взаимодействия всех участников цифровых виртуальных коммуникаций в нашей стране, но так и осталась в статусе несогласованного законопроекта, хотя потребность в ней назрела давно, ввиду необходимости противодействия киберугрозам и преступлениям в сфере Интернет.

Данной проблеме продолжает уделяться внимание отраслевыми экспертами и на страницах научных публикаций.

Таким образом, на сегодняшний день в Российской Федерации до сих пор отсутствует базовый, отвечающий современным реалиям нормативный акт, содержащий в себе основы кибербезопасности на государственном уровне.

Примечательно, что зарубежный законодатель и правоприменитель пытаются соблюсти баланс между таких крайностей, как чрезмерное вмешательство в регулировании информационной сферы и игнорирование информационной сферы со стороны государства. Другими словами, в регулировании вопросов противодействия киберпреступлениям на национальном уровне необходимо обеспечить баланс.

В этой связи, работу над созданием демократической по своей сути Концепции кибербезопасности, применительно к российским реалиям, стоит продолжать. Данный документ мог бы стать необходимым и даже ключевым элементом системы противодействия преступлениям, совершаемым в сфере Интернет (киберпреступлениям).

Основным приоритетом в международной практике становится акцент на сотрудничество государства, бизнеса и гражданского общества, — то есть на создание экосистемы по противостоянию киберугрозам.

За рубежом активное взаимодействие между органами власти и коммерческим сектором, а также институтами гражданского общества, постепенно выходит на передний план в качестве потенциально эффективного фактора повышения качественного уровня решения актуальных проблем общества. Один из путей налаживания подобного взаимодействия – это, так

называемое, государственно-частное партнерство, активно развиваемое в настоящее время, в том числе, в нашей стране.

Как отмечается отдельными исследователями, «в последние годы в противодействии киберпреступности сложилась ситуация, заставляющая государство серьезно укреплять взаимодействие с частным бизнесом и в этой сфере. Решая соответствующие масштабные задачи, правоохранительные органы испытывают острую потребность в задействовании значительного числа квалифицированных специалистов, получивших серьезную подготовку в области информационных технологий (оперативные сотрудники, следователи, аналитики, эксперты, программисты и др.), в разработке и внедрении комплексного программного обеспечения и приобретении сложного дорогостоящего оборудования, в создании мощных центров для хранения и обработки цифровых данных. В условиях бюджетных ограничений полностью удовлетворить эту потребность без привлечения значительных инвестиций практически невозможно» [29, с. 37].

Очевидно, что уже сейчас, в настоящее время, в России есть довольно много организаций IT-сектора, которые обладают высоким потенциалом в данной сфере профессиональной деятельности, которые оказывают на коммерческой основе услуги по противодействию киберугрозам в отношении граждан и юридических лиц, а также производят весь спектр аналитических работ и компьютерных экспертиз.

Данные организации занимают высокие позиции в сфере информационных технологий, проявляя эффективность в решении задач, связанных с кибербезопасностью, обладая при этом наработанным опытом, и коллективом, включающим в себя квалифицированных специалистов.

Подобные организации, наряду с правоохранительными государственными структурами, определенно могут вовлекаться в систему противодействия преступлениям, совершаемым в сфере Интернет (киберпреступлениям).

Без сомнений, главным звеном регулирования подобной деятельности может и должно выступать государство в лице соответствующих органов, наделённых властными полномочиями, так как именно государство реализуя правоохранительную функцию, стоит на защите интересов личности, общества и государства, имея возможности для обеспечения реализации названной функции использовать меры государственного принуждения. В частности, полномочиями, связанными с выявлением и расследованием преступлений (в том числе, совершаемых в сети «Интернет»), обладают исключительно правоохранительные органы.

Тем не менее, к подобной реализации даже сугубо государственно-властных полномочий в сфере противодействия киберпреступлениям, можно и нужно привлекать, на законной основе, коммерческие организации, имеющие необходимый потенциал и желание его использовать в контексте противодействия преступлениям в сфере Интернет.

Представляется, что подобное, обозначенное выше, единение усилий в направлении эффективного противодействия преступлениям, совершаемым в сфере Интернет, весьма целесообразно производить в контексте развития государственно-частного партнерства.

Основными формами реализации такого взаимодействия при этом могут быть:

- контракты на выполнение определенных работ и предоставление услуг;
- взаимное консультирование, информационный обмен;
- совместное ведение баз данных;
- независимая экспертиза проектов нормативных правовых актов указанной сферы;
- подготовка и внесение совместных предложений по реализации государственной политики в киберпространстве;

- информационное обеспечение государственных и коммерческих предприятий, общественных объединений и граждан по вопросам обеспечения кибербезопасности и т.д.

Как отмечает А.Л. Осипенко, «в общем виде цель любого государственно-частного партнерства – удовлетворение общественно значимых интересов. Думается, что таким интересом в рассматриваемом ключе является создание условий для безопасного функционирования киберпространства, что необходимо и государству, обществу и бизнесу» [29, с. 39].

Кибербезопасность с точки зрения коммерческих интересов становится все более насущной проблемой. Особенно в сфере банковского, IT-бизнеса и защиты персональных данных.

Соответственно, в виде глобальной цели выступает создание отлаженной и максимально эффективной системы противодействия киберпреступности.

В штате многих организаций, осуществляющих свою деятельность в IT-сфере работает множество востребованных в силу имеющейся высокой квалификации специалистов, ряд которых имеет необходимые познания, необходимые для расследования киберпреступлений.

В соответствии с требованиями Уголовно-процессуального кодекса Российской Федерации [42] (УПК РФ) назначение и производство предварительных исследований допускается до возбуждения уголовного дела на этапе проверки сообщения о преступлении (ст. 144 УПК РФ). Соответственно, привлечение лиц, обладающих специальными познаниями в IT-сфере в процессуальном качестве специалиста допустимо с позиций действующего законодательства.

В данном процессуальном качестве указанные специалисты могут привлекаться и на этапе предварительного расследования, в форме дознания или предварительного следствия, при производстве следственных действий

для повышения их эффективности и получения необходимых сведений, которые могут быть в дальнейшем использованы в процессе доказывания.

Кроме того, участие специалиста в сфере IT-технологий в расследовании может стать способом вовлечения в процесс доказывания отдельных видов доказательств: заключения и показаний специалиста (ст. 80 УПК РФ).

«Практика оперативных подразделений подтверждает высокую эффективность сотрудничества с IT-предприятиями при раскрытии киберпреступлений» [10, с. 47] – указывают отдельные авторы.

Обладающие достаточным опытом специалисты ряда крупных компаний готовы с использованием самого современного оборудования квалифицированно производить обследование компьютерных систем, подвергшихся противоправным воздействиям, с соблюдением установленных требований собирать и анализировать данные, на основании которых может быть принято решение о возбуждении уголовного дела.

Данные специалисты, кроме того, могут привлекаться и на не процессуальной основе – в качестве IT-консультантов, чьи знания могут помочь следователю в выдвижении следственных версий, а также помочь верно сформулировать вопросы, которые надлежит поставить перед судебным экспертом при назначении судебной экспертизы по соответствующей категории уголовных дел.

Безусловно, лучше предупредить совершение противоправного посягательства, чем предпринимать шаги в плане реагирования на покушение на преступление, или уже совершённое преступление в сфере Интернет. Именно поэтому предупреждение киберпреступлений – первичный элемент противодействию данным противоправным деяниям.

«С применением высокотехнологичных продуктов отечественных компаний может производиться защита информационных ресурсов критически важных объектов, достигаться повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования. При разработке указанных средств дополнительно

решается задача повышения конкурентоспособности перспективных российских информационных технологий, укрепления отечественного научно-технического потенциала в области обеспечения информационной безопасности» [29, с. 42] – пишут специалисты.

Отдельное внимание в контексте обеспечения противодействия киберпреступлениям заслуживает вопрос организации комплекса мероприятий, объединяемых понятием «мониторинг сетевых информационных ресурсов».

Основными направлениями мониторинга, позволяющего получать значительные объемы ценной с точки зрения противодействия киберпреступности информации, являются:

- автоматизированный поиск сетевых ресурсов, содержащих запрещенную к распространению информацию;
- исследование материалов выявленных ресурсов, связанных с деятельностью преступных сообществ;
- наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности.

Существенно повысить эффективность крайне трудоемкого мониторинга, осуществляемого правоохранительными органами, может привлечение к его проведению специализированных коммерческих структур. Объединение усилий позволит получать наиболее полную картину оперативной обстановки в сфере противодействия киберпреступности в результате аккумулирования информации, поступающей из многочисленных источников, сформированных в государственных структурах и частном секторе. При повышении уровня взаимного доверия возможно создание объединенных информационных систем с обменом данными по единому регламенту в случаях обнаружения определенных событий.

Как уже говорилось ранее, один из факторов, препятствующих эффективному противодействию киберпреступлениям – низкий уровень специальной подготовки сотрудников правоохранительных органов, которые

должны предупреждать, раскрывать и расследовать преступления в сфере информационных технологий.

Максимально устранить данный фактор способно, с одной стороны, привлечение высококвалифицированных специалистов частных компаний к работе, связанной с противодействием киберпреступлениям (в том числе, в процессуальном качестве специалистов при проведении предварительной проверки сообщений о преступлении, а также при производстве расследования), а с другой стороны – повышение качественного уровня подготовки специалистов правоохранительных органов за счет привлечения к ней квалифицированных представителей IT-индустрии.

В данном отношении является перспективным осуществление привлечения профессионалов IT-компаний для организации плановых мероприятий, направленных на повышение квалификации сотрудников правоохранительных органов по конкретным направлениям противодействия киберпреступности в форме курсов повышения квалификации в рамках образовательных программ дополнительного образования, а также в форме образовательных семинаров и т.д.

Подобное сотрудничество в обозначенном направлении вполне моджет создать качественную основу, в том числе, для проведения совместной работы по созданию рекомендаций по значимым вопросам противодействия преступности в сфере Интернет (киберпреступности) в рамках не процессуальных форм организационного взаимодействия.

По итогам третьей главы работы, сформулируем следующие выводы.

Представляется, что предпринимаемые со стороны государства меры, направленные, в первую очередь, на предупреждение киберпреступлений, должны носить системный характер, должны объединяться едиными задачами. В противном случае разрозненные, противоречивые меры не будут эффективными.

В этой связи, следует поддержать идею о принятии Концепции стратегии кибербезопасности Российской Федерации и продолжить работу

над её созданием. Данный документ мог бы стать необходимым и даже ключевым демократическим по своей сути элементом системы противодействия преступлениям, совершаемым в сфере Интернет (киберпреступлениям).

Также представляется необходимым развивать государственно-частное партнёрство в направлении противодействия киберпреступности. В виде глобальной цели такого партнёрства выступает создание отлаженной и максимально эффективной системы противодействия киберпреступности.

Для государства, в лице правоохранительных структур, важно повысить эффективность выявления, раскрытия и расследования преступлений в сфере Интернет, а также повысить уровень подготовленности кадровых сотрудников правоохранительных органов.

Обеспечив комплексный подход в противодействии киберпреступности, можно рассчитывать на постепенное достижение значимых результатов в данном направлении.

Важно при этом осуществлять как совершенствование действующих уголовно-правовых норм, так и осуществлять предупреждение совершения рассматриваемых преступлений, путём разработки и реализации Концепции стратегии кибербезопасности Российской Федерации и расширения государственно-частного партнёрства в указанном направлении

Заключение

В заключении проведённой работы сформулируем основные предложения, направленные на совершенствование действующего законодательства и правоприменения в анализируемой сфере.

В плане терминологии в науке и правоприменительной практике используются самые разные обороты с разным смысловым содержанием. Однако, наибольшую популярность обретает использование таких взаимосвязанных категорий, как «киберпреступность» и «киберпреступления». Российский законодатель и правоприменитель, как правило, говоря о преступлениях, связанных с высокими технологиями используют категории «цифровой», «информационный» и т.д.

Тем не менее, категории «киберпреступление» и «киберпреступность» содержательно шире смежных понятий, таких как, например, «компьютерные преступления», или «преступления, с использованием компьютерных технологий».

Исходя из отмеченных выше признаков, можно сформулировать следующие определения киберпреступления и киберпреступности.

Киберпреступление – это умышленное общественно опасное деяние, предусмотренное УК РФ, совершенное с использование виновным компьютерных (а также иных цифровых) технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающее на общественные отношения в сфере безопасности обращения компьютерной информации в качестве основного, либо дополнительного объекта посягательства.

При таком понимании категории «киберпреступление», понятие «киберпреступность» следует понимать следующим образом.

Киберпреступность – это совокупность преступлений, совершаемых с использованием виновным компьютерных (а также иных цифровых) технологий и информационно-телекоммуникационных сетей, в том числе сети Интернет, посягающих на общественные отношения в сфере безопасности обращения компьютерной информации в качестве основного, либо дополнительного объекта посягательства.

Киберпреступность, как отмечается в современных публикациях, является одной из глобальных угроз развитого «цифрового» общества. При этом, сам уровень технологического развития на современном этапе, во многом, предопределяет её, поскольку киберпреступность – закономерное следствие глобализации информационно-коммуникационных технологий.

С учётом развития Интернет-индустрии, данный сегмент преступности является наиболее быстрорастущим, так как в настоящее время продолжается неуклонный рост числа Интернет-пользователей, а также параллельный рост профессионализма лиц, совершающих преступления данного рода.

В ходе анализа отдельных проблем квалификации отдельных разновидностей преступлений, совершаемых в сфере Интернет (киберпреступлений) и нормативного регулирования ответственности за них, были выдвинут ряд предложений, направленных на совершенствование норм действующего законодательства.

Относительно рассмотренных проблем, связанных с нормативной регламентацией составов, связанных с доведением до самоубийства, а также склонением или содействием в совершении такового, что как правило, учитывая современное развитие технологий и существующие тенденции, совершается с использованием сети «Интернет», представляется необходимым скорректировать текст ст. 110 и 110.1 УК РФ.

В качестве рекомендуемых изменений:

- объединение склонения и содействия, в качестве альтернативных деяний, в рамках ч. 1 ст. 110.1 УК РФ с установлением наказания за такое деяние, имеющееся в настоящее время в ч. 2 ст. 110.1 УК РФ;
- корректировка способов совершения склонения к самоубийству, а также содействия в совершении самоубийства, указанных в ст. 110.1 УК РФ;
- указание на «заведомость» несовершеннолетия потерпевшего для виновного при формулировании п. «а» ч. 2 ст. 110 УК РФ и ч. 3 ст. 110.1 УК РФ;
- включение в текст ч. 2 ст. 110 УК РФ и ч. 2 предлагаемой редакции ст. 110.1 УК РФ п. «а.1», содержащего в качестве квалифицирующего признака совершение преступления родителем, педагогическим работником либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего.

Учитывая высказанные критические замечания по поводу конструкции данных составов преступлений, представляется целесообразным изменить действующие редакции ст.ст. 110 и 110.1 УК РФ.

Говоря о выявленных проблемах нормативного регулирования преступлений, совершаемых в сфере Интернет (киберпреступлений) в общем и целом, прослеживается определённая непоследовательность в выделении соответствующих составов – отсутствие единой концепции таких законодательных корректировок, что является недостатком существующего регулирования вопросов ответственности за данного рода деяния.

По какому именно принципу федеральный законодатель вводит указанный признак в уголовно-правовую норму не до конца ясно.

Представляется, что в данном вопросе законодателю следует проявлять последовательность и вносить данный признак в нормы особенной части УК РФ системно.

Однако, «снабжать» отдельные составы преступлений, совершение которых может быть сопряжено с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», соответствующим квалифицирующим признаком – не единственное возможное решение. Тем более, что системное внесение такого квалифицирующего признака требует глубокой проработки.

Простой и доступный, не требующий глубокого анализа составов преступлений, обозначенных в действующем УК РФ способ противодействия уголовно-правовыми средствами совершению противоправных посягательств с использованием сети «Интернет» – это включение в ст. 63 УК РФ нового отягчающего обстоятельства в виде совершения умышленного преступления с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Такое нормативное изменение позволит учесть данный аспект реализации преступного умысла в тех случаях, когда ни в конструкции состава преступления, ни в квалифицирующих признаках нет указания на данный способ совершения преступления и, таким образом, дифференцировать наказание.

Что касается противодействия совершению преступлений в сфере Интернет (киберпреступлений) то представляется, что предпринимаемые со стороны государства меры, направленные, в первую очередь, на предупреждение киберпреступлений, должны носить системный характер, должны объединяться едиными задачами. В противном случае разрозненные, противоречивые меры не будут эффективными.

В этой связи, следует поддержать идею о принятии Концепции стратегии кибербезопасности Российской Федерации и продолжить работу над её созданием. Данный документ мог бы стать необходимым и даже ключевым демократическим по своей сути элементом системы

противодействия преступлениям, совершаемым в сфере Интернет (киберпреступлениям).

За рубежом активное взаимодействие между органами власти и коммерческим сектором, а также институтами гражданского общества, постепенно выходит на передний план в качестве потенциально эффективного фактора повышения качественного уровня решения актуальных проблем общества. Один из путей налаживания подобного взаимодействия – это, так называемое, государственно-частное партнерство, активно развиваемое в настоящее время, в том числе, в нашей стране.

В этой связи представляется необходимым развивать государственно-частное партнёрство в направлении противодействия киберпреступности. В виде глобальной цели такого партнёрства выступает создание отлаженной и максимально эффективной системы противодействия киберпреступности.

Для государства, в лице правоохранительных структур, важно повысить эффективность выявления, раскрытия и расследования преступлений в сфере Интернет, а также повысить уровень подготовленности кадровых сотрудников правоохранительных органов.

Соответственно, государство может привлекать высококвалифицированных специалистов IT-организаций России и сами организации к сотрудничеству на основе взаимовыгодного партнёрства в следующих вариантах:

- сотрудничество, связанное с привлечением IT-специалистов для участия в выявлении и расследовании киберпреступлений как на этапе проверки сообщения о преступлении, так и на этапе предварительного расследования (при производстве следственных действий) в процессуальном качестве специалиста;
- сотрудничество, связанное с привлечением IT-специалистов в качестве консультантов на непроцессуальной основе для оказания помощи следователю в выдвижении следственных версий, а также помощи в формулировании вопросов, которые надлежит поставить

перед судебным экспертом при назначении судебной экспертизы по соответствующей категории уголовных дел;

- сотрудничество, связанное с организацией и проведением «мониторинга сетевых информационных ресурсов» в целях предупреждения совершения киберпреступлений;
- сотрудничество по организации совместной работы по созданию развёрнутых обоснованных рекомендаций по различным вопросам противодействия преступности в сфере Интернет (киберпреступности);
- сотрудничество по организации повышения квалификации сотрудников правоохранительных органов по конкретным направлениям противодействия киберпреступности.

Таким образом, обеспечив комплексный подход в противодействии киберпреступности, можно рассчитывать на постепенное достижение значимых результатов в данном направлении.

Важно при этом осуществлять как совершенствование действующих уголовно-правовых норм, так и осуществлять предупреждение совершения рассматриваемых преступлений, путём разработки и реализации Концепции стратегии кибербезопасности Российской Федерации и расширения государственно-частного партнёрства в указанном направлении.

Список используемой литературы и используемых источников

1. Group-IB: оборот нелегальной онлайн-продажи алкоголя в 2018 году превысил 2,1 млрд рублей. [Электронный ресурс] // URL: https://www.group-ib.ru/media/alco-2018/.
2. Абрамян Т.А. Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий // Юрист. 2018. № 5. С. 68-72.
3. Аминов И.И. Криминологическая характеристика современной киберпреступности // Тенденции развития науки и образования. 2018. № 38-1. С. 5-8.
4. Борзенков Г.Н. Преступления против жизни и здоровья: закон и правоприменительная практика: учеб.-практ. пособие. М., 2008. 201 с.
5. Бугаев В.А., Чайка А.В. Факторы преступности в сфере компьютерных технологий // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. Т. 5. № 4 (71). С. 139-145.
6. Бутусова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3. С. 28-31.
7. Варшавская декларация (Итоговая декларация саммита) (Вместе с «Планом действий», «Руководящими принципами отношений между Советом Европы и Европейским Союзом», «Декларацией о сотрудничестве между Советом Европы и Организацией по безопасности и сотрудничеству в Европе») (Принята в г. Варшаве 16.05.2005 г. - 17.05.2005 г.) // Совет Европы и Россия. 2005. № 1. С. 26-37.
8. Генпрокуратура: число преступлений в IT-сфере возросло [Электронный ресурс] // URL:// https://roskomsvoboda.org/40925/
9. Гундерич Г.А. Состояние киберпреступности // Научный вестник Крыма. 2018. № 4 (15). С. 8-10.

10. Дерюгин Р.А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского института МВД России. 2019. № 2. С. 46-49.

11. Долженко Н.И., Хмелевская И.Г. К вопросу о содержательных аспектах киберпреступности // Философия. Социология. Право. Том 45. 2020. № 2. С. 315-322.

12. Дремлюга Р.И. Интернет-преступность: монография. Владивосток: Изд-во Дальневосточного ун-та, 2008. 240 с.

13. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Право и кибербезопасность. 2014. № 2. С. 33-38.

14. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25-33.

15. Ищук Я.Г. Состояние киберпреступности граждан в контексте обеспечение защиты их основных прав и свобод // Обеспечение прав и свобод человека в деятельности правоохранительных органов: сборник статей / под ред. А.Я. Грищко. Рязанский филиал МосУ МВД России им. В.Я. Кикотя, 2018. С. 37-42.

16. Казакова В.А. Условия, способствующие росту вооруженной преступности в России // Современное право. 2003. № 7. С. 32-35.

17. Карпова Д.Н. Киберпреступность: глобальная проблема и решение // Власть. 2014. № 8. С. 46-50.

18. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001 г.) // СПС «Консультант плюс».

19. Косенков А.Н, Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал ОГУЭП. 2012. № 3 (21). С. 35-37.

20. Криминология / Под ред. В.Н. Бурлакова, Н.М. Кропачева. М., 2004. 652 с.

21. Кувшинова В.С. Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 5-4 (44). С. 53-57.

22. Лакомов А.С. Киберпреступность: современные тенденции // Академическая мысль. 2019. № 2 (7). С. 53-56.

23. Леонов А.В., Назаренко А.Я. Проблемы предупреждения преступлений с использованием сети Интернет // Закон и право. 2018. № 8. С. 166-169.

24. МИД РФ: ущерб мировой экономике от киберпреступности в 2019 году может достичь $ 2 трлн. [Электронный ресурс] // URL: https://tass.ru/politika/5551244

25. Михайлева Ю.В. Новые виды преступлений против жизни и здоровья человека, совершаемые посредством системы «Интернет» // Электронный научный журнал «Наука. Общество. Государство». 2019. Т. 7. № 1 (25). С. 10-18.

26. Никитина А.Н. Общественная опасность склонения к самоубийству и содействия совершению самоубийства // Ученые записки Казанского юридического института МВД России. 2018. Т.3. № 1. С. 25-28.

27. Ожегов С.И. Словарь русского языка / под ред. Н.Ю. Шведовой. М.: Рус. яз., 1987. 797 с.

28. Оноколов Ю.П. Теоретические аспекты определения понятий, связанных с предупреждением преступности // Миграционное право. 2011. № 3. С. 23-26.

29. Осипенко А.Л. Государственно-частное партнёрство в сфере противодействия киберпреступности // Вестник Воронежского института МВД России. 2016. № 4. С. 37-44.

30. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск : Омская акад. МВД России, 2009. 480 с.

31. Особенности противодействия киберпреступности подразделениями уголовного розыска / под ред. Б.П. Михайлова, Е.Н. Хазова. М. : ЮНИТИ-ДАНА: Закон и право, 2016. 151 с.

32. Постановление Железнодорожного районного суда г. Рязани от 19.10.2018 г. по делу № 1-1-35/2019 // ГАС «Правосудие».

33. Постановление Пленума Верховного Суда РФ от 30.11.2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. № 2, февраль, 2018.

34. Приговор Козельского районного суда Калужской области от 08.05.2018 г. по делу № 1-57/2018 // ГАС «Правосудие».

35. Приговор Ленинского районного суда г. Кирова. Дело № 1-674/2013 // Документ официально опубликован не был. СПС «Консультант плюс».

36. Расулаев А. Киберпреступность: причины и условия, личность преступника // Review of law sciences. 2020. С. 108-115.

37. Рекомендация № CM/Rec (2014) 6 Комитета министров Совета Европы «О Руководстве по правам человека для пользователей Интернета» (Принята 16.04.2014 г. на 1197-ом заседании заместителей министров) // СПС «Консультант плюс».

38. Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2. С. 2-5.

39. Томашевич Е.А. Криминологическая характеристика и предупреждение киберпреступности среди несовершеннолетних // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений. сборник материалов. 2018. С. 198-20.

40. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Автореф. дис. ... канд. юрид. наук. Владивосток, 2005. 26 с.

41. Уголовное право России. Общая и Особенная части: Учебник / Под ред. В.К. Дуюнова. М. : РИОР, ИНФРА-М, 2015. 695 с.

42. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

43. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

44. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Консультант плюс».

45. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru

46. Указ Президента РФ от 30.11.2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // СЗ РФ. 2016. № 49. Ст. 6886.

47. Указ Президента РФ от 31.12.2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1 (часть II). Ст. 212.

48. Устинова Т.Д. Склонение к самоубийству: критический анализ // Lex Russica. 2020. Т. 73. № 3 (160). С. 151-159.

49. Федеральный закон от 07.06.2017 г. № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» // СЗ РФ. 2017. № 24. Ст. 3489.

50. Халиуллин А.И. Подходы к определению киберпреступления // Российский следователь. 2015. № 1. С. 34-39.

51. Ханахмедов А.С. Основы противодействия киберпреступности на территории Российской Федерации // Вестник Уфимского юридического института МВД России. 2019. № 3 (85). С. 44-48.

52. Хисамова З.И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий // Юридический мир. 2016. № 2. С. 58-62.

53. Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1 (55). С. 118-201.

54. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола. Ижевск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2015. С. 120-125.

55. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Департамента информационной безопасности Банка России. Обзор несанкционированных переводов денежных средств за 2016-2019 год [Электронный ресурс] // URL: https://www.cbr.ru/ Content/Document/File/62930/gubzi18.pdf/

56. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53-56.